



A ZMNE BOLYAI JÁNOS KATONAI MŰSZAKI KAR
ÉS A KATONAI MŰSZAKI DOKTORI ISKOLA
ON-LINE TUDOMÁNYOS KIADVÁNYA

IV. Évfolyam 4. szám 2009. december

**ZMNE
BUDAPEST**

A szerkesztőbizottság elnöke:

Prof. Dr. Halász László

A szerkesztőbizottság elnökhelyettese:

Prof. Dr. Munk Sándor ezredes

A szerkesztőbizottság tagjai és egyben rovatvezetők:

Prof. Dr. Berek Lajos nyá. ezredes CSc (Biztonságtechnika)

Dr. Eleki Zoltán PhD. (Fizikai felkészítés)

Dr. Haig Zsolt mk. alezredes PhD. (Védelmi elektronika, informatika és kommunikáció)

Dr. habil. Horváth László alezredes PhD. (Védelmi igazgatás)

Dr. Jászay Béla PhD. (Védelemgazdaság)

Prof. Dr. Lukács László nyá. mk. alezredes Csc. (Katonai műszaki infrastruktúra)

Dr. Paskó József CSc. (Térképészet és geoinformatika)

Dr. Szűcs László nyá. ezredes CSc. (Katonai logisztika és közlekedés)

Prof. Dr. Turcsányi Károly nyá. mk. ezredes Csc. (Haditechnika)

Dr. Földi László mk. alezredes PhD. (Környezetbiztonság, ABV- és katasztrófavédelem)

Főszerkesztő: Dr. Kovács László PhD. mk. őrnagy

Szerkesztő: Poroszlai Ákos nyá. mk. alezredes

Webmester: Dr. Kovács László PhD. mk. őrnagy

A szerkesztőség elérhetősége:

Zrínyi Miklós Nemzetvédelmi Egyetem, 1101. Budapest, Hungária krt. 9-11. A. épület 8. emelet

Postacím: 1581. Budapest Pf.:15.

Telefon: +36-1-432-9048

Fax: +36-1-432-9208

HM: 29-734

e-mail: hadmernok@zmne.hu

web: <http://hadmernok.hu>

Kiadó: Zrínyi Miklós Nemzetvédelmi Egyetem (ZMNE)

Kiadásért felelős: Prof. Dr. Szabó János, a ZMNE rektora

ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Dr. Berkovics Gábor nyá. alezredes – ZMNE BJKMK egyetemi docens

Dr. Bottyán Zsolt – ZMNE RLI egyetemi docens

Bunyitai Ákos – ZMNE BJKMK hallgató (MSc)

Deák Ferenc – NCT Ipari Elektronikai Kft.

Dr. Földi László mk. alezredes – ZMNE BJKMK egyetemi docens

Fürjes János mk. őrnagy – ZMNE KMDI doktorandusz

Fleiner Rita – ZMNE KMDI doktorandusz

Hankó Márta százados – ZMNE KMDI doktorandusz

Dr. Horváth Attila alezredes – ZMNE BJKMK egyetemi docens

Prof. Dr. Halász László – ZMNE BJKMK egyetemi tanár

Illési Zsolt – ZMNE KMDI doktorandusz

Inkovics Ferenc – ZMNE KMDI doktorandusz

Dr. Kassai Károly mk. alezredes – HM Informatikai és Információvédelmi Főosztály

Kis László – Budapesti Műszaki és Gazdaságtudományi Egyetem doktorandusz

Koleszár Béla – ZMNE KMDI doktorandusz

Koós Tamás mk. alezredes – ZMNE BJKMK egyetemi adjunktus

Kozma Tibor r. alezredes – Hajdú-Bihar MRFK, ZMNE KMDI doktorandusz

Krasznay Csaba – ZMNE KMDI doktorandusz

Dr. Kucsera Péter – Budapesti Műszaki Főiskola főiskolai adjunktus

Dr. Kun István – LSI Alapítvány

Prof. Dr. Lantos Béla – Budapesti Műszaki és Gazdaságtudományi Egyetem egyetemi tanár

Dr. Leitold Ferenc – Dunaújvárosi Főiskola főiskolai docens

Dr. Molnár András – Budapesti Műszaki Főiskola főiskolai docens

Molnár Árpád mk. alezredes – ZMNE KMDI doktorandusz

Prof. Dr. Munk Sándor – ZMNE BJKMK egyetemi tanár

Nagy Tibor István – ZMNE KMDI doktorandusz

Pap Andrea százados – ZMNE KMDI doktorandusz

Regula Gergely – BMGE doktorandusz

Dr. Sipos Jenő – BJKMK főiskolai tanár, dékán

Dr. Sipos Marianna – BJKMK főiskolai tanár

Prof. Dr. Szabolcsi Róbert mk. ezredes – ZMNE BJKMK egyetemi tanár

Szénási Sándor – Budapesti Műszaki Főiskola

Tóth Attila – Magyar Közút Nonprofit ZRt. Pest megyei Igazgatóság

Dr. Tóth Bálint – ZMNE BJKMK

Dr. Vámosy Zoltán – Budapesti Műszaki Főiskola

Varga Péter – ZMNE KMDI doktorandusz

Sipos Jenő

sipos.jeno@zmne.hu

Bunyitai Ákos

bunyitai.akos@gmail.com

REJTETT SZÚRÓ-VÁGÓ –ÉS LŐFEGYVEREK JELLEMZŐ ANYAGA ÉS KIALAKÍTÁSA

Absztrakt

A rejtett fegyver fogalmának bevezetése, definíció, jogi megközelítés. A rejtett szúró-vágó –és lőfegyverek jellemző anyagainak vizsgálata: kerámiák, polimerek, fémek, kompozitok és ásványi anyagok. Kialakításuk célszerű csoportosítása: rejtett fegyverként gyártott eszköz, használati tárgynak álcázott fegyver; használati tárgyból célszerűen átalakított fegyver; tényleges használati tárgy, melyen átalakításokat nem kellett eszközölni, de fegyverként alkalmazható és detektálása nehézkes.

This paper examines the meaning of concealed weapon, its definition, and legal approach. The main materials of these weapons: ceramic, polymer, steel, composite, mineral. The appearance of concealed stabbing- cutting and shooting weapons: constructed for weapon, seems to be daily-use object; modified object; real daily-use object which can be used for weapon and difficult to detect.

Kulcsszavak: *rejtett, álcázott, fegyver ~ concealed weapon*

BEVEZETÉS

Földünkön kialakult megoldatlan politikai/vallási/etnikai és egyéb konfliktusok hatására a biztonságot fenyegető tényezők száma növekedni látszik. Ezek hatására és a technika gyors fejlődésével a XXI. században a biztonsági szakembereknek újfajta problémákkal kell szembenézniük. Korunk „vívmányai” közé tartozik a relatíve alacsony költségvetésű, arctalan hadviselés, a terrorizmus. Ellene védekezni igen nehéz, áldozatai nagyrészt vétlen polgári személyek. Az agresszió egyre nagyobb térnyerésével mindinkább előtérbe kerülnek a rejtett szúró-vágó – és lőfegyverek. A rejtett fegyverek csoportosíthatók többek között jellemző anyag, alkalmazók köre, előfordulási helyek, jellemző kialakítás szerint. Alkalmazásuk több száz évre nyúlik vissza és napjainkban is dinamikusan fejlődnek. Ennek oka, hogy

kialakításuknak csak az emberi találékonyság, az alapanyag tulajdonságai és a technika korlátai szabnak határt.

A cikk célja, hogy bevezesse és definiálja a „rejtett fegyver” fogalmát, vázolja a rejtett szűrő-vágó – és lőfegyverek lehetséges csoportosítását és bemutassa sokszínűségük egy szeletét jellemző anyagukon és kialakításukon keresztül.

1. MI AZ A REJTETT FEGYVER?

1.1 Rejtett fegyverek

Rejtett fegyvereknek nevezhetjük azokat az eszközöket, amelyek fegyverként alkalmazhatóak, birtoklásuk vagy az adott objektumba, ill. rendezvényre való bejuttatásuk nem megengedett (veszélyt vagy biztonsági kockázatot jelentenek a többi emberre nézve), ezért rejtett módon kísérlik meg. Értsd „rejtett:” kialakításukat tekintve (méret, anyag, forma, stb.) nehezen detektálhatóak. Ennek megfelelően rejtett fegyvernek nevezzük:

- a) azokat a tárgyakat, amelyeket személyi sérülés okozására és/vagy az élet kioltására terveztek, készítettek vagy más tárgyból célszerűen átalakítottak, esetleg használati tárgynak álcáztak
- b) az olyan tárgyakat, amelyet nem személyi sérülés okozására és/vagy az élet kioltására terveztek, készítettek, átalakításokat nem kellett végrehajtani rajta, de birtoklója fegyvernek alkalmazza.
- c) minden olyan fegyvert, amelyet ruházátvizsgálással, motozással, fémdetektorral való kereséssel, testszkennel (terahertzen, vagy röntgen elven működő) vagy egyéb detektálási módszerrel nehezen megtalálható.

1.2 Rejtett fegyverek lehetséges definíciója

Az 1-es pontban meghatározott kritériumok figyelembe vételével rejtett lőfegyvernek tekinthetjük mindazon eszközöket, melyek személyi sérülés okozására és/vagy az élet kioltására alkalmas szilárd anyagú tárgyat képesek kilőni, függetlenül a kilövés módjának technikai megoldásától, illetve a lövedék energiájától.

Jogi megközelítés: egy rejtett szűrő-vágó vagy lőfegyver testi sérülés okozására alkalmas, de nem feltétlenül tartozik a közbiztonságra különösen veszélyes eszközök közé.

Igen fontos kérdés megismerni a mai gyakorlatban használatos ellenőrzési eljárásokat, az ezt segítő eszközöket a rejtett fegyver, mint definíció megértése, egyértelműsítése céljából. Az elterjedt fegyverdetektálási módszerek a felsőruházat-átvizsgálás, a motozás és a csomagátvizsgálás. A detektálást segítő berendezések a kézi fémkereső, a fémkereső kapu és a csomagátvilágító berendezés. Ezeket túl fejlesztések folynak – egyrészt a meglévő technikák finomítására – pl.: „dual-energy” és „back scatter” csomagvizsgáló, másrészt biztató újításnak tekinthető, előremutató berendezések pl.: terahertz „testskenner”.

A rejtett szűrő-vágó – és lőfegyverek lehetséges csoportosítása igen széles skálán mozog. Csoportosíthatjuk többek között anyag, kialakítás, felhasználók, gyártási év, stb. alapján. A csoportosítás mindaddig elméleti jelentőségű, míg nem konkrét biztonságtechnikai feladat megoldásáról van szó. Az előfordulások valószínűsége eltér(het) tömegrendezvényeken résztvevőknél (tüntetés, sportrendezvény, koncert, stb.), a Büntetés-végrehajtási intézetekben, a repülőtéri utasbiztonsági ellenőrzéseknél, stb. vagyis: az ellenőrzést és áteresztést, beléptetést végzőknek különböző szituációkban mást kell keresni és erre fel kell őket készíteni!

Az alábbiakban a rejtett szűrő-vágó –és lőfegyverek jellemző anyagát és kialakítását tárgyaljuk.

2. A REJTETT FEGYVEREK JELLEMZŐ ANYAGA

A fegyvertervezés és gyártás rendkívül fontos lépése a célszerű anyag kiválasztás. Ezen kiválasztást első sorban műszaki, másodsorban gazdasági szempontok kell, hogy vezéreljék. A műszaki szempontokat a termék funkciója, a fegyverrel szembeni követelmények határozzák meg, vagyis a méret, alak, felületi minőség, gyártandó darabszám, stb. szempontok alatt a fejlesztési és tervezési költségeket, az anyagköltségeket, a technológiai költségeket, és az igazgatási általános költségeket értjük. A rendelkezésünkre álló anyagokat többféle szempont szerint csoportosíthatjuk: halmazállapot, eredet, felhasználás, stb. szerint. Felhasználás szerint az alábbi szerkezeti anyagok kerülnek előtérbe: kerámiák, polimerek, fémek, kompozitok és ásványi anyagok.

Rejtett fegyver tervezésekor célszerűen figyelembe veszik a gyakorlatban elterjedt fegyverdetektálási módszereket és az ezeket segítő eszközöket.

2.1. Kerámiák

Azok a nemfémek (fém-detektorral nem kimutatható) szervesetlen anyagok a kerámiák, amelyek nagy része egyszerűbb vegyület, például oxidok (Al_2O_3 , SiO_2 , CaO , stb.). A műszaki kerámiák között megkülönböztethetünk egyatomos kerámiákat, oxidmentes vegyületkerámiákat (ezen belül: keményfémek, cermetek, keramikus lapkák) és oxidkerámiákat (üveg, kristályos oxidkerámiák, kristályos hidrátok).

Cermeteknek nevezzük azokat a porkohászati úton előállított fémkerámiákat, amelyeket Ti, Ta, Nb, W és Mo nitrideinek, valamint boridok, szilicidek és nagy szívósságú fémek (Co, Ni, Cr) porából állítunk elő.

A különféle kerámiák nagyszerű alapanyagok szűrő-vágó eszközökhöz, azonban előállításuk ipari technológiát feltételez, tömegük viszonylag kicsi, élük tartós, anyaguk rideg, kemény, nem rozsdásodnak. A vágószerszámra szánt kerámiák általában ZrO_2 , Al_2O_3 , BN, TiC, TiN alapúak. A kereskedelemben kaphatóak kerámia pengéjű kések (ld. 2. 1. ábra), azonban sok gyártó – a visszaélések elkerülése végett – kis mennyiségű fémeket tesz a késbe.



2. 1. ábra. Kerámia kés

2.2. Polimerek

A polimerek lényegében molekulacsoportok alkotta láncok, amelyek – eredetüket tekintve – lehetnek élő organizmusok termelte természetes anyagok vagy mesterségesen előállított anyagok. Felhasználhatóságuk széles skálán mozog, emellett általános jellemzőjük, hogy nagy az ellenállásuk vegyi hatásokkal szemben, hő-és villamos vezetőképességük kicsi, kis sűrűségűek, tömegegységre származtatott szilárdságuk nagy, nagyon vékony, ill. kis átmérőben is előállíthatók. Nagy előnyük továbbá, hogy relatíve nehezen detektálható anyagok.

- **Természetes polimerek:** növényi vagy állati eredetű szálak/rostos anyagok (pl. fa, bőr, szőr, gyapot, selyem). A szálak/rostok kis keresztmetszetű, hosszú anyagok, szakítószilárdságuk viszonylag nagy, jól hajlíthatóak.
- **Műanyagok:** szintetikus úton előállított anyagok. A műanyagok lehetnek:
 - hőre lágyulók (termoplasztok), pl.: teflon, PE (polietilén), PP (polipropilén), PVC (polivinilklorid), PS (polisztirol), stb.
 - hőre keményedők (duroplasztok), pl.: EP (epoxi-gyanta), UP (poliésztergyanta), stb.
 - műkaucsukok (elasztomerek), pl.: PUR (poliuterán), SI (szilikon), stb.
 Példaként említhető az USA-ban megjelent műanyag borotvapenge (ld. 2. 2 ábra).



2. 2. ábra. Műanyag borotvapenge

2.3. Fém

Az ember kb. i.e. 5000-tól használ fémet kés, nyíl-és lándzsahegy, valamint baltafej készítésére. Először bronzból (90% vörösréz, 10%órn), majd i.e. 1000-tól vasból készültek ezek az eszközök. A vas szélesebb körű elterjedése után rövid időn belül megjelent az acél, illetve az edzés, ötvözés, stb. technológiája. A fémből készült szűrő-vágó fegyverek kialakításuknál fogva (álcázás vagy kis méret) válnak nehezen detektálhatóvá.

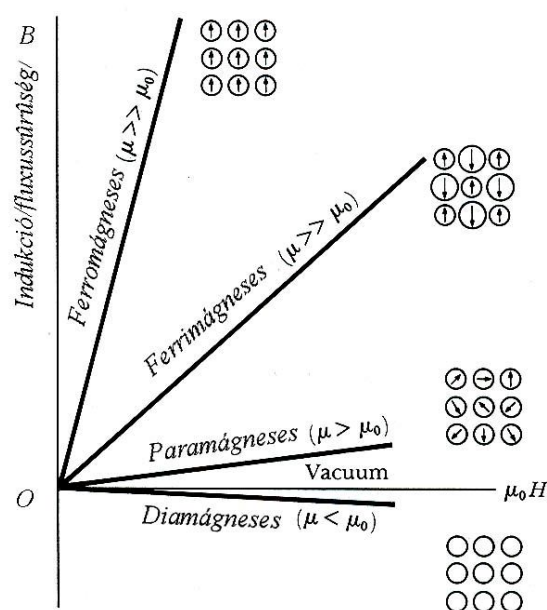
A fémkeresés az egyik elterjedt módszer a fegyverdetektálásban, a fémek általános jellemzője mágneses tulajdonságuk. A célszerűség kedvéért a fémeket mágneses tulajdonságaik alapján csoportosítjuk.

A mágneses tulajdonságok attól függően, hogy az anyagok mágneses indukciója külső mágneses mező hatására hogyan változik meg, az alábbi lehet:

- **Gyengén mágneses anyagok**
 - *Paramágneses:* azok a páratlan vegyértékelektronokat tartalmazó atomokból álló anyagok, amelyek atomjai permanens mágneses momentummal rendelkeznek. Ezek az atomok a külső mágneses tér hatására a tér irányába beforduló mágneses nyomatékot mutatnak és erősítik a külső mágneses teret. A külső mágneses tér megszűnésével ezek az atomok mágneses nyomatékának irányítottasága véletlenszerűvé válik és ezért a makroszkopikus anyag eredő dipólusmomentuma zérus. Paramágneses viselkedést mutatnak pl.: a Ti, Al, Cr, Pt, W, K, Ca, Na, Mn, Sn, stb.

- **Diamágneses:** azok az anyagok, amelyeket a permanens mágnesek taszítanak. Ezek fő jellemzője, hogy atomjainak eredő mágneses momentuma zérus, mivel a külső mágneses térrel ellentétes irányban mágnesesződnek. Külső mágneses mező hiányában nem mutatnak semmiféle mágneses viselkedést. Diamágneses viselkedést mutat a Cu, Pb, Bi, Au, Ag, stb.
- **Erősen mágneses anyagok**
 - **Ferromágneses:** azok a kristályos szerkezetű szilárd testek, amelyek atomcsoportjai rendezett permanens mágneses dipólussal rendelkeznek. Ezek az anyagok makroszkopikusan nem mutatnak mágneses tulajdonságot, mivel a különböző domének véletlenszerű orientációja következtében az eredő mágneses momentum zérus. A külső mágneses erőter rendező hatása következtében az erőterrel megegyező irányítottságú domének növekedni kezdenek az ellentétes orientációjú domének térfogatcsökkenése mellett és a külső mágneses erőterrel megegyező irányítottságú permanens mágneses momentumra tesznek szert. Ferromágneses anyagok a Fe, Co, stb.
 - **Ferrimágneses:** különös mágneses viselkedésű anyagok a ferrimágneses anyagok csoportjába tartozó ferritek, amelyeket alkotó atomok mágneses momentumai páronként ellentétesek, de eltérő nagyságúak. A ferritek porított fémoxidkeverékek szinterelt változata, amelyek szerkezetében megtalálható a $\text{ZnO} \cdot \text{Fe}_2\text{O}_3$, $\text{ZnO} \cdot \text{Mn}_2\text{O}_3$ és $\text{ZnO} \cdot \text{Ni}_2\text{O}_3$ keveréke. A ferritekben a nagyfrekvenciás áramok tartományában csak gyenge örvényáramok keletkeznek.
 - **Antiferromágneses:** azok a paramágneses anyagok, amelyek szomszédos doménjeiben az atomok elektronspinjeitől származó mágneses momentumok páronként antiparalelek. Pl.: MnO , FeO , CrSb , stb.).

A fentiekhez kiegészítésképp: a permanens mágnes a kislexikon szerint olyan „ferromágneses anyag, mely mágneses tulajdonságait (külső mágneses terét) mágnesezés nélkül megtartja. Előállítására olyan anyag előnyös, melynek koercitív ereje nagy.”



2. 3. ábra. Az anyagok mágneses viselkedését jellemző $\vec{B}$ indukcióváltozás külső $\vec{H}$ mágneses mező hatására. A dipólusnyomatékok külső térhez viszonyított helyzete.

Az alábbiakban tekintsük a periódusos rendszer elemeit mágneses tulajdonságaik alapján!

1 H
 2 He
 3 Li
 4 Be
 5 B
 6 C
 7 N
 8 O
 9 F
 10 Ne

11 Na
 12 Mg
 13 Al
 14 Si
 15 P
 16 S
 17 Cl
 18 Ar

19 K
 20 Ca
 21 Sc
 22 Ti
 23 V
 24 Cr
 25 Mn
 26 Fe
 27 Co
 28 Ni
 29 Cu
 30 Zn
 31 Ga
 32 Ge
 33 As
 34 Se
 35 Br
 36 Kr

37 Rb
 38 Sr
 39 Y
 40 Zr
 41 Nb
 42 Mo
 43 Tc
 44 Ru
 45 Rh
 46 Pd
 47 Ag
 48 Cd
 49 In
 50 Sn
 51 Sb
 52 Te
 53 I
 54 Xe

55 Cs
 56 Ba
 57 La
 58 Ce
 59 Pr
 60 Nd
 61 Pm
 62 Sm
 63 Eu
 64 Gd
 65 Tb
 66 Dy
 67 Ho
 68 Er
 69 Tm
 70 Yb
 71 Lu

67 Fr
 68 Ra
 69 Ac

72 Hf
 73 Ta
 74 W
 75 Re
 76 Os
 77 Ir
 78 Pt
 79 Au
 80 Hg
 81 Tl
 82 Pb
 83 Bi
 84 Po
 85 At
 86 Rn

87 Fr
 88 Ra
 89 Ac

90 Th
 91 Pa
 92 U
 93 Np
 94 Pu
 95 Am
 96 Cm
 97 Bk
 98 Cf
 99 Es
 100 Fm
 101 Md
 102 No
 103 Lr

104 Rf
 105 Db
 106 Sg
 107 Bh
 108 Hs
 109 Mt
 110 Ds
 111 Rg
 112 Cn
 113 Nh
 114 Fl
 115 Mc
 116 Lv
 117 Ts
 118 Og

119 Uue
 120 Uub
 121 Uut
 122 Uuq
 123 Uuh
 124 Uus
 125 Uuq
 126 Uuh
 127 Uus
 128 Uue
 129 Uub
 130 Uut
 131 Uuq
 132 Uuh
 133 Uus
 134 Uue
 135 Uub
 136 Uut
 137 Uuq
 138 Uuh
 139 Uus
 140 Uue
 141 Uub
 142 Uut
 143 Uuq
 144 Uuh
 145 Uus
 146 Uue
 147 Uub
 148 Uut

2. 4. ábra.

2.4. Komposit

A kompozit olyan szilárd anyag, amely legalább két, egymásban nem oldódó alkotóból áll, külső terhelés hatására azonban mechanikailag és makroszkopikusan egységes anyagként viselkedik. A kompozitok lehetnek részecskések, szálasak, rétegesek vagy bevonatosak, mindegyik csoporton belül fém-, polimer-, ill. kerámiamátrixúak. Ez a gyakorlatban annyit tesz, hogy a kompozitokkal elérhető mechanikai, mágneses, stb. tulajdonságok igen széles spektrumot fednek le.

2.5. Ásványi anyag

Az első kések kb. i.e. 180 ezerben kovakőből készültek, az első szűrőfegyverek kb. i.e. 40 ezerben jelentek meg. Kialakításuk kezdetben durva volt és kemény munkát igényelt (pattintással elért forma). Ma gyakorlatilag csak történelmi jelentőségük van. Ennek oka, hogy jóval kedvezőbb tulajdonságú anyagok állnak rendelkezésünkre. Ugyan fémdektorral az ásványi anyagok sem kimutathatók, ám ridegek és tömegük jelentős, így valószínűleg nem a legalkalmasabb alapanyag rejtett szűrő-vágó fegyver készítésére a XXI. században. A legismertebb és legősibb szűrő-vágó fegyver anyag az obszidián. Ennek a szilíciumdús vulkáni kőzetnek az előnye, hogy kagylós törése nagyon éles.

Megjegyzendő, hogy obszidián kések a kereskedelmi forgalomban hozzávetőlegesen 8 ezer Forinttól megvásárolhatók (ld. 2. 5 ábra).



2. 5. ábra. Obszidián kés agancs nyéllel

3. A REJTETT FEGYVEREK JELLEMZŐ KIALAKÍTÁSA

A rejtett fegyverek kialakítására jellemző a kis méret (a könnyű ruházat alá rejtés érdekében) és/vagy a használati tárgynak álcázás. Jellemző kialakításait az alábbiak szerint csoportosíthatjuk: rejtett fegyverként gyártott; használati tárgyból célszerűen átalakított; használati tárgynak álcázott és olyan ténylegesen használati tárgy, melyen átalakításokat végrehajtani nem kellett, de fegyverként alkalmazható és detektálása nehézkes.

Ezen csoportosítás elvi jelentőségű, ugyanis sok esetben nehéz pontosan azonosítani milyen céllal készült az eszköz, illetve milyen célra akarták felhasználni. Vagyis: az adott eszköz fegyvernek készült-e illetve annak akarták-e használni, néhány esetben az is vitaalapot szolgáltat, hogy testi sérülés okozására mekkora mértékben alkalmas.

3.1. Rejtett fegyverként gyártott, használati tárgynak álcázott fegyver

Egyes esetekben utólag igen nehezen lehet kideríteni, hogy az adott eszköz arra készült-e, hogy rejtett fegyvernek alkalmazzák vagy csak célszerűen lett átalakítva. Vannak azonban minden kétséget kizáró esetek. Jó példa lehet az alábbi – a világsajtót is bejárta – mobiltelefon-lőfegyver (ld. 3. 1. ábra). A fegyver 4db 0.22 kaliberű, jellemzően sportcélra használt lőszer magába foglaló tárral rendelkezik, a lövést az 5, 6, 7, 8 gombokkal lehet kiváltani. A képekből látható és egyértelműen eldönthető, hogy ezt a „mobiltelefont” azzal a céllal tervezték, gyártották, hogy később rejtett lőfegyverként alkalmazzák.



3. 1. ábra.

A rejtett fegyverként gyártott eszköz egyik legegyszerűbb rejtési módja, hogy olyan használati tárgynak álcázzák, amely rendeltetésszerűen nem kelt feltűnést.

3.2. Használati tárgyból célszerűen átalakított fegyver

Használati tárgyaink igen jelentős része alkalmas arra, hogy szúrós véget és/vagy élet alakítsunk ki rajta, így viszonylag kis energia és időráfordítással fegyver készíthető. Ilyen átalakítások jellemzőek a BV intézményeiben, illetve egyéb olyan helyeken, ahol erősen korlátozottak az előállítás lehetőségei. Az átalakításra alkalmasak: evőeszközök, olló, fogkefe (ld. 3. 2. ábra), szerszámok, csavar, stb. Mivel egy használati tárgyat igen nehéz átalakítani lőfegyverré úgy, hogy megőrizze a nehezen detektálhatóságát, az esetek nagy részében azok a személyek vagy szervezetek, amelyek erre képesek, inkább gyártanak egy lőfegyvert, amit használati tárgynak álcáznak.

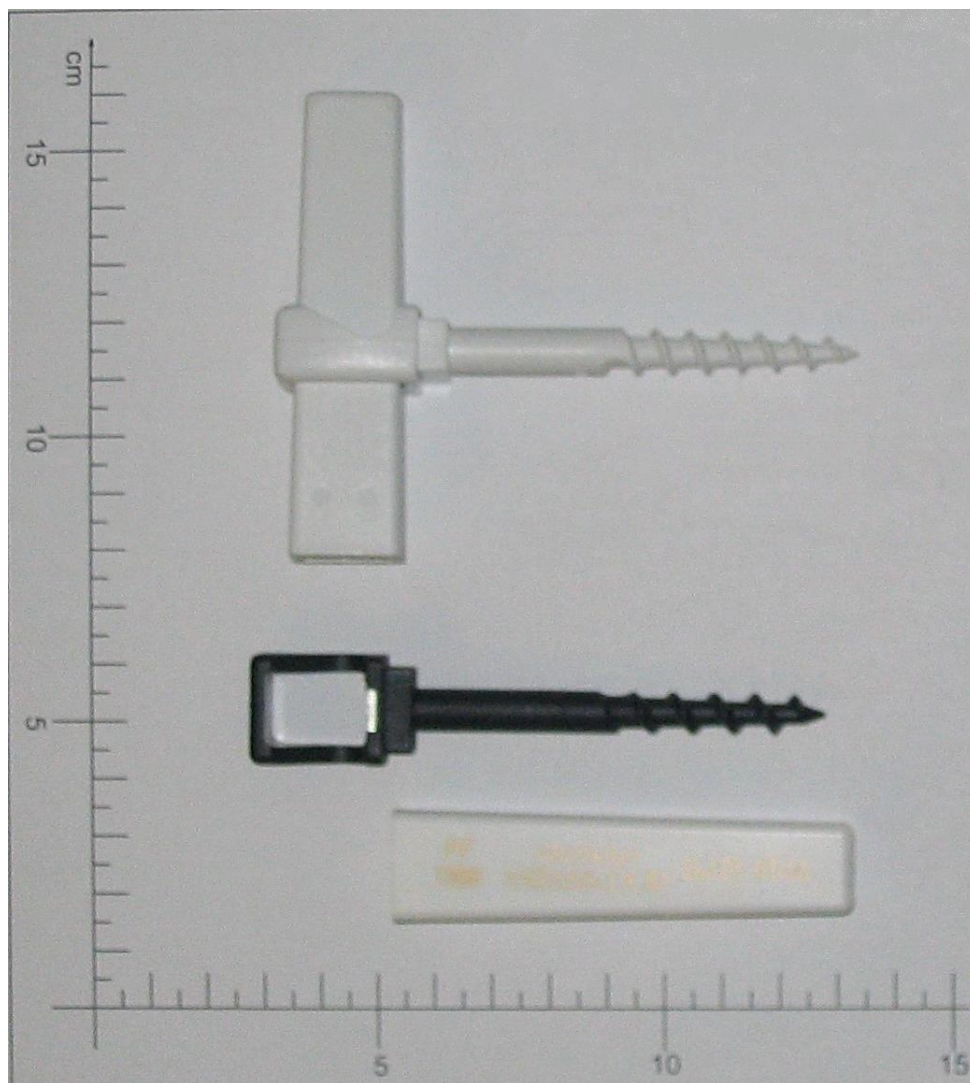


3. 2. ábra.

3.3. Tényleges használati tárgyak

Meg kell vizsgálnunk az olyan eszközöket is, amelyek hétköznapi szemmel nézve egyszerű használati tárgyak, annak is tervezték, gyártották, az emberek nagy része annak is alkalmazza őket. Birtoklásuk jogszabályba nem ütközik, ruházatátvizsgálás idejére nagy valószínűséggel elveszi az átvizsgálást végző, ugyanis testi sértés okozására alkalmasak. Testi sértés okozására alkalmas használati tárgyaink pl.: kötőtű, olló, csavarhúzó, dugóhúzó, stb. Ezek az eszközök mindaddig használati tárgyak, míg nem alkalmazzák őket fegyverként. A fentiek azonban nem felelnek meg a rejtett fegyver definíciójának, mivelhogy méretükből, anyagukból és formájukból adódóan egyszerűen detektálhatóak.

A csoportosítás szükségességének könnyebb megértése céljából példaként tekintsük az alábbi – hotelekben közkedvelten alkalmazott – eszközt (3. 3. ábra). Első ránézésre sörnyítő, ám aki széthúzza (a szár tökéletesen beleillik az üreges tokba) felfedezheti, hogy a termék „2 in 1”, ugyanis dugóhúzóként is használható. További érdekesség, hogy a tok beleillik a sörnyítőba, így képezve biztos fogást a dugóhúzó-szárnak. Ez az eszköz mindaddig sörnyítő és dugóhúzó, míg annak használjuk. Azonban ha egy őrzött objektumba, az öröket kijátszva (anyaga műanyag) bejuttatjuk és fegyverként alkalmazzuk, rejtett fegyverként definiálhatjuk.



3. 3. ábra.

ÖSSZEFOGLALÁS

A rejtett szűrő-vágó és lőfegyverekkel történő több hónapos ismerkedés, kutatómunka során bizonyossá vált, hogy ezeknek az eszközöknek van múltja, jelene és – valószínűleg – lesz jövője is, így jelen írás valós problémával foglalkozik. Megírásában rendkívül nagy segítséget jelentett, hogy a fegyverek fő előfordulási helyein sikerült kutatómunkát végezni, az ott dolgozó kollégákkal konzultálni. Ezen eszközök anyaga, kialakítása igen széles skálán mozog, így – sajnos – a cikkben is csak a legtipikusabbaknak számító eszközök jelentek meg példaként. A cikk megírásakor szem előtt tartottuk, hogy tartalmát tekintve figyelemfelkeltő legyen, ügyelve arra, hogy ne segítse azokat, akik ki akarják játszani a kollégákat.

Felhasznált irodalom:

1. Bunyitai Ákos: Rejtett szűrő-vágó –és lőfegyverek szakdolgozat, 2009.
2. 175/2003. (X.28) Kormányrendelet a közbiztonságra különösen veszélyes eszközökről
3. Dr. Bagyinszki Gyula – Dr. Kovács Mihály: Anyagismeret, Nemzeti Tankönyvkiadó, Budapest, 2004.
4. Komócsin Mihály: Gépipari anyagismeret, COKOM Mérnökiroda Kft., Miskolc, 2008.
5. Wikipédia, a szabad enciklopédia
http://hu.wikipedia.org/wiki/Kerámia_kés
6. Hartink: Kések enciklopédiája, Gabo könyvkiadó, 2001.
7. Biró – Domokos: Mágneses jelenségek
8. University of Cambridge: Types of magnetism,
<http://www.doitpoms.ac.uk/tlplib/ferromagnetic/types.php>
9. Chris Pellant: Kőzetek és ásványok, Egyetemi Nyomda, Budapest, 1996.
10. Dark Roasted Blend: Miniature Spy Guns
<http://www.darkroastedblend.com/2008/04/miniature-spy-guns-part-2.html>
11. 1994. évi XXXIV. törvény a Rendőrségről

Képek jegyzéke:

2. 1. ábra: http://hu.wikipedia.org/wiki/Kerámia_kés
2. 2. ábra: <http://toolmonger.com/2008/01/25/plastic-razor-blades/>
2. 3. ábra: felhaszn. irod. 7.
2. 4. ábra: felhaszn. irod. 8.
2. 5. ábra: www.obsidianarts.com
3. 1. ábra: felhaszn. irod. 10.
3. 2. ábra: saját felvétel
3. 3. ábra: saját felvétel

Bottyán Zsolt

bottyán.zsolt@zmne.hu

LÉGKÖRI ÜVEGHÁZHATÁS A KÖZETBOLYGÓKON

Absztrakt

A Naprendszer kőzetbolygóinak átlaghőmérsékletét légkör nélküli esetben, a napállandó és a planetáris albedó alakítja. A légkörrel rendelkező planeták esetében a számított egyensúlyi hőmérséklet azonban alacsonyabb, mint a tényleges átlaghőmérséklet, amit az ún. üvegházhatású gázok infravörös tartományon történő elnyelése okoz. Az így kialakuló üvegházhatás a Vénuszon rendkívül nagy, a Földön és a Marson jelentős mértékű átlaghőmérséklet-emelkedést okoz, a légkör nélküli esethez viszonyítva. A vénuszi igen magas felszíni hőmérsékletért az ún. megfutó üvegházhatás, a marsi alacsony intenzitású üvegházhatásért pedig a megszűnt vulkanizmus eredményeképpen eltűnt légkör a felelős.

The mean planetary temperature of Earth-like planets in our Solar System basically depend on both solar constant and planetary albedo, too if they have not any atmosphere. The calculated effective radiating temperature is lower than the real mean global temperature on these planets where there is a significant atmosphere around them. This phenomenon so called greenhouse effect based on the strong infrared absorption of some gases like H₂O, CO₂ and others. The mentioned greenhouse effect is very strong on the Venus and also significant on the Earth and Mars. The very high temperature on the Venus is based on its runaway greenhouse effect and the weaker martian greenhouse effect can be derived from volcanism had been finished a long time ago.

Kulcsszavak: üvegházhatás, kőzetbolygók, planetáris energia-egyenleg, egyensúlyi hőmérséklet ~ greenhouse effect, Earth-like planets, planetary energy balance, effective radiating temperature

Bevezetés

Napjainkban igen gyakran hallunk a globális felmelegedésről, mint az általános éghajlat-változás talán legmarkánsabb tényezőjéről. A globális átlaghőmérséklet mintegy 0,74 °C-os növekedése az elmúlt 150 évben Földünkön tetten érhető (*IPCC jelentés, 2007*). A globális felmelegedés legfőbb oka az emberi tevékenység során a Föld légkörébe juttatott és ott ún. üvegházhatást kifejtő gázok feldúsulása. Jelen munkánkban magával a természetes (nem

antropogén eredetű) légköri üvegházhatással, mint univerzális jelenséggel és ennek éghajlat-módosító hatásával foglalkozunk a Naprendszer kőzetbolygóit illetően.

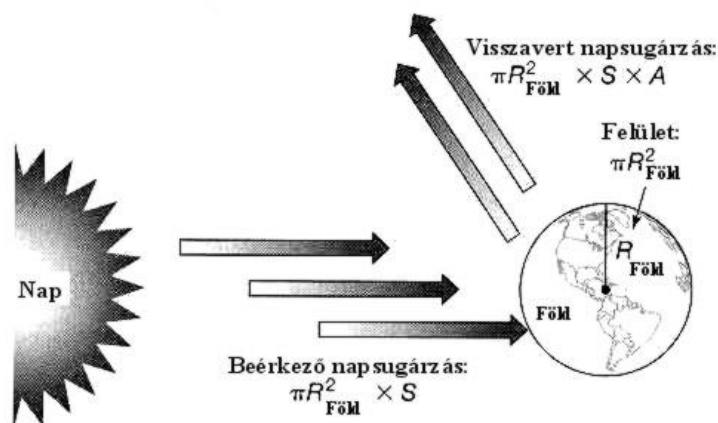
A természetes légköri üvegházhatás bolygónkon - egy rendkívül összetett folyamat részeként – a földtörténet során biztosította az élet kialakulásának és fennmaradásának a klimatikus feltételeit (elsősorban a globális átlaghőmérséklet szabályozásán keresztül). Ez a fontos moderáló hatás a Földön, a szén geokémiai körforgásának köszönhetően jelent meg és ez a folyamat a mai napig hatással van a légköri szén-dioxid koncentrációjára is (*Lunine, 1999*). A többi kőzetbolygó esetében ez a folyamat, ha be is indult, valamilyen oknál fogva megállt, így – ahogy majd látjuk – a többi planétán jelenleg rendkívül szélsőséges éghajlat uralkodik (*Kasting, 1988*). Hogy mennyire fontos a légköri üvegházhatás, azt egyetlen példán keresztül illusztrálhatjuk: amennyiben nem működne bolygónk légkörében ez a folyamat a jelenlegi +15 °C helyett -18 °C lenne a globális átlaghőmérséklet, ami bizonyosan a magasabb rendű élet végét jelentené a Földön, egy intenzív jégkorszak kialakulása következményeként!

Az üvegházhatás tehát szükséges ahhoz, hogy éghajlatunk megfelelő korlátok között maradjon. Ugyanakkor az elmúlt mintegy 150 év éghajlatának története azt is jelzi, hogy az ember képes drasztikusan beavatkozni ezekbe a – tőle függetlenül is működő – folyamatokba, ugyanakkor a hatásaival kevésbé van tisztában! Ennek az antropogén hatásnak (jelen esetben az üvegházhatást előidéző gázok szinte korlátok nélküli légkörbe bocsátása) eredménye a globális felmelegedés, aminek rendkívül komoly következményeivel még csak ezután kell igazából szembe néznünk.

Planetáris energia-egyensúly

Egy **légkör nélküli bolygó** esetében a felszín hőmérsékletének alakulását fizikai értelemben két tényező szabja meg: a napból érkező **besugárzás teljesítménye** és a felszín **fényvisszaverő képessége** (albedó). Amennyiben feltételezzük, hogy a bolygó éghajlata „nyugalomban van” azaz fennáll a **kvázi-sztatikus állapot**, akkor a napból beérkező rövidhullámú és a bolygó által kisugárzott hosszuhullámú energiák egyensúlyban vannak (*Kump et al., 2002*). A valóság nem pontosan ezt mutatja, hiszen ha így lett volna, akkor a Föld átlagos felszíni hőmérséklete a földtörténet során végig állandó marad. Természetesen ez nem volt mindig így, de igen rövid időskálán jó közelítéssel fennáll a kvázi-sztatikus helyzet. A két említett hőmérséklet-alakító hatás eredőjeként definiálható egy ún. **egyensúlyi hőmérséklet** (T_e) mely a bolygó átlaghőmérsékletét, mint sugárzási egyensúlyi hőmérsékletet reprezentálja. Ez a hőmérséklet jó közelítéssel a légkör nélküli esetben a tényleges átlaghőmérséklettel egyezik meg.

A planetáris energia-egyensúlyi egyenlet meghatározása nem túl bonyolult, de előzetesen néhány geometriai tényt figyelembe kell venni hozzá. A következőkben a Nap – Föld rendszert vizsgáljuk, de ugyanígy járhatunk el tetszőleges bolygó esetében is (*Kump et al., 2002*).



1. ábra. A beérkező és a visszavert napsugárzás mennyisége a Föld esetén (Kump et al., 2002 után módosítva)

Ha a Földet úgy tekintjük, mint fekete test, melynek egyensúlyi hőmérséklete T_e , akkor a Stefan – Boltzmann-törvény alapján az egységnyi felületről kisugárzott energia σT_e^4 -vel lesz egyenlő, ahol σ az ún. Stefan – Boltzmann állandó ($\sigma = 5,67 \times 10^{-8} \text{ W/m}^2/\text{K}^4$). Mivel a Föld a teljes felületéről bocsátja ki az energiát, amely a $4\pi R_{Föld}^2$ nagyságú gömbfelszínnel egyezik meg, ahol $R_{Föld}$ a bolygó sugara, így a Föld által kibocsátott teljes energia mennyisége (1. ábra):

$$E_{\text{kibocsát}} = 4\pi R_{Föld}^2 \cdot \sigma T_e^4$$

Bolygó	Közepes naptáv. (CSE)	Napállandó (W/m^2)
Merkúr	0,39	9007
Vénusz	0,72	2643
Föld	1,00	1370
Mars	1,50	609

1. táblázat. A Naprendszer közetbolygóinak közepes naptávolsága (CSE, csillagászati egység) és a hozzájuk tartozó napállandók értékei

Egy bolygóra a Naptól érkező rövidhullámú elektromágneses sugárzás teljesítményét egyrészt magának a központi csillagnak a teljesítménye, másrészt a bolygó naptávolsága szabja meg. Tekintve, hogy Kepler törvénye értelmében a bolygók naptávolsága változik, célszerű bevezetni az ún. **napállandó** (S) fogalmát, mely a légkör külső határán, közepes naptávolság esetén, időegység alatt, egységnyi felületre merőlegesen beeső energiát jelenti. A napállandó értéke a Föld esetében (S_0) 1370 Wm^{-2} . A Naprendszer közetbolygóinak távolságát ismerve, könnyen meghatározhatjuk mindegyik esetben a helyi napállandó értékét, ha figyelembe vesszük a *sugárzási energia változásának távolság-törvényét* (1. táblázat).

A Nap irányából nézve a Föld egy körnek látszik, melynek a sugara $R_{Föld}$ és felszíne $\pi R_{Föld}^2$. Jegyezzük meg, hogy a sugárzást felfogó felszín nem azonos a teljes felszín felével,

mert a napsugarak nem esnek mindenhol merőlegesen bolygónk adott felületére. A teljes felfogott energiát a Föld kör keresztmetszetének ($\pi R_{\text{Föld}}^2$) és a napállandónak (S_0) a szorzata adja. A visszavert energia egyenlő a beérkező energia ($\pi R_{\text{Föld}}^2 S$) és az albedó (A) szorzatával. Ha most figyelembe vesszük a nyilvánvaló összefüggést:

$$E_{\text{elnyelt}} = E_{\text{beérkező}} - E_{\text{visszavert}}$$

akkor azt kapjuk, hogy

$$E_{\text{elnyelt}} = \pi \cdot R_{\text{Föld}}^2 \cdot S_0 - \pi \cdot R_{\text{Föld}}^2 \cdot S_0 \cdot A = \pi \cdot R_{\text{Föld}}^2 \cdot S_0 \cdot (1 - A)$$

Tegyük egyenlővé ezek után a beérkező és a kimenő energia-mennyiségeket (az előzőek alapján ezek megegyeznek)! Ekkor a következő egyenlőség adódik:

$$E = 4 \cdot \pi \cdot R_{\text{Föld}}^2 \cdot \sigma \cdot T_e^4 = \pi \cdot R_{\text{Föld}}^2 \cdot S_0 \cdot (1 - A)$$

Egyszerűsítve a fenti egyenletet, megkapjuk az ún. **planetáris energia-egyenleg egyenletét**:

$$\sigma \cdot T_e^4 = \frac{S_0}{4} \cdot (1 - A).$$

Ez a formula mutatja a planetáris energia-egyensúlyt a beérkező rövidhullámú és a kimenő infravörös energia között a Földre vonatkozóan.

Az egyensúlyi hőmérséklet

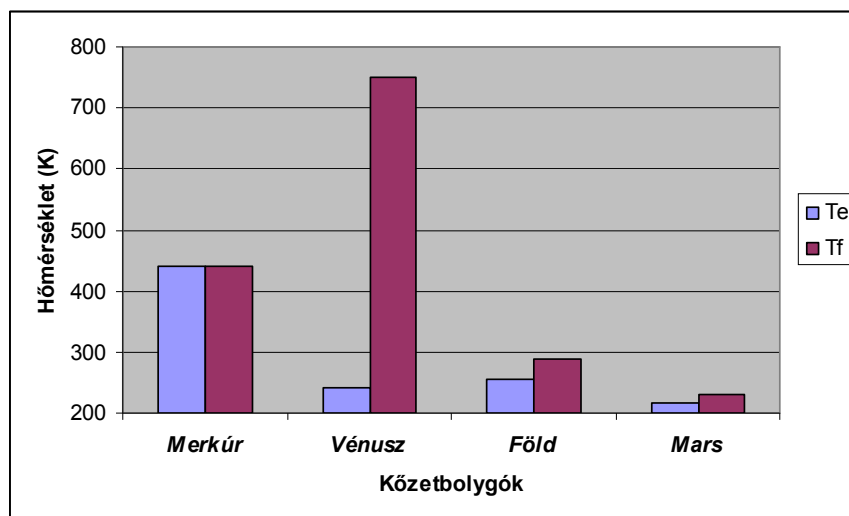
A planetáris energia-egyenleg egyenletét megismerve lehetőség nyílik arra, hogy kiszámítsuk egy bolygó egyensúlyi hőmérsékletét, ha ismerjük a bolygóra vonatkozó globális albedót és napállandót. Az egyensúlyi hőmérséklet számítása a planetáris energia-egyenleg egyenletéből a következő formulával történik:

$$T_e = \sqrt[4]{\frac{S_0 \cdot (1 - A)}{4 \cdot \sigma}}$$

Amennyiben a Föld megfelelő adatait behelyettesítjük ($S_0 = 1370 \text{ W/m}^2$, $A = 0,3$), akkor azt kapjuk, hogy bolygónk egyensúlyi hőmérséklete $T_e = 255 \text{ K}$ azaz $-18 \text{ }^\circ\text{C}$, ami jóval hidegebb, mint a valóságban tapasztalt $+15 \text{ }^\circ\text{C}$ -os érték. Ahogy korábban jeleztük, légkör nélküli objektum esetében (pl. Merkúr vagy Hold) az egyensúlyi hőmérséklet jó közelítéssel a tényleges felszíni átlaghőmérsékletet adja meg.

Joggal merül fel a kérdés, vajon mi okozhatja ezt a jelentős átlaghőmérséklet különbséget? Tételezzük fel, hogy a napsugárzáson kívül más külső forrásból nem jut energiához a Föld! Ebben az esetben a többlet-energiának a forrása (ami a $33 \text{ }^\circ\text{C}$ -os hőmérsékleti különbséget okozza), csak a Föld légkörének rendszere lehet, hiszen bolygónk szilárd belsejének hőtermelése (ami alapvetően radioaktív bomlásból és a Föld keletkezésekor képződött hőenergia maradványából származik) rendkívül csekély mértékű a napenergiához képest (Lunine, 1999). Erősíti ezt a feltevést az a tény is, miszerint a Naprendszer légkörrel

rendelkező kőzetbolygóinak (Vénusz, Föld és Mars) felszíni átlaghőmérséklete minden esetben **magasabb** az adott planéta egyensúlyi hőmérsékleténél (2. ábra).



2. ábra. A kőzetbolygók egyensúlyi (Te) és tényleges felszíni átlaghőmérséklete (Tf)

A többlet-energia forrása nem lehet más, mint a légkörben lévő összetevők sugárzás-elnyelése, ami viszont – figyelembe véve az elektromágneses spektrumot – csakis az **infravörös tartományban** valósulhat meg, hiszen a látható tartományban nagyrészt transzparens a légkör. Az atmoszféra bizonyos összetevői tehát erős elnyeléssel (abszorpció) és – *Kirchoff törvénye* szerint – kibocsátással (emisszió) rendelkeznek az infravörös tartományban. Ez azt jelenti, hogy a bolygó felszíni hőmérsékletéből származó termikus sugárzását (*Stefan – Boltzmann törvény*) a légkörben levő gázok egy csoportja elnyeli és egy részét a felszín felé visszasugározza. Ezt a mechanizmust nevezzük **légköri üvegházhatásnak**. Elmondhatjuk tehát, hogy az üvegházhatást produkáló gázok lényegében csapdába ejtik a bolygó felszínéről emittált energia jelentős hányadát (ami egyébként a világűrbe távozna), majd ennek egy részét a felszín felé visszasugározzák, többlet energia-bevételhez juttatva a bolygó felszínét.

Az eddig leírtak alapján feltételeztük, hogy a rövidhullámú tartományon nincs jelentős sugárzásgyengítése a légkörnek, szemben az infravörös tartományban tapasztalt elnyeléssel. Ez jó közelítéssel így is van, bár az ózon és egyéb gázok (oxigén, nitrogén) abszorbeálják a nagyenergiájú fotonokat (0,29 μm alatti tartomány) teljes egészében. A napsugárzás teljes energiaspektrumát (*Planck törvény*) figyelembe véve azonban az említett hullámhossz-tartományban a napból érkező energiának csak lényegesen kisebb része érkezik bolygónkra, mint a 0,29 μm -nél nagyobb hullámhosszokon (*Péczeley, 1980*).

Az üvegházhatás erőssége és jelenléte a bolygókon

Az eddig leírtakból következik, hogy az **üvegházhatás erőssége** ($\Delta T_{\text{ü}}$) közvetlenül becsülhető az egyensúlyi és a tényleges felszíni hőmérséklet különbségével:

$$\Delta T_{\text{ü}} = T_{\text{f}} - T_{\text{e}}$$

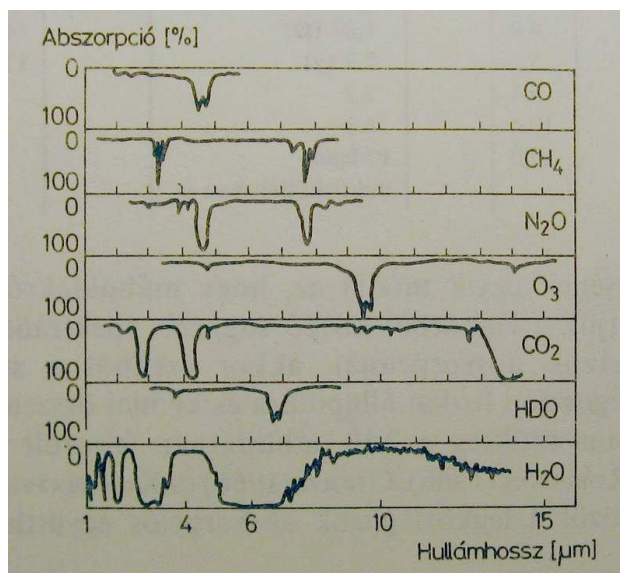
ahol $\Delta T_{\text{ü}}$ az üvegházhatás erőssége, T_{f} a bolygó tényleges felszíni átlaghőmérséklete és T_{e} pedig a bolygó egyensúlyi hőmérséklete. Földünk esetén $\Delta T_{\text{ü}} = 33^\circ\text{C}$, tehát a légkör 33 fokkal

emeli bolygónk felszínének átlaghőmérsékletét. A 2. táblázatban a Naprendszer bolygóira vonatkozóan bemutatjuk az üvegházhatás erősségét. Jól látható, hogy a légkör nélküli **Merkúron** az üvegházhatás erőssége gyakorlatilag **nulla**, viszont a **Vénuszon** több, mint **500 Kelvin** melegebb van az üvegházhatás miatt. Még a Mars esetén is hozzávetőlegesen 13 Kelvinnel magasabban tartja a felszín hőmérsékletét a viszonylag ritka légkör (a földi levegő sűrűségének csak kevesebb, mint századrésze).

Bolygó	Táv.(CSE)	A	S (W/m ²)	T _e (K)	T _f (K)	ΔT _ü (K)
Merkúr	0,39	0,06	9007,2	439,8	440	0,2
Vénusz	0,72	0,71	2642,7	242,1	750	507,9
Föld	1,00	0,30	1370,0	255,0	288	33,0
Mars	1,50	0,17	608,9	217,3	230	12,7

2. táblázat. A Naprendszer kőzetbolygóinak közepes naptávolsága (**Táv.**), átlagos planetáris albedója (**A**), napállandója (**S**), egyensúlyi hőmérséklete (**T_e**), átlagos felszíni hőmérséklete (**T_f**) és az üvegházhatás erőssége (**ΔT_ü**).

Felmerül a kérdés, hogy a Föld belső szomszédjának (a Vénusznak) a felszíni hőmérséklete miért ilyen kiugróan magas (750 K ≈ 480 °C)? A 2. táblázatban észrevehető, hogy ez a magas hőmérséklet egy rendkívül intenzív üvegházhatás eredménye (ΔT_ü=507,9 K)! A magyarázat a bolygó légkörének összetételében és sűrűségében rejlik (3. táblázat). A vénuszi atmoszférát kb. 96%-ban CO₂ alkotja és a felszínen a légnyomás mintegy 90-szer nagyobb, mint a Földön, amiből következik, hogy az említett bolygó légkörében a CO₂ koncentráció több nagyságrenddel nagyobb, mint a mi planétánkon! A CO₂ gáz ugyanakkor – hasonlóan néhány más gázhoz - igen jó elnyelő a korábban említett infravörös tartományban és így már érthető, miért ilyen erős az üvegházhatás a Vénuszon (3. ábra).



3. ábra. A gázok abszorpciója 1-16 μm között a földi légkörben (Bence et al., 1982.)

Összetevő	Vénusz	Mars
CO ₂	96,5%	95,3%
N ₂	3,5%	2,7%
SO ₂	≈100 ppm	
Ar	70 ppm	1,6%
CO	45 ppm	
H ₂ O	45 ppm	

3. táblázat. A Vénusz és a Mars légkörének fontosabb összetevői és koncentrációjuk (McFadden et al., 2007)

A Föld esetében a **természetes** (nem antropogén) **üvegházhatást** döntően a légkörünkben lévő **vízgőz (H₂O)**, **szén-dioxid (CO₂)** és **ózon (O₃)** okozza (Bence et al., 1982). A vízgőznek és az ózonnak szintén jelentős sugárzás-elnyelése van az 1-15 µm-es tartományban (3. ábra). Vegyük figyelembe továbbá, hogy bolygónk termikus sugárzásának (ami a 288 K-es átlagos felszíni hőmérsékletéhez tartozik) maximális intenzitása a *Wien-féle törvény* alapján 10 µm-es hullámhossznál jelentkezik, ami szintén ebbe a tartományba esik! Meg kell említeni még két fontos természetes légköri összetevőt, a **metánt (CH₄)** és a **dinitrogén-oxidot (N₂O)**, melyek szintén üvegházhatású gázok, de szerepük az elmúlt 150 évben, az antropogén kibocsátás megjelenésével vált igazán fontossá (3. ábra). Ugyanakkor, az említett gázoknak a légköri koncentrációja csekély (együttesen még a troposzférában is 4% alatt van), amiből világosan adódik, hogy a Vénuszhoz hasonló erősségű természetes üvegházhatást semmiképp nem várhatunk a Föld esetében!

A másik szomszédos bolygón (Mars) is azt tapasztalhatjuk, hogy az ottani – igaz rendkívül kis sűrűségű (átlagos felszíni nyomás 6,1 mb) – légkör domináns összetevője szintén a szén-dioxid (kb. 95%), mely ebben a csekély mennyiségben is jelentős üvegházhatást produkál. A marsi üvegházhatás erőssége közel 13 K (3. ábra)!

Felmerül a kérdés, hogy mi lehet az oka a vénuszi igen tekintélyes és a marsi rendkívül csekély mennyiségű szén-dioxid légköri jelenlétének? Ahogy korábban említettük, a szén geokémiai körforgásának a szerepe alapvető a szén-dioxid légköri koncentrációjának szabályozásában. Ez a mechanizmus bolygónkon, a lemeztectonikán és a hozzá kapcsolódó vulkanizmuson keresztül fejt ki hatását hosszú időskálán (10-100 millió év). A légköri szén-dioxid koncentrációja a jelzett időskálán a gáz kőzetekbe való beépülése és a vulkanizmus során történő légkörbe jutása közti különbség eredményeképpen alakul, mely bonyolult fizikai és kémiai folyamatokon keresztül realizálódik. Amennyiben a körforgás valamelyik ága megszakad, a légköri szén-dioxid koncentráció jelentősen megváltozik. Jelenlegi ismereteink szerint a Vénuszon a gáz kivonódása a légkörből megszakadt és a vulkanizmus eredményeképpen fokozatosan növekvő CO₂ szint miatt az ún. **megfutó üvegházhatás (runaway greenhouse effect)** jelenségét tapasztalhatjuk, a már említett magas felszíni hőmérséklettel (Kasting, 1988). A Mars esetében pedig a megszűnt vulkanizmus (tektonizmus) nem tudta a kőzetekben megkötött szén-dioxidot visszajuttatni a légkörbe ezért (és a relatíve gyenge gravitációja miatt) a marsi atmoszféra elvesztette légkörének és ezzel együtt üvegházhatásának jelentős részét is. A Merkúr esetében a napközelségből adódó nagy energiaáram és a bolygó kis tömegéből származó gyenge gravitáció nem tette lehetővé semmilyen légkör tartós fennmaradását.

Tekintve, hogy a szén-dioxid egy viszonylag gyakori vegyület az univerzumban, várható, hogy más bolygórendszerekben is előfordul gázneműként és ott üvegházhatást fejt ki. Ráadásul, a szén-dioxid $-79\text{ }^{\circ}\text{C}$ -nál magasabb hőmérsékleten (gáznemű halmazállapotban) is meglehetősen stabil vegyület, szemben pl. a vízgőzzel, mely elég könnyen disszociációt szenved az UV-B sugárzás hatására. (Földünkön, a sztratoszférában jelenlevő ózon rétege védi meg a vízgőzt a disszociációtól és egyben az atmoszférából történő végleges disszipációtól). Viszonylagos gyakoriságából és stabilitásából adódóan jelentős szerepet játszhat más bolygórendszerek planétáin kialakuló éghajlatok alakításában és stabilizálásában is.

Meg kell ugyanakkor jegyeznünk, hogy még messze nem ismerjük pontosan a bolygók esetében az átlaghőmérséklet alakító folyamatokat, valamint léteznek olyan jelenségek, amiket nem tudunk megmagyarázni az ismertetett üvegházhatás elmélettel. További kutatásokra van szükség a bolygók légkörének hőmérséklet alakításában betöltött szerepét illetően.

Összefoglalás

Egy adott bolygó esetén a rövidhullámú besugárzás és a hosszuhullámú kisugárzás egyensúlyban van (planetáris energia-egyensúly). A Naprendszer bolygóinak (légkör nélküli esetben) a felszíni globális átlaghőmérsékletét - az adott helyen - a napállandó és a planetáris albedó szabja meg. Az így számított ún. egyensúlyi hőmérséklet – minden légkörrel rendelkező bolygó esetén – alacsonyabb, mint a tényleges (mért) felszíni átlaghőmérséklet. A két hőmérséklet különbségének oka a légkörben lévő – infravörös tartományon elnyelni képes – speciális tulajdonságú gázok jelenléte (szén-dioxid, vízgőz, ózon stb.). A légköri gázok által, az infravörös tartományon történő elnyelés utáni visszasugárzás az ún. üvegházhatás, mely energia-többletet jelent a bolygó számára a légkör nélküli esethez viszonyítva. Az említett hőmérséklet különbség egyben az üvegházhatás mértéke is. A közetbolygók esetében a Merkúron nincs, a Földön és a Marson jelentős, míg a Vénuszon rendkívül intenzív az üvegházhatás mechanizmusa, amelynek erőssége az adott bolygó légkörének sűrűségétől és az ún. üvegházhatású gázok (elsősorban a szén-dioxid) koncentrációjától függ. A vénuszi igen magas felszíni hőmérsékletért az ún. megfutó üvegházhatás, a marsi alacsony intenzitású üvegházhatásért pedig a megszűnt vulkanizmus eredményeképpen eltűnt légkör a felelős.

Irodalom

Bencze, P., Major, Gy., Mészáros E. (1982): Fizikai Meteorológia. Akadémiai Kiadó, Budapest, 300 pp.

IPCC (2007): Az Éghajlatváltozási Kormányközi Testület negyedik értékelő jelentése. Természettudományos alapok. <http://www.ipcc.ch/pdf/reports-nonUN-translations/hungarian/ar4-spm.pdf>

Kasting, J., F. (1988): Runaway and Moist Greenhouse Atmospheres and the Evolution of Earth and Venus Icarus 74. 472-494

Kump, L., R., Kasting J., F., Crane, R., G. (2002): The Earth system with global change update. Prentice Hall, Pearson Custom Publishing, Boston, 351 pp.

Lunine, J., I. (1999): Earth: evolution of a habitable world. Cambridge University Press Boston, 319 pp.

McFadden, L., A., Weissman P., R., Johnson, T., V. (2007): Encyclopedia of the Solar System. Academic Press, 966 pp.

Péczely, Gy., (1978): Éghajlattan. Tankönyvkiadó, Szeged, 280 pp.

Hankó Márta

marti1222@gmail.com

Földi László

foldi.laszlo@zmne.hu

ÉLETTERÜNK KÖRNYEZETBIZTONSÁGI KÉRDÉSEI

Absztrakt

A cikk a környezetbiztonság igen komplex kérdéskörét igyekszik elemezni. Mit jelent a környezet biztonsága, milyen összetevői vannak, mi az ökoszisztéma, és hogyan kapcsolódik a környezetbiztonság fogalmához?

Az emberi beavatkozás nem marad következmények nélkül, és a globális klímaváltozás századában az antropogén tevékenység számos környezeti problémát generál. A helyesen alkalmazott technológiai eljárások nagyban javíthatják életterünk állapotát, és zöldebb jövőt biztosíthatnak számunkra. A cikk az eddig elért eredményeket, és a jövő további fejlesztési lehetőségeit mutatja be a teljesség igénye nélkül.

The article tries to analyze the very complex circle of questions of the environmental security. What does environmental security mean, what are its components, what is the ecosystem and how are they joined to the definition of the environmental security?

The human interference will have consequences and in the century of the climate-change antropogen activities generate several environmental problems. The correctly applied technological procedures may improve the state of our environment very much. Furthermore they may guarantee greener future for us. The article introduces the results which have been achieved so far, and shows us the development possibilities of the future without the demand of the completeness.

Kulcsszavak: környezetbiztonság, ökoszisztéma, környezetvédelem, összefüggések, zöld technológiák ~ environmental security, ecosystem, environmental protection, the inherences, green technologies

BEVEZETÉS

A környezet állapotának fenntartása mindannyiunk érdeke. Évekkel ezelőttig kényelmesen élveztük a napfürdőt, a viszonylag állandónak mondható hőmérsékleti viszonyokat, és mit sem sejtettünk a klímaváltozás mikéntjéről.

Ma azonban kénytelenek vagyunk szembenézni kihívásaival, reagálni végbemenő folyamataira, és felkészülni a jövőben készülődő veszélyekre.

Át kell gondolnunk a mindennapokban alkalmazott berendezéseink tényleges hasznát, új fogalmat kell alkotnunk a környezetvédelmi elgondolásokról, és meglévő technológiáinkat is át kell értékelnünk.

A közlekedés, az ipar és minden szektor hatalmas mennyiségű energiát emészt fel, melynek melléktermékeként káros kibocsátással terheli a környezetet.

Az antropogén beavatkozások hatással vannak az ökoszisztéma egészére, így mielőtt tovább rontanánk jelenlegi helyzetünkön, mérlegelnünk kell, mit látunk majd szívesebben a jövőben: elhullott madarak tetemeit, vagy szélerőművek erdejét? Vízisztító berendezéseket, vagy szennyezett folyókat? Változatlan állapotokat, vagy élhetőbb környezetet?

Az új technológiák már terjedőben vannak, de számos nehézséggel kell még szembenézniük. Az ember természeténél fogva minden újat fenntartással fogad, anyagi nehézségek támadhatnak, és az sem biztos, hogy az alkalmazott új technológiák maradéktalanul beváltják a hozzájuk fűzött reményeket.

Elképzeltető, hogy a jövőnket képletesen szólva meg kell majd vennünk, és először többletkiadással járó kísérleteket kell folytatnunk azért, hogy később aztán ezek a ráfordítások saját életvitelünkben érzékelhetően megtérüljenek.

A dolgozat bemutatja a környezetbiztonság fogalmát, rámutat néhány szóban az emberi beavatkozás és az ökoszisztéma összefüggéseire, végezetül pedig a jelen és a jövő lehetséges technológiai újításait mutatja be.

A KÖRNYEZETBIZTONSÁG FOGALMA

Egy komplex fogalom és egy sajátos terület megértésére vállalkozik, aki a környezetbiztonság fogalmát járja körül.

Mindenképpen tisztázni szükséges a „környezet” és a „biztonság” fogalmakat, majd magát a szakterületet kell görcső alá vonni és a szó mögött megbúvó mögöttes tartalmat kell vizsgálni.

A „környezet” általános megfogalmazásban az embert körülvevő közvetlen életteret jelenti. A Magyar Értelmező Kéziszótár szerint a környezet: *a valakit, valamit körülvevő tárgyak összessége, vagy az élőlény életfeltételeit megszabó külső tényezők összessége.* [1] Tudományos megfogalmazást keresve az alábbi bővebb és pontosabb definíciót találjuk:

„Az ember környezete a bennünket körülvevő világnak az a része, amelyben él és tevékenységét kifejti. Ez a környezet térbeli kiterjedését tekintve gyakorlatilag azonos az élővilág életterével, a bioszférával, amely a földkéregnek (litoszféra), a vizeknek (hidroszféra) és a légkörnek (atmoszféra) azt a részét foglalja magában, amelyet az élő szervezetek benépesítenek.” [2]

A környezet egyes részei egymástól elválaszthatatlan kölcsönhatással működnek. Ha az egyik részbe beavatkozunk, akkor az más területeken is jelentkezik. Épp ezért az említett beavatkozásokat szabályozni kell, a közvetlen életterünket pedig védelem alá kell helyeznünk.

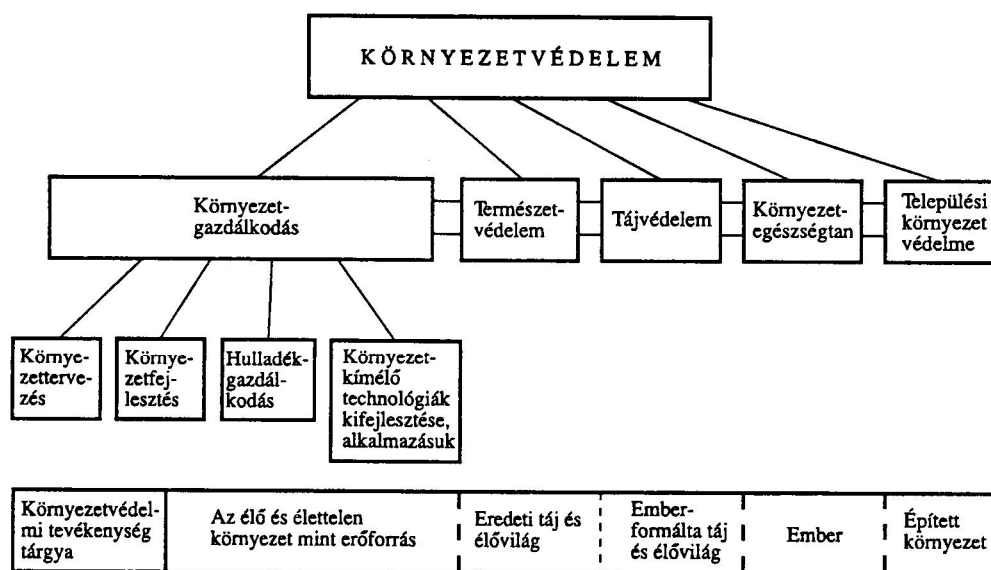
Daniel Quinn¹ szavaival élve *kultúránk mitológiája azt zümögi a fülünkbe, hogy hódítsuk meg a világot.* [3]

¹ Daniel Quinn: A Nebraska állambeli Omahában született 1935-ben, tanulmányait a St. Louis Egyetemen, a bécsi Vienna Egyetemen és a chicagói Loyola Egyetemen végezte. 1975-ben felhagyott hosszú kiadói

Rachel Carson² óta azonban létezik egy „környezetvédelem” nevű *intézmény*, mely épp ezt a hódítást hivatott kordában tartani.

A Környezet -és természetvédelmi lexikon szerint: *a környezetvédelem olyan céltudatos, szervezett, intézményesített emberi (társadalmi) tevékenység, melynek célja az ember ipari, mezőgazdasági, bányászati tevékenységéből fakadó káros következmények kiküszöbölése és megelőzése az élővilág és az ember károsodás nélküli fennmaradásának érdekében.*”[4]

Az 1. számú ábra a környezetvédelem és az ember szerteágazó és igen összetett kapcsolatát mutatja. Egyértelműen kiderül, hogy ez a szakterület számos feladatot kell, hogy ellásson és kölcsönhatásainál fogva különböző szektorokat kapcsol össze egymással.



A tágabbban értelmezett környezetvédelem fontosabb tevékenységi területei és a tevékenységek tárgya

1. ábra. A környezetvédelem területei ^[1]

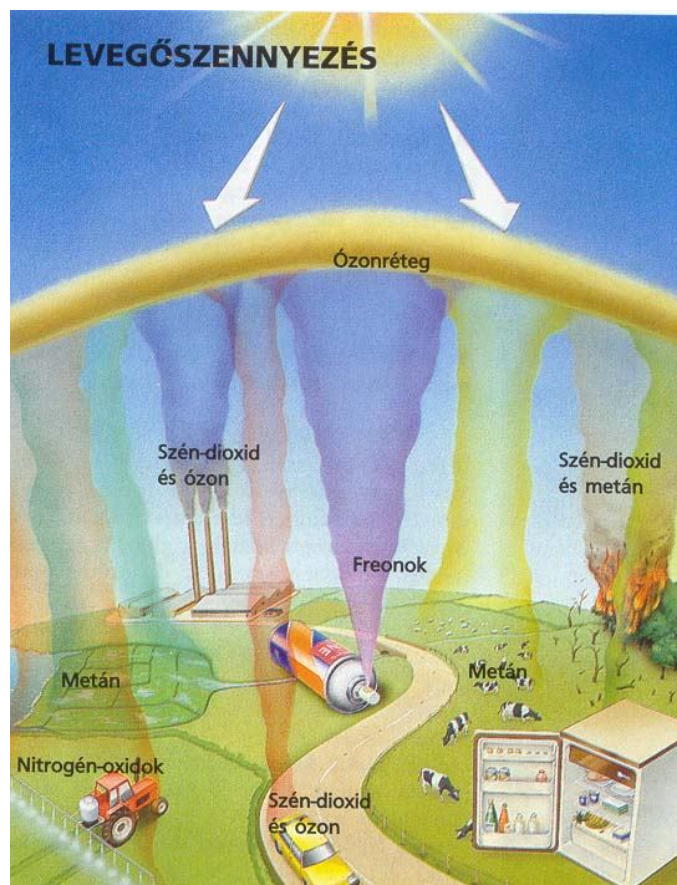
A *biztonság* fogalmának meghatározása elméleti síkon már csak azért sem mondható triviálisnak, mert egyrészt minden ember számára mást - és mást jelent, másrészt viszont száz százalékos biztonság egyáltalán nem is létezik. Így viszont már kicsit komplexebben kell értelmeznünk. Általánosságban talán az a megfogalmazás a legegyszerűbb, ha azt mondjuk, hogy a biztonság egy veszélyektől mentes állapot.

A biztonság a XXI. században már egészen más jelentéstartalommal bír, mint évekkel ezelőtt. Megváltozott a világ, újfajta kihívások, fenyegetések jelentek meg. A terrorizmus – bár évek óta jelen van- 2001. szeptember 11. óta egészen mást jelent a világ szótárában. A sokszínű kultúrák békés együttélése is számos viszályt szít, hazánk esetében a roma kérdést, a nagyvilág palettájáról pedig az iszlám fanatizmust említhetnénk példaként.

Az éghajlatváltozás is más, eddig ismeretlen környezeti problémákat generál. Míg a nyolcvanas évek közepén az ózonréteg elvékonyodása jelentette a központi kérdést, - annak csökkenését 1985-ben észlelték először- ma a klímaváltozás adja a környezeti világkonferenciák fő témáját.

pályafutásával, hogy idejét csakis az írásnak szentelhesse. Jelenleg Texasban él. (Forrás: <http://www.ishmael.org/origins/DQ/> Letöltés ideje: 2009. május 25.)

² Rachel Louise Carson:1907-ben született Pennsylvániában. Tengerbiológus, ökológus, író. A tudósok a nagy port kavart Néma tavasz című DDT-ről szóló könyvének 1962-es megjelenésétől datálják a környezetvédelem létrejöttét.



2. ábra. Az ózonréteget károsító anyagok [2]

A globalizáció révén a betegségek terjedése, a növény - és állatvilág átalakulása, a gazdasági, politikai problémák ma komplexen terjednek ki a bolygó egészére. (Lásd az USA-ból szertegyűrűző gazdasági válságot, mely napjainkra világválsággá alakult át, hazánkat is érintve, hiszen Magyarország magas államadóssággal küzdő, külkereskedelemre utalt, vagyis a világgazdasági kockázatoknak fokozottan kitett ország.)

A pozitívan ható változások mellett nagyon sok negatívum is megfigyelhető a világban, így nyilvánvaló, hogy a globalizációnak nem csak nyertesei, de sajnos vesztesei is akadnak szép számmal.

A biztonság fogalma állandóan változik és ez a tendencia a jövőben is megmarad. Ahogyan a világ átalakul, az emberiség megpróbál ahhoz mindinkább idomulni és alkalmazkodni. Megfigyelhető, hogy az egyes régiók biztonsági problémái igen eltérőek.

Évek múlva talán a vízárt folytatott háborúk jelentik majd a legnagyobb veszélyt a föld számos pontján. Az is biztos, hogy az országokban dúló belső problémák felerősödése is várható lesz, gondoljunk csak a jelenlegi magyar politikai viszonyokra.

A *biztonság* fogalmának legáltalánosabb definícióját az Egyesült Nemzetek Nevelésügyi és Kulturális Szervezete (United National Educational Scientific Cultural Organisation – UNESCO) társadalomtudományi szótára tartalmazza. Eszerint: „ *A biztonság a fizikai veszély hiányát, vagy az e veszéllyel szembeni védelmet jelenti* ”.

Meghatároztuk a környezet és a biztonság fogalmát külön-külön. Elérkeztünk a fő alapfogalomnak, magának a *környezetbiztonság* fogalmának meghatározásához. A fentiek tükrében kijelenthetjük, hogy a *környezet* és a *biztonság* fogalmak egyre jobban összefüggenek.

A környezetbiztonság a biztonsághoz hasonlóan nagyon komplex és folyamatosan megújuló tartammal bíró dolog. Az Európai Közösség által elfogadott definíció szerint:

„A környezeti biztonság az Európai Közösség azon képességét jelenti, hogy a környezeti erőforrások szűkössége és a környezeti károsodás elkerülésével képes fejlődését biztosítani.”

Egy másik definíció szerint: *a mindenkori környezetvédelem adott állapota, annak egyes elemei vonatkozásában külön-külön és együttesen. A föld, a vizek, a levegő, a természetes és mesterséges környezetnek az emberekre, a társadalomra, az egész érintett élő –és élettelen világra, valamennyi értékre gyakorolt, negatív hatással szembeni védettségnek a mértékében.* [5]

Ha állást kellene foglalni valamely meghatározás mellett nehéz dolgunk lenne. Leginkább a két meghatározást összevonva, egymással kiegészítve közelíthetnénk a valósághoz.

AZ ÖKOSZISZTÉMÁRÓL NÉHÁNY SZÓ

Az ökoszisztémák szerveződése több mint három milliárd éven keresztül az ember nélkül történt. A Homo Sapiens megjelenése nem jelentett komoly változást az élőlényközösségekben, hisz az első emberek halásztak, vadásztak, gyűjtögettek; azaz annyit vettek el a természetből, amire feltétlenül szükségük volt. Ma viszont egy ún. antropocén³ korban élünk, ahol a ma természetesnek nevezett társulásokat is érik emberi behatások.

A társulás (biocönózis) fogalmát Möbius használta először, 1877-ben, tengeri sziklák teljes életközösségének leírására. A társulás egy adott helyen, adott pillanatban koegzisztáló (együtt létező) populációk közössége. „Dahl (1908) megalkotta a biotóp (élőhely) fogalmát, miután biocönózison csak az életközösségek alkotó- részét értették. A két fogalom (biotóp és biocönózis) együttes megnevezésére megalkották az ökoszisztéma kifejezést.” [6]

Szokás még beszélni természetközeli társulásokról, (pl. erdőművelés), domesztikált ökológiai rendszerekről (pl. ültetvényszerűen művelt területek), valamint fabrikált, természetidegen ökoszisztémákról (lásd a városok). A kategóriák egymással összefüggenek, vagy inkább egyfajta átmenetet alkotnak.

Az ökoszisztémában a levegő a talaj és a víz elválaszthatatlan egészt képez. A fentiek alapján kijelenthetjük, hogy ha az ember beavatkozik a három tényező akár egyetlen természetes folyamatába és megváltoztatja összetételét, vagy felborítja megszokott folyamatait, akkor sérül, átalakul maga az ökoszisztéma is.

Elég csak a szén, a nitrogén, az oxigén vagy a víz körfolyamataira gondolnunk, máris látható, hogy az egyes részek egymással szoros kapcsolatban állnak. (Terjedelemi megkötés miatt a körforgási folyamatok részletes leírását most mellőzzük. Részletes leírását lásd: [7])

Ha egy olyan egyszerű példát veszünk, amelyben egy vegyipari cég toxikus anyagot juttat egy folyóba, megfigyelhetjük hogyan hatnak a mérgező anyagok az ökoszisztémára.

A folyó növény -és állatállománya, de maga a víz is méreggel telítődik. Természetes folyamatai leállnak. A kifogott halak az emberekhez, majd azok szervezeteibe kerülnek, ahol rövid és hosszú távú mérgező folyamatokba kezdenek, míg a szennyezett víz elpárolog, és eső formájában visszahullva szennyezi a talajt is. Az itt termelt kultúrnövények felszívják a mérget, ami szintén az emberi szervezetbe kerül.

Ez a leegyszerűsített példa azt mutatja, hogy az emberi felelőtlenség egyetlen meggondolatlan vagy hanyag tette lavinát indít el a teljes ökoszisztémában.

Épp ezért nem elég körültekintően eljárni a környezettel való gazdálkodás területén, már a tervezésnél a lehető legtöbb figyelmet kell fordítani a környezetvédelmi szempontokra.

³ Antropocén-kor: A Föld az emberi tevékenység különböző erősségű tevékenységeinek hatása alatt áll.
Forrás: Pásztor Erzsébet-Oborny Beáta: Ökológia, Nemzeti Tankönyvkiadó, Budapest, 2007.p.364.

A fejlesztéseket is az élhetőbb környezet, a fenntartható fejlődés⁴ szolgálatába kell állítani, és úgy kell végezni minden emberi tevékenységet, hogy a lehető legkevesebb kárt okozzuk a természetes rendszerekben. Minimalizálni kell a káros anyag kibocsátást, és ésszerűen kell kezelni a keletkezett hulladékmennyiséget is.

A környezetkímélő technológiák bevezetésével és elterjesztésével, környezettudatos neveléssel és az emberi felelősség hangsúlyozásával kell felhívni az emberiség figyelmét a lehetséges következményekre.

Az utolsó fejezetben ezeket a technológiákat vizsgáljuk meg nagy vonalakban.

A KÖRNYEZET ÉS A TECHNOLÓGIÁK ÖSSZEFÜGGÉSEI

Ma a legkomolyabb veszélyt a szén-dioxid nagy mennyiségű kibocsátása jelenti, hiszen földünk hőszabályozása roppant összetett és kifinomult mechanizmus. A szén-dioxid az alapvető mozgatórugó és leginkább a fosszilis tüzelőanyagok melléktermékeként kerül be a légkörbe.

Földünk tele van szénnel, mely oxidálódik, majd nagyon sokáig megmarad. Mindennek eredményeképpen olvadó gleccserekkel, aszályal, üvegházgázok koncentrációjával, tengerszint emelkedéssel kell számolnunk a közeli és a távoli jövőben.

Hogyan tehetünk a káros emisszió ellen? Néhány megoldás kézenfekvő módon adja magát. Gépjárműveinket hibrid hajtásúakra kellene cserélnünk, a meglévő készülékpallettáról az energiatakarékosabbakat kellene választanunk, és a politikusok közül azokat kellene támogatnunk, akik fontosnak tartják a szén-dioxid kibocsátás csökkentését.

Kellene, de! Sok a feltételes mód, illetve az akadály, hiszen bár a technikai eszközök adottak, a felismerés hiánya, a pesszimizmus, az aktuális gazdasági és politikai helyzet, valamint a különböző érdekek akadályokat gördítenek a tényleges megvalósítás útjába.

A klímaváltozás fogalma már-már közhelynek számít, pedig nagyon sokan nem értik a lényegét, és nincsenek tisztában a lehetséges következményekkel.

De térjünk vissza a technológiák problémáihoz. Közlekedési rendszereink szén-dioxid kibocsátása nagyon magas, így ezek csökkentésére kellene ösztönözni a fogyasztói társadalmat. Napjainkban azonban még csak a jó minőségű, márkás autó a divat és nem a környezetkímélő típus.

A repülés is nagy sűrűségű üzemanyagokat használ, így fokozottan előtérbe kerül a megújuló energiák hatékony felhasználásának kérdése, a biomassza, a szél, és a nap energiájának kihasználása.

A megújuló forrásokat kiválóan használják fel például Brazíliában, ahol a gépjárművek bioetanollal⁵ működnek, amit az ott termelt cukornádból vonnak ki.

⁴ A *fenntartható fejlődés* röviden olyan fejlődés, amely biztosítja a jelen szükségleteinek a kielégítését anélkül, hogy lehetetlenné tenné a jövő generációk szükségleteinek a kielégítését. (Közös Jövők 1987-Brundtland-bizottság)

Egy kissé továbbfejlesztett definíció szerint a fenntartható fejlődés az emberi életminőség javulását jelenti úgy, hogy közben a támogató ökoszisztémák eltartó képességének határain belül maradunk. (World Resources Institute 1992)

A fogalom tágabb értelmezés szerint jelenti a fenntartható gazdasági, ökológiai és társadalmi fejlődést is, de szokás használni szűkebb jelentésben is, a környezeti értelemben (értsd időben folyamatos optimális erőforrás használat és környezeti menedzsment) vett fenntartható fejlődésre korlátozva a fogalom tartalmát.

(Forrás: Kerekes Sándor: A környezetgazdaságtan alapjai, Budapest, 1998. <http://mek.niif.hu/01400/01452/html/fenntarthato/index.html> Letöltés ideje: 2009. május 24.)

⁵ Bioetanol: A bioetanolt már a XX. század első felében is ismerték és alkalmazták üzemanyagként, de széles körű elterjedése csak a jelenlegi szempontok (energiafüggés és környezetvédelem) miatt vált szükségessé. A bioalkohol motor hajtóanyagként való felhasználása történhet tiszta állapotban vagy benzinnel, esetleg dízzel keverve (ez utóbbi egyelőre csak kísérleti stádiumban van). A bioetanol mindenféle szénhidrátból előállítható, napjainkban ipari jelentősége a keményítő és cukortartalmú növényi termékeknek van. (Forrás: http://images.google.hu/imgres?imgurl=http://www.agrener.hu/Images/Misc/bioetanol1.jpg&imgrefurl=http://www.agrener.hu/bioetanol2.php&usq=__Pj5k2EVDb74xoN5D22Ea5JvgWB0=&h=334&w=357&sz=61&hl=hu&

Az Amerikai Egyesült Államokban az etanolt a gabonából nyerik, ami viszont azért nem mondható jónak, mert a kivonáshoz szükséges energia jelentős része, nagy mennyiségű fosszilis üzemanyagot igényel.

Magyar tekintetben is történnek próbálkozások, ilyen például a nagyrédei üzemünk, ahol energiatüzelésével állítanak elő energiát. Az energiatüzelésű kazánokat egyebek mellett a cementiparban és a távfűtésben, valamint mezőgazdasági üzemekben is használják már, eddig körülbelül negyven berendezést állítottak üzembe.

Azonban a hazai viszonyokat mutatja, hogy a megújuló energiaforrások áfája nem került be a kedvezményes, 18 százalékos áfa körbe a Bajnai-csomag nyomán, így ez az ösztönző erő is távlati cél marad egyelőre. Pedig ha a szennyező azért részesülhet pénzügyi támogatásban, hogy szennyezést csökkentő intézkedéseket hajtson végre, akkor az pozitív ösztönzést jelent környezetkímélő vállalati magatartás előmozdítására és azt célozza, hogy „...a korábbinál szigorúbb normáknak a termelők anyagi tönkremenetelük nélkül tudjanak eleget tenni. Ennek értelmében bizonyos környezetvédelmi célokra úgy fordíthat nagyobb összegeket a termelő, hogy anyagi terheit megosztja a költségvetéssel, amennyiben a környezeti kiadásokat, vagy azok egy részét le lehet írni az adóalapból. Mivel az állami költségvetés mértéke és struktúrája politikai döntések alapján alakul, azokban az országokban, amelyekben a környezetvédelem társadalmi támogatottsága gyenge, az adókedvezményeket is igen szűkmarkúan mérik.” [8]

Pedig a brüsszeli eBio jelentéséből kiderül, hogy Magyarország az ötödik helyen áll a bioetanolt előállító országok közötti rangsorban, a maga 150 millió literes termelésével.

A műszaki fejlesztések azonban robbanásszerűen haladnak előre. A japán autógyártás látványos és zöld megoldásokkal van jelen az autópiacon- gondoljunk csak a hibrid⁶ Toyotákra. Nemcsak szépek, és okosak, de sokkal kevesebb üzemanyagot fogyasztanak intelligens módon.



3. ábra. Hibrid jármű [3]

A Toyota Prius üzemanyag fogyasztása és szén-dioxid kibocsátása mintegy 70%-kal alacsonyabb. Ez pont az a mennyiség amennyivel a tudósok szerint 2050-re szükséges lenne a világgazdaság kibocsátását csökkenteni az éghajlatváltozás megakasztása érdekében. [9]

start=2&tbnid=wZD45MvTjoN9JM:&tbnh=113&tbnw=121&prev=/images%3Fq%3Dbioetanol%26gbv%3D2%26hl%3Dhu%26sa%3DGLetöltés ideje: 2009. 05. 30.)

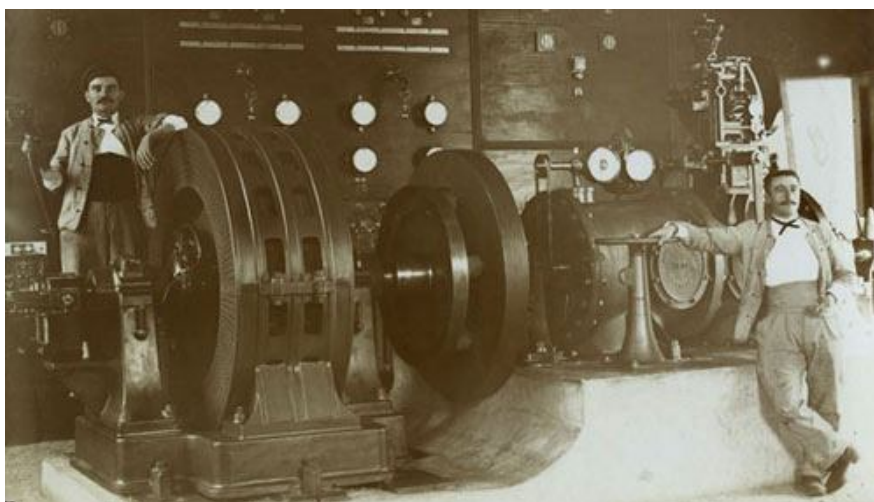
⁶ Hibrid autó: A hibrid kifejezés azokra az autókra (és egyéb járművekre) utal, ahol a gépjármű meghajtását kettő vagy több elv is biztosítja. Ezek jellemzően a belső égésű motor és a villanymotor.

A többféle meghajtásnak az a szerepe, hogy az adott igénybevételhez szükséges energiát minél kisebb befektetéssel állítsuk elő. Így városban belül, ahol az ember általában rövid távokat tesz meg, egyik lámpától a másikig, vagy a dugóban várakozva, az a villanymotor lép működésbe, amelynek nincs károsanyag-kibocsátása, magasabb sebességnél, hosszabb távon pedig a már jól megszokott belső égésű motorra hagyatkozhatunk. Forrás: <http://mindenamiauto.blogter.hu/> Letöltés ideje: 2009. 05.30.

Az elektromos autók működtetéséhez szükséges technológia nagyon rég készen volt. Volta⁷ 1800-ban állította össze első kémiai elven működő elemét. A gondot az jelentette, hogy nem lehetett újratölteni, csak az aktív részek cseréjével lehetett további energiát csiholni belőle. Az első autók is szenvedtek ettől a problémától, és csak 1860-ban oldódott meg a kérdés, amikor Gaston Faure felfedezte az újratölthető ólom-savas akkumulátor elvét.



4. ábra. Elektromos-benzines hibrid autó 1903-ból^[4]



5. ábra. Gaston Faure^[5]

Európa útjain új technológiai vívmányként megjelent a sűrített levegővel működő Air car is, melyet az indiai óriáskonszern Tata gyárt, s a volt Forma-1-es mérnök Guy Négre cége fejlesztett ki. A sűrített levegővel hajtott kocsik fejlesztésébe a kilencvenes évek hajnalán fogott bele a volt Forma-1-es fejlesztőmérnök Négre, megalapítva a luxemburgi MDI⁸ céget, mely kizárólag az alternatív meghajtású járművekkel foglalkozik. Az Air Car sűrített levegőt használ motorja dugattyúinak mozgatására.

⁷ Alessandro Volta 1745. február 18-án született Észak-Itáliában, Comóban, egy olasz nemesi család sarjaként. Volta fizikus volt, az elektromosságtan úttörője. Rá emlékeztet ma is a feszültség mértékegysége, a "Volt". Az olasz tudós grófi címet kapott Napóleontól felfedezése miatt.

⁸ MDI: Moteur Development International



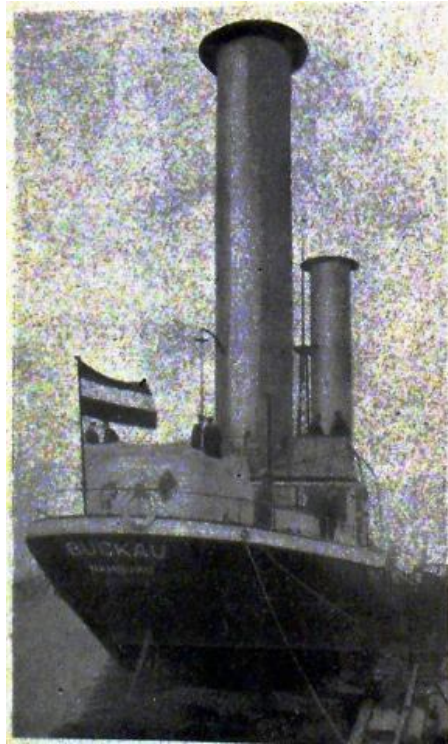
6. ábra. Az indiai Air car és motorja ^[6]

Az Air Car előnye, hogy nincs berobbanás, így a motorolajat elegendő ötvenezer kilométerenként cserélni, és a kipufogón keresztül csak a tiszta levegő távozik. És most mindezt kombináljuk a szélerőművek gondolatával, melyek képesek az autót feltölteni és máris egy tisztább világ képe rajzolódik ki előttünk.

Az autókön kívül a repülőgépek és a hajózás is gigantikus méretű üzemanyag mennyiséget használ fel. A nemzetközi hajózás (kereskedelem, turisztika) egyre növekszik, így a felhasznált olaj mennyisége is fokozatosan növekvő tendenciát mutat. Napjaink megújuló energiái a nap és a szél és egyéb energiaforrások kiutat jelenthetnének az olaj csapdájából, energiatakarékos motorok használatával kombinálva. A régmúlt idők hajósai is befogták a szelet, és annak segítségével utaztak a világóceánokon. Napjainkban már sokkal több lehetőség áll rendelkezésre a technika vívmányainak köszönhetően, csak okosan kellene tudnunk használni azokat.

Már 1925-ben Flettner Antal frankfurti mérnök, aki akkor az amszterdami Légi és Hidrodinamikai Intézet igazgatója volt, Kielben vízrebocsátotta új szerkezetű hajóját, a Buckau-t, melyet a szél ereje mozgatott.

Ezen a hajón nem volt vitorla, a szél nyomását két nagy. 2.8 m átmérőjű, 15.6 m magas vashenger vette föl, melyet 10—15 lóerős motor forgatott a tengelye körül, percenként 120 fordulattal, s ez a két henger tízszer nagyobb sebességet kölcsönzött a hajónak, mintha a szél erejét a hengereknek megfelelő nagyságú vitorlával hasznosították volna.



7. ábra. Flettner Antal hajója ^[7]

A légi közlekedés sem különbözik a másik kettőtől, csak kerozint használ fel, melyet ráadásul csak fosszilis üzemanyagokból lehet előállítani, s amelynek mennyiség évről-évre egyre csak nő. Az utasok száma is növekvő tendenciát mutat, hisz a repülés egyre több ember számára válik elérhetővé.

Az a keverék, melyet a repülőgépek bocsátanak ki, az ellenkező módon fejti ki hatását. Mivel a legmodernebb sugárhajtású gépek a troposzféra közelében közlekednek, a vízgőz, a nitrogén-oxid és a kén-dioxid kibocsátása különös következménnyel jár. Habár a kikerült nitrogén-oxid fokozhatja az ózonképződést a troposzférában és a sztratoszféra alsó rétegeiben, mégis rombolja ugyanazt a sztratoszféra felső rétegeiben a kén-dioxid hűtő hatása miatt. [10]

Egyik fontos emissziós anyag a vízpára, mely alapja a repülőgépek kondenzcsíkjának. A kondenzcsík a magas légkörben zajló repülés "mellékterméke". A repülőgépek kipufogógáza kondenzációs magként szolgál, mivel a léghőmérséklet negatív, a levegő, pedig túltelített, a vízcseppek jégkristályokként kondenzálódnak. Így alakul ki a mesterséges *cirrus*.⁹

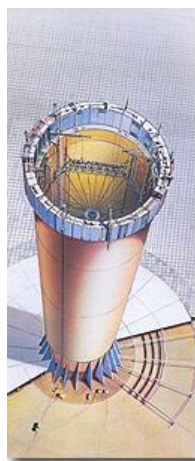
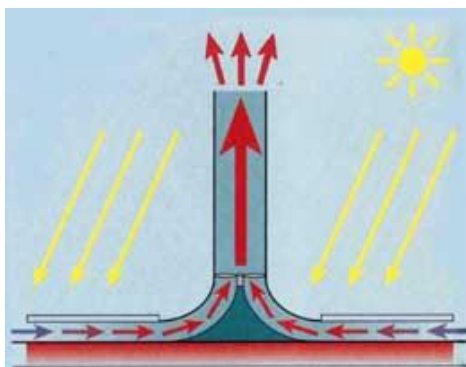
Amikor viszonylag kevés nedvességet tartalmaz a magas légkör, akkor gyorsan feloszlik a kondenzcsík, vagy gyakorlatilag földről, szemmel már nem látható létrejön. Nagy nedvességtartalom esetén, viszont erős, vastag és hosszú ideig fennmaradó cirruscsík képződik, amelyet a szél fodrozódása alakít tovább. Tartós kondenzcsík, nagy nedvességtartalomra utal, amely egyben, egy front előhírnöke is.

⁹ Cirrus: pelyhefelhő Forrás: Letöltés ideje: 2009. május 30.



8. ábra. Kondenzcsíkok ^[8]

Új technológiákat kutatva megemlíthetjük még a napkémények elterjedését is, melyek szintén alternatív energiaforrásként jöhetnek számításba. A napkémény azon egyszerű elven alapszik, hogy a meleg levegő felszáll. A folyamat lényege az, hogy a nap energiáját összegyűjtő tető alatt a levegő felmelegszik és a kémény felé áramlik, melyben felszáll, és közben lehűl. A levegő az egész rendszer körül cirkulál, mivel oldalról újabb hideg levegő áramlik a felmelegedett helyére. A kéménybe elhelyezett turbinák termelik, a felszálló levegő mozgási energiáját felhasználva, az elektromos energiát. A napkémények elvi működését a 12. ábra szemlélteti.



9. ábra. Napkémények elvben és a valóságban ^[9]

A nap ereje mellett a víz hullámait is próbálják kihasználni kísérletező kedvű és elszánt kutatók. A Földön nagyjából 100 kis vállalat dolgozik azon, hogy a tenger energiájából elektromos áramot állítson elő. Számos közülük európai, ahol a kormányok sok pénzt fektetnek be ebbe az iparágba. A cégek a kormányokhoz hasonlóan arra számítanak, hogy a költségek az idővel csökkenni fognak. Mindemellet jelen pillanatban csak kevés energiát termelnek az óceán segítségével, kivéve néhány elszórt teszt-telepet.

Az óceán-energiát két fő kategóriába lehet osztani, az apály-dagály jelenséget és a hullámot kihasználó technológiákra. A hullám-módszer, melyet a Finavera¹⁰ is alkalmaz, a víz fel-le mozgásából állítja elő az energiát. Az apály-dagály jelenségnél a szélkerekekhez hasonló turbinákkal fejleszti az elektromos áramot. (Van egy pár évtizede létező módszer is, melyet Franciaország és Kanada is alkalmaz, ahol gátrendszerrel érik el a dagályt. Ezek a rendszerek jóval nagyobb méretűek, mint a mostani, víz alatti technológiák.)

Létezik egy harmadik típus is, a hőenergiával működő, mellyel az óceán felszíne és mélye közti hőmérséklet-különbséget használják ki, ez főleg a trópusokon alkalmazható.

Az óceán-energia sokkal hatásosabb lehetne a szélenergiánál, mivel a víz közel 850-szer sűrűbb a levegőnél. Ezen kívül a hullámok és az apály-dagály jelenség könnyebben előre jelezhető, mint a szél.

A módszer hátránya, hogy a tengervíz sokkal jobban korrodálja a szerkezeteket, valamint drága víz alatti kábelekre van szükség az áram szárazföldre szállításához. Ezen kívül a rendszerek felépítése is költséges.



10. ábra. Hullámerőművek Portugáliában^[10]

Ahhoz, hogy a fenti problémákat leküzdhessük, már az új generációknak is környezettudatos nevelésben kell részesülniük. Példamutatással, játékos ismeretterjesztéssel sokat tehetünk a felnövő (és a saját) korosztály későbbi sorsáért, a kímélőbb technológiák alkalmazása, a kutatások ez irányba történő elmozdítása révén pedig új távlatokat nyithatunk a környezetvédelem és a technológiák kapcsolatában.

¹⁰ Finavera: A Finavera Renewables, az a kanadai cég, mely nemrég újrahasznosította az Oregonnál elsüllyedt, 2,5 milliós hullám-energiát hasznosító berendezését, aláírt egy szerződést a Pacific Gas & Electric-kel arról, hogy 2012-ig Kalifornia partjainál energiát fognak termelni a számukra.

CSAK RAJTUNK MÚLIK – ÖSSZEGZÉS

Kulcsfontosságú döntés az éghajlatváltozás elleni harcban a környezetbiztonság helyes értelmezése és annak fenntartása. A klímaváltozás új kihívások elé állította az emberiséget, s új értelmet nyert a biztonság fogalma is.

Komplexitása révén a környezetbiztonság kérdései nem csak a politikát, a gazdaságot, de a környezetvédelmet is alaposan felforgatták

A fenti példákból kiderült, hogy erőinket a közlekedésre, vagy a villamos-hálózatra kell összpontosítanunk. Mindkettőre egyszerre lehetetlen, hiszen nem áll rendelkezésünkre elegendő forrás és idő.

Cél, a szén-dioxid kibocsátás jelentős mértékű csökkentése. Vannak országok, ahol már élen járnak a megújuló energiák befogadásában, Dánia például világelső a szélenergia üzemeltetése terén.

A szél azonban nem folyamatos energiaforrás, így szóba jöhet még a nap, vagy a geotermikus energia is. A napenergia háztartási-célú felhasználása eleinte drágának tűnhet, de a költségek később megtérülnek.

Terjednek a napkémények is, dagály és hullámenergiát használnak bizonyos országokban, és - a Gaia elmélet¹¹ megszületése óta a nukleáris energia is új alternatívát jelent a fosszilis energiahordozók helyett. (E szektor kifejtése külön tanulmányt igényelne, ezért erre a területre most nem térünk ki.)

A fejlődő országok – különösen Kína és India – egyre inkább meghatározó szerepet játszanak a megújuló energiák gyártásában és telepítésében is. (Például Kína szélenergia kapacitása 2008-ban megduplázódott – és ez már negyedik éve így van.)

Ember és bolygó sorsa összekapcsolódik. A technoszféra megjelenése, - amelynek térhódítását az ipari forradalom segítette elő- kiemelt jelentőséggel bír, hiszen a közel 500 millió év során felhalmozódott szén, kőolaj és földgáztelepek fogyatkoznak, így néhány korábbi tényező veszélytényezővé vált.

„Új megoldásokra lesz szükség, a fenti forrásokból előállított energiának a jelenleginél sokszorosan környezetkímélőbb és biztonságosabb tárolásában, szállításában, és felhasználásában is.” [10]

A REN21¹², a megújuló energiatermelés terjesztésére létrejött globális hálózat 2009. május 13-án jelentette meg legújabb világjelentését, melynek már a címe is reménykeltő: Az energiatermelés átalakulása a gazdasági lassulás ellenére folytatódik.

A REN21 idén negyedik alkalommal adta ki jelentését a megújuló energiák globális helyzetéről. Mohamed El-Ashry, a REN 21 elnöke így mutatta be a művet: *"Összefoglalónkat egy történelmi és globális méretű gazdasági válság idején adjuk közre. Bár a jövő bizonytalan, ez a jelentés okot ad az optimizmusra."*

¹¹ *Gaia-elmélet*: A Gaia-elmélet lényege, hogy a Föld bolygó összes élő és élettelen része egy szorosan összefüggő rendszert alkot, amely rendszer homeosztatikus működésű, azaz képes fenntartani létezésének feltételeit. A Gaia-elmélet megalkotója dr. James Lovelock, aki "Daisy World" elnevezéssel - az 1970-es években - egy képzelte világot modellezett, melyben lényegében két "lény" él és alkot egyensúlyt. Az egyik egy sötét színű növény (szákszorszép), a másik egy világosabb. Előbbi jól tűri a hideget és elnyeli a napfényt, míg a másik melegtűrő és visszaveri a sugarakat az űrbe.

Az elmélet lényege, hogy a hideg környezetben a sötét virág begyűjti a meleget és kialakítja az ideális hőfokot, míg a melegedéssel a világos veszi át a szerepet és hűti a környezetet szintén az ideálisra. Addig, amíg ez a két organizmus egymással egyensúlyban él, a környezetük ideális mindkettő számára, de amennyiben bármelyik eltűnik lényegében a teljes szervezet a Föld vagy Gaia elpusztul. Az elmélet az élő és nem élő organizmusok kényes és egymásra ható, ideális életfeltételekre törekvő egységét mutatja be. Lovelock könyvének - mely 1979-ben jelent meg - "Gaia: A new look at life on Earth" a címe. Forrás: <http://hu.wikipedia.org/wiki/Gaia-elmélet> Letöltés ideje: 2009. május 30.

¹² REN21: Renewable Energy Policy Network for the 21st Century
Forrás: <http://www.ren21.net/ren21/default.asp> Letöltés ideje: 2009. május 30.

A hatékony technológiaváltás elősegítheti az antropogén eredetű klímaváltozás kordában tartását. Ha elavult technológiákat használunk, emelkedik a szén-dioxid szint, ami felmelegedő klímát eredményezhet. „*A globális évi átlaghőmérséklet változásának intervalluma 2-5 Celsius fokra tehető.*” [11]

Klímánk változik, biztonságunk mindinkább veszélybe kerül. A klíma stabilitásától függő lét több ponton megingott. Civilizációnk jövője rajtunk, embereken múlik. Itt az idő cselekedni.

Irodalomjegyzék

- [1] Juhász – Szőke - O. Nagy: Magyar Értelmező Kéziszótár. Akadémiai kiadó, 2002.
- [2] Dr. Halász László- Földi László: Környezetvédelem–környezetbiztonság. Egyetemi jegyzet2000.
- [3] Daniel Quinn: Ismael. Katalizátor kiadó, 2008.
- [4] Láng István: Környezet-és természetvédelmi lexikon. Akadémiai kiadó, 2002.
- [5] Nagy Tibor: Biztonság és biztonságstudomány, Magyar Biztonságstudományi Társaság, 2001.
- [6] Dr. Halász László- Földi László: Környezetvédelem–környezetbiztonság. Egyetemi jegyzet, 2000.
- [7] Dr. Halász László- Földi László: Környezetvédelem–környezetbiztonság. Egyetemi jegyzet, 2000.
- [8] Kerekes Sándor: A környezetgazdaságtan alapjai. 1998.
- [9] Tim Flannery: Időjáráscsinálók. Borsodi nyomda, Akkord Kiadó, 2006.
- [10] Tim Flannery: Időjáráscsinálók. Borsodi nyomda, Akkord Kiadó, 2006.
- [11] Szesztay Károly- Sz. Gábor Margit: Bolygónk véges türelme. Akadémiai Kiadó,1992.

Ábrajegyzék

- 1. ábra A környezetvédelem területei.
Dr. Halász László - Földi László: Környezetvédelem–környezetbiztonság, Budapest, 2000, Egyetemi jegyzet, ZMNE
- 2. ábra Az ózonréteget károsító anyagok
<http://nov.lkg-bp.sulinet.hu/~aaa/oxi/ozon.htm> Letöltés ideje: 2009. május 25.
- 3. ábra Hibrid jármű
<http://mindenamiauto.blogter.hu/> Letöltés ideje: 2009. május 30.
- 4. ábra Elektromos-benzines hibrid autó1903-ból
<http://totalcar.hu/magazin/szerelem/elauto/> Letöltés ideje: 2009. május 30.
- 5. ábra Gaston Faure
http://images.google.hu/imgres?imgurl=http://www.edsb.fr/images/histoire/moustachus.jpg&imgrefurl=http://www.edsb.fr/histoire.html&usq=__WyrHpIISq9-IffygfaNjzITcMnM=&h=283&w=500&sz=31&hl=hu&start=1&um=1&tbnid=DJm87PbfGNVffM:&tbnh=74&tbnw=130&prev=/images%3Fq%3D%2522Gaston%2BFaure%2522%26hl%3Dhu%26lr%3Dlang_hu%26sa%3DN%26um%3D1 Letöltés ideje: 2009. május 30.

6. ábra Az indiai Air car és motorja
http://hvg.hu/Tudomany/20070529_suritett_levego_auto_air_car.aspx?s=2007530nl
Letöltés ideje: 2009. május 30.
7. ábra Flettner Antal hajója
<http://www.husadikszazad.hu/index.php?apps=cikk&cikk=15963> Letöltés ideje:
2009. május 30.
8. ábra Kondenzcsíkok
http://hu.wikipedia.org/wiki/Globális_homály Letöltés ideje: 2009. május 30.
9. ábra Napkémények elvben és a valóságban
<http://www.sulinet.hu/thinkquest/honlapok/sunband/napkemeny.html> Letöltés ideje:
2009. május 30.
10. ábra Hullámerőművek Portugáliában
<http://kitekinto.hu/galeria/hullamermvek/1/> Letöltés ideje: 2009. május 30.

Hankó Márta

marti1222@gmail.com

Földi László

foldi.laszlo@zmne.hu

A KÖRNYEZETI KOCKÁZATOK ELEMZÉSE

Absztrakt

A XXI. század egyik alapvető problémája a jelentős mértékű emberi eredetű környezetszennyezés. A cikk a környezettel való ésszerű gazdálkodás fontosságára és összetettségére hívja fel a figyelmet.

Bemutatja a légkörrel, a vízzel és a talajjal összefüggő környezeti problémákat, azok összefüggéseit, nagy vonalakban körüljárja a hulladékok helyes tárolásának és feldolgozásának napjainkra kialakult problematikáját, valamint előtérbe helyezi a technológiaváltás fontosságának kérdését.

One of the basic problems of the 21st century is the significant extension of pollution caused by the humans. The article calls the attention to the importance and complexity of the reasonable economics of the environment. Furthermore, the article presents the environmental problems with atmosphere, water and soil. Besides it refers to their connections. Moreover, it deals with recent problems of waste materials, their storing and recycling. Last, but not least it puts the stress on importance of the question of technology modernization.

Kulcsszavak: *környezetgazdálkodás, általános problémák, légkör, víz, talaj, hulladékok ~ environmental management, general problems, atmosphere, water, soil, waste materials*

BEVEZETÉS

A környezet állapotának fenntartása mindannyiunk érdeke. A gazdálkodó szervezetek tevékenységük „melléktermékeként” szennyezik is a környezetet, így annak minősége könnyen leromolhat.

A környezetszennyezést gazdasági szempontból csak egy ideje elemezzük, és a tapasztalatok újabb és újabb vizsgálatokra sarkallják a kutatókat.

A századfordulón Alfred Marshall (1842) angol közgazdász bevezette a külső költségek és hasznok fogalmát a "Gazdaság alapelvei" c. művében. Ezzel megalapozta a környezeti gazdaságtan, vagy más néven a környezetgazdálkodás tudományát is.

Marshall olyan jelenségeket kívánt jellemezni, ahol egy pénzügyileg önálló egység, közvetlenül befolyásolja egy másik, pénzügyileg önálló egység, egy vállalkozás vagy egy fogyasztó helyzetét, anélkül, hogy a piacon kerülnének kapcsolatba.

A környezetszennyezés is egy ilyen befolyásoló tényező. Két vagy több fél között jön létre, anélkül, hogy a felek akár valaha is találkoznának, ám a kapcsolat - és tegyük hozzá a környezetgazdászok fogalomtárában ez mindig negatív kapcsolat- közöttük mégis kialakul.

Ez általános és speciális problémákat is felvet, és megjelenik olyan területeken, melyek mindannyiunk életterét érintik.

A környezetszennyezés befolyásolja a légkört és annak folyamatait, a hidroszférát és a benne élő egyedeket, azok kapcsolatait, viszonyait, valamint a litoszféra egyensúlyát is.

A környezeti elemekben jelentkező problémák kihatással vannak az ökoszisztéma egészére, így új kihívások elé állítják az emberiséget.

Megoldást csak az új technológiák bevezetése és alkalmazása, a keletkező hulladékmennyiségek ésszerű és szabályozott kezelése, valamint a „zöldebb” életvitel adhat.

Az alábbi dolgozat ezeket a területeket járja körbe a teljesség igénye nélkül.

A KÖRNYEZETGAZDÁLKODÁS FOGALMA

Mielőtt alaposabban belemerülnénk a témába a vizsgálandó terület fogalmát mindenképpen tisztáznunk kell. Mit értünk pontosan a megnevezés alatt? Első hallásra talán egyszerűnek tűnik, ám ha jobban belegondolunk nem is olyan könnyű megfogalmazni.

A *környezetgazdálkodás* a környezetvédelem része, a természetvédelemmel, a tájvédelemmel, környezet egészségüggyel, és a települési környezetvédelemmel egyetemben.

A környezetgazdálkodás a gazdasági tevékenységek olyan megtervezését, megszervezését és végrehajtását jelenti, amelynek során a gazdálkodók ésszerűen, környezetkímélő módon, távlatokban gondolkodva gazdálkodnak a természeti erőforrásokkal, ennek érdekében környezetkímélő technológiákat alkalmaznak, tevékenységük során törekszenek arra, hogy ne pusztítsanak el élőlényeket, ne károsítsanak élő rendszereket és élettelen természeti értékeket, és ne károsodjon az emberek egészsége sem.

Környezetgazdálkodás alatt a természetes és az ember alkotta környezet hosszú távra szóló, szabályozott hasznosítását értjük, tudatos, tervszerű fejlesztését és hatékony védelmét az ökológiai rendszerek stabilitásának tartós megőrzésével és a társadalom igényeinek figyelembevételével. Egy olyan gazdálkodási folyamat, amelyben az erőforrások felhasználása, a technika fejlesztése, a beruházások irányítása és az intézményi rendszer egymással összhangban fejlődik, s mindez lehetővé teszi az emberi szükségletek kielégítésének hosszú távú biztosítását.

Ha már itt tartunk, nem árt tisztázni magának a környezetvédelemnek a fogalmát sem.

Az 1995. évi LIII. törvény a környezet védelmének általános szabályairól kimondja, hogy „a környezetvédelem: olyan tevékenységek és intézkedések összessége, amelyeknek célja a környezet veszélyeztetésének, károsításának, szennyezésének megelőzése, a kialakult károk mérséklése vagy megszüntetése, a károsító tevékenységet megelőző állapot helyreállítása.”[1]

A környezetgazdálkodás vizsgálata igen széles ismeretanyagot igényel, hiszen a terület nemcsak a víz, a talaj, vagy a levegő védelmével kapcsolatos kérdésekkel foglalkozik, hanem a zajvédelem, vagy akár a közgazdaságtan alapkérdéseinek ismeretét is megkívánja. Az említett területek speciális problémáit, összefüggéseit az alábbiakban elemezzük.

ÁLTALÁNOS PROBLÉMÁK

Napjainkban a Föld nincsen könnyű helyzetben. Népességszáma 35 évenként a duplájára nő, az élelmiszerellátottság nem egyenletes, mert míg fekete-Afrika éhezik, addig például Amerika lakosságának nagy része túlsúllyal küzd, az ipari termelés robbanásszerűen

megnöveli a káros emissziót, - így egyre nagyobb becsben tartják a valóban tiszta levegőjű területeket- az energiafelhasználás pedig az egeket ostromolja. Ivóvízkészleteinkre fokozottan oda kell figyelnünk, a megújuló energiákkal pedig újfajta módon kell gazdálkodnunk.

A bolygó népességszámának növekedése köztudott. A növekedés gyors ütemű és szinte robbanásszerű. Az eloszlás egyenetlen, a népességszabályozás pedig évek óta komoly gondokat jelent az olyan térségekben, mint Kína, vagy India.

A növekvő népesség több energiát, ivóvizet és élelmet kíván, de több szemetet, hulladékot is termel, és a levegőt is jobban terheli.

Érinti mindez a víz, a talaj, és az atmoszféra szennyezésének problémáját is, így ha valóban átfogó képet szeretnénk a környezetgazdálkodás eme kérdéseiről, akkor e területeket egyenként kell megvizsgálunk.

A LÉGKÖR KOCKÁZATAI

Bolygónkat egy levegőburok veszi körül, mely a bolygó felszínétől számított 560 km-es magasságig tart. Alkotói 78% nitrogén, 21% oxigén, és egyéb összetevők, mint pl. argon, szén-dioxid, ózon.

A légkör összetétele nem volt mindig ugyanilyen. Óriási mennyiségű légköri oxigén megkötése történt meg tengeri mészvázak élőlények felhalmozódása, valamint szárazföldi növények fotoszintézise révén. Így jött létre a mai oxigénben dús légkör.

A légkör összetétele az emberi tevékenység függvényében változik, hiszen az *ipari forradalom* (1769-1850) óta jelentősen több szennyező anyag kerül ki az atmoszférába.

Az *üvegházhatású gázok* (metán, szén-dioxid, dinitrogén-oxid... stb.) koncentrációjának kismértékű változása is új átlaghőmérsékletet eredményez a Földön.

A levegő szennyeződése helyi és globális szinten egyaránt jelentkezik, ami viszont az átlaghőmérsékleti mutatók átalakuláshoz, ezáltal pedig változó klímaviszonyokhoz vezet.

Az ember által belélegzett levegő összetétele megváltozik, kén-dioxid, szén-monoxid, nitrogén-dioxid...stb. dúsul fel benne, ami az egészségre igen ártalmasan hat. Szükségessé válik a szennyezők kibocsátásának szabályozása, erre kitűnő példa volt többek között az 1987-ben hatályba lépő, a *Nagy távolságra jutó, országhatárokon áterjedő levegőszennyezésről* szóló 1979. évi Egyezményhez kapcsolódó *SO₂, Jegyzőkönyv*, melyben az aláírók vállalták, hogy legalább 30%-kal csökkentik *SO₂*, kibocsátásukat vagy határon keresztüli *SO₂*, transzportjukat 1993-ig.[2]

A szennyezőanyagok kedvezőtlen meteorológiai viszonyok között nagyon feldúsulhatnak így a tiszta levegőt felváltja a szmog.

A szmognak két alaptípusa ismeretes, a londoni szmog hűvösebb időben, kora reggel alakul ki, és a kén-dioxid, szén-monoxid, szilárd szennyezők stb. magas koncentrációja jellemzi.

A másik ismert típus a los angelesi típusú szmog, amely melegben, intenzív sugárzáskor jön létre, és oxidáló hatású anyagok, valamint ezek átalakulási termékei a fontosabb alkotói.

„Különösen veszélyesek a légköri reakciókban az illékony szerves vegyületekből a nitrogénoxidok, illetve az ózon hatására képződő vegyületek az úgynevezett peroxi-acetil-nitrátok (PAN), amelyek rákkeltő hatásúak.” [3]

A levegőt károsító emisszió ellen aktívan és passzívan is védekezhetünk. A passzív védelem nem csökkenti a környezetbe kikerülő szennyezőanyag mennyiségét, de jelentősen csökkentheti a szennyezőanyag által kiváltott káros hatásokat például magas kémények építésével.

„A kéményméretezés célja az, hogy a technológiai norma által megengedett szennyezőanyag mennyiséget elegendően magasban bocsássuk ki ahhoz, hogy talajszinten betartható legyen az immisszió norma.” [4]

Az aktív védelem a szennyező anyagok keletkezésének megakadályozását tűzi ki célul. A környezetszennyező technológiákat más, azoknál kedvezőbbekkel igyekszik helyettesíteni. (pl. széntüzelés helyett megújuló energiával történő fűtés)

Levonhatjuk tehát a következtetést, hogy ha terheljük a bolygónk légkörét, az újabbnál-újabb és számos területen megjelenő problémákat generál. A változások érezhetőek lesznek mind egészségügyi, mind gazdasági területeken, de hatásosabb és környezetkímélőbb megoldások keresésére is sarkallják majd a kutatókat.

A levegőtisztaságot érintő gazdasági tevékenységeket oly módon kell megtervezni, hogy azok környezetkímélő módon, távlatokban gondolkodva töltsék be funkciójukat.

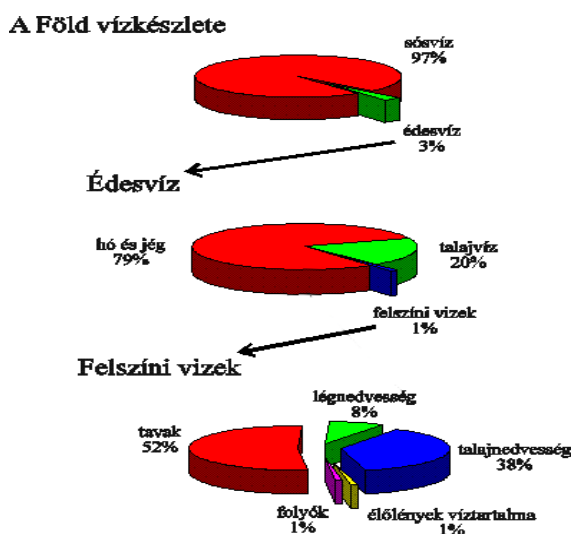
A HIDROSZFÉRA KÖRNYEZETI PROBLÉMÁIRÓL

H₂O. Ilyen egyszerű a földi lét egyik alapjának képlete. A víz egy vegyület, melynek molekuláit két hidrogén, és egy oxigén atom alkotja. A föld felületének mintegy 71 %-át borítja víz, ami akár azt is jelenthetné, hogy bővelkedünk ebben az értékes anyagban, ám ha figyelembe vesszük, hogy ebből mindössze 2% az édesvíz, akkor már más megvilágításba kerülnek a dolgok.

Az édesvíz a gleccserek, a hótakarók és a felszín alatti vizek természetes raktáraiból nyerhető ki, és ha azt is számításba vesszük, hogy a vízkészletnek csak egy bizonyos része tiszta ivóvíz, akkor bizony rádöbbenünk, hogy nagyon is értékes forrással állunk szemben. Magyarország tekintetében a felszín alatti vizekből nyerhető az ivóvízkészletek 95%- a.

„Felszíni vizeink mellett, annak mintegy 10 %-át kitevő mennyiségű felszín alatti vízkészlettel (parti szűrészű víz, talajvíz, karsztvíz, rétegvíz) is rendelkezünk, ebből főleg ivóvíz szükségletünket fedezzük. A felső talajrétegből, forrásokból kitermelhető víz mennyisége mind korlátozottabb. Így hazánkban is a víznyerés a felszíni vizek használata felé tolódik el. Az ivóvízellátást szolgáló vízműveink zömükben parti szűrészű és mélységi vizet adnak.”[5]

Az ember szimbiózisban él a vízzel, hiszen a sejt és testnedvek nagy részét is víz alkotja, amit folyamatosan pótolnunk kell. Táplálék, másoknak megélhetés, vagy éppen kellemes kapcsolódási lehetőség. Az egyre növekvő népességszám, egyre nagyobb mennyiségű vizet igényel. Az egyes ábrán a Föld vízkészleteinek megoszlását figyelhetjük meg az óceánok és a szárazföld között. Láthatjuk, hogy édesvizünk csak 3 százaléknyi van, ráadásul ez sem mind ivóvíz tisztaságú.



1.ábra. A Föld vízkészleteinek megoszlása az óceánok és a szárazföld között ^[1]

Az emberiség újkori életmódja egyre több szennyeződést juttat a folyókba, tavakba, melyek sok esetben toxikus hatásuknál fogva veszélyt jelentenek a fogyasztók számára.

Említhetnénk itt a minamata betegséget, mely az 50-es években a japán Minamata-öbölben ütötte fel fejét, és amelynek több száz halálos áldozata is volt. Utólag kiderült, hogy a táplálékul szolgáló halak és kagylók szervezetében felhalmozódott higany okozta a mérgezést. Ugyancsak nehézfém-szennyezés okozza az "itai-itai"¹ kór tüneteit is.

Nem szabad megfélekednünk a növényvédőszeres káros hatásairól sem, melyek a víz körforgása révén jutnak el az élő szervezetekhez és okoznak azokban jelentős és hosszú távú károkat.

„Az édes – és sósvízi halastavak az élelem fontos forrásai, és nem kétséges, hogy a beléjük kerülő vegyszerek súlyosan veszélyeztetik őket.” [6]

A DDT², a detergens³, az olaj és annak származékai, a hőszenyezés (pl. erőműveknél), a savas esők mind-mind károsan hatnak az élővizek egyensúlyára. Nemcsak az ott kialakult életformákat borítják fel, hanem közvetve az embert is károsítják. Elmocsarasodás, ivóvízhiány, a halgazdaság csődje, az üdülési ágazatok tönkremenetele, és a jövőben esetlegesen a tiszta vízért vívott háborúk veszélye fenyegethet bennünket.

Az, hogy egy-egy terület milyen minőségű vizet igényel, természetesen eltérő lehet. Az „élő” vizeket a természeteshez legközelebb állapotban kellene megőriznünk, az ember igényeit pedig a lehetőségekhez mérten szabadna csak kiszolgáltatnunk.

„Az egyes felhasználásokhoz szükséges vízminőségi követelmények szabványokban rögzítettek. Így pl. az ivóvíz-felhasználás minőségi követelményeit az EU előírásait közelítő MSZ 448 magyar szabvány tartalmazza.” [7] Éppen ezért az egyre hatékonyabb mechanikai, fizikai - és biológiai víztisztítási módszerek támogatása, a meglévő tiszta vizek fokozott védelme, valamint a takarékos, ésszerű vízfelhasználás jelenthet kiutat az emberiség számára. A környezetkímélő technológiák kiemelt alkalmazása, az emberi törekvés a tiszta víz fenntartására, közös céllá kell, hogy váljon.

A TALAJJAL ÖSSZEFÜGGŐ KÖRNYEZETI PROBLÉMÁK

A talaj a földkéreg legfelső, laza, szilárd, termékeny rétege, amelyet a növények gyökérzete és a mikroorganizmusok együttes tevékenysége hozott létre a kőzetek és elhalt szerves maradékok anyagából.

A talaj sok szempontból fontos az emberiség számára, egyfelől építési terület (utak, épületek... stb), másrészt nyersanyagforrás (pl. kőolaj, víz... stb), harmadrészt pedig a letűnt korok tanúja, hiszen a földkéregből vett furatminták alapján számos eredményt ért már el a modern tudomány. Ezt a nagyon fontos szférát azonban számos szennyezés éri, különböző források által.

- A talajban lejátszódó természetes folyamatok, a víz szállító funkciója révén terjednek tovább, így az esetleges szennyeződések is ekképpen „utaznak”.
- A lakossági –kisebb mértékű– szennyeződések is beszivárognak a litoszférába az infrastruktúrán keresztül.
- Az ipar, mint nagyfelhasználó a gyártelepek szennyét közvetlenül, a levegőn át pedig közvetve juttatja a földbe. Az elsavanyodás, a porszenyezések, és a közlekedés is hozzájárul a talajminőség romlásához.
- A mezőgazdaság a növényvédőszeres vagy más néven peszticidek, trágyák révén járul hozzá az egyetemleges talajszennyezéshez. A különféle kemikáliák, a technológiai fegyelem esetleges megsértése, a veszélyes hulladékok szakszerűtlen, „kényelmes”

¹ A kadmium által okozott betegséget Itai-itai kórnak nevezzük (japánul azt jelenti: nagyon fáj).

² diklór-difenil-triklór-etán

³ Szerves szintetikus tisztítószer

talajba juttatása számos nehézséget okoz. Itt kell megemlítenünk az öntözés káros hatásait is, melyek csak az öntözést követő években jelentkeznek szikesedés formájában.

Mivel a talaj helyhez kötött, ezért a szennyeződések is nehezen távoznak belőle. Termékenységének megőrzése, valamint a természetes folyamatok fenntartása komoly tervezőmunkát és alapos ismereteket kíván meg a földet „használók” széles táborától.

A talajt rombolja az ember mellett a szél, és a víz is, melyek ellen különféle mezőgazdasági kultúrákkal, talajmegkötéssel lehet védekezni. Az ember természetátalakító tevékenysége már összetett gazdasági, környezetvédelmi és ökológiai kihívásokat jelent.

Magyarország jelentősebb talajtípusai

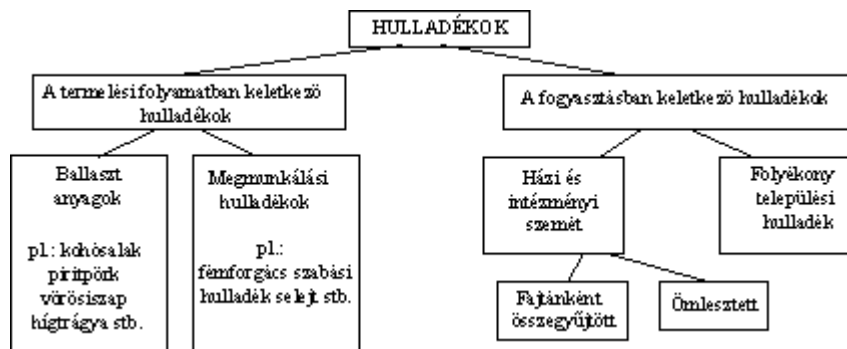
:

- Csernozjom talajok
- Barna erdőtalajok
- Réti talajok
- Homoktalajok (váztalajok)
- Szikes talajok
- Váztalajok
- Sötét színű litomorf (közethatású) erdőtalajok

- Láptalajok
- Öntés- és lejtőhordalék- talajok

HULLADÉKOK, KÖRNYEZETBARÁT TECHNOLÓGIÁK

Szinte nincsen emberi tevékenység hulladékok nélkül. Hulladéknak olyan anyagokat és energiákat nevezünk, amelyek a feldolgozás vagy felhasználás során eredeti használati értéküket elvesztették és meghatározott helyeken a termelési vagy fogyasztási folyamatból kiválnak. Számos csoportosításuk létezik, az alábbi táblázat az egyik legcélszerűbb tagozódást mutatja be.



2. ábra. A hulladékok csoportosítása ^[2]

„Commercial review”... azaz, a hulladék nemcsak addig hulladék, amíg létrejön, hanem a válogatást követően is az marad. Külön ki kell azonban emelni a veszélyes hulladékok csoportját. A veszélyes hulladékokra a 102/1996. (VII.12.) Kormányrendelet vonatkozik, mely szerint veszélyes hulladék az a hulladék, amely, vagy amelynek bármely összetevője, ill. átalakulási terméke a rendeletben meghatározott veszélyességi jellemzők valamelyikével rendelkezik, és a veszélyes összetevő olyan koncentrációban van jelen, hogy ez által az élővilágra, az emberi életre és egészségre, a környezet bármely elemére veszélyt jelent, ill. a nem megfelelő tárolása és kezelése esetében károsító hatást fejt ki. [8]

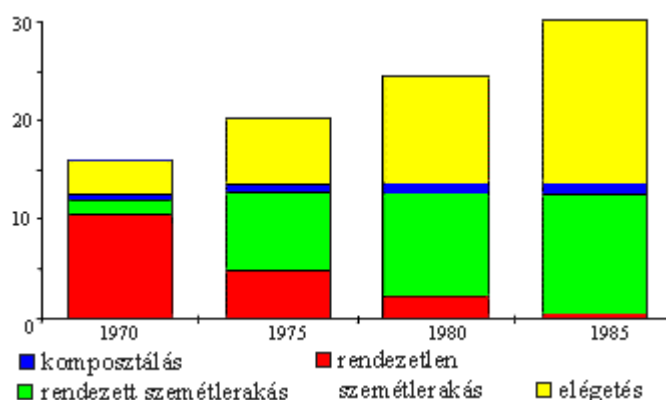
Mivel a hulladékok nem helyhez kötöttek ezért szükségessé vált egy- az országokon átívelő egyezmény létrehozása is. Így született meg 1992.május 05-én a magyar tagsággal bővült Bázeli Egyezmény.[9]

A hulladékok a termelésben káros kísérőjelenségeként vannak jelen, míg a fogyasztói oldalon szükségleteket elégítenek ki.

A hulladékok hatékony felhasználására több módszer is létezik. Gyűjtést, majd szállítást követően a keletkezés függvényében, - ipari, lakossági - vagy mezőgazdasági hulladék-, az alábbi módszerekkel helyezik el vagy semmisítik meg a hulladékokat:

- területfeltöltés - a lakott helytől min. 1 km-re helyezkedhet el.
- komposztálás- régi eljárás, amelyet világvárosok is alkalmaznak.
- elégetés- legkorszerűbben a füstmentes szeméttégető erőművekben oldható meg.(Más esetekben: légszennyezés, kellemetlen szaghatás)
- izotóp temetők (atomreaktorok, kutatóintézetek, kórházak esetében)

Folyékony hulladékok esetében pedig más szilárd szeméttel illetve tőzeggel keverik majd trágyaként hasznosítják azokat. A szennyvíztisztító telepek szennyvíziszapjainak elhelyezése is nagy gond, mert ezek többnyire igen fertőzöttek.



3. ábra. A fontosabb hulladékártalmatlanítási módszerek fejlődése (millió tonnában)^[3]

Magyarországi körülményeink között a hulladékkezelés még messze elmaradt a XXI. századi követelményektől és még nem vált a tervezés, a technikai megoldások komplex részévé. A hatósági rendelkezések és intézkedések, jogi és közgazdasági szabályozások azok betartása és betartatása ezúttal is eredményes lehet.

Környezetbarátnak akkor nevezhetnénk egy terméket, ha maga a termék, előállításának folyamata és a fogyasztása során keletkező hulladékai sem környezetszennyező hatásúak. Láthattuk, hogy számos hulladékfajta keletkezik az ember termelő-fogyasztó tevékenysége során. Közös cél, hogy olyan környezetbarát termékek, technológiák és eljárások honosodjanak meg, melyek megfelelnek a fenntartható fejlődés elvének. Az eddigi tapasztalatok bizonyítják, hogy a környezetpolitika nem nélkülözheti a környezetbarát termékekkel kapcsolatban kialakult fogyasztói mozgalmakat.

Ugyanis szinte biztosnak mondható, hogy ha megjelenik egy új anyag, termék, vagy eljárás, akkor a fogyasztók azonnal két táborra szakadnak. Lesznek, akik üdvözlnek az új dolgokat, és természetesen lesznek, akik azonnal valami kivetnivalót találnak benne. Nem könnyű megítélni, hogy kinek van igaza.

Vegyünk egy példát: ha a PVC hasznosságát, vagy káros hatásait elemezzük, megállapíthatjuk, hogy a vélemények e tekintetben megoszlanak.

A poli-vinil-klorid nehezen lebontható, elégetésekor sósavgáz képződik, ráadásul a vinil-klorid mérgező, rákkeltő hatású, ami alá is támasztja a kedvezőtlen megítélést. Más oldalról viszont a PVC gyártás annak köszönheti óriási fejlődését, hogy egyik alapanyagaként a nátronlúggyártásnál keletkező klórt hasznosítja. A PVC-feldolgozás ráadásul kis energiaigényű, amelynek környezetvédelmi vonzata sem elhanyagolható. Következtetéseket tehát csak összetett, és alapos vizsgálatok után vonhatunk le. Az anyagok technológiák egyik esetben pozitív, más esetben viszont negatív elemként jelentkeznek.

Egy-egy termék, technológia környezeti-ökológiai értékelése társadalmi szerződés kérdése is. Sokszor hiábavaló a gazdasági vagy tudományos racionalizálás, ha a társadalmi szerződés nem jön létre, a technológia nem terjed el.

A technológiaváltásokat komoly tervezés, egyfajta jövőbelátás kell, hogy megelőzze. A felelősség nagy, a következmények olykor kiszámíthatatlanok. Sokrétű és alapos célkitűzésekre és eredményes megvalósításra van szükség.

Az emberi tevékenység az alábbi szempontokat kell, hogy figyelembe vegye:

- biztosítani az ökológiai rendszer stabilitását az ökoszisztémák regenerálódó képességének megőrzésével,
- megvédeni a biocönózisok sokféleségét,
- fenntartani a lényeges ökológiai folyamatokat az utánunk jövő nemzedékek számára,
- megakadályozni bármiféle irreverzibilis változást a bioszférában. [10]

Új anyagok, másfajta igények, környezettudatosabb gondolkodásmód jelentkezik, ami új kihívások elé állítja a fejlődő világot. Számos alternatívát, különböző érdekeket, eltérő preferenciákat kell figyelembe venni. A környezetvédelem egyes területekre gyakorolt hatása erősen differenciált. Míg a környezetvédelem bizonyos ágazatokban többletráfordítást jelent, addig a beruházási javakat előállító ágazatokban, kifejezetten serkentő hatású.

Minden fejlesztést környezetvédelmi oldalról is meg kell alapozni, figyelembe véve, hogy egyetlen termék és technológia sem kerül el a környezetbarátság szempontjából történő megmértetést.

A média világát sokkal jobban ki lehetne használni, hiszen általa sokkal könnyebben, gyorsabban és hatékonyabban lehetne megszólítani embertömegeket.

A figyelemfelkeltés, a környezetvédelmi elképzelések reklámozása, az esetleges kooperáció a vállalatok és a fogyasztók között új utakat nyithat a környezetvédelemben. Ma azonban még nem ez a jellemző. A reklám elsődleges szerepe még nem a környezetvédelmi információk közvetítése, hanem a termék kelendőségének fokozása - amihez csak eszköz lehet a termék "zöldre festése".

Egyes felmérések szerint mintegy 200 milliárd forintot költünk reklámra, ebből mindössze 10 millió forintot tesznek ki a közcélú, környezetvédelmi reklámok. Ha már közterületeken, hirdetőoszlopokon és óriásplakátokon, televíziókban, rádiókban, buszok oldalain, szórólapokon árasztanak el bennünket a kéretlen anyagok, akkor miért ne használhatnánk őket okosabban?

“A képek a világ és az ember közé állnak. Térképeknek kell lenniük, és tapétává lesznek. Ahelyett, hogy bemutatnák a világot, meghamisítják, míg végül az ember az általa létrehozott képek funkciójában kezd élni.” Vilém Flusser⁴

⁴ Vilém Flusser: Az 1920-ban, Prágában született, és 1991-ben elhunyt Vilém Flusser az új technológiák teóriájának világszerte ismert alakja. (Magyarul az 1990-ben megjelent, A fotográfia filozófiája , majd pedig folyóiratokban (2000; Atheneum) megjelent írásai íásaival vált ismertté.)

Flusser a II. világháború alatt Brazíliába emigrált, ahol nyelvfilozófiai, valamint kommunikációelméleti munkásságával szerzett magának országos hírnevet. 1972-ben Olaszországban, majd Franciaországban települt le. Ettől kezdve számos európai és amerikai egyetemen adott elő. Az iránta megnyilvánuló figyelmet szerteágazó érdeklődése és színgazdag személyisége éppúgy magyarázza, mint eredeti gondolkodása és egészen rendkívüli íráskészsége.



4. ábra. Óvd a környezetet! ^[4]

ÖSSZEGZÉS

A környezetszennyezés optimális szinten tartása az emberiség közös érdeke. A dolgozat nem tért ki a környezetpolitikai szabályzók szakterületeire, melyek ösztönző hatással bírnak e területre vonatkozóan.

Az állam nyílt tiltásokkal, normákkal, különféle engedélyekhez kötéssel, szankciókkal próbálja meggátolni a gazdálkodó szervezetek szennyező tevékenységét. Gazdasági szempontból korántsem egyszerű ezek hatékonyságának megítélése, hiszen kiépítésük és ellenőrzésük igen költséges feladat, ami általában az amúgy is gondokkal küzdő államkasszát terheli.

Sokszor előtérbe kerülnek a személyes érdekek is, amik visszavethetik a szakhatóságok következetességét. Támogatásokkal, piacteremtéssel ösztönözhetik a pozitív jellegű, környezetbarát technológiák és a természetbarát termékek elterjedését.

Élhető környezetünk nagy kincs, melynek megőrzésén egyre több ember munkálkodik. A talaj, a víz és a levegő védelme mindannyiunk közös feladata, a fenntartható fejlődés elveinek betartása a jövőre nézve is komoly kihívás.

Láthattuk, hogy a bolygón végbemenő folyamatok egyetlen nagy egésszé állnak össze, így ha az ember termelő tevékenysége során beavatkozik akár csak egyetlen szféra folyamataiba, akkor az kihatással van a másik két területre is.

Napjaink egyik középponti kérdése a globális klímaváltozás pedig csak tovább ront a helyzeten. Az ember generálta változások fokozottan visszahatnak ránk, és negatív visszacsatolásokat hoznak létre a természeti környezetben.

A megfelelő szabályozás, a nemzetközi összefogás, a most felnövő generációk környezetbarát tudatra nevelése- valamint a jelen generációk *zöldebb* tudatra ébresztése- hatékonyan segítheti elő a fejlődési elvek betartását.

A megújuló természeti erőforrások felhasználását előtérbe kell helyoznünk, de azokkal ésszerűen kell tudnunk bánni. A hulladékokat olyan ütemben kellene csak gyártani, amit később fel is tudunk dolgozni, a kimerülő erőforrások a helyett pedig tisztább, ésszerűbb módszereket kellene alkalmaznunk, különben csak szűkös erőforrások állnak majd rendelkezésünkre, ami pedig ki tudja hová vezet majd.

Flusser elsősorban az új technológiák, ezen belül is elsősorban a technikai kép "első vonalbeli" teoretikusának számít. Utóbb megjelent könyvei (Ins Universum des technischen Bildes, Nachgeschichten) és publikációi e problémakör alapszövegeinek számítanak; haláláig neves művészeti folyóiratok (Kunstforum, European Photography etc.) rendszeresen felkért szerzője volt.

(Forrás: <http://www.c3.hu/~tillmann/forditasok/FLUSSER/iras.html> Letöltés ideje: 2009. május 24.)

Irodalomjegyzék

- [1] 1995. évi LIII. törvény a környezet védelmének általános szabályairól
- [2] Dr. Halász László: Környezetvédelem II. Egyetemi jegyzet, 2007.
- [3] Kerekes Sándor: A környezetgazdaságtan alapjai, Budapest, 1998.
- [4] Dr. Halász László: Környezetvédelem II. Egyetemi jegyzet, 2007.
- [5] Dr. Halász László- Földi László: Környezetvédelem- környezetbiztonság. Egyetemi jegyzet, ZMNE 2000.
- [6] Rachel Carson: Néma tavasz. Katalizátor Könyvkiadó, 2007.
- [7] Dr. Halász László: Környezetvédelem II. Egyetemi jegyzet, 2007.
- [8] 102/1996. (VII. 12.) kormányrendelet a veszélyes hulladékokról
- [9] 101/1996. (VII. 12.) kormányrendelet a veszélyes hulladékok országhatárokat átlépő szállításának ellenőrzéséről és ártalmatlanításáról szóló, Bazelben, 1989. március 22. napján aláírt egyezmény kihirdetéséről
- [10] Kerekes Sándor: A környezetgazdaságtan alapjai, Budapest, 1998.

Ábrajegyzék

- 1. ábra A Föld vízkészleteinek megoszlása az óceánok és a szárazföld között
Kerekes Sándor: A környezetgazdaságtan alapjai, Budapest, 1998.
- 2. ábra A hulladékok csoportosítása
Kerekes Sándor: A környezetgazdaságtan alapjai, Budapest, 1998.
- 3. ábra A fontosabb hulladékártalmatlanítási módszerek fejlődése (millió tonnában)
Kerekes Sándor: A környezetgazdaságtan alapjai, Budapest, 1998.
- 4. ábra Óvd a környezeted!
http://standby.blog.hu/2007/12/04/kornyezetvedelem_reklam

Kozma Tibor

kozmatibor@yahoo.com

GONDOLATOK MAGYARORSZÁG ENERGIABIZTONSÁGÁRÓL

Absztrakt

A felhasználók számára biztosított energia „értéke” és a mindennapok során betöltött szerepe alapján könnyen belátható, hogy gazdaságunk és társadalmi életünk egyik alapvető, és nélkülözhetetlen eleméről van szó. A biztonság átfogó értelmezése magában foglalja a folyamatos energia ellátás biztonságát is. A folyamatos és stabil: ár, szállított mennyiségi és időparaméterek mentén biztosított energiaellátás jelentősége napjainkban felértékelődött, erre elsősorban a hazai energiabiztonság külső tényezőknek kitett függősége mutatott rá. A magyarországi energia felhasználás struktúrája egyértelműen jelzi, hogy elsősorban a nem megújuló energiaforrásokra épül a hazai gazdasági felhasználás, beleértve a lakossági és intézményi fogyasztást is, domináns szerephez juttatva a szénhidrogén alapú energiahordozókat. Az import energiától való függőség és a szénhidrogén dominancia együttesen rávilágít a hazai energiabiztonság sérülékeny pontjaira. Az energiafelhasználás során kulcskérdés, hogy: milyen típusú energiát, milyen forrásból, milyen mértékben, és milyen hatékonyan fogyasztunk? Képesek vagyunk-e környezettudatos szempontokat figyelembe venni, amikor a hazai energiapolitikáról, illetve energiabiztonságról alkotunk véleményt? Jelen cikk a hazai energiaellátás és energiabiztosítás sajátosságainak bemutatása mellett a felhasznált energiahordozók struktúrájával is kíván foglalkozni.

It is conceivable that energy is a basic and indispensable material for our economy and social life due to the “value” which it provides to the final consumers and also due to the role of energy in our everyday life. The security of a constant energy supply is an essential part of the comprehensive security complex. Recently, a greater amount of importance has been placed on a constant and stable energy supply by price, quantity transferred and timing, especially the multiple foreign factors which impact Hungarian energy security. The nature of Hungarian energy consumption unambiguously indicates that it has been based on non renewable energy sources within the institutional and private energy consumption sectors. That gives a dominant role to the carbon-hydrogen based energies. Energy import dependence and the carbon-hydrogen dominance together highlights the weak points of Hungarian energy security. The key questions in the energy consumption process are: what sort of energy, from which source, in what quantity and how efficiently do we use it? Are we able to consider

environmental safety view points when we shape our opinion of Hungarian energy policy and energy security? This article is intended to introduce some points regarding the Hungarian energy supply and energy security. Additionally, it gives an introduction of the structure of Hungarian energy consumption.

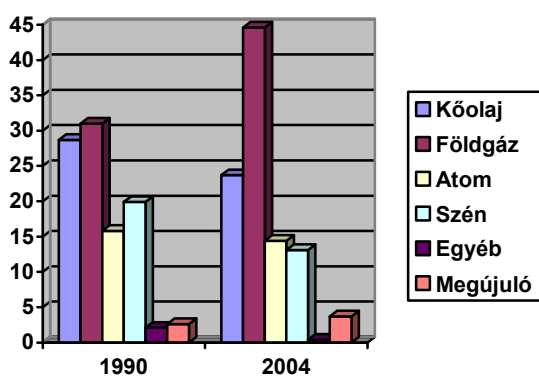
Kulcsszavak: energiabiztonság, energiaforrás, energiafüggőség, importfüggőség, kőolaj, földgáz, atomenergia, alternatív energiahordozók, környezetvédelem ~ energy security, energy source, energy dependency, import dependency, oil, gas, atomic energy, alternative energy supply, environment protection.

BEVEZETÉS

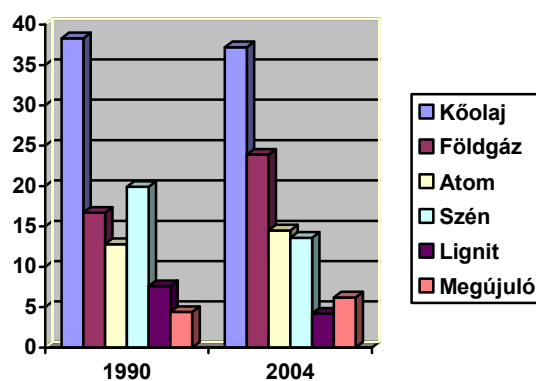
Az Európai Unió fosszilis energiaforrásoknak való kitettsége az elmúlt másfél évtizedben közel 8%-al növekedett. A hagyományos, jellemzően Európában megtalálható fosszilis energiaforrások (feketeszen, lignit) felhasználásnak csökkenését legnagyobb mértékben a földgáz (60%) majd a megújuló energiaforrások (58%), és az atomenergia (28%) felhasználásnak növekedése kísérte. A nagy részben importból származó energiaforrások túlsúlya miatt az energiabiztonság kérdése egyre fokozottabban az Európai Unió energiapolitikai törekvéseinek a fókuszába kerül. [1]

Magyarország 2008. évi energiafelhasználásának négyötödét együttesen a fosszilis energiahordozók adták, ebből 39% a földgáz, 30% a kőolaj és 12% volt a szén részesedése. Az EU-27-ben a fosszilis energiahordozók felhasználásának aránya szinte ugyanannyi volt, mint hazánkban, különbség csak az energiahordozók szerinti összetételben volt. (Az unióban a felhasznált energiaforrások között a kőolaj szerepe a legjelentősebb, 2007-ben 37%, a földgáz 24%-os aránya mellett.) [2]

A teljes energia felhasználás összetételének változása:



Magyarországon
1990 - 2004



Az EU 25 országaiban
1990 - 2004

Az EU teljes energia felhasználásában (a 2004-es adatok alapján) a legfontosabb energiahordozó a kőolaj, és csak második helyen szerepel a földgáz. Jellemezően dinamikus

növekedést mutat a földgáz felhasználása a többi energiahordozóhoz képest, ugyanakkor erőteljes növekedést mutat a megújuló energiaforrások felhasználása is.

Hazánkban is megfigyelhető a földgáz felhasználás növekvő szerepe, de a mi esetünkben a két vizsgált időszak vonatkozásában súlypont áthelyeződés látható. A korábbi időszak jellemző paramétereire képest mára a földgáz az elsődleges energiaforrásunk, 2004-es évben a teljes hazai energiafelhasználás 44,6%-t a földgáz adta. A magyarországi energiafelhasználás összetétele jelentősen növeli az ország energiabiztonsága szempontjából jelentkező kockázatokat. A külföldi piacoktól való függőség jellemzi a szénhidrogén energiahordozók beszerzését, az importfüggőség közelít a 80%-os érték felé.

A következő táblázat az ország energiamérlegéről ad tájékoztatást a 1999 – 2008-as időszakban. A táblázatban szereplő értékek petajouleban kerültek feltüntetésre. [2]

Év	Termelés	Behozatal	Forrás összesen	Kivitel	Készletváltozás (-)	Felhasználás Összesen
1999	500,0	657,7	1 157,7	84,4	-4,2	1 077,5
2000	485,2	665,4	1 150,6	82,8	12,7	1 055,1
2001	478,8	675,8	1 154,6	96,6	-29,1	1 087,2
2002	462,8	716,5	1 179,2	106,0	6,4	1 066,8
2003	434,7	786,5	1 221,2	108,2	21,5	1 091,6
2004	425,0	784,7	1 209,7	120,5	1,1	1 088,1
2005	428,0	873,6	1 301,6	140,8	7,5	1 153,2
2006	428,8	884,4	1 313,2	158,9	2,3	1 152,0
2007	427,0	850,9	1 277,9	153,6	-1,1	1 125,4
2008	435,9	868,0	1 303,9	145,3	32,3	1 126,3

A táblázatban szereplő értékek vizsgálat alapján látható két ellentétes irányú tendencia: a termelési mutatók csökkenése, illetve a teljes energia felhasználás növekedése, az import növekedése mellett. 1999-ben a teljes felhasználáshoz képest az import energia mértéke 61%-os volt, míg 2008-ban 77%-os értéken áll a mutató.

A saját energia termelés - az 1999-es évhez viszonyítva - az elmúlt 10 év vonatkozásában jelentős visszaesést mutat, még 2008-ban is közel 8%-al marad el a tíz évvel korábbi szinttől. A megújuló energiaforrások tekintetében a hazai energiaszektor nem tudta behozni az EU 25 országra vetített lemaradást, viszont a fejlődés dinamikájával lépést tudott tartani. (Megújuló energiaforrások EU 1990: 4,4% 2004: 6,2 Magyarország: 1900: 2,6% 2004:3,7%). A legjelentősebb mértékben hasznosított megújuló energia a biomassa, felhasználása nagyságrenddel előzi meg a többi megújuló energiaforrást.

A cikk további fejezeteiben az egyes energiahordozókra jellemező sajátos helyzetet tekintem át.

A FOSSZILIS ENERGIAHORDOZÓK

Földgáz

Az országos földgázfogyasztást és a forrásainak az összetételét a 2008-as évben a következő adatok jellemzik: [3]

Országos földgázfogyasztás	14,011	milliárd köbméter
Hazai termelés	2,608	milliárd köbméter
Import	11,403	milliárd köbméter
-keleti irányból	9,418	milliárd köbméter
-nyugati irányból	1,985	milliárd köbméter

Az import földgázforrások elsősorban orosz eredetűek, még az ausztriai Baumgartenből érkező HAG vezetéken a Gaz de France-tól és az E.ON Ruhrgas-tól vásárolt földgáz is orosz eredetű. A keleti irányú import 16%-a türkmén földgáz, a többi orosz eredetű.

A földgázforrások szerkezete egyértelműen jelzi az ország importfüggőségét: 80,9%-os a külföldről érkező földgáz aránya a teljes felhasználáshoz viszonyítva. Az általános importfüggőség mellett az egyoldalú beszerzési forrás és szállítási függőség együttesen jelentkezik, hiszen Beregdarócnál keleti irányból beérkező földgáz a teljes hazai fogyasztás 61,6%-a. A közelmúlt tapasztalatai rámutattak a rendszer sebezhetőségére. Az orosz-ukrán gázviták, és a mögötte húzódó politikai küzdelmek a Magyarországra keleti irányból érkező földgázimport folyamatos biztosíthatóságát veszélyeztették, illetve sértették. Oroszországgal azzal, hogy „elzárja a gázcsapot” illetve Ukrajnával azzal, hogy a tranzit gázszállítást egyoldalúan csökkentti, vagy időlegesen megszünteti reális fenyegetettséget jelent a hazai ellátás biztonságára. Ez a fajta kockázati tényező csökkenthető a hazai tárolókapacitás bővítésével, illetve közép és hosszútávon új szállítókapacitások kiépítésével. Új, magyar határt is keresztező transzkontinentális földgázvezeték rendszerek, mint a Déli áramlat, a Kék áramlat, Adria LNG és különösen a Nabucco jelentősen növelnék a gáz forrás és szállítási diverzifikációját. Hazánk számára talán a legfontosabb a Nabucco rendszer, amelynek műszaki tervezésének koordinációja elkezdődött, a projektet több európai ország is támogatja. A Nabucco vezetéken keresztül számos földgázimportra szoruló európai országhoz juthat el a Közel-Kelet és Közép-Ázsia térségéből a földgáz Oroszországgal és Ukrajnával érintése nélkül.

Az ellátásbiztonság fokozása érdekében a 2006. évi XXVI törvény [4] előírja, az ország földgáztároló kapacitásának a bővítését 2010-ig el kell érni, ami abszolút számokban: 1,2 milliárd köbméter földgáz ellátásbiztonsági célú tárolását jelenti. A földgáz biztonsági készletet olyan tárolóban kell elhelyezni, amelynek kitérítési kapacitása 20 millió köbméter/nap legalább 45 napon keresztül.

A Magyar Szénhidrogén Készletező Szövetség felügyelete alatt a MOL Nyrt. mint beruházói és üzemeltetői tender győztese 2007-től megkezdte a biztonsági készlet tárolására alkalmas infrastruktúrát és berendezéseket kialakítani. A kivitelező az algyői gázmező részét képező Szőreg-I. telepen új kétfunkciós (termelő-besajtoló) kutakat alakított ki. A 2008-as év során a tervezett 44 kútból 34-et fúrtak le, a további kutak kialakítása az eredeti ütemtervnek megfelelően halad. A 2008-as év végéig a Szőreg-I. telepen 300 millió köbméter földgázt tároltak be. A 2008-as év során a tároló kapacitás tovább növelést engedélyezte a Magyar Energia Hivatal, így mintegy 700 millió köbméter kapacitásbővítésre kapott engedélyt a telephely. A biztonsági földgáztárolás mellett ki kell emelni a kereskedelmi földgáztárolást, amellyel szemben támasztott hazai ellátás biztonsági követelmény, hogy az országos napi csúcsgény több mint felét a már meglévő kereskedelmi tárolókból tudja a rendszer biztosítani. [5]

A Délalföldön Makó térségében talált nem konvencionális gázmező kitermelése szintén javíthat az importfüggőségen. A kitermeléssel kapcsolatban számos technikai kihívás jelentkezik, ezek eredője elsősorban a gázmező elhelyezkedésének mélységével és a gáz igen magas hőmérsékletével magyarázható. A kitermelhető földgáz mennyiségét probablisztikus módszerrel kísérelték megállapítani. A kitermelhető földgázmennyiség valószínűségi szintje:

- 90%-os valószínűségi szinten: 620 milliárd köbméter,
- 50%-os valószínűségi szinten: 1550 milliárd köbméter,
- 10%-os valószínűségi szinten: 3330 milliárd köbméter. [6]

A hazai már meglévő 2,6 milliárd éves földgáztermelés mellett a 90%-os valószínűségi szinten megadott mennyiség, amennyiben kitermelésre kerül, több mint ötven évre váltaná ki a földgázimportot és stabilizálná a hazai földgázellátást. A Makói-árok földgázkincsét külön felértékeli az a tény, hogy Magyarországon elsődleges felhasznált energiahordozó a földgáz, a lakossági fűtés és távfűtés közel 80%-a földgáz rendszerű.

Kőolaj

Az Európai Unió leginkább a kőolaj esetében rá van utalva a behozatalra, energiafüggőségi rátája e termék esetében mintegy 80%. Magyarországon az éves fogyasztási igény mintegy 7 millió tonna, ebből csupán 1 millió a hazai termelés, tehát az importfüggőségünk meghaladja a 85%-os mértéket. Hazánkban a földgáz esetében a vezetékes szállítás dominál, addig a kőolaj vonatkozásában eltérő szállítási alternatívák állnak rendelkezésre. Ukrajna irányából a Barátság kőolajvezeték és Horvátország felől az Adria vezeték (kétirányú) képvisel jelentős szállítókapaacitást. További alternatívák: vasúti, folyami, közúti szállítás, illetve termékvezetékek.

A kőolaj felhasználását tekintve domináns az üzemanyagok tekintetében, ez a teljes felhasználás 60%, míg vegyipari kenőanyag és alapanyag estében a felhasználás 25%-os. A további 15%-os felhasználást az energetikai felhasználás, tüzelés adja. A kőolaj vonatkozásában a központi készletezés a teljes hazai felhasználást minimum 90 napig képes biztosítani külső forrás nélkül, ugyanakkor a finomítói, kereskedelmi és nagyfogyasztói készletek tovább növelik az ellátás biztonságát.

Szintén az ellátás biztonságát növelik a hazai előállítású bio-üzemanyagok (bioetanol, biodizel) amely az Energia Hivatal prognózisa alapján 2010-ben a teljes üzemanyag felhasználás 6%-t fogják biztosítani. Érdemes megjegyezni, hogy további jelentős előnye a bio-üzemanyagok felhasználásnak a környezetvédelmi szerepük.

A hazai olajfinomító rendszer kapacitását kizárólag a Százhalombattai Kőolaj Finomító komplexum jelenti. A korábbi finomító kapacitás a 90-es évek során leépült, ezzel megnőtt a rendszer sebezhetősége. [7]

Szénfélésegek

Hazánk energia felhasználásának szerkezete történelmi távlatokban a szénfélésegek jelentős csökkenését mutatja. Ötven évvel ezelőtt ez az energiahordozó adta a teljes hazai felhasználás 2/3-át, míg napjainkra már csak 11-12%-os a felhasználási mutató. [8]

A széntermelés hazai struktúrája elsősorban a lignitre épül, jelentős mennyiséget tesz ki a barnaszén, míg a feketeszén bányászat elenyésző. A hazai szánbányászat mellett folyamatosan importtal tudta az ország biztosítani az elégséges ellátást. A századfordulót megelőzően az importmutató jellemzően stabil szintre állt be, akkor a hazai felhasználás mintegy 30%-t tette ki. A 2000-es évtől kezdve folyamatos emelkedést mutat a szénfélésegek importmutatója, 2008-as évben elérte a 44%-t. Importfüggőségről mégis kevésbé beszélhetünk, több tényező miatt. Elsősorban, azért mert az importot csökkenteni lehet a jelentős hazai tartalékokra épülő bányászat fejlesztésével, (lásd mecseki szénbányák) illetve a szénfélésegek külföldi árupiacán a kínálat folyamatosan kielégítő.

A VILLAMOS ENERGIA

A hazai villamos energia ellátottság és termelés bemutatását a „villamos energia mérleg” utolsó 8 évének a sarkalatos adataival kezdeném. (Az adatok millió KWh-ban szerepelnek)

Év	Termelés	Behozatal	Forrás összesen	Belföldi felhasználás	Kivitel	Felhasználás összesen
2000	35 191	6 197	41 388	30 859	2 757	41 388
2001	36 418	6 946	43 364	32 197	3 775	43 364
2002	36 158	7 624	43 782	33 332	3 367	43 782

2003	34 145	8 905	43 050	34 077	1 966	43 050
2004	33 708	8 601	42 309	34 744	1 129	42 309
2005	35 755	11 809	47 564	35 519	5 582	47 564
2006	35 859	13 266	49 125	36 591	6 058	49 125
2007	39 958	14 278	54 236	37 247	10 291	54 236
2008	40 026	13 348	53 374	37 397	9 446	53 374

(A táblázatban nem szerepelnek az előállítás és a szállítás során jelentkező veszteségek.)

A villamos energia mérleg is azt jelzi, hogy hazánk ebből az energiahordozóból is behozatalra szorul. Azonban a hazai termelést és az export adatokat is figyelembe véve az import nem értékelhető függőségként.

A Magyar Energia Hivatal a hazai villamosenergia-ellátás biztonság vizsgálata során a következőket állapította meg:

Az erőművek felkészültsége (beleértve a téli időszakot is) megfelelő, a készletek, illetve a szerződések alapján a tüzelőanyag ellátás biztosított. A hazai biztonságos villamos energia ellátást kapacitás mérlege akár télen is (emelt fogyasztási időszak) megnyugtatónak tekinthető (beleértve a tartalékképzést is) a következő hipotézisek megvalósulása során:

- a keleti és az északi határokon az import kapacitások nem csökkenek jelentős mértékben,
- és a déli határon nem nő jelentős mértékben az energia kiáramlás.[6]

Az ellátásbiztonság fokozása érdekében 2003.01.01-től a villamos energia ipari szektorban egy ösztönző – büntető mechanizmus került bevezetésre. Európában ötödikként Olaszország, Írország, Norvégia és Anglia után Magyarország is bevezette az ösztönző tarifa szabályozást.[8]

ATOMENERGIA

A nem fosszilis eredetű nukleáris energia előnye, hogy környezet-károsító hatása kicsi (ami annak köszönhető, hogy nem bocsát ki káros anyagot és megfelelő biztonsági előírások mellett a radioaktív sugárzás minimális), hátránya, hogy költséges, hosszú távon megtérülő beruházást igényel. Hazánkban 1983 óta termelnek nukleáris energiát Pakson. A négy reaktorból álló atomerőmű összteljesítménye 1760 MW-ról a fejlesztések során 1866 MW-ra nőtt. Az itt előállított nukleáris energia 1990-ben az összes energiatermelés 25%-át, tíz évvel később a 33%-át, 2007-ben pedig 38%-át adta. Magyarország 2007-ben 3,8 millió tonna kőolajnak megfelelő nukleáris energiát termelt, ami az unió termelésének 1,6%-át tette ki, aránya a hazai energiafelhasználásban 14% volt.[2]

Az atomenergia hazai előállítása a kezdetektől fogva napjainkig orosz (szovjet) importon keresztül biztosított, az importfüggőség 100%-os. A Paksi Atomerőműben blokkonként 2 évre elegendő fűtőanyag van tárolva, így ebben az energia kategóriában a stratégiai készlet nagyságrendekkel meghaladja a fosszilis energiahordozók hasonló paramétereit. A rendkívüli energiasűrűségnek köszönhetően az atomerőmű tonna/év alapján megadott tüzelőanyag felhasználása roppant előnyös és nagyságrendekkel tér el a hagyományos erőművektől.

Példaként egy 1 Giga Watt teljesítményű erőmű tüzelőanyag felhasználásának igénye tonnában:[9]

- Szén: 2000
- Lignit: 7600
- Olaj: 1300
- Földgáz: 920
- Atom: 0,02

A szállítás és a forrás diverzifikációja elméletileg biztosított, függőségünk megítélésénél ezeket a tényezőket feltétlenül számításba kell venni. A szállítás vonatkozásában a jelenleg használt vasúti szállítás mellett rendelkezésre állhat a vízi és a légi szállítás is. Az import eredeti forrását tekintve az orosz beszerzés mellett, illetve adott esetben azt kiváltva elképzelhető Bulgária, illetve Örményország is, mint export partner.

A 2008-as évben a paksi 4 blokk termelői kihasználtsága 84-86%-os volt.[9] Figyelembe véve a termelési korlátokat, az ország energiabiztonságát jelentősen javítaná további blokkok építése, üzembe állítása.

A MEGÚJULÓ ENERGIAFORRÁSOK

A megújuló energiaforrások azokat az energiaforrásokat jelölik, amelyek hasznosítása közben a forrás nem csökken, hanem azonos ütemben újratermelődik, vagy megújul. Ide sorolható a napenergia, a szélenergia, a vízenergia, a biomassza és a biogáz. A felsorolás nem teljes, elsősorban a hazai viszonyok vonatkozásában reális megújuló energiaforrásokat tartalmazza.

A hazai megújuló energiaforrások termelésének összefoglaló adatai 2007-ben, a KSH adatközlése alapján. [2]

Energiaforrás	1000 tonna olajegyenérték		Megoszlás	
	Magyarország	EU-27	Magyarország	EU-27
Biomassza	1288	96179	91,7	69,3
Vízenergia	18	26653	1,3	19,2
Geotermikus	86	5771	6,1	4,2
Szél	9	8965	0,7	6,5
Nap	3	1263	0,2	0,9
Összesen	1404	138831	100%	100%

A 2008 júliusában a Gazdasági és Közlekedési Minisztérium által kidolgozott: „Stratégia a magyarországi megújuló energiaforrások felhasználásnak növelésére 2008 – 2020” [1] dokumentum alapján 2 éves intézkedési terveket tartalmazó végrehajtási program (Megújuló Energiahordozó Program) kerül majd kidolgozásra.

A stratégiát tartalmazó dokumentum részletesen foglalkozik a megújuló energiaforrások alkalmazásával a villamosenergia és a hőenergia termelésben, illetve horizontális síkon áttekinti a megújuló energiafelhasználás lehetőségeit. A stratégia a Policy forgatókönyv (a megújuló energiaforrások részarányának intenzív növekedését modellezi) célértékeinek 2020-as megvalósíthatóságával számol. A sarokszámok: 2020-ban a megújuló energiaforrások felhasználása összesen 186,4 PJ-t tesz ki, ezen belül a villamosenergia-termelésben 79,9PJ, a hőtermelésben 87,1PJ az üzemanyag fogyasztáson belül 19,6 PJ bioüzemanyagot használ fel az ország. [1]

Jelenleg Magyarországon döntő többségben a biomasszának és mellette még a geotermikus energiatermelésnek van nagyobb jelentősége, amitől lényegesen elmarad a többi megújuló energiaforrásunk. A biomassza a mezőgazdaságból, erdőgazdálkodásból és ezekhez a tevékenységekhez közvetlenül kapcsolódó iparágakból származó termékek, hulladékok, valamint az ipari és települési hulladékok biológiailag lebontható részét jelenti. A hazai teljes biomassza-készlet 350–360 millió tonnára becsülhető, amelynek tized részét használjuk fel energetikai célokra, ami megújuló energiatermelésünk közel 92%-t adja. A biomassza egyik terméke a biogáz rendkívül sokoldalúan hasznosítható: fűtési célra, villamos-és hőenergia-termelésre, illetve tisztított (biodízel) formában üzemanyagként. Hazánk geotermikus

adottságai igen kedvezőek. A geotermikus energia fő hasznosítási területe a közvetlen hőhasznosítás (üvegházak, uszodák, épületek fűtése) és a balneológia (gyógyforrások, gyógyvizek gyógyfürdői alkalmazása). Ma Magyarországon több mint 900 termálkút (a kifolyásánál 30 Celsiusnál melegebb kút, forrás) üzemel, amelynek mintegy 31%-a balneológiai célú, több mint negyedük az ivóvízellátásban hasznosul, és közel fele szolgál fűtésre. A vízenergia szerepe a hazai energiatermelésben – különböző föld- és vízrajzi, valamint gazdasági okok miatt – nem jelentős. Magyarországon a jelenleg meglévő 31 vízerőmű összteljesítménye 55 MW, villamosenergia-termelése közel 190 GWh, ami a teljes hazai villamos energia felhasználás kevesebb, mint fél százaléka.

A napenergia hasznosítása szempontjából hazánk természeti adottságai kedvezőek, a napsütéses órák éves száma 1900–2200. Az adottságok kihasználása azonban még éppen csak megkezdődött. Jelenleg a napenergia-termelés az összes megújuló energia 0,2%-át teszi ki.

Magyarországon a szélenergia alkalmazására az első szél erőmű 2000-ben épült. Számuk 2007-ben 40 db, beépített kapacitásuk több mint 61 MW volt. Az általuk termelt energia mennyisége egyelőre ugyancsak nagyon alacsony. [2]

NEMZET ÉGHAJLATVÁLTOZÁS STRATÉGIA 2008-2025

Az Országgyűlés 2008.03.17-én fogadta el a „Nemzeti Éghajlatváltozás Stratégia 2008-2025” országgyűlési határozatot. [10]

A stratégiai a következő érdemi megállapításokat teszi:

- visszafordíthatatlanul megváltoztak a légköri viszonyok
- időben kell cselekedni, a káros hatásokat megelőzni illetve csökkenteni
- a megváltozott viszonyokra fel kell készíteni a társadalmat, a gazdaságot
- a nemzetközi klímatudatosságot erősödésével kell számolni
- Magyarországnak is részt kell venni a vállalásokban
- a felkészülés mindig olcsóbb, mint a károk utólagos helyreállítása

A kormány a 2007. évi LX. törvény [11] értelmében 2 évente Nemzeti Éghajlatváltozási Programot fogad el, illetve a program végrehajtásáról évente beszámol az Országgyűlésnek.

Az éghajlatváltozási stratégia 3 alappillére:

- ellátásbiztonság
- versenyképesség
- fenntarthatóság

Nemzeti Éghajlatváltozási Program 2009 – 2010 főbb célkitűzései:

- üvegházhatású gázkibocsátás csökkentés/korlátozás
- az éghajlatváltozás hazai hatásaihoz való alkalmazkodás
- a hazai kibocsátások költséghatékony csökkentéséhez és az éghajlatváltozás hatásaihoz kapcsolódó kutatások. [12]

A magyar éghajlatváltozási stratégia harmonizál az Európai Tanács 2007. célkitűzéseivel (új EU energia-klíma csomag vállalásai). Az Európai Tanács által 2007 márciusában elfogadott új európai uniós energia- és környezetvédelmi politika a közösségi energiapolitika három központi célkitűzésére, nevezetesen a fenntarthatóságra, a versenyképességre és az ellátás biztonságára irányuló, előretekinthető szakpolitikai programot határozott meg. A program megvalósítása érdekében az EU elkötelezte magát a „20-20-20” kezdeményezés mellett, azaz vállalta, hogy 2020-ig az üvegházhatást okozó gázok kibocsátását 20%-kal csökkenti, az energiafelhasználáson belül a megújuló energiaforrások részarányát a jelenlegi 8,5%-ról 20%-ra növeli, és az energiahatékonyságot 20%-kal javítja. [13]

ÖSSZEFOGLALÁS

Magyarország energiafelhasználásnak jellemzőit elsősorban a jelentkező biztonsági kockázatok feltárása mentén próbáltam bemutatni. Elsődleges megállapításaim összefoglalása:

Hazánk energia felhasználási szerkezete és a közelmúltban tapasztalt szerkezet változási dinamika irányultsága is eltér az EU átlagától. A hazai szerkezet kiegyensúlyozatlan, a szénhidrogének dominanciája a jellemező, a megújuló energiaforrások alulkondicionáltak. Leghangsúlyosabb szerepet a földgáz kap, ami számos járulékos kockázati tényezőt hordoz: elsősorban az import mértéke, az egyoldalú és versenyhelyzetet nélkülöző beszerzés, és a szállítókapaacitások kötöttsége miatt. A hazai nem- konvencionális gázmező kiaknázásával, újabb tárolókapaacitások bővítésével és középtávon a most tervezési stádiumban lévő transzkontinentális gázszállító rendszerek építésével csökkenthető hazánk kiszolgáltatottsága. Ezen kívül a felhasználás hatékonyságának növelésében még jelentős tartalékok vannak, kiemelten fontos kell, hogy legyen a takarékoság kérdése, illetve számos területen a fűtésre használt földgáz alternatív energiaforrásokkal kiváltható lehet.

A kőolaj vonatkozásában is nagyfokú az importfüggőségünk, ugyanakkor a kevésbé kötött beszerzési források, szállítási módszerek diverzifikációja a függőségünket csökkenti. A kőolajból előállított végtermék üzemanyagok felhasználása esetében a növelt hazai bioetanol és biodizel termelői kapaacitás lehet a függőség csökkentésének további iránya. A közlekedésben használt belső égésű motorok mellett a villamos energiát, illetve hidrogén forrást használó új motorok jelentős elterjedése csökkenthetné a hagyományos üzemanyag felhasználási igényt ezen keresztül a kőolaj függőségünket. A szénfűtésűek felhasználása valószínűsíthetően továbbra is csökkenő tendenciát fog mutatni, felhasználásuk részben kiváltható lehetne más energiahordozóval. Mindhárom fosszilis energiahordozó vonatkozásban kiemelendő, hogy felhasználásuk jelentős környezetszennyezéssel jár.

Az atomenergia felhasználása a jövőben is létfontosságú marad, a meglévő kapaacitások fenntartása, és újabbak létesítése javítaná a hazai energiatermelési mérlegét, összességében hozzájárulna a fosszilis energiahordozók importcsökkentéséhez.

Az összefoglaló részben eddig bemutatott elemek mindegyike erősíti azt a konklúziót, hogy az energiaszektor szerkezetét át kell alakítani. Ezt a folyamatot jelentős állami támogatással fel kell gyorsítani. Hazánk energiabiztonságának növelését és környezetünk védelmét együttesen szemlélve látni kell, hogy kizárólag a környezettudatos, elsősorban a megújuló energiaforrásokra épülő technológiák „tömeges” alkalmazásával tudjuk célunkat elérni. A fokozódó energia igény kielégítése és a napjainkban jelentkező éghajlatváltozási hatások mérséklése új szemlélet követel meg, nemzetgazdasági és globális szinten egyaránt. A Nemzeti Éghajlatváltozás Stratégia és a kapcsolódó Nemzeti Éghajlatváltozás Program rámutat a cselekvési kényszerre és alkalmas keretet ad az előttünk álló feladatok megvalósításához.

Hivatkozások

- [1] Stratégia a magyarországi megújuló energiaforrások felhasználásnak növelésére 2008-2020, Budapest, 2008. Július
http://energiakozpont.hu/download.php?path=files/fooldal/strategia/megujulo_strategia_2008-2020.pdf (letöltés 2009.10.20)
- [2] Központi Statisztikai Hivatal: Fosszilis és nem fosszilis energiaforrások, Statisztikai Tükör 2009/107 (2009. Július 28) 1-2

- [3] Központi Statisztikai Hivatal: Országos Energia Mérleg 1990-2008,
http://portal.ksh.hu/pls/ksh/docs/hun/xstadat/xstadat_eves/tabl3_08_01i.html
(letöltés: 2008.10.21)
- [4] 2006. évi XXVI törvény a földgáz biztonsági készletezéséről
- [5] Magyar Energia Hivatal: Tájékoztató a Magyar Energia Hivatal 2008. évi tevékenységéről.
<http://www.eh.gov.hu/home/html/index.asp?msid=1&sid=0&lng=1&hkl=148>
(letöltés:2009.10.27)
- [6] Bakosné Diószegi Mónika: A hazai energiabiztonság növelésének lehetőségei, Hadmérnök, 2009 június, <http://hadmernok.hu/archivum> (letöltés: 2009.10.20)
- [7] Török Bálint: A százhalombattai kőolaj-finomító baleset-elhárító rendszere, Hadmérnök, 2006 december, <http://hadmernok.hu/archivum> (letöltés: 2009.10.20)
- [8] Horváth J. Ferenc: A Magyar Köztársaság energiabiztonsága, előadás a Magyar Hadtudományi Társaság: „Energiabiztonság – 2009” Konferencia, Budapest, 2009.05.11.
- [9] Cserhádi András: Atomenergia és energiabiztonság, előadás a Magyar Hadtudományi Társaság: „Energiabiztonság – 2009” Konferencia, Budapest, 2009.05.11.
- [10] 29/2008. (III. 20.) Országgyűlési Határozat: A Nemzeti Éghajlatváltozás Stratégiáról
- [11] 2007. évi LX. törvény2007. évi LX. Törvény az ENSZ Éghajlatváltozási Keretegyezménye és annak Kiotói Jegyzőkönyve végrehajtási keretrendszeréről
- [12] Szabó Imre: Megújuló energia használata az éghajlatváltozás elleni küzdelemben, előadás, „Kezünkben a jövőnk” Megújuló Energiák 2008 Nemzetközi Konferencia és Kiállítás, Budapest 2008. November 20-21
- [13] Az Európai Tanács: (2007.03) Új Európai Unió Energia- és Környezetvédelmi Politika http://www.euvonal.hu/index.php?op=kozossegi_politikak&id=21, (letöltés: 2009.10.20)

Molnár Árpád

molnar.arpad1@chello.hu

Halász László

halasz.laszlo@zmne.hu

ARANY SZOL BEVONATÚ VEGYI ÉRZÉKELŐK VIZSGÁLATA DIIZOPROPIL-FLUOROFOSZFONÁTTAL SZENNYEZETT LÉGTÉRBE

Absztrakt

A cikkben egy katonai vegyi érzékelő alkalmazhatóság szempontjából meghatározó fő paraméterek diizopropil-fluorofoszfonáttal szennyezett légtérben történő vizsgálatának eredményeit mutatjuk be. A vizsgálat során felhasznált érzékelők interdigitális elektródaira felvitt arany szolt alkil-tiollal stabilizálták. A szolban az egymástól elszigetelt arany részecskék jellemző mérete 3-4 nm volt. Az érzékelők vizsgálat előtti minősítése egy Transzmissziós elektron-mikroszkópos és Elektrokémiai impedancia spektroszkópiás vizsgálati módszeren alapuló eljárással történt. A vizsgálatok eredményeként a vizsgálati módszer továbbfejlesztésére teszünk javaslatot.

The results of examination of the main parameters determining applicability of military chemiresistors are showed in this paper. The examination was carried out in an environment contaminated with Diisopropyl fluorophosphate. The gold sol covering interdigital electrodes of chemical sensors examined was stabilized with alkyl-thiol. In sol the typical size of gold particles isolated from one another was between 3 and 4 nm. Qualification of the sensors prior to the examination was performed by the use of a procedure based on measurements with Transmission Electron Microscope and Electrochemical Impedance Spectroscopy. As a result, further development of method of examination is proposed.

Kulcsszavak: szenzor, érzékelő, arany, nanorészecske, érzékenység, szol, diizopropil-fluorofoszfonát ~ sensor, gold, nanoparticles, sensitivity, sol, diisopropyl fluorophosphate

BEVEZETÉS

Az ABV laboratóriumok intenzív fejlesztése világszerte a környezeti minták szennyező anyag tartalmának meghatározására és monitorozására szolgáló egyszerű, gyors és megbízható eljárások kidolgozására irányul.

Ebbe a kutatási-fejlesztési irányvonalba illeszthetők, a kémiai érzékelőkkel végzett kutatások, amelyek szorosan kötődnek a nanoszerkezetű anyagokkal folytatott kutatások területén jelentkező eredményekhez. A mikro- és nano-méretű (részecskeméret: 10^{-6} – 10^{-9} m) „objektumokkal” végzett kutatások során egyfelől az anyagok olyan új különleges tulajdonságait ismerik meg, amelyek csak erre a mérettartományra jellemzők, másfelől új vagy a különleges körülményekre adaptált meglévő módszerekkel és technikákkal érnek el eredményeket.

Az érzékelők világát a hordozók, az érzékelő anyagok, a működési elvek és a műszaki megvalósítások változatossága jellemzi. Természetesen igaz ez a vegyi érzékelőkre is. [1-3]

A vegyi érzékelők kialakítását tekintve a jellemzően olcsó és egyszerű hordozó típusok az egymásba fogazott fésűs úgynevezett interdigitális elektródák, amelyek a dielektrikum kapacitásának és vezetőképességének mérésére alkalmasak. [1,4-7]

Az interdigitális elektródák bevonására a közkedvelt szol-gél módszer elterjedten alkalmazott. Ez a módszer többek között alkalmas vékony rétegek, nagyon finom és különleges alakú porok, valamint rendkívül porózus aerogélek kialakítására is. [1]

Az arany széles körben használatos nemesfém a szenzorgyártásban és a mikroelektronikában, mert nemcsak jó vezetőképességgel rendelkezik, hanem alkalmas önszerveződő anyagok létrehozására is. [1,5,7,8,9]

A nanoméretű aranyrészecskék szabályozott előállítása jól ismert az irodalomban. [10-13] A vizsgált érzékelők esetében az interdigitális elektródákra felvitt érzékelő anyag alkil-tiollal stabilizált arany szol volt.

Az általunk vizsgált vegyi érzékelő típusoknál megfigyelték, hogy az érzékelő anyagban lévő arany nanoszemcsék méretének meghatározó hatása van a vezető- képességre. [14] Az optimális szemcseméretet az irodalomban 1 és 5 nm közé teszik. [15]

A szemcseméret meghatározására jól bevált technológia a Transzmissziós Elektron-Mikroszkópos (TEM) vizsgálat. [1,4,16]

Az elkészült laboratóriumi érzékelőket az elektrokémiai reakciók mechanizmusainak és különböző, például önszerveződő rétegek vizsgálatában sikerrel alkalmazott [17-20] Elektrokémiai Impedancia Spektroszkópiás (EIS) vizsgálatnak vetettük alá, amelynek eredményeit a felhasználhatóság szempontjából értékeltük.

Az impedancia spektroszkópia lehetővé teszi összetett folyamatok egyidejű vizsgálatát, a dielektromos tulajdonságok megváltozásának nyomon követését és az optimális mérési helyek meghatározását.

Az impedancia spektrumok ábrázolása Nyquist ($\text{Im}Z$ vs. $\text{Re}Z$) valamint Bode ($|Z|$ vs. f és θ vs. f) módban történik. Az impedancia kétféle ábrázolása közötti összefüggés:

$$\tan \theta = \frac{\text{Im}(Z)}{\text{Re}(Z)}, \text{ ill. } |Z| = \sqrt{\text{Re}(Z)^2 + \text{Im}(Z)^2}$$

ahol:

Θ : A fáziseltolás szöge

f: A frekvencia

|Z|: Az impedancia magnitúdó

Re(Z): Az impedancia reális része

Im(Z): Az impedancia képzetes része

Eredményeink reprezentálása szempontjából a spektrum Bode ábrázolását részesítettük előnybe.

A toluolra telített légtérben minősített érzékelőket diizopropil-fluorofoszfonáttal szennyezett légtérben vizsgáltuk.

MÓDSZEREK

Az érzékelők

A vizsgálati célra kialakított kémiai érzékelők hordozói mindenesetben az Auter Elektronika Kft. által legyártott interdigitális elektródák voltak. A polimer alapra hagyományos nyomtatott áramkörök készítése technológiával alakították ki a néhány μm vastagságú réz elektródamintázatot. Az 1 cm^2 felületű interdigitális elektródák fogazatainak szélessége $0,5\text{ mm}$ volt. A 13 pár fogazatú kialakítást $15\text{ }\mu\text{m}$ fogközi távolság jellemezte.

Az érzékelő anyag előállítása (Trif László MTA KK) az irodalomban is ismert, és más kutatócsoportok által már érzékelő készítésre alkalmazott kétfázisú kémiai redukciós Brust-Schiffirin módszerrel történt [16,21,22]

A szintézis lényege, hogy az AuCl_4 -t vizes oldatból tetra-oktil-ammónium-bromid tenzides fázistranszferrel toluolos oldatba viszik és NaBH_4 -al redukálják tiol jelenlétében. A nanorészecskék méretét az arany-tiol aránnyal szabályozzák. Az alkil-tiollal stabilizált arany nanorészecskéket tartalmazó szol levegőn hosszú ideig stabil marad és többnyire az egyszerű szerves vegyületekhez hasonló módon kezelhető.

A Transzmissziós elektron-mikroszkópos vizsgálatok során nagy energiájú elektronsugár halad át egy vékony mintán, többek között információt biztosítva a minta részecske eloszlásáról. [1] A TEM technológia hasznosságát jól jellemzi az 1 nm -es vagy annál jobb felbontás. A vegyi érzékelő készítéséhez előállított szolban az arany nanoszemcsék méretét Morgagni 268D Transzmissziós elektron-mikroszkóppal határozták meg.

Az előállított vegyi érzékelők Elektrokémiai Impedancia Spektroszkópiás vizsgálatára az MTA KK Elektrokémiai laboratóriumában került sor. A Solartron 1286 potenciosztát és a Solartron 1250 Frekvenciaválasz analizátorból álló műszerrel 10 mérési pont/dekád felbontásban, a $0,1\text{ Hz} - 65\text{ kHz}$ frekvenciatartományban végezték a méréseket. A 10 mV amplitúdójú szinuszos bemeneti jelet adva az érzékelőre mérik az autointegrációval szabályozott áram válaszjelet. Az impedancia mérés vezérlése a Zplot szoftverrel, az impedancia spektrum ábrázolása és kiértékelése Zview szoftverrel történt. Az eredményeket alátámasztó diagramok az alapadatok importálását követően MS Excel szoftverrel ábrázoltuk.

Az érzékelőket párhuzamos RC körrel modelleztük. Az ellenállást és a kapacitást egy adott frekvencián az impedancia értékek valós és képzetes részéből a következő összefüggések alapján számoltuk:

$$R = \frac{\operatorname{Re}(Z)^2 + \operatorname{Im}(Z)^2}{\operatorname{Re}(Z)},$$

valamint:

$$C = \frac{-\operatorname{Im}(Z)}{\omega \cdot (\operatorname{Re}(Z)^2 + \operatorname{Im}(Z)^2)}$$

ahol:

C: A kapacitás

R: Az ellenállás

$\omega = 2\pi f$

Vizsgálatok szennyezett légtérben

A diizopropil-fluorofoszfónáttal (DFP) szennyezett légtér koncentrációjának beállítása egy dinamikus koncentráció beállító készülékkel történt. A szennyezett légtérből vett minták DFP tartalmát egy Varian 3800 Gázkromatográfból (GC) és 1200 MS/MS kombinált tömegspektrométerből (MS) kialakított GC-MS berendezéssel mértük. A DFP-vel szennyezett légtérben végzett vizsgálatokra HM FLÜ Technológiai Igazgatóságának Vegyi laboratóriumában került sor az MTA KK Felületmódosítás és Nanoszerkezetek Osztálya által biztosított mérőberendezéssel.

A mérőberendezés a Zplot szoftvervezérlésű Solartron 1286 potenciosztát és a 1250 frekvenciaválasz analizátor elemekből került kialakításra. A kételektródos elrendezésben 10 mV amplitúdójú szinuszos potenciáljelet adva az érzékelőre, mértük az áram válaszjelet. A mérési elrendezést az 1. ábrán mutatjuk be.

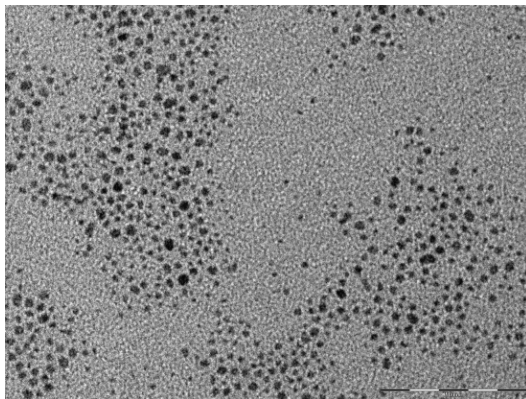


1. ábra. Az alkalmazott mérési elrendezés (Molnár Árpád)

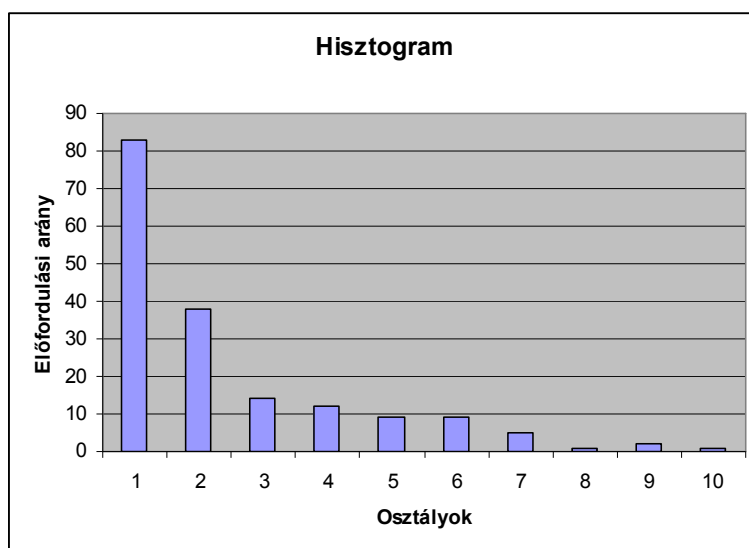
EREDMÉNYEK

Az érzékelők

Az elkészített arany nanoszolokban a részecskeméret meghatározást a transzmissziós elektronmikroszkópos felvételek alapján végezték (2. ábra). A kiértékelő szoftver felületintervallumokba tartozó részecskéket számlál meg, majd ábrázolja a felületi intervallum-előfordulási arány függvényét.



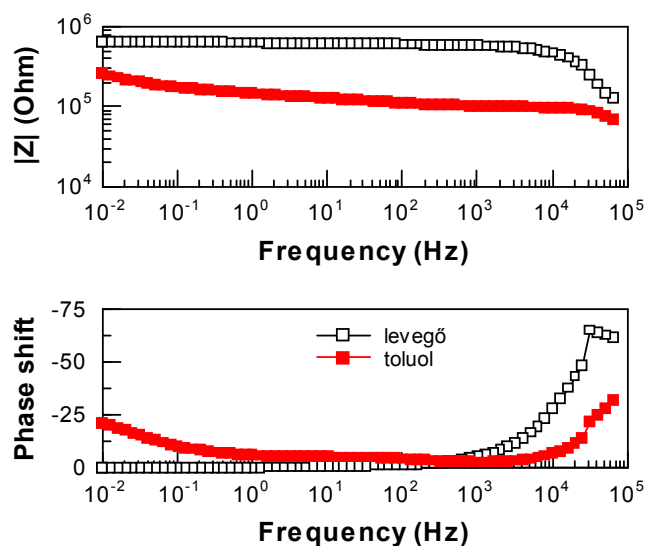
2. ábra. TEM felvétel a szolról 50 nm-es skálával (Német Péter MTA KK)



3. ábra. A részecske felület előfordulási arány (Német Péter MTA KK)

A TEM felvétel alapján a meghatározott átlagos részecskeátmérő 3-4 nm (3. ábra) volt.

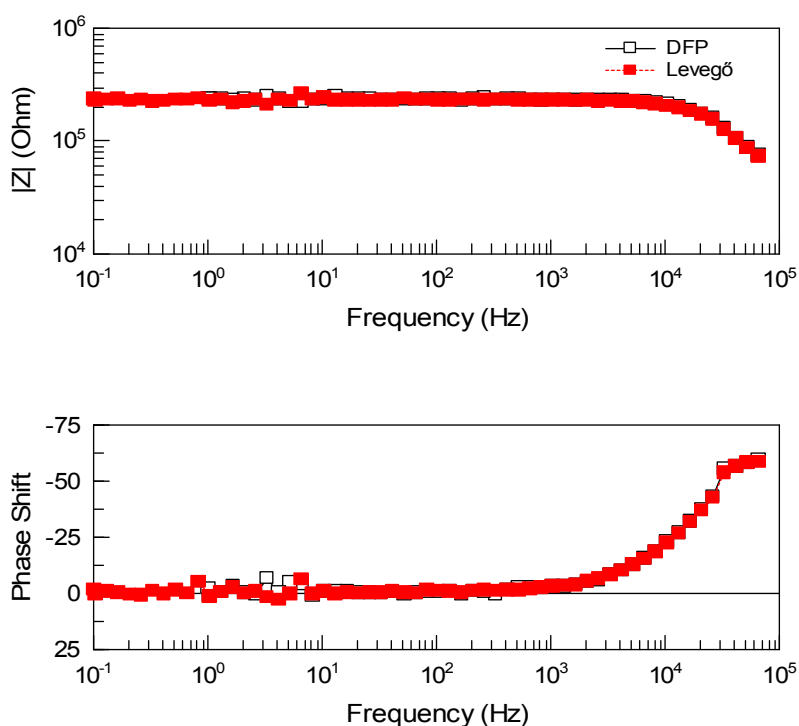
Elektrokémiai impedancia spektroszkópiás vizsgálat eredményeként jól látható a levegőn és a toluolra telített légtérben mért impedancia különbsége, ami 1 és 1 kHz között meghaladja 6×10^5 Ohm-ot.



4. ábra. A vegyi érzékelő tiszta levegőn és toluolra telített levegőn mért EIS spektrumának Bode ábrázolása (Felhősi Ilona MTA KK)

Vizsgálatok szennyezett légtérben

A mérőeszközzel mért egyik jellemző EIS spektrumot az 5. ábrán mutatjuk be.



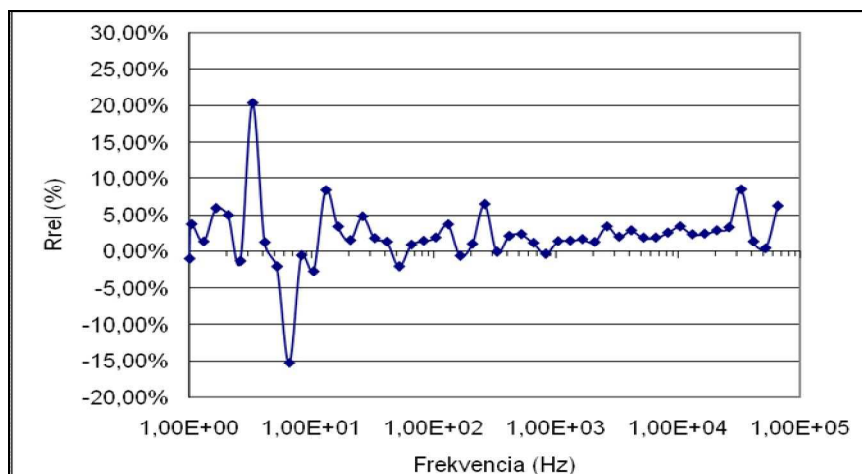
5. ábra. A vegyi érzékelő tiszta levegőn és DFP vel szennyezett levegőn mért EIS spektrumának Bode ábrázolása (Felhősi Ilona MTA KK)

Az 5. ábrán az ábrázolásban nem látható a levegőn és DFP-vel szennyezett légtérben mért magnitúdók különbsége ezért célszerű bevezetni az R_{rel} relatív ellenállás fogalmát, amivel jellemezhető az érzékenység. [1,6]

$$R_{rel} = \frac{R_a - R}{R}$$

Ahol: R_a : Az analizált anyag ellenállása
 R : A levegőn mért ellenállás

Az alkil-tiollal stabilizált arany nanorészecskéssel bevont vegyi érzékelő esetében a relatív ellenállás változást a frekvencia függvényében a 6. ábrán mutatjuk be



6. ábra. A vegyi érzékelőn mért relatív ellenállás változása a frekvencia függvényében (Molnár Árpád)

A 6. ábra jól látható, hogy a zaj miatt 1 KHz-nél vagy a felett érdemes a vegyi érzékelő koncentráció-relatív ellenállás változás függését felvenni.

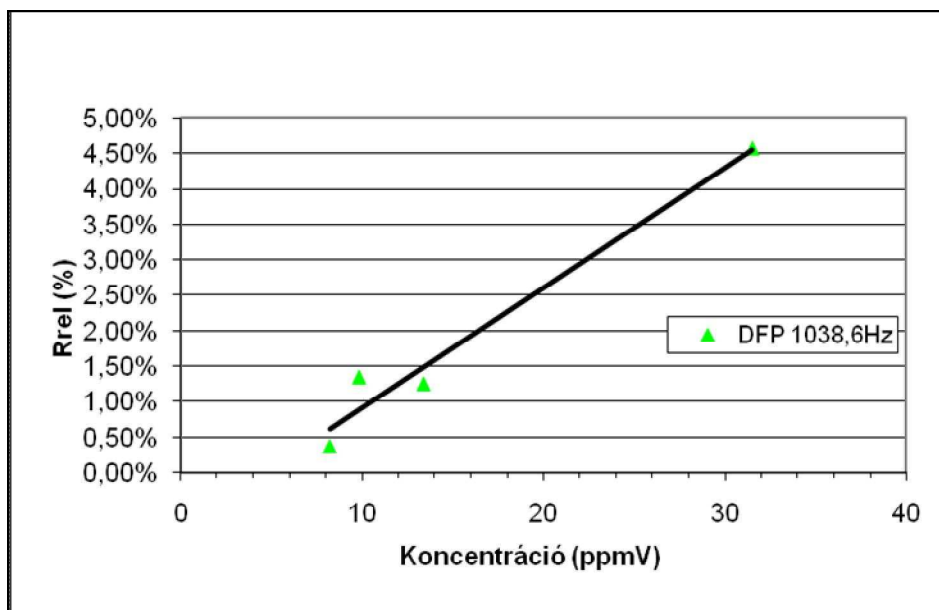
A vizsgálat során mért DFP koncentrációkat az 1 táblázatban adjuk meg.

1. táblázat. DFP szennyezettségi adatok

Koncentráció		Rrel
ng/ml	ppmV	1038,6 Hz
60,1	8,2	0,4%
71,9	9,9	1,3%
97,5	13,4	1,3%
230,2	31,5	4,6%

A DFP koncentráció és a 1038,6 Hz-en mért impedanciákból számolt relatív ellenállásokat a következő diagramon mutatjuk be. (7. ábra) A diagram adatait lineáris regresszió módszerével közelítettük.

Az egyenes egyenlete: $R_{rel} = 0,00169 \times K + 0,00779$
ahol a K: A DFP koncentráció ppmV-ben megadva
A korreláció értéke: $r^2 = 0,98389$



7. ábra. A vegyi érzékelő koncentráció relatív ellenállás karakterisztikája (Molnár Árpád)

AZ EREDMÉNYEK ÉRTÉKELÉSE

A vizsgált alkil-tiollal stabilizált arany szolokkal bevont vegyi érzékelő típusoknál megfigyelték, hogy az érzékelő anyagban lévő arany nanoszemcsék méretének meghatározó hatása van a vezetőképességre. [14] Az optimális szemcseméretet az irodalom szerint 1 és 5nm között van. [15]

A TEM vizsgálatok eredményeként az átlagos részecskeátmérő 3 - 4 nm volt, ami alapján megállapíthatjuk, hogy a vizsgált szol alkalmazható az interdigitális elektródákon. Az elektrokémiai impedancia spektroszkópiás mérés eredmény jó egyezése a korábbi mérések eredményeivel igazolja, hogy a vegyi érzékelők elkészítése nyomán az érzékelő anyag felvitele során a megfelelő borítottságot, [16, 22] úgy alakították ki, hogy az arany nanorészecskék a művelet közben nem aggregálódtak.

A vegyi érzékelő koncentráció relatív ellenállás karakterisztikáját vizsgálva megállapíthatjuk, hogy a lineáris regresszióval illesztett egyenest interpolálva 4 ppmV DFP koncentrációt érhetünk. Ez a koncentráció egy nagyságrenddel haladja meg az irodalomban található adatokat. [23]

Figyelembe véve a méréstechnológia fejlődését,[7] egy célműszerrel kedvezően befolyásolható a vegyi érzékelő érzékenysége.

KÖVETKEZTETÉSEK

Egy vegyi érzékelő gyártás kritikus lépéseinek ellenőrzéséhez és kézben tartásához, jól kihasználhatók a TEM és az EIS lehetőségei. A vizsgálatok megbízható információt biztosítanak az elkészült szolok arany nanoszemcse méret eloszlásáról és minősítik a szol felvitelét.

A relatív ellenállás vizsgálatával, amely szoros kapcsolatban áll az érzékelő érzékenységevel, felvehető a koncentráció relatív ellenállás karakterisztika, amely az az adott vegyi érzékelőt minősíti a mért gázra.

Figyelembe véve a méréstechnológia fejlődését, javasoljuk egy célműszer fejlesztését, amely várhatóan javíthatja a mérés érzékenységét.

KÖSZÖNETNYILVÁNÍTÁS

A szerzők köszönetüket fejezik ki Dr. Felhősi Ilonának, Trif Lászlónak, Molnár-Vörös Nikoletta és Dr. Németh Péter, az MTA Kémiai Kutatóközpont műszereinek használatáért, az eredmények értékelésében nyújtott tanácsokért, valamint az NKTH-nak a METANANO projekt támogatásáért.

Irodalomjegyzék

- [1] K. Kalantar-zadeh, B. Fry: Nanotechnology-Enabled Sensors. Springer Science+Business Media, LLC, New York, 2008.
- [2] M.K. Patra, K. Manzoor, M. Manoth, S.C. Negi, S.R. Vadera, and N. Kumar: Nanotechnology Applications for Chemical and Biological Sensors. Defence Science Journal, Vol. 58, No. 5, September 2008, pp. 636-649.
- [3] V.K. Khanna: Nanoparticle-based Sensors. Defence Science Journal, Vol. 58, No. 5, September 2008, pp. 608-616.
- [4] H. Ahn, A. Chandekar, B. Kang, C. Sung, J.E. Whitten: Comparison of Solubility and Vapor Sensing Properties of Methyl- and Thiophene-Terminated Alkanethiol-Protected Gold Nanoparticle Films. Journal of Macromolecular Science, Part A: Pure and Applied Chemistry, 42 (2005) 1477–1487.
- [5] L. Wang, N.N. Kariuki, M. Schadt, D. Mott 1, J. Luo, C. Zhong, X. Shi, C. Zhang, W. Hao, S Lu, N. Kim, J. Wang: Sensing Arrays Constructed from Nanoparticle Thin Films and Interdigitated Microelectrodes. Sensors, 6 (2006) 667-679.
- [6] P. Pang, J. Guo, S. Wu, Q. Cai: Humidity effect on the dithiol-linked gold nanoparticles interfaced chemiresistor sensor for VOCs analysis. Sensors and Actuators B 114 (2006) 799–803.
- [7] D. Rairigh, A. Mason, M. P. Rowe, E. T. Zellers: Baseline Resistance Cancellation Circuit for High Resolution Thiolate-Monolayer-Protected Gold Nanoparticle Vapor Sensor Arrays. Circuits and Systems, (2008) 2002-2005.
- [8] R.W. French, E.V. Milsom, A.V. Moskalenko, S.N. Gordeev, F. Marken: Assembly, conductivity, and chemical reactivity of sub-monolayer gold nanoparticle junction arrays. Sensors and Actuators B 129 (2008) 947–952.

- [9] J. Rivera-Gandí, C.R. Cabrera: Self-assembled monolayers of 6-mercapto-1-hexanol and mercapto-n-hexyl-poly(dT)18-fluorescein on polycrystalline gold surfaces: An electrochemical impedance spectroscopy study. *Journal of Electroanalytical Chemistry* 605 (2007) 145–150.
- [10] M. Brust, C.J. Kiely, Some recent advances in nanostructure preparation from gold and silver particles: a short topical review, *Colloids Surf. A: Physicochem. Eng. Aspects* 202 (2002) 175–186.
- [11] V.H. Perez-Luna, K. Aslan, P. Betala: Colloidal Gold, in: H.S. Nalwa (Ed.), *Encyclopedia of Nanoscience and Nanotechnology*, vol. 2, American Scientific Publishers, 2004 pp. 27–49.
- [12] Y. Tan, Y. Li, D. Zhu: Noble Metal Nanoparticles, in: H.S. Nalwa (Ed.), *Encyclopedia of Nanoscience and Nanotechnology*, vol. 8, American Scientific Publishers, 2004 pp. 9–40.
- [13] M.-C. Daniel, D. Astruc, Gold nanoparticles: assembly, supramolecular chemistry, quantum-size-related properties, and applications toward biology, catalysis, and nanotechnology, *Chem. Rev.* 104 (2004) 293–346.
- [14] R.R. Smardzewski, N.L. Jarvis, A.W. Snow, H. Wohltjen: “Metal-Insulator-Metal Ensemble (MIME) Chemical Detectors”, *Nanotech2004 Nanotechnology Conference & Trade Show, Proceedings Vol. 3*, pp. 163–4, Boston, 7–11 March 2004.
- [15] M.G. Ancona, A.W. Snow, E.E. Foos, W. Kruppa, R. Bass: Scaling Properties of Gold Nanocluster Chemiresistor Sensors. *IEEE Sensors Journal*, vol. 6, No. 6, (2006).
- [16] N. Molnár Vörös, R. Patakfálvi, I. Dékány: Alkylthiol-functionalized gold nanoparticles for sensing organic vapours: The connection between the adsorption isotherm and the sensor resistance. *Colloids and Surfaces A: Physicochem. Eng. Aspects* 329 (2008) 205–210.
- [17] D.D. Macdonald: Reflections on the history of electrochemical impedance spectroscopy. *Electrochimica Acta* 51 (2006) 1376–1388.
- [18] P. L. Bonora, F. Deflorian, L. Fedrizzi: Electrochemical impedance spectroscopy as a tool for investigating underpaint corrosion. *Electrochimica Acta*. Vol. 41. Nos. 1/8. pp. 1073. 1082, 1996.
- [19] J.M. McIntyre, H.Q. Pham: Electrochemical impedance spectroscopy; a tool for organic coatings optimizations. *Progress in Organic Coatings* 27 (1996) 201–207.
- [20] I. Felhősi, E. Kálmán, P. Póczik: Corrosion Protection by Self-Assembly. *Russ. J. Electrochem.*, 38 (2002) 230–237
- [21] M. Brust, M. Walker, D. Bethell, D.J. Schiffrin, R.J. Whyman: Synthesis of Thiol-Derivatized Gold Nanoparticles in a two-phase Liquid-Liquid system, *J. Chem. Soc., Chem. Commun.* (1994) 801–802.

- [22] A.W. Snow, H. Wohltjen: Colloidal Metal-Insulator-Metal Ensemble Chemiresistor Sensor Anal. Chem. 1998, 70, 2856-2859
- [23] Halász, L.; Grósz, Z.: ABV védelem; Egyetemi jegyzet, ZMNE, Budapest, 2001

Molnár Árpád

molnar.arpad1@chello.hu

Halász László

halasz.laszlo@zmne.hu

ARANYSZOL BEVONATÚ VEGYI ÉRZÉKELŐK ALKALMAZHATÓSÁGA A KATONAI EGYÉNI VÉDŐESZKÖZÖK VÉDŐKÉPESSÉGÉNEK VIZSGÁLATÁRA

Absztrakt

A NATO erők alkalmazhatóságát a mérgező harcanyagokkal vagy ipari mérgező anyagokkal szennyezett környezetben az egyéni védőeszközök védelmi képessége határozza meg. Az egyéni védőeszközök e paraméterét mind a fejlesztés mind pedig a rendszerben tartás időszakában ellenőrizni kell. A szerzők ezt a fontos paraméterét az egyéni védőeszköznek speciális érzékelőkkel vizsgálták bisz(2-kloroetil)szulfiddal. A vizsgálta interdigitális elektródákat alkiltiollal stabilizált aranyszollal vonták be. A szolban az arany részecskék tipikus mérete 3-4 nm volt. A vizsgálatok előtt az érzékelők minőségét egy Transzmissziós elektron-mikroszkópián és Elektrokémiai impedancia spektroszkópián alapuló eljárással ellenőriztük. A cikkben az egyéni védőeszköz e fontos paraméterének meghatározására javasolunk egy katonai érzékelőt használó alternatív módszert.

Applicability of NATO forces in environment contaminated with Chemical Warfare Agents or Toxic Industrial Chemicals is determined by the protective capability of their individual protective equipments (IPE). This parameter of IPE should be checked during development and lifetime in the army. Authors have investigated this important parameter of IPE with specific sensors. The examination was carried out in air contaminated with bis(2-chloroethyl) sulfide. The gold sol covering interdigital electrodes of chemical sensors examined was stabilized with alkyl-thiol. In sol, the typical size of gold particles was between 3 and 4 nm. Qualification of the sensors before the examination was checked by the use of a procedure basing on Transmission Electron Microscopy and Electrochemical Impedance Spectroscopy. For determining this important parameter of IPE, an alternative method using military chemical sensor was proposed.

Kulcsszavak: *Szenzor, érzékelő, arany, nanorészecske, bőrvédő eszköz, szol, bisz(2-kloroetil)szulfid ~ sensor, gold, nanoparticles, skin protection device, sol, bis(2-chloroethyl) sulfide*

BEVEZETÉS

A NATO hadműveleteit, az erői ellen irányuló fenyegetések tudatában tervezi és vezeti. Erőinek nem csak a hagyományos támadásokkal szembeni védelemre, de huzamosabb időn keresztül a műveleti tevékenység folytatására a mérgező harcanyagok, biológiai harcanyagok és ipari mérgező anyagok hatásának kitett környezetben is képesnek kell lenni. Ezen anyagok elleni védekezés hatékonyságát alapvetően meghatározza a bőrvédő eszközök védőképessége.

A védőképesség rendszeres vizsgálata szükséges mind a fejlesztés, mind a rendszerben tartás időszakában. Ezért a Honvédelmi Minisztérium Fejlesztési és Logisztikai Ügynökség Technológiai Igazgatóság (HM FLÜ TI) gyakorlatában a fejlesztési eredmények ellenőrzése épp úgy jelen van, mint az alkalmazók által felvetett műszaki problémák vizsgálata és kezelése.

A Honvédelmi Minisztérium háttérintézeteinél 2007-ben végrehajtott szervezeti változtatások nyomán kialakult személyi feltételek, valamint a rendelkezésre álló, egyre szűkülő pénzügyi források megkövetelik az egyszerűbb és olcsóbb, ugyanakkor megbízható vizsgálati eljárások kutatását és alkalmazását.

A vegyivédelmi szakterületen sajátos helyzet kialakulása várható a 93 M vegyivédelmi védőruha készletek tárolása területén. Az eszközök egy része raktári készletként fogja elérni a szavatossági idejének lejártát. Ha a szükségleteknek megfelelő mennyiségű új eszköz beszerzésére nem lesz lehetőség, ami valószínűsíthető, a HM FLÜ TI-nek reálisan kell számolnia a szavatossági idő meghosszabbítására irányuló igényekkel. Mindez azt jelenti, hogy sürgető aktualitása van a katonai bőrvédő eszközök védőképességének vizsgálati eljárásai műszaki, gazdasági és személyi vonatkozásainak kutatására.

Ebbe a kutatási-fejlesztési irányvonalba illeszthetők, a kémiai érzékelőkkel végzett kutatások, amelyek szorosan kötődnek a nanoszerkezetű anyagokkal folytatott kutatások területén jelentkező eredményekhez. A mikro- és nano-méretű (részecskeméret: 10^{-6} 10^{-9} m) „objektumokkal” végzett kutatások során egyfelől az anyagok olyan új különleges tulajdonságait ismerik meg, amelyek csak erre a mérettartományra jellemzők, másfelől új vagy a különleges körülményekre adaptált meglévő módszerekkel és technikákkal érnek el eredményeket. [1]

Az érzékelők világát a hordozók, az érzékelő anyagok, a működési elvek és a műszaki megvalósítások változatossága jellemzi. Természetesen igaz ez a vegyi érzékelőkre is. [2]

A vegyi érzékelők kialakítását tekintve a jellemzően olcsó és egyszerű hordozó típusok az egymásba fogazott fésűs úgynevezett interdigitális elektródák, amelyek a dielektrikum kapacitásának és vezetőképességének mérésére alkalmasak. [3]

Az interdigitális elektródák bevonására a közkedvelt szol-gél módszer elterjedten alkalmazott. [1] Ez a módszer többek között alkalmas vékony rétegek, nagyon finom és különleges alakú porok, valamint rendkívül porózus aerogélek kialakítására is. [2]

Az arany széles körben használatos nemesfém a szenzorgyártásban és a mikroelektronikában, mert nemcsak jó vezetőképességgel rendelkezik, hanem alkalmas önszerveződő anyagok létrehozására is. [1,4] A nanoméretű aranyrészecskék szabályozott előállítása jól ismert az irodalomban. [5,6]

A vizsgált érzékelők esetében az interdigitális elektródákra felvitt érzékelő anyag alkil-tiollal stabilizált arany szol volt. Az ilyen vegyi érzékelő típusoknál megfigyelték, hogy az érzékelő anyagban lévő arany nanoszemcsék méretének meghatározó hatása van a vezetőképességre. [7] Az optimális szemcseméret a vonatkozó irodalmi adatok alapján 1 és 5 nm közé esik. [8]

A szemcseméret meghatározására jól bevált technológia a Transzmissziós Elektron-Mikroszkópos (TEM) vizsgálat. [1,2,9]

Az elkészült érzékelőket az elektrokémiai reakciók mechanizmusainak és különböző, például önszerveződő rétegek vizsgálatában sikerrel alkalmazott [10] Elektrokémiai Impedancia Spektroszkópia (EIS) vizsgálatnak vetettük alá.

Az impedancia spektroszkópia lehetővé teszi összetett folyamatok egyidejű vizsgálatát, a dielektromos tulajdonságok megváltozásának nyomon követését és az optimális mérési helyek meghatározását.

Az impedancia spektrumok ábrázolása Nyquist ($\text{Im}Z$ vs. $\text{Re}Z$) valamint Bode ($|Z|$ vs. f és θ vs. f) módban történik. Az impedancia kétféle ábrázolása közötti összefüggés:

$$\tan \theta = \frac{\text{Im}(Z)}{\text{Re}(Z)}, \text{ ill. } |Z| = \sqrt{\text{Re}(Z)^2 + \text{Im}(Z)^2}$$

ahol:

Z: Az impedancia

f: A frekvencia

$\text{Re}Z$: Az impedancia reális része

$\text{Im}Z$: Az impedancia képzetes része

θ : Az impedancia vektor reális tengellyel bezárt szöge

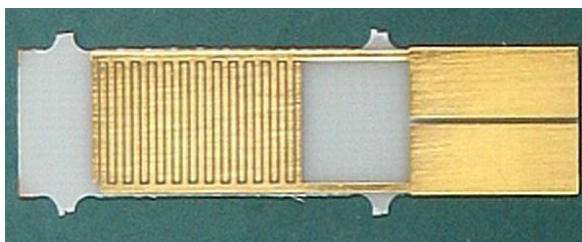
Eredmények bemutatására a spektrum Bode ábrázolását részesítettük előnybe.

A katonai gyakorlatban a vegyvédelmi bőrvédő eszközök védőképességének vizsgálatát bis(2-kloroetil)szulfid-dal (Sm) végzik, ezért a toluolra telített légtérben minősített érzékelők alkalmazhatóságát Sm-mel szennyezett légtérben vizsgáltuk.

MÓDSZEREK

Az érzékelők elkészítése [11]

A vizsgálati célra alkalmazott kémiai érzékelők hordozói mindenesetben az Auter Elektronika Kft. által legyártott interdigitális elektródák voltak. A polimer alapra hagyományos nyomtatott áramkörök készítői technológiával alakították ki a néhány μm vastagságú réz elektródamintázatot. Az 1 cm^2 felületű interdigitális elektródák (1. ábra) fogazatainak szélessége 0,5 mm volt. A 13 pár fogazatú kialakítást 15 μm fogközi távolság jellemezte.



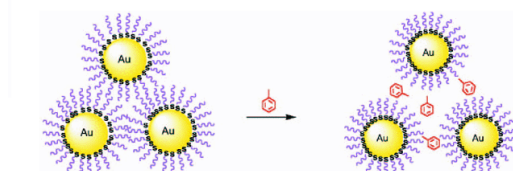
1. ábra. Interdigitális elektródák

Az érzékelő anyag előállítása az irodalomban is ismert, és más kutatócsoportok által már érzékelő készítésre alkalmazott kétfázisú kémiai redukciós Brust-Schiffrin módszerrel történt [5,6,9]

A szintézis lényege, hogy az AuCl_4 -t vizes oldatból tetra-oktil-ammónium-bromid tenzides fázistranszferrel toluolos oldatba viszik és NaBH_4 -al redukálják tiol jelenlétében. A nanorészecskék méretét az arany-tiol aránnyal szabályozzák.

Az alkil-tiollal stabilizált arany nanorészecskéket tartalmazó szol levegőn hosszú ideig stabil marad és többnyire az egyszerű szerves vegyületekhez hasonló módon kezelhető.

Az nanoarany-szollal bevont interdigitális érzékelők működésének alapja, hogy az alkil-tiol bevonat elszigeteli egymástól a nanoméretű aranyrészecskéket. Az így kialakított dielektrikum ellenállása nagyobb a tisztán aranyat tartalmazónál. Ha az érzékelőt például toluollal szennyezett légtérbe helyezzük a szennyező anyag bekerül az egymástól szigetelt aranyrészecskék közé, ami megváltoztatja a dielektrikum elektromos tulajdonságát. A folyamatot a 2. ábra szemlélteti.



2. ábra. A toluol adszorpciója a szolban [7]

Az érzékelő minősítése

A vegyi érzékelő készítéséhez előállított szolban az arany nanoszemcsék méretét Morgagni 268D Transzmissziós elektron-mikroszkóppal határozták meg. [12]

A Transzmissziós elektron-mikroszkópos vizsgálatok során nagy energiájú elektronsugár halad át egy vékony mintán, többek között információt biztosítva a minta részecskeméret eloszlásáról. [2]

Az előállított vegyi érzékelők Elektrokémiai Impedancia Spektroszkópiás vizsgálatára az MTA KK Elektrokémiai laboratóriumában került sor. A Solartron 1286 potenciosztát és a Solartron 1250 frekvenciaválasz analizátorból álló műszerrel 10 mérési pont/dekád felbontásban, a 0,1 Hz – 65 kHz frekvenciatartományban végezték a méréseket. 10 mV amplitúdójú szinuszos bemeneti potenciáljelet adva az érzékelőre mérték az autointegrációval szabályozott áram válaszjelet. Az impedancia mérés vezérlése a Zplot szoftverrel, az

impedancia spektrum ábrázolása és kiértékelése Zview szoftverrel történt. Az eredményeket alátámasztó diagramok az alapadatok importálását követően MS Excel szoftverrel ábrázoltuk.

Az érzékelőket párhuzamos RC körrel modelleztük. Az ellenállást és a kapacitást egy adott frekvencián az impedancia értékek valós és képzetes részéből a következő összefüggések alapján számoltuk:

$$R = \frac{\operatorname{Re}(Z)^2 + \operatorname{Im}(Z)^2}{\operatorname{Re}(Z)},$$

valamint:

$$C = \frac{-\operatorname{Im}(Z)}{\omega \cdot (\operatorname{Re}(Z)^2 + \operatorname{Im}(Z)^2)}$$

ahol:

C: A kapacitás

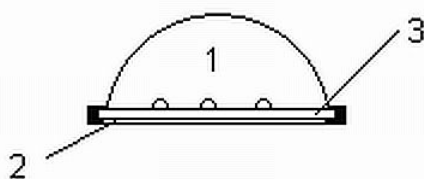
R: Az ellenállás

$\omega = 2\pi f$

Vizsgálatok szennyezett légtérben

A katonai bőrvédő eszközök védőképességét bisz(2-kloroetil)szulfid (Sm) tesztanyaggal határozzák meg. Az anyag szoba hőmérsékleten színtelen viszkózus folyadék. Sűrűsége: 1,2963 g/cm³. A tiszta anyag atmoszférikus forráspontja 217,5 °C, olvadáspontja 14,5 °C, csaknem szagtalan, de már nyomnyi szennyeződés sárga színt ad a folyadéknak. Szerves oldószerekben, alkoholban jól, vízben gyakorlatilag nem oldódik 0,8 g/l. [13]

A katonai bőrvédő eszközök védőképességét átütés vizsgálat során meghatározható átütési idővel jellemzik. A vizsgálat klasszikus elrendezését szemlélteti az 3. ábra.

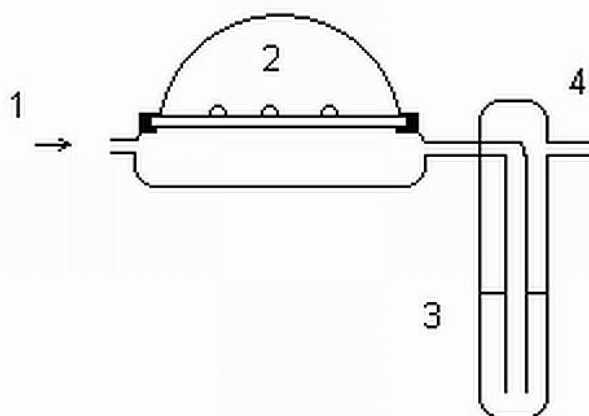


3. ábra. Katonai bőrvédő eszköz anyagának átütés vizsgálata.

1: Tesztanyag-cseppek, 2: Indikátorpapír 3: Vizsgálati minta

Az eljárás lényege, hogy a minta eszközből kivágott mintegy 5 cm² felszínű vizsgálati minta színére tesztanyagot cseppentenek, amely az anyagon átjutva az indikátor papír színváltozását okozza. A felcseppentéstől a színváltozásig eltelt időt nevezik az átütési időnek. Az eljárás rövid leírása is jól érzékelteti az eredmény bizonytalanságát.

Az átütés vizsgálat egyik legkorszerűbb módszerének a gázkromatográffal ellenőrzött eljárást nevezhetjük. A vizsgálat elrendezését a 4. ábrán láthatjuk.



4. ábra. Katonai bőrvédő eszköz anyagának átütés vizsgálata
gázkromatográffal (elvi vázlat). 1: Tiszta levegő belépése, 2: Tesztanyag-cseppek
3: Elnyelő közeg, 4: A levegő kilépése a szűrő irányába.

Az eljárás lényege, hogy a minta eszközből kivágott vizsgálati minta színére tesztanyagot cseppentenek, amelyet miután az anyagon átjut és keveredik a tisztított levegővel oldódik az elnyelő közegben. A rendszerből kilépő levegőt természetesen szűrik. Az átütési idő meghatározásához az elnyelő közegből vesznek mintát, amelynek tesztanyag tartalmát gázkromatográffal vizsgálják. Ebben az esetben az átütési időnek a tesztanyag felcseppentésétől az adott fajlagos koncentráció ($4 \mu\text{g}/\text{cm}^2/24 \text{ óra}$) kialakulásáig eltelt időt tekintik.

A rendszer természeténél fogva nagyfokú precizitást és szakértelmet igényel, mert túl azon, hogy a levegőáramot úgy kell beállítani, hogy a vizsgálati mintára gyakorolt szívása elhanyagolható legyen, a drága laboratóriumi műszert is kalibrálni kell a tesztanyagra. A vázolt eljárás jól alkalmazható nagyszámú sorozatok vizsgálatára, de beszerzési ára meglehetősen magas, és éves technikai kiszolgálásának (karbantartás, fogyóanyag pótlása stb.) költsége elérheti a milliós nagyságrendet is.

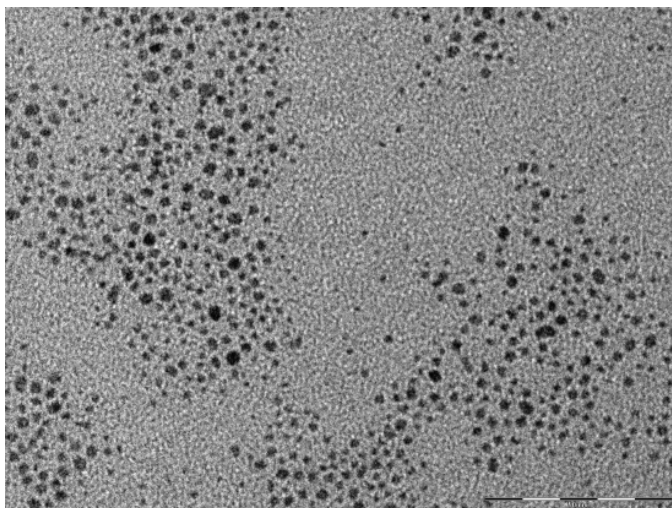
A vizsgálat során az Sm-mel szennyezett légtér koncentrációjának beállítása egy dinamikus koncentráció beállító készülékkel történt. A szennyezett légtérből vett minták Sm tartalmát egy Varian 3800 Gázkromatográfból (GC) és 1200 MS/MS kombinált tömegspektrométerből (MS) kialakított GC-MS berendezéssel mértük.

Az Sm-mel szennyezett légtérben végzett vizsgálatokra HM FLÜ Technológiai Igazgatóságának Vegyi laboratóriumában került sor az MTA KK Felületmódosítás és Nanoszerkezetek Osztálya által biztosított mérőberendezéssel. A berendezés a Zplot szoftvervezérlésű Solartron 1286 potenciosztát és a 1250 frekvenciaválasz analizátor berendezésekből került kialakításra. A kételektródos elrendezésben 10 mV amplitúdójú szinuszos potenciáljelet adva az érzékelőre, mértük az áram válaszjelet.

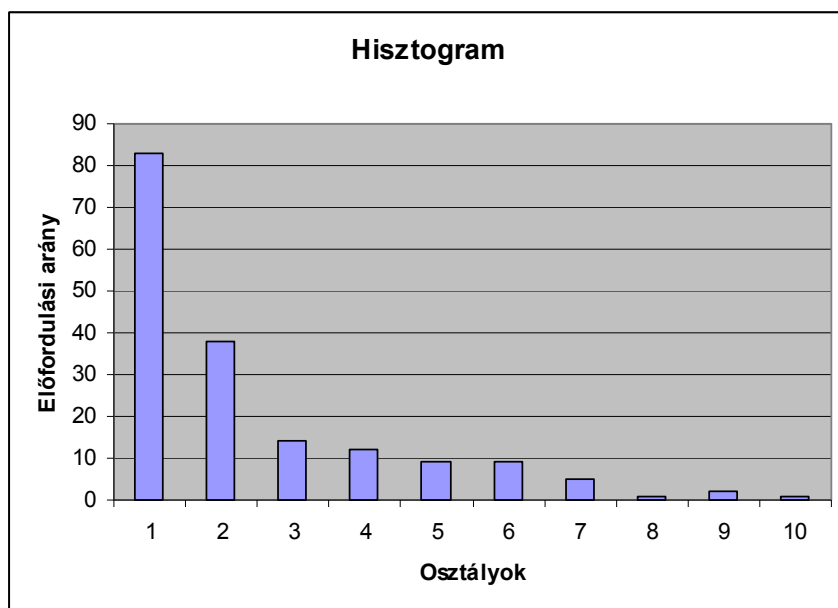
EREDMÉNYEK

Az érzékelők minősítése

Az elkészített arany nanoszolokban a részecskeméret meghatározást a transzmissziós elektronmikroszkópos felvételek alapján végezték (5. ábra). A kiértékelő szoftver felületintervallumokba tartozó részecskéket számlál meg, majd ábrázolja a felületi intervallum-előfordulási arány függvényét. (6.ábra)



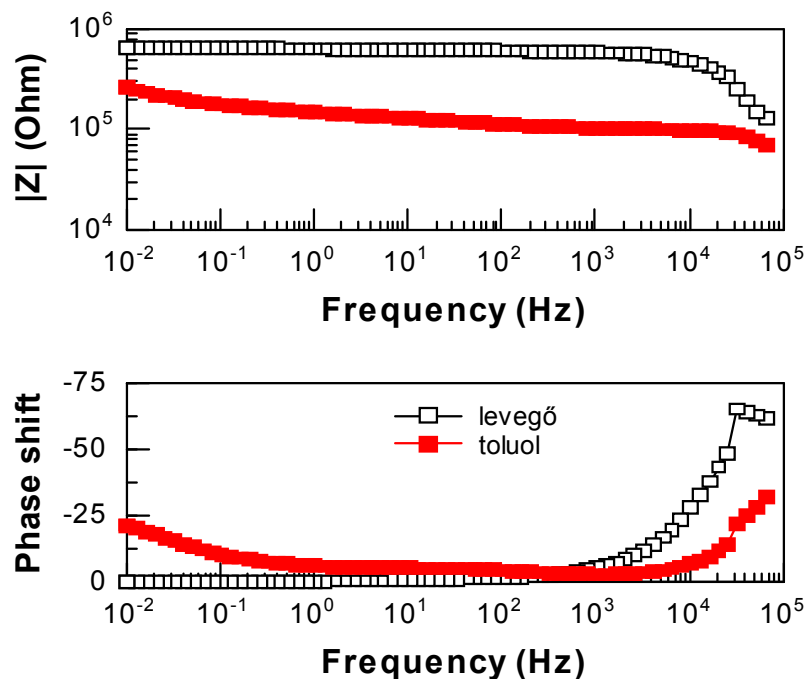
5. ábra. TEM felvétel a szolról 50 nm-es skálával [12]



6. ábra. A részecske felület előfordulási arány [12]

A TEM felvétel alapján a meghatározott átlagos részecskeátmérő 3-4 nm volt. (6.ábra)

Elektrokémiai impedancia spektroszkópiás vizsgálat eredményeként jól látható a levegőn és a toluolra telített légtérben mért impedancia különbsége, ami 1 Hz és 1 kHz között meghaladja 6×10^5 Ohmot.



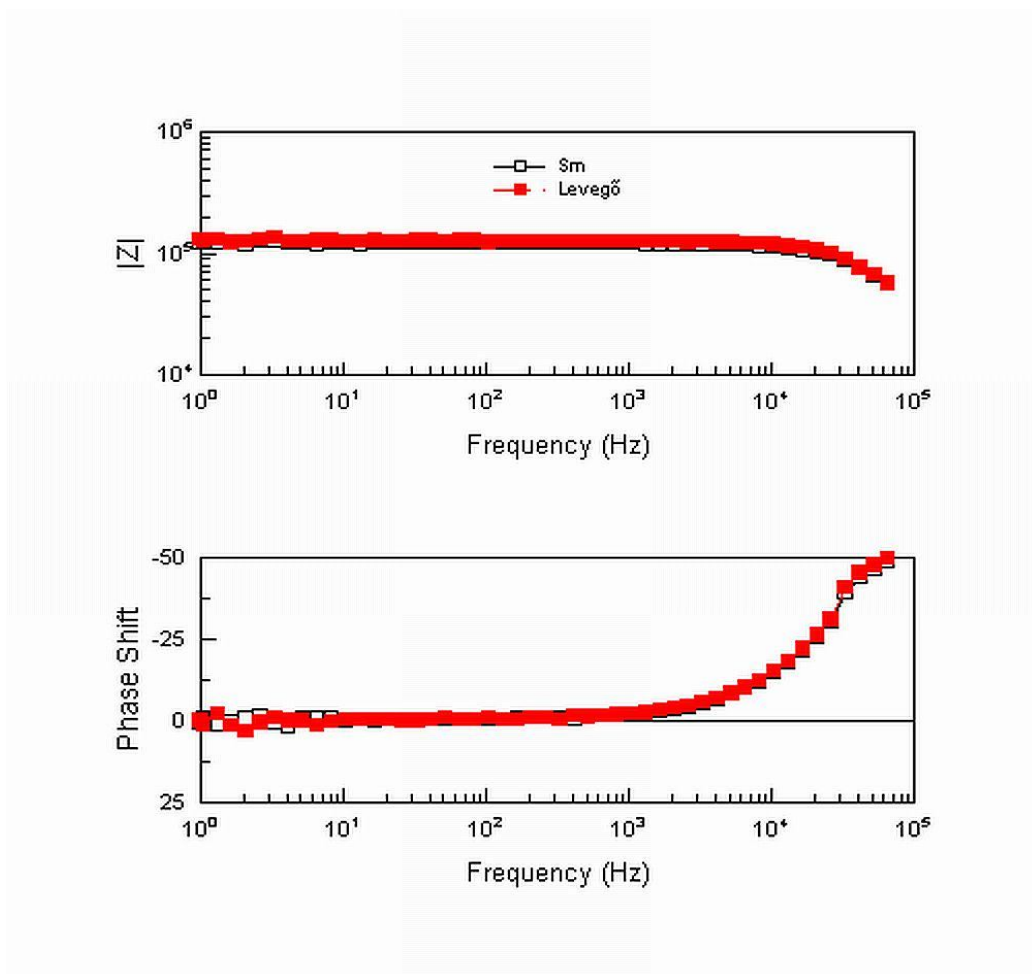
7. ábra. A vegyi érzékelő tiszta levegőn és toluolra telített levegőn mért EIS spektrumának Bode ábrázolása [14]

Vizsgálatok szennyezett légtérben

A mérőeszközzel toluolra telített levegőn mért egyik jellemző EIS spektrumot a 7. ábrán mutatjuk be. A 8. ábrán az ábrázolásban nem látható a levegőn és Sm-mel szennyezett légtérben mért magnitúdók különbsége ezért célszerű bevezetni az R_{rel} relatív ellenállás változás fogalmát, amivel jellemezhető az érzékenység. [2,3]

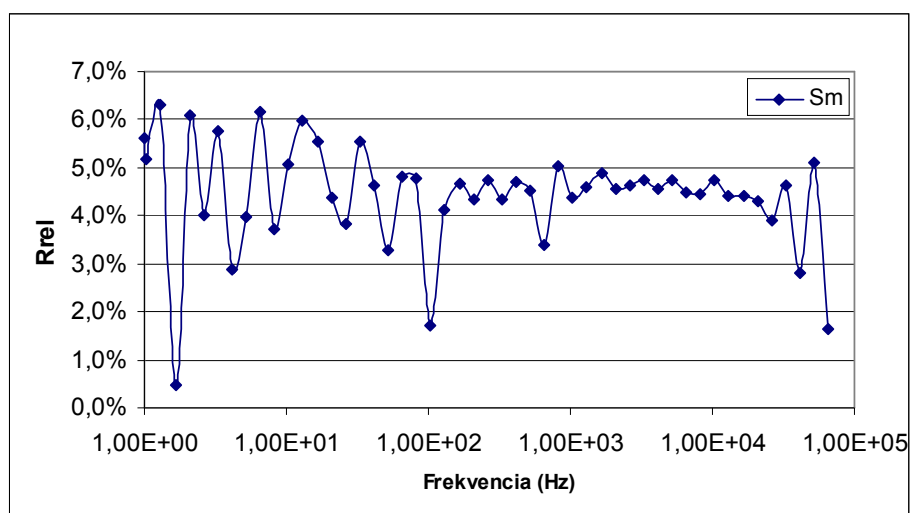
$$R_{rel} = \frac{R - R_a}{R}$$

Ahol: R_a : Az ellenállás az analizált anyaggal szennyezett légtérben
 R : Az ellenállás levegőn.



8. ábra. A vegyi érzékelő tiszta levegőn és Sm-mel szennyezett levegőn mért EIS spektrumának Bode ábrázolása [14]

Az alkil-tiollal stabilizált arany nanorészecskékkal bevont vegyi érzékelő esetében a relatív ellenállás változást a 9. ábrán mutatjuk be



9. ábra. A vegyi érzékelőn mért relatív ellenállás változása a frekvencia függvényében ábrázolva

A 9. ábrán jól látható, hogy a zaj miatt 1 kHz-nél vagy a felett érdemes a vegyi érzékelő koncentráció-relatív ellenállás változás függését felvenni.

A vizsgálat során mért Sm koncentrációkat az 1 táblázatban adjuk meg.

1.táblázat. Sm szennyezettségi adatok

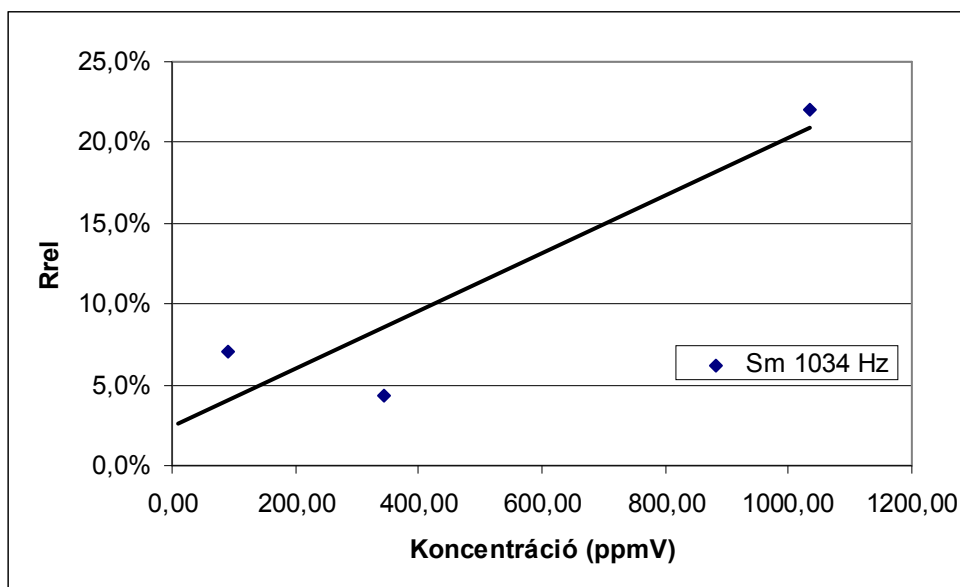
Koncentráció		Rrel
ng/ml	ppmV	1038,6 Hz
549,5	90,1	7,1%
2100,0	344,4	4,4%
6300,0	1033,2	22,0%

Az Sm koncentráció és a 1038,6 Hz-en mért relatív ellenállásokat a következő diagramon mutatjuk be. (10. ábra) A diagram adatait lineáris regresszió módszerével közelítettük.

Az egyenes egyenlete: $R_{rel} = 2,93 \times 10^{-5} \times K + 0,02406$

ahol a K: Az Sm koncentráció ppmV-ben megadva

A korreláció értéke: $r = 0,91846$



10. ábra. A vegyi érzékelő koncentráció-relatív ellenállás változás karakterisztikája

AZ EREDMÉNYEK ÉRTÉKELÉSE

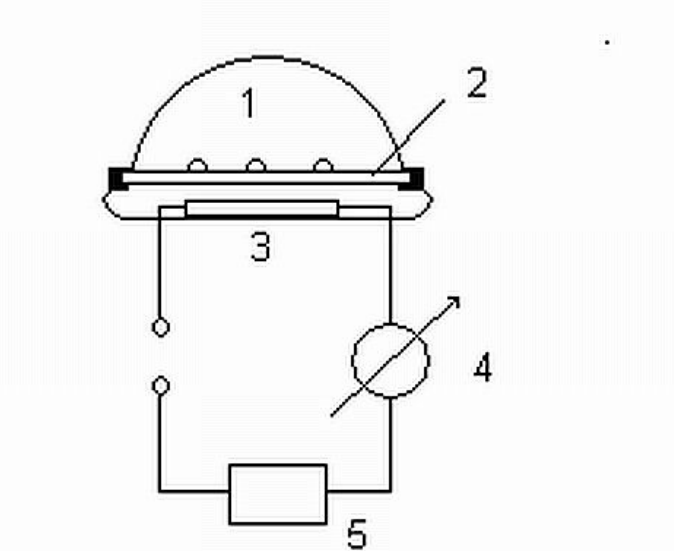
A vizsgált alkil-tiollal stabilizált aranyzszollal bevont vegyi érzékelő típusoknál megfigyelték, hogy az érzékelő anyagban lévő arany nanoszemcsék méretének meghatározó hatása van a

vezetőképességre. [7] Az optimális szemcseméretet az irodalomban 1 és 5nm közé esik.[8] A TEM vizsgálatok eredményeként az átlagos részecskeátmérő 3 - 4 nm volt, ami alapján megállapíthatjuk, hogy a vizsgált szol alkalmazható az interdigitális elektródákon.

Az elektrokémiai impedancia spektroszkópiás mérés eredménye jó egyezést mutat a korábbi mérések eredményeivel igazolva, hogy a vegyi érzékelők elkészítésekor az érzékelő anyag felvitele során a megfelelő borítottságot, [6,9] úgy alakították ki, hogy az arany nanorészecskék a művelet közben nem aggregálódtak.

A katonai bőrvédő eszközök átütés vizsgálatának gyakorlatából és követelményéből kiindulva meghatározhatjuk a C_h átütési koncentrációt, amely nem más, mint a detektálási oldalon kialakított térfogatban 24 óra alatt megjelenő Sm tömege. Ha figyelembe vesszük, hogy a vizsgálati minta felülete 5 cm^2 és egy legfeljebb 1 cm magas ilyen alapterületű hengerben helyezzük el a vizsgálatunk során használt érzékelőt, akkor a gázkromatográfós vizsgálatoknál előírt követelményt alapul véve a $C_h = 4\text{ }\mu\text{g}/\text{cm}^3/24\text{ óra}$.

Az elrendezés vázlatát a 11. ábrán szemlétetjük.



11. ábra. Javasolt mérési elrendezés az átütés vizsgálatra

1: Tesztanyag-cseppek, 2: Vizsgálati minta 3: Érzékelő 4: Indikátor műszer
5: Adatfeldolgozó egység

A vegyi érzékelő koncentráció-relatív ellenálás változás karakterisztikáját vizsgálva megállapíthatjuk, hogy $C_h = 656\text{ ppmV}$ koncentráció a lineáris regresszióval illesztett egyenes közel közepén található, ami mérés technikai kellemesnek mondható.

KÖVETKEZTETÉSEK

A TEM és EIS technológián alapuló eljárással minősített alkiltiollal stabilizált nanoarany szol bevonatú vegyi érzékelők alkalmasak definiált körülmények között a katonai bőrvédő eszközök védőképességének vizsgálatára és az alkalmazott bis(2-kloroetil)szulfid tesztanyag megbízható detektálására. Erre a következtetésre alapozva javasolható a fent vázolt, vegyi

érzékelővel jelzett átütés vizsgálati módszer bevezetése, amely természetesen megköveteli az eljárás részletes kidolgozását.

KÖSZÖNETNYILVÁNÍTÁS

A szerzők köszönetüket fejezik ki Dr. Felhősi Ilonának, Trif Lászlónak, Molnár-Vörös Nikoletta és Dr. Németh Péter, az MTA Kémiai Kutatóközpont műszereinek használatáért, az eredmények értékelésében nyújtott tanácsokért, valamint az NKTH-nak a METANANO projekt támogatásáért.

Irodalomjegyzék

- [1] A. Csanády, E. Kálmán, G. Konczos: Bevezetés a nanoszerkezetű anyagok világába. ELTE EÖTVÖS KIADÓ, Budapest, 2009.
- [2] K. Kalantar-zadeh, B. Fry: Nanotechnology-Enabled Sensors. Springer Science+Business Media, LLC, New York, 2008.
- [3] P. Pang, J. Guo, S. Wu, Q. Cai: Humidity effect on the dithiol-linked gold nanoparticles interfaced chemiresistor sensor for VOCs analysis. Sensors and Actuators B 114 (2006) 799–803.
- [4] J. Rivera-Gandí, C.R. Cabrera: Self-assembled monolayers of 6-mercapto-1-hexanol and mercapto-n-hexyl-poly(dT)18-fluorescein on polycrystalline gold surfaces: An electrochemical impedance spectroscopy study. Journal of Electroanalytical Chemistry 605 (2007) 145–150.
- [5] M. Brust, M. Walker, D. Bethell, D.J. Schiffrin, R.J. Whyman: Synthesis of Thiol-Derivatized Gold Nanoparticles in a two-phase Liquid-Liquid system, J. Chem. Soc., Chem. Commun. (1994) 801-802.
- [6] A.W. Snow, H. Wohltjen: Colloidal Metal-Insulator-Metal Ensemble Chemiresistor Sensor Anal. Chem. 1998, 70, 2856-2859
- [7] R.R. Smardzewski, N.L. Jarvis, A.W. Snow, H. Wohltjen: "Metal-Insulator-Metal Ensemble (MIME) Chemical Detectors", Nanotech2004 Nanotechnology Conference & Trade Show, Proceedings Vol. 3, pp. 163- 4, Boston, 7-11 March 2004.
- [8] M.G. Ancona, A.W. Snow, E.E. Foos, W. Kruppa, R. Bass: Scaling Properties of Gold Nanocluster Chemiresistor Sensors. IEEE Sensors Journal, vol. 6, No. 6, (2006).
- [9] N.Molnár Vörös, R. Patakfálvi, I. Dékány: Alkylthiol-functionalized gold nanoparticles for sensing organic vapours: The connection between the adsorption isotherm and the sensor resistance. Colloids and Surfaces A: Physicochem. Eng. Aspects 329 (2008) 205–210.
- [10] J.M. McIntyre, H.Q. Pham: Electrochemical impedance spectroscopy; a tool for organic coatings optimizations Progress in Organic Coatings 27 (1996) 201-207.
- [11] Készítette: L. Trif,

[12] Mérte: P. Németh

[13] Halász, L.; Grósz, Z.: ABV védelem; Egyetemi jegyzet, ZMNE, Budapest, 2001

[14] Mérte: I. Felhősi

Berkovics Gábor
berkovics.gabor@zmne.hu

THE APPEARANCE, DEVELOPMENT AND SITUATION OF AIR DEFENSE ARTILLERY (ADA) IN HUNGARY UNTIL THE TRIANON PEACE TREATY

Absztrakt/Abstract

Az első világháború kezdetéig számos légi cél fejlesztése történt meg nagyon rövid idő alatt. 1900-ban megépült az első irányítható Zeppelin típusú léghajó, és Németországban egy léghajó zászlóalj jött létre. A Wright testvérek, Wilbur és Orville, motoros repülőjének megjelenése egy hatalmas lépés volt a repülés történetében. 1903. szeptember 14-i sikeres kísérletük a katonai vezetés figyelmét arra hívta fel a, hogy a ezek az eszközök katonai téren is kiválóan alkalmazhatóak. Főként a németek és a franciák fordítottak nagy figyelmet erre a tényre. Röviddel az után, hogy első repülőgépek megjelentek a háborúban, megjelent a légvédelem is. jelen írás a légvédelmi tüzéség magyarországi fejlődésével foglalkozik az I. világháború végéig.

Until the World War the development of various air targets was extremely fast. In 1900 the first steerable ZEPPELIN-type airship was built and in Germany an airship battalion was formed. The work of the Wright brothers, Wilbur and Orville, practically the appearance of engine airplane, was a huge step in the history of flying. Their successful experiment on 14 September 1903 called the attention of military leaderships on these devices, of which military utility was obvious. Mainly the German and the French paid great attention to them, and, even if with not as huge priority. Shortly after the first use of airplanes in war, the air defense had appeared. This paper deals with the development of air defense artillery in Hungary until the end of World War I.

Kulcsszavak/Keywords: légvédelem, első világháború ~ air defense, World War I.

THE APPEARANCE AND DEVELOPMENT OF AIR DEFENSE ARTILLERY UNTIL THE WORLD WAR I.

Almost at the same time as the Montgolfier brothers' balloon appeared and was used in military (reconnaissance) came up the idea and also the practical realization of fighting against it too. The successful balloon-experiment on 5 June 1783 was followed by I.C.G. Hayze Prussian engineer's book in 1784, in which he dealt with the usage of this new military

device. In this writing there are some parts about counter-intelligence as well. Out of the weapons of those times he pointed out rifle, howitzer, mortar and rocket as possible and effective tools. It neither took long that the artillery should be used in air defense. No longer than in 10 years the Austrians too shot a French balloon with their cannons on 13 June 1794 near Mabeuge.¹ The shots of the 2 howitzers were against the device and its staff spying on the fortress. The principle, which later got a role in the usage of ADA, emerged even then: the defensive force didn't so much necessarily try to eliminate the air device as they rather wanted to encourage their troops by shooting and scaring away the staff of the balloon, also to deprive the enemy from reaching its desired aim (which was practically reconnaissance these times). The elimination of the balloon was, naturally, unsuccessful.

The next notes are from 80 years later, from the 1870-71 Prussian-French war. The Germans blockaded Paris. The French used balloons to keep in touch with and send mails to the rest of the country.² To stop it The Germans assembled a 3.7cm "balloon-repelling cannon". 5 cannons like that were built and carried on carts. Their efficiency was still not good enough. Out of the 66 launched balloons the Germans could shoot down probably(!) only one on 12 Nov 1870.

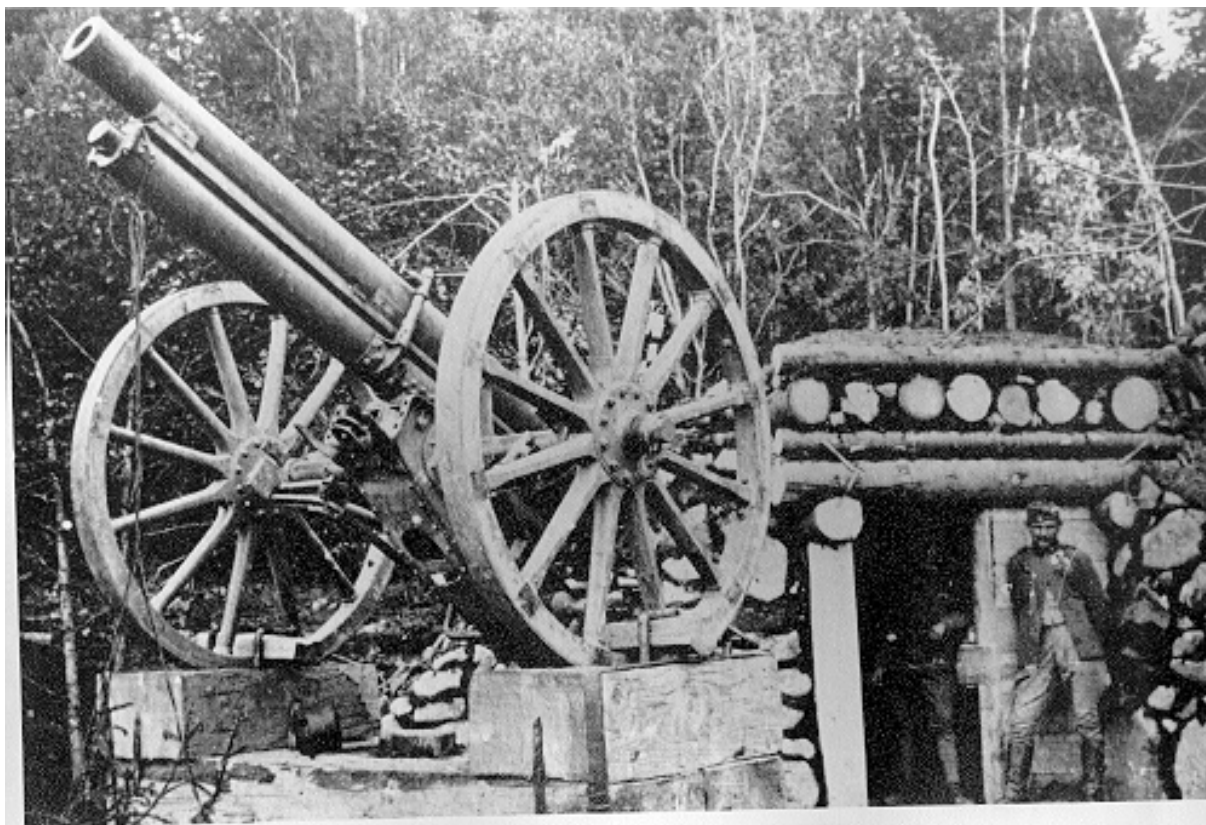
Until the World War the development of various air targets was extremely fast. In 1900 the first steerable ZEPPELIN-type airship was built and in Germany an airship battalion was formed. The work of the Wright brothers, Wilbur and Orville, practically the appearance of engine airplane, was a huge step in the history of flying. Their successful experiment on 14 September 1903 called the attention of military leaderships on these devices, of which military utility was obvious. Mainly the German and the French paid great attention to them, and, even if with not as huge priority, they also started to deal with effective counter-intelligence.

In 1909 Blériot managed to fly across the La Manche Canal and by this act the relative protection of England (by their fleet) started to disappear. In the major French, Russian, German and Austro-Hungarian trainings, airplanes were used as reconnaissance and mail service as well.

To the question of 'How can these devices be repelled?' there were 2 answers then. The first was: by the aircraft itself. But then again the effective shooting was not solved yet. The other possibility – naturally not excluding the 1st one but being developed at once – was to develop the artillery and eliminate the air targets. These questions were also discussed by every European power, but with much smaller emphasis, compared to aircrafts. The Austro-Hungarian and German military leadership wanted to solve it mainly by camp and fortress artillery. Even though the Austro-Hungarian Monarchy experimented on creating special devices since 1894, these were not successful. In SKODA factory an "air vehicle antimissile" was planned in 1910 but its production started only way too later. So when the world war started, the Monarchy didn't own an antimissile.

¹ Siménfalvy Tihamér főhadnagy: A léghajó a tábori és várharcban. Magyar Katonai Közlöny (MKK) 1909/11. page 1016

² Same as previous page 1017



Picture 1. Camp artillery device on an off-the-cuff air defense shooting display

The German put much more emphasis on the issue of air defense by cannons. In the 1906 year's car exhibition they introduced a middle cornered 5cm air-balloon-repelling gun built on an armoured infantry vehicle. But they didn't take too much effort either on mass producing modern air vehicle repelling devices. In the beginning of the world war even Germany owned only 6 car-drawn air defense cannons and 8 horse-drawn experimental(!) air defense cannons. It may have been the French who cared most about creating an air defense artillery. They were planning cannons and munitions against air targets in 1906 and they started the practical experiments in 1907. But they still used 75M cannons for this for a long time during the war.

AIR DEFENSE ARTILLERY DURING THE WORLD WAR

In the beginning of the war, except for the German, practically no armies owned a device especially constructed to repel an air target. But it soon turned out that using an aircraft for military purpose – even if not by direct strikes but by reconnaissance, messenger and spotting correction activities – can cause serious damages. The first mass produced cannons used specifically for air defense were made by the German since 1916, with the cubic measures of 8 cm, 8.8 cm and 10.5 cm. By the end of the war they had 197 times more air defense cannons than in the beginning of the war (2576 pieces).

As the Austro-Hungarian Monarchy didn't have any air defense cannons, they tried to use the ones they looted from the Russians against air targets. Primarily the 5M and 5/8 M type camp cannons, later of which the latter had a longer history in Hungary. Because of their being unsuccessful, firstly the general staff of the Monarchy commandeered 3 air defense

cannons which were made for Holland and Romania in SKODA factory.³ After that they ordered to mass produce the type. These were horse-drawn air defense cannons assembled with the barrels of 5/8Ms. Later Hungary inherited some of them. The 14M8 type air vehicle repellent cannons looted from the Russians were also successful. During the war the 8cm 17M camp cannons were also developed into air defense cannons. The classic, camp and fortress cannons were difficult to use as air defense cannons. For the flying attributes of air warfare devices, neither their side-angle nor their angle of elevation manoeuvrability was satisfying. To compensate it, firstly primitive solutions, later less primitive ones were introduced. Placing the cannons on off-the-cuff displays then later on scaffoldings widened the possibilities somewhat, but the effectiveness and its improvement was still far behind even the minimal expectations. Only the production of the cannons specifically prepared for air defense targets with KÖZÉSARKAS technique solution and building them on vehicles brought some real change.

From 1915 not only the technical improvement started but the operational one too. Firstly, some air defense subunits were established, then, from 1917 batteries used in air vehicle repelling were set up within the artillery regiment as its 5. battery. They consisted of 2-2 pieces of 14.O.M. cannons. In 1918 all infantry divisions had a camp cannon regiment. Every second regiments 5th battery was an air defense one.⁴ The 1 November 1918 'Army Arrangement Table' shows the revaluation of this branch, in which the home-defense troops had the following power:

- 13 pieces of 8cm anti-aircraft guns for the heavy artillery regiments;
- 75 pieces off-the-cuff 8cm anti-aircraft guns for the defence of the cities, for the camp artillery regiments and for the heavy artillery regiments;
- 16 pieces off-the-cuff 8cm anti-aircraft platoons for the camp artillery regiments;
- 1 piece of 7cm motorized cannon;
- 1 piece of 2cm automatic gun platoon;
- 1 piece of 3.7cm automatic gun platoon;
- 1 piece of 7 ½ Italian anti-aircraft cannon.⁵

It is worth saying some words about the effectiveness of the air defense artillery during the World War I. In 1914 to shoot down a target approximately 11000 shots were needed, in 1918 about 3500. The ADA shot down the 18-20% of the total eliminated targets.

³ Dr. Barcy Zoltán: A magyar légvédelmi tüzérség fejlesztése és rejtése 1922-1938. Hadtörténeti Közlemények 1985/4. page 878

⁴ Dr. Varga József: A légvédelmi tüzérség története a kezdetektől a második világháború végéig. Magyar Honvédség Légvédelmi Rakéta- és Tüzérfőnökség kiadványa, 1996., page 28

⁵ A Magyar Tüzér. page 142



Picture 2. Camp artillery device in off-the-cuff air defense shooting position

We can say that by the end of the war the air vehicle repellent devices, especially the cannons got bigger role and more emphasis in the battles. But they didn't get independent from the camp and fortress artillery in the Austro-Hungarian Monarchy. On the other hand the construction and mass production of really effective and primarily air defense cannons never happened. During the collapse the majority of the Monarchy's cannons used in air defense either got destroyed or got taken away by the enemy. So the Hungarian Republic of Council too owned only ten cannons suitable for air defense. Four of them were 14M, six were 5M. They were going to protect the capital and the 43. artillery regiment with its five air defense batteries was also set up.⁶

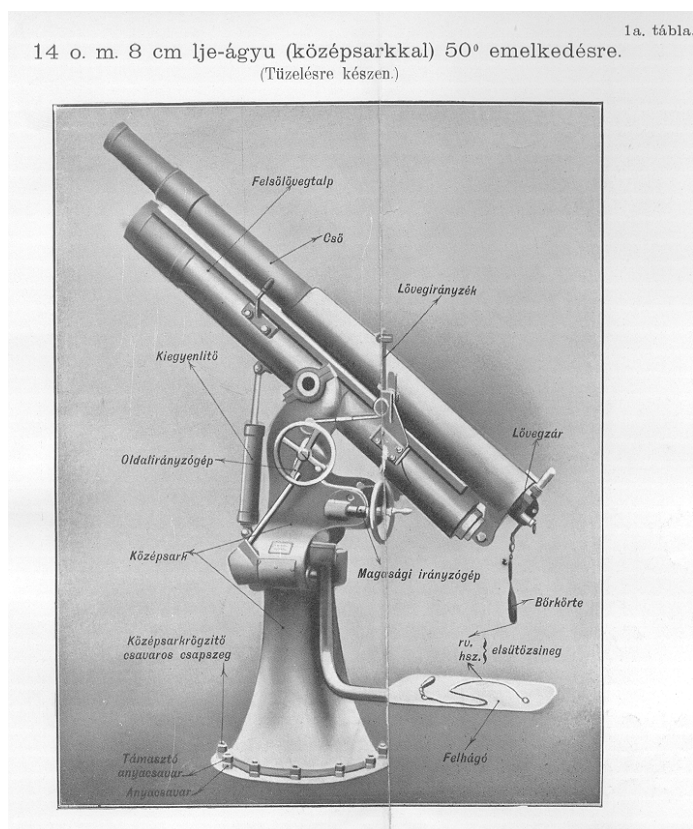
THE HUNGARIAN ADA UNTIL TRIANON⁷

After the fall of the Republic of Council the country was divided into seven military regions. Though, this was only a theory for a while because the Romanians didn't withdraw their troops from Duna-Tisza köze and Trans-Tisza until the December 1919. So by the end of the year only four military regions were formed, in Budapest, Székesfehérvár, Kaposvár and

⁶ Dr. Varga József: im. page 35

⁷ Dr. Barcy Zoltán: im. page 877-878

Szeged. There were no aircraft-repellent cannons in the order of battle. The reason for this was mainly the shortage of cannons. In the beginning of 1920 a resolution was passed to set up a 2-cannon 14M material 'repel' training batteries within the will-be-formed artillery trainee regiment.



Picture 3. 14 O.M air defense cannon

The cannons were taken down the armoured trains. The troops practically didn't have air defense in the plans to get back the Hungarian regions. Though, the leadership wanted to solve the protection of the capital by all means, as far as possible. In August 1920 the Ministry of Defense ordered to set up the 'Aircraft-repellent Battery of Budapest Gun Battalion'. It consisted of four pieces of 14M air vehicle repellent cannons and one piece of 75M signal cannon. The battalion appeared in the November order of battle in the Budapest division as the 4th battalion of the artillery regiment. Truly enough, there were only 3 pieces of 8cm cannon and 1 piece of 7.5cm one here. Besides, 'Gellért Guard' also had two air defense cannons.⁸

The Ministry of Defense was going to set up seven infantry battalions and one horse battalion. They would have got one four-cannon aircraft repellent battalion each. Furthermore, they were going to send a 'Training battalion' with four cannons into the order of battle. The Hungarian Army owned only ten cannons out of the 36 ones that would have been necessary for these plans. There were no particular hopes for it to be able to make it up. So this quite poor inheritance was strongly felt in quantitative and qualitative points of view as well between the two world wars, especially in the 20s.

The Peace Treaty, which was signed on 4 June 1920 and came to life on 26 July 1920 by all means "solved the problem" of air defense artillery for a long time. The treaty sent

⁸ Hadtörténeti Levéltár (HL), HM A.o.1. tétel 69019. 1920.

Hungary into a complete hopeless situation in the field of military. Air defense, excluded its passive form, was completely forbidden.

The Vth part of the 'Hungarian Peace Treaty', the 'Instructions for the military, warship and airship' was dealing with the artillery. 104 section 3. paragraph stated the Hungarian armed forces can only own cannons according to the Vth Table. So all in all 105 cannons with 1000 bullet-munition. The usage of bigger than 105 mm devices were banned. As the Vth part 1st chapter 108. section stated: 'All troops not mentioned in this Table are forbidden', Hungary was not allowed to have either aircraft forces or air defense cannons. The XIth part which dealt with 'Air transport' stated in its 260. section that 'The air vehicles belonging to the allied and accompanied forces are allowed to fly above and land on the whole territory of Hungary...' The 117th section stated that the "all the weapons, munitions and war materials exceeding the allowed amount, including all the aircraft-repelling devices' must be surrendered.⁹

Bibliography

Dr. Barcy Zoltán: A magyar légvédelmi tüzérség fejlődése a Horthy korszakban. HL, Tanulmánygyűjtemények

Cziegler István: A légvédelmi tüzérség keletkezése és fejlődése. MKK 1930/12

Dombrády Lóránd – Tóth Sándor: A magyar királyi honvédség 1919–1945. Zrínyi Katonai Kiadó, Budapest 1987.

Dömötör Gergely: A fegyvernemek szerepe a Tanácsköztársaság harcaiban. Hadtörténeti Közlemények 1954/3-4

Groehler, Olaf: A légi háborúk története 1910–1970. Zrínyi Katonai Kiadó, Budapest 1980.

Dr. Varga József: A légvédelmi tüzérség története a kezdetektől a második világháború végéig. Magyar Honvédség Légvédelmi Rakéta- és Tüzérfőnökség kiadványa, 1996.

A Magyar Tüzér, Reé László könyvkiadó és terjesztővállalat, Budapest 1938.(?)

Source of pictures: Hadtörténeti Intézet és Múzeum

⁹ A Magyar Békeszerződés, Kiadja a M.Kir. Külügyminisztérium Bp. M. Kir. Tud. - Egyetemi Nyomda 1920.

Horváth Attila
horvath.attila@zmne.hu

A REPÜLŐTEREK ÉS A LÉGIIRÁNYÍTÁS, MINT KRITIKUS INFRASTRUKTÚRÁK

Absztrakt

A tanulmány a repülőterek elleni terrortámadások tapasztalataival foglalkozik. A szerző a repülőgépek ellen elkövetett szabotázs akciókat és a repülőgép-eltérítéseket csak olyan esetben érinti, ha azok a repülőtereken, illetve azok közvetlen közelében következtek be. A repülőterek nem véletlenül tartoznak a kritikus infrastruktúra védelmi rendszer meghatározó alrendszereihez. A cikk a modernkori terrorizmus történetében vizsgálja a repülőterek terrortámadásokkal szembeni sérülékenységet.

The study deals with the experiences of terror attacks against airports. The author deals with sabotage actions against airplanes and hi-jacks only in case those happened on the ports or in the vicinity of them. It is not accidental that airports belong to the determinant subsystems of the critical infrastructure's system. The article examines the terror sensitivity of airports in the history of prevailing terrorism.

Kulcsszavak: *terrorizmus, légiközlekedés, repülőterek, kritikus infrastruktúra védelem, terrorism, air transportation, airports, critical infrastructure protection*

BEVEZETŐ

Az erőszak és a terror végigkísérte az emberiség történelmét. A biztonsági és biztonságpolitikai szakemberek körében szinte közhelynek számít az a megállapítás, hogy az ún. modernkori terrorizmus kialakulása a múlt század 1960-as éveinek végén elkövetett repülőgép-eltérítésekhez, illetve a repülőterek elleni terrortámadásokhoz köthető (Horváth A. 2008/a). Az 1960-as évek végén, az 1970-es évek második feléig szinte mindennaposnak számítottak a repülőgép-eltérítések és a repülőterek elleni terrortámadások. A légiközlekedés elleni terrorakciók – nem utolsósorban a szigorodó biztonsági nemzetközi előírásoknak köszönhetően – gyakorisága az 1970-es évek második felétől kezdődően jelentős mértéken csökkent. A légiközlekedés elleni terrortámadások célja nem csak az volt, hogy a repülőtereket pusztítsák, a légijárműveket, utasokat és a személyzetet megsemmisítsék (Szabó

M. 1999). A repülőterek és légijárművek elleni támadásokkal a terrorcsoportok általában a politikai céljaikat akarták megvalósítani, vagy azoknak a médián keresztül nyilvánosságot biztosítani.

A légiközlekedésben a biztonsági szint a javulása, valamint a repülőgépek és repülőterek elleni terrortámadások ritkulása nem jelentette azt, hogy az 1970-es években megszűnt volna az alágazat terrorfenyegetettsége. Ezért nem tekinthető véletlennek, hogy az 1990-es években az Egyesült Államokban megjelenő kritikus infrastruktúra védelem fogalmi rendszerében a légiközlekedés, és ezen belül a repülőterek kiemelt helyet és szerepet kaptak. A fogalom és a hozzá kapcsolódó feladatok akkor váltak ismertté, amikor Clinton elnök 1998 májusában kiadta a 63. számú elnöki direktíváját (Presidential Decision Directive). A dokumentum életbe léptetésére azért volt szükség, mert az 1990-es években világossá vált, hogy a nemzetközi terrorizmus komolyan veszélyezteti az Egyesült Államok infrastrukturális rendszerét és szolgáltatásait (Horváth A. 2009). A terrorfenyegetettség és a bekövetkezett katasztrófák tapasztalatai függvényében az alapidokumentumnak tartható direktíva kiadása óta természetesen változott a kritikus infrastruktúra védelmének tartalma, azonban a légiközlekedés biztonsága ma is kiemelt helyet foglal el a rendszerben (J. D. Moteff. 2008).

Közlekedésműszaki értelemben a repülőterek funkcióit az alábbiakban lehet összefoglalni: itt történik a légijárművek indítása, fogadása, a földi mozgatásuk, a repülőgépek kiszolgálása, az utasok kiszolgálása, valamint a teherforgalommal kapcsolatos logisztikai folyamatokat is itt végzik (Havas P. 2004). Közlekedésüzemi és biztonsági szempontból talán egyetlen közlekedési alágazatban sincs olyan jelentősége a termináloknak, mint a légiközlekedésben a repülőtereknek. Üzemzavarok, rendkívüli helyzetek keletkezésekor, terrortámadás bekövetkezésekor a közlekedés pályáján, vagyis a levegőben, a repülőgépek személyzetének, illetve a földi kiszolgálóknak és a légiirányítóknak csak korlátozott mértékű beavatkozásra van lehetősége. Különösen igaz ez a terrorcselekményekre, hiszen a terroristák a fegyvereiket, robbanóanyagait csak a repülőtereken keresztül tudják felcsempészni a légijárművekre. Biztonsági szempontból ugyan az is igaz, hogy a rakétatámadások kivételével a terroristák csak a repülőtereken juthatnak fel a repülőgépekre, és csak ott csempészhetik fel a támadáshoz szükséges fegyvereket és felszereléseket is. Ezért nem csak a repterek, hanem a légiközlekedés egésze szempontjából fontos kérdés a terminálok biztonságának szavatolása.

A modernkori terrorizmus történetében a terrorfenyegetettségnek kitett célpontok a repülőtereken:

1. repülőgépek a kifutópályákon, vagy gurulópályákon;
2. az induló és érkezési csarnokok;
3. a légiirányítási és radarberendezések.

A REPÜLŐGÉPEK ELLENI SZABOTÁZSAKCIÓK TAPASZTALATAI

Az 1960-as évek végén a terroristák először nem csak a repülőgép-eltérítésekkel, hanem a repülőgépek repülőtereken való fegyveres támadásával próbálkoztak. Ezek a kísérletek, azonban nem voltak igazán sikeresek. Jó példát jelent a Népi Front Palesztina Felszabadításáért (PFLP) nevű terrorcsoport támadása Svájcban, a zürichi nemzetközi repülőtérén 1969. február 18-án. A szervezet négy fegyveres támadója gépkocsival hajtott rá a repülőtér kifutópályájára és a fegyvereikből 200 lövedéket lőttek ki, valamint gyújtógránátokat dobtak az El Al izraeli légitársaság Zürichből Tel Avivba tartó felszállás közben levő repülőgépére. A palesztin gerillák és a repülőgép biztonsági személyzete között tűzharc alakult ki, amelynek során egy támadó meghalt, hárman sebesültek, a járat három

utasa is megsebesült.¹ Ez az eset rávilágított arra, hogy egy viszonylag nagy sebességgel felszálló repülőgépet megállásra lehet kényszeríteni, de kézifegyverekkel nehéz feladatot jelent elpusztítani. Ennek az esetnek a tanulságait valamennyi olyan terrorcsoport levonta, amelyek a repülőgépek ellen szándékoztak terrorakciókat végrehajtani. A terroriszervezetek ezután a gyakorlatilag sikertelen kísérletet követően hasonló módszerrel már ritkábban próbálkoztak. A következő években a terroristák inkább a repülőgép eltérítések módszerét választották. Az esetnek másik tanulsága is volt. Az El Al izraeli légitársaságnál a légiközlekedés elleni terrorfenyegetettség jelenségének észlelése után viszonylag gyorsan alkalmaztak ún. úti marsalokat, akik ezúttal sikeresen elhárították a terrortámadást. Természetesen a polgári légi járatokon nem oldhat meg minden veszélyhelyzetet még egy jól kiképzett és jól felszerelt biztonsági személyzet sem, de a terroristákat visszatarthatja a repülőgépek elleni terrorakcióktól.

A repülőgépek elleni terrortámadásokkal kapcsolatban nem elég csupán a repülőterek üzemi területeinek biztonságáról gondoskodni. Napjainkban szinte lehetetlen megbecsülni azoknak – a főként amerikai és szovjet fejlesztésű a föld-levegő rakétáknak – a számát, amelyeket az illegális fegyverpiacokon komolyabb nehézség nélkül be lehet szerezni. Ezeknek a részben elavult, részben korszerű föld-levegő rakétáknak az alkalmazása (használata) elsősorban a repülőterek közelében komoly veszélyt jelenthet a fel és leszálló repülőgépek számára. A hordozható, vállról indítható föld-levegő rakéták kezelése könnyen elsajátítható, emiatt is valós fenyegetettséget jelenthetnek a katonai és polgári légiforgalomban egyaránt.

A repülőgépek elleni rakétatámadások veszélye nem csak a válságövezetekben áll fenn, bár azokon a területeken a repülőterek fenyegetettsége kétségtelenül nagyobb, mint a világ más térségeiben található repülőtereken. Ezért Afganisztánban, Irakban, Kasmírban, Pakisztánban ahol a terrorfenyegetettség napi veszélyt jelent, a repülőterek biztonsági ellenőrzését ki kell terjeszteni azokra a területekre is, ahonnan a föld-levegő rakétákat a fel- és leszálló repülőgépekre indíthatják.

A terrortámadásoknak ez a formája szerencsére még nem tekinthető gyakorinak, ezért a válságövezetekeken kívül a biztonsági zónákon a fokozott folyamatos katonai és rendőri jelenlét nem szükséges. A terrorfenyegetettség szintjének emelkedésekor azonban haladéktalanul gondoskodni kell ellenőrzés megszigorításáról, amelyet ki kell terjeszteni a repülőterek környékére is. Ilyen eset történt 2003. február 12-én, amikor a brit titkosszolgálat arról tájékoztatta az Egyesült Királyság kormányát, hogy az al-Kaidával kapcsolatban álló iszlám szélsőségesek Sam-7-es rakétákat csempésztak be Angliába. A brit kormány haladéktalanul elrendelte a Heathrow Nemzetközi Repülőtér őrzésének a szigorítását. A rendkívüli biztonsági intézkedések nyomán a veszélyhelyzet ideje alatt 1000 katonával és rendőrrel ellenőrizték a környékbeli utakat és településeket.² Ilyen váratlan esetek kezelésére minden államnak és forgalmas nemzetközi repülőtérnek fel kell készülnie. A repülőterek és azok környékének biztonságát nem csak katonai és rendőri ellenőrzésekkel lehet biztosítani, hanem pl. a CCTV rendszerek kiépítésével és működtetésével is.

A föld-levegő rakéták elleni védelemre, azonban nem csak a repülőtereket biztonsági rendszerét kell felkészíteni, hanem szükség esetén repülőgépeket is el lehet látni rakéta-elhárító berendezésekkel. Ez a megoldás meglehetősen költséges, de eredményes lehet. Ez már néhány esetben bebizonyosodott. Jó példát jelent erre a 2002. november 28-án Kenyában történt eset. Ezen a napon a Paradise Hotelben történt robbantással szinte egy időben a Mombasa Nemzetközi Repülőtértől 8 mérföldnyire délre, terroristák két rakétát lőttek ki az El Al izraeli légitársaság utasszállító chartergépre. A rakéták szerencsére a repülőgépre szerelt

¹ Forrás: <http://www.tkb.org/Incident.jsp?incID=110> (letöltés: 2005. 12. 16). Megjegyzés a MIPT terrortámadásokkal foglalkozó adatbázisa a <http://www.mipt.org> web oldalon érhető el.

² Forrás: <http://www.guardian.co.uk/uk/2003/feb/13/september11.terrorism> (letöltve: 2005. 12. 15).

rakéta-elterelő rendszernek köszönhetően célt tévesztettek. A Paradise Hotelnél történt robbantás és a repülőgép elleni támadási kísérlet jól megszervezett és összehangolt akció volt, hiszen nem sokkal korábban ezzel a géppel érkeztek azok az izraeli turisták akik ellen a robbantásos merénylet irányult. A felszálló gép utasai pedig zömében azok kerültek ki, akik a szállodában korábban pihentek. Az izraeli utasszállító repülőgép esete is bizonyítja, hogy bár csökkent a légiközlekedés elleni terrortámadások száma, ennek ellenére „megéri” a biztonsági berendezésekre és eljárásokra pénzt költeni (Horváth A. 2008/b).

A REPÜLŐTEREK ELLENI TERRORTÁMADÁSOK TAPASZTALATAI AZ INDULÁSI ÉS ÉRKEZÉSI CSARNOKOKBAN

A repülőterek elleni támadások is meglehetősen gyakoriak voltak az ún. modernkori terrorizmus történetében. Ezeknek a száma az elmúlt évtizedekben jelentős mértékben csökkent, de a veszélyt nem csak a biztonság szigorú értelmezése, hanem az utóbbi évek szerencsére sikertelen kísérleteinek tapasztalatai alapján sem lehet lebecsülni. Az eddigi módszerek között egyaránt megfigyelhetünk robbantásos terrorakciókat és fegyveres támadásokat is. A terrortámadásokkal szemben a repülőterek talán leggyengébb pontjának lehet tekinteni az indulási és érkezési csarnokokat. Az interneten és egyéb utastájékoztatói forrásokból könnyen hozzáférhető menetrendi adatok ismeretében a terrorcsoportok viszonylag könnyen meghatározhatják, hogy mikor és melyik csarnokban „érdemes” támadniuk. Az időpont és a hely kiválasztása a cél elérése és az áldozatok maximalizálása szempontjából lehet érdekes. Budapest Ferihegy Nemzetközi Repülőtéren napjainkban már laikusok számára is jól látható, a szakmai folyóiratokban is többször közölték, hogy különleges biztonsági protokollok előzik meg pl. az El Al izraeli légitársaság jártainak az indítását, illetve fogadását. (Szabó M. 1999) Egy repülőtér elleni támadás megszervezésekor főként az alkalmazottaktól szerzett információk alapján, valamint a személyes megfigyelés tapasztalatai alapján, ma már a terrorakció kockázatát is minimalizálni tudják. Természetesen ez a megállapítás nem igaz, ha egy terrorcsoport egy szigorúbban védett légitársaság utasai ellen kísérel meg terrortámadást végrehajtani egy repülőtér termináljában. A következőkben fontosnak tartom érinteni a modernkori terrorizmus eddigi történetéből néhány terrortámadás tapasztalatait.

A légitársaságok képviselői ellen irányuló támadások tapasztalatai

A modernkori terrorizmus történetének kezdetén légitársaságok irodái ellen nem csak a Palesztin Felszabadítási Szervezethez kapcsolódó terrorcsoportok (pl. a PFLP, a Fekete Szeptember – BSO) követtek el terrortámadásokat. A palesztin terroristák a repülőgépek eltérítésén kívül főként az El Al izraeli légitársaság nyugat-európai kirendeltségei ellen követtek el robbantásos terrorakciókat. A légitársaságok irodái elleni terrortámadások a különböző európai baloldali és széparatista terrorszervezetek is körében is „népszerűek” voltak. Egyebek között a Mérges Brigádok, az ETA, és a Baader-Meinhof Csoport is gyakran fordult ehhez a polgári lakosság számára látszólag veszélytelennek látszó cselekvési formához. Ugyanis ezeknek a terrortámadásoknak az volt a közös jellemzője, hogy általában csak anyagi károkat okoztak (Horváth A. 2008/b).

Az utasok elleni terrortámadások tapasztalatai

A beszálló utasok és kísérőik, valamint a kiszálló utasokra várakozók teljes körű, mindenre kiterjedő ellenőrzését nem lehet olyan hatékonysággal elvégezni, mint a hangárok, irányítóberendezések, kifutópályák stb. őrzését. A terminálokon a terrortámadások az ott

várakozókra irányulnak. Általánosságban elmondható, hogy ezeknek az akcióknak az a közös jellemzőjük, hogy a fegyveresek válogatás nélkül lönek, vagy ott robbantanak, ahol nagyobb tömegre lehet számítani. Bár ezzel kapcsolatban azt is meg kell jegyezni, hogy a palesztin terrorcsoportok elsősorban az izraeli utasokat választották ki célpontként. Olyan szigorú check in rendszert nem lehet alkalmazni a repülőtérre való belépés előtt, mint a repülőgépekre való beszállítás előtt. Egyrészt nem lenne értelme, másrészt nehezen lehet megvalósítani, így repterek várócsarnokait a támadószándékú terroristák viszonylag könnyen megközelíthetik.

A terminálok könnyű sebezhetőségére a terroristák is hamar rájöttek. Az első súlyos következményekkel járó terrortámadást a Tel Aviv Lod Nemzetközi Repülőtéren követték el 1972. május 31-én.³ A Japán Vörös Hadsereg (JRA) nevű terrorcsoport három felfegyverzett tagja miután kiszálltak a Párizsból érkező repülőgépből a bőröndjeikből elővették a fegyvereiket, majd tüzet nyitottak a várakozó utasokra és kézigránátokat dobta feljűk. A terrorakció következtében 25-en haltak meg és 76-an sebesültek meg.⁴ Az eset számos kérdést vetett fel, ezek közül talán az volt a legfontosabb, hogyan jutathatták fel a támadók a fegyvereiket az Air France légitársaság repülőgépére Párizsban? Az ilyen események miatt kellett és kell napjainkban is módosítani időről időre a repülés biztonságával kapcsolatos nemzetközi egyezmények biztonsági előírásait. (Horváth A. 2008/b) Ez a terrorakció azt is bebizonyította, hogy a terrorcsoportok már az ún. modernkori terrorizmus korai szakaszában is képesek voltak nemzetközi szinten együttműködni. A véres terrorakció, mint utólag kiderült, kapcsolódott a hírhedtté vált az 1970. szeptember 6-án kezdődő Dawson Field-i esethez.⁵ A japán terrorcsoporttal szövetséges PFLP közleményben tudatta, hogy a terrorakciót a japán terroristák a néhány héttel korábban repülőgép-eltérítése közben lelőtt társaik, illetve annak a Patrick Arguellonak az emlékére követték el, akit 1970. szeptember 6-án az El Al izraeli légitársaság Tel Aviból Amszterdam érintésével New Yorkba tartó járatán a biztonsági személyzet halálosan megsebesített.⁶ 1970. szeptember 6-án a palesztin terroristák négy Európából New Yorkba tartó repülőgépet kíséreltek meg eltéríteni. Ebből hármat sikerült Jordániába egy használaton kívüli volt brit katonai reptéren való leszállásra kényszeríteni. A szélső-baloldali nicaraguai születésű Arguellt és társát Leila Khaled szándékát azonban a biztonsági személyzet megghiúsította. A LOD nemzetközi repülőtéren történt eset egyik pikantériája az volt, hogy a PFLP elhatárolódott a japán terrorszervezettől. A terrorcsoport kiadott közleménye szerint a szövetségeseiknek ugyanis arra nem volt felhatalmazása, hogy az Air France légitársaság utasaira lőjenek.⁷

A különböző alapon szerveződő terrorcsoportok, a Tel Aviv-i eseten kívül is nagyon sok terrortámadást hajtottak végre a repülőtereken. Nyugat-Európa légikikötői közül talán a párizsi Orly Nemzetközi Repülőtér volt legjobban a terrorfenyegetettségnek kitéve, terjedelmi okokból azonban nincs lehetőségem a franciaországi incidensek elemzésére. Az 1985. december 27-én a bécsi Schwechat-i és a római Leonardo Da Vinci reptereken történt összehangolt terrortámadásokról még egy rövid tanulmányban is szükséges említést tenni. Az Abu Nidal terrorcsoport fegyveresei által elkövetett támadás következtében Bécsben 2 ember halt meg és 39-en sebesültek meg⁸, míg Rómában 16-an haltak meg a sérültek száma 99 fő

³ A terminált napjainkban Izrael Állam első miniszterelnökének, Ben Gurion a nevét viseli.

⁴ Forrás: <http://www.tkb.org/Incident.jsp?incID=430> (letöltve: 2005. 12. 15).

⁵ Ezzel kapcsolatban lásd bővebben: Horváth A. 2008/a: A polgári repülőgépek elleni terrortámadások tapasztalatai. Repüléstudományi Közlemények. A Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Repülő és Légvédelmi Intézet on-line folyóirata. Szolnok, 2008. pp.: 14. URL cím: <http://www.szrfk.hu/rtk/>

⁶ Forrás: <http://www.tkb.org/Incident.jsp?incID=430> (letöltve: 2005. 12. 15).

⁷ Forrás: <http://www.tkb.org/Incident.jsp?incID=430> (letöltve: 2005. 12. 15).

⁸ A sérültek között magyar állampolgár is volt, Szegedi Molnár Géza előadóművész, aki egy izraeli fellépésre utazott volna az osztrák fővárosra a keresztül. A 2008. márciusában elhunyt művész a tüzharcban gerinclövést kapott és deréktól megbénult.

volt.⁹ A Jasszer Arafattal szembeforduló Abu Nidal vezette csoport az al-Kaida megjelenése és megerősödése előtt talán a legfélelmetesebb terrorszervezet volt. Egyes feltételezések szerint a bécsi akció eredeti célja egy repülőgép eltérítése lett volna, amelyet később Tel Aviv légtérében akartak felrobbantani. Ez a terv azonban a reptéri biztonsági emberek éberségének köszönhetően hiúsult meg. A terrorcsoport szervező készségére és a végrehajtók fegyelmezettségére jellemző, hogy a korabeli telekommunikációs viszonyok között egyszerre két különböző ország fővárosának repülőterén voltak képesek súlyos következményekkel járó terrortámadást végrehajtani (Horváth A. 2008/b).

Figyelmeztetés az Egyesült Államoknak és az Egyesült Királyságnak

A repülőterek indulási és érkezési csarnokai elleni akciók közül még két terrorakció kísérlet tárgyalása látszik szükségesnek. Az első az ún. modernkori terrorizmus történetének legsúlyosabb terrortámadás-sorozata 2001. szeptember 11-e előtt 15 hónappal történt Los Angelesben. A metropolisz nemzetközi repülőtere (LAX) a világon személyforgalom szempontjából az ötödik, az áruforgalmat tekintve pedig a hatodik legforgalmasabb repülőternek számít. (D. Stvens et. al. 2006) Nem lehet véletlennek tekinteni, hogy a terminál kiemelt helyet foglal el az Egyesült Államok kritikus infrastruktúra elemei között. A kitüntetett figyelmet nem csak a személy- és áruforgalom nagysága, hanem a légikikötő biztonsági helyzete is indokolta.¹⁰ A terminál ellen többször kíséreltek meg terrortámadást, az első robbantásos merényletet az ún. „Alphabet Bomber”-nek nevezett – jugoszláv származású – Muharem Kurbegovic követte el. A gyúlékony anyagokat tartalmazó robbanószerkezet működésbe hozása 1974 augusztusában három ember halálát okozta, és 36-an sebesültek meg. (D. Stvens et. al. 2006) Ugyanitt 1982 májusában robbanószerkezet elhelyezését kísérelte meg a Titkos Örmény Hadsereg Örményország Felszabadításáért (ASALA) nevű szervezet is.¹¹

1999. december 14-én a világ közvéleményét megdöbbenetette a médiában későbbiekben csak az ún. „Millennium Bomber”-nek hívott, Ahmed Ressam algériai származású férfi letartóztatása. Ressam 1998-ban az al-Kaida terrorszervezet egyik kiképző táborában, Afganisztánban kapott kiképzést. (The 9/11 Commission Report) A férfinak és támogatóinak az volt az elképzelése 2000. január 1-jén robbantanak (innen ered a millenniumi robbantó elnevezés) a Los Angeles-i nemzetközi repülőtéren.

Az Oszama bin Laden által vezetett al-Kaida terrorszervezet ebben az időben már túl volt néhány külföldi amerikai érdekeltség elleni sikeres támadáson. Ezek közül a közel azonos időben az Egyesült Államok kenyai és tanzániai nagykövetségei ellen végrehajtott öngyilkos merényletek jártak a legsúlyosabb következményekkel. Nairobiban és Dar es Salaamban a tehergépkocsikba rejtett robbanószerkezetek felrobbanása 224 halálos áldozatot követelt. A diplomáciai képviselők elleni öngyilkos merényletek egyúttal megmutatták azt is, hogy az Oszama bin Laden vezette al-Kaida befolyása növekszik és már nem csak a Közel-Keleten és az Öböl-térségében képesek az Egyesült Államok érdekeltségeit támadni. A Los Angeles-i repülőtér elleni terrortámadással Oszama bin Ladennek nyilvánvalóan az volt a célja, hogy megmutassa az al-Kaida már képes az iszlám „első számú ellensége”, az Egyesült Államok

⁹ Forrás: <http://www.tkb.org/Incident.jsp?incID=4452>, <http://www.tkb.org/Incident.jsp?incID=4453> (letöltve: 2005. 12. 15).

¹⁰ A biztonsági szakértők és a közlekedési szakemberek a légikikötőt napjainkban is az Egyesült Államok a legsérülékenyebb, viszonylag könnyen támadható közlekedési kritikus infrastruktúra elemei közé sorolják.

¹¹ Ez a terrorcsoport főként az 1980-as években több sikeres merényletet követett el Nyugat-Európában is, elsősorban Franciaországban. Egyik legemlékezetesebb akciójukat a párizsi Orly Nemzetközi Repülőtéren hajtották végre 1983. június 5-én. Az elkövetők a robbanószerkezetet egy túlsúlyos poggyászban helyezték el, amelyért állítólag még 65\$ pótdíjat is fizettek. A detonáció, amely a terminál bőronszállítóján következett be 7 halálos áldozatot követelt és 56-an sebesültek meg. A szakirodalomban a szervezetet egyébként Orly Csoport néven is szokták említeni.

területét is támadni. A tervek szerint Ressaam az utas-terminálon belül négy időzítő szerkezettel ellátott pokolgépet hozott volna működésbe. Egyértelmű volt az is, hogy a támadás kitalálói az áldozatok maximalizálására törekedtek, mert Újévet megelőző és az azt követő napokban az amerikai repülőtereket általában zsúfoltság jellemzi. Az időpont megválasztásának szimbolikus jelentősége is volt. Egy, a keresztény időszámítás 2000. évének és a nyugati média által eltúlzott millenniumnak az első napján sikeres merénylet csapásként lehetett volna értékelni a kereszténység egészére és a nyugati életformára is. Szerencsére ez a támadási kísérlet a Jordániából származó titkosszolgálati információknak, illetve az amerikai határőrök éberségének köszönhetően megghiúsult.

A másik eset 2007. június 17-én történt Glasgowban. A skót nagyváros repülőterének indító csarnokába egy égő Jeep Cherokee kísérelt meg behajtani. A gépkocsi olyan volt, mint egy hatalmas Molotov-koktél, vagy egy égő emberi fáklya. Szerencsére a gépkocsi nem robbant fel, csak kiégett.¹² Az akció része volt annak terrortámadás a sorozatnak, amelyet fundamentalista muzulmán orvosok az Egyesült Királyságban kíséreltek meg végrehajtani. A gépkocsit gáztartályokkal szerelték fel és két elkövető minden bizonnyal a zsúfolt várócsarnokban akarta felrobbantani. (Joint Homeland Security Assessment 2007)

A Glasgowban történt merényletkísérlet egyik tanulsága az volt: a terroristák a repülőterek elleni terrortámadások számának csökkenése ellenére nem mondtak le, arról, hogy a légiközlekedés létesítményeit pusztítsák. Ennek sikere érdekében egyre radikálisabb eszközöket és módszereket választanak. Nem lehet tudni pontosan, Glasgowban milyen következményekre számítottak a terroristák. A szakértők szerint egy esetleges sikeres robbantás emberek százainak az életét követelte volna. Ezért a kritikus infrastruktúra elemek között a repülőtereket továbbra is kiemelten kell kezelni. A repülőterek biztonságára komoly veszélyt jelenthet, ha a terrorcsoportok a légikikötőkben is öngyilkos merényleteket alkalmaznak. Az öngyilkos merényletek megakadályozása rendkívül nehéz feladatot jelenthet a biztonsági szakemberek és a hatóságok számára. A kamikaze módjára támadó terroristák elleni védelem jelenleg még szinte megoldhatatlan feladatot jelent, mert az öngyilkos merényletök több szempontból is helyzeti előnyben vannak.

Az Egyesült Királyságban dolgozó orvosok merényletkísérlet-sorozata sokkolta a brit közvéleményt. Olyan orvosok váltak terroristává, akik arra esküdtek, hogy még a legnehezebb körülmények között is emberi életeket mentsenek. Az Angliában és Skóciában az 2007. június végén történt események egyben figyelmeztetést jelentettek abban a tekintetben is, hogy a radikális iszlám fundamentalisták már képesek a középosztály és a magasan kvalifikált értelmiségiek közül tagokat toborozni. A titkosszolgálatok dolga is egyre nehezebbé válik, ma már szinte lehetetlen a régi klisék és módszerek alapján felrajzolni a potenciálisan terrorcselekményt elkövetők profilját.

A LÉGIIRÁNYÍTÁS ÉS MÁSHATÁRATOKAI RENDSZEREK ELLENI TÁMADÁSOK VESZÉLYEI

A légiirányító berendezések elleni terrortámadásokat nem tekinthetjük gyakorinak a terrorizmus eddigi történetében. A felületes elemzők könnyen juthatnak arra a megállapításra, hogy a légiirányítás terrorfenyegetettségének alacsony szintje főként annak köszönhető, hogy ezeket a berendezéseket a repülőterek jól védhető üzemi területein helyezték el. A repülőterek üzemeltetői szinte mindenhol a világon nagy gondot fordítanak az irányító tornyok és radarok védelmére. A biztonsági kérdésekben kicsit is járatos emberek körében joggal merülhet fel a kérdés: minden radar, minden berendezés védelme biztosított? A repülés biztonságát szavatoló repülőtéren kívüli radarok fizikai védelme az illetéktelen behatolók

¹² Forrás: <http://www.guardian.co.uk/terrorism/story/0,,2115693,00.html> (letöltve: 2005. 12. 16).

ellen megoldottnak tekinthető, de egy fegyveres csoport számára nem jelenthet akadályt a radar állomások elfoglalása.

A légiközlekedésben a légiirányító berendezések különlegesen érzékeny és sebezhető elemnek számítanak, ezért kiemelten kell kezelni a ezeknek a védelmét és üzembiztonságát. Napjainkban szerencsére csupán hipotetikus veszélynek lehet tekinteni a légiközlekedés elleni hackertámadásokat, vagy a cyberterrorizmus eszközeivel való beavatkozásokat. A veszélyt azonban komolyan kell venni, mert a cybertérben elkövetett terrorakciók nem csak káoszt, hanem katasztrófhelyzeteket is képesek előidézni. A terroristáknak a légiirányítás rendszerében való sikeres közbelépése beláthatatlan következményekkel járna a nemzetközi forgalom egészére.

A légiközlekedésben nem elég az informatikai rendszerek biztonságát a légiirányítás létesítményeire és berendezéseire kiterjeszteni. A terrorcselekmények megelőzése szempontjából is kiemelten kell kezelni a check-in, és a poggyászkísérés informatikai rendszereit. (Kovács L., Krasznay Cs. 2009) Az utastájékoztató rendszerek biztonságáról is fontos gondoskodni, mert az ezen a területen az esetleges sikeres behatolás, olyan kaotikus helyzeteket idézhetnek elő, amelyek a terroristáknak kedvezhetnek.

A MEGELŐZÉS ÉS A VÉDELEM NEMZETKÖZI JOGI SZABÁLYOZÁSA

A légiközlekedésben az egész világon hasonló eljárásokat és módszereket szükséges alkalmazni a közlekedés biztonsága érdekében. Így lehet csak sikeres a repülőgépek és repülőterek elleni terrortámadások megelőzése. A 2001. szeptember 11-i terrortámadás tapasztalatai megmutatták, hogy milyen sérülékeny a légiközlekedés és milyen súlyos következményei lehetnek egy terrorakciónak. Hasonló nagyságrendű veszteségek bekövetkezhetnek a világ nagy repülőterein is. Katonai szempontból a béketámogató műveletek során pedig a repülőterek biztonsága műveleti és logisztikai szempontból egyaránt fontos.

A repülőgépek és a repülőterek elleni terrortámadások kapcsán az egyértelmű lett, hogy nemzetközi szinten egységesíteni kell a politikai, jogi, légiforgalmi és biztonsági fellépéseket a már eltérített repülőgépekkel kapcsolatos krízishelyzetek megoldásakor. Az 1970-es évek első éveiben a repülőgép-eltérítések, a repülőgépek és repülőterek elleni terrortámadások megelőzése érdekében megújították, illetve kiegészítették a légiközlekedést szabályzó, az 1940-es és az 1950-es években, Montrealban és Chicagóban aláírt nemzetközi szerződéseket és egyezményeket. (1971. évi 25. törvényerejű rendelet) A terrorfenyegetettség miatt módosított egyezmények ratifikációja után már egyértelműen büntetendő cselekménynek számított a repülőgépek jogtalan igénybevétele, amelynek büntetőjogi következményei alól a nemzetközi jogi egyezmények által nyújtott garancia mellett elméletileg nem lehet kibújni.

A módosított nemzetközi légügyi egyezmények közül tálán a legfontosabb az ún. Chicagói Egyezmény, 17-es számú „A nemzetközi polgári repülés védelme a jogellenes beavatkozás cselekményei ellen” című melléklete, amely meghatározza azokat a biztonsági intézkedéseket és rendszabályokat, amelyek a légi utazásokkal kapcsolatosak. (20/1997. (X.21) KHVM rendelet) A melléklet behatárolja azokat a biztonsági előírásokat, eljárásokat, amelyeket a repülőtereken, repülőgépeken a repülés biztonsága érdekében az utasok a poggyászok és egyéb küldemények vonatkozásában el lehet és el kell végezteni. Egy-egy terrortámadás, vagy terrorakcióval való fenyegetés, illetve más jellegű repülőesemény kapcsán az International Civil Aviation Organization (ICAO) a biztonsági előírásokat felülvizsgálja, illetve az ideiglenesen bevezetett szigorításokat kiegészíti, elveti, vagy helyben hagyja. Ez történt a 2001. szeptember 11-i terrortámadás hatására. A Nemzetközi Polgári Repülésügyi Szervezet Tanácsa kiegészítette a nemzetközi ún. 17. számú mellékletet a repülés biztonságát veszélyeztető információk cseréjéről, a belföldi és nemzetközi légiforgalomban résztvevő

utasok személyi és poggyász ellenőrzésének szigorításáról, a pilótafülkék repülés közbeni zárásáról és védelméről, valamint a légi jármű biztonságát veszélyeztető események értesítési kódjainak alkalmazásáról.

Hasonló szigorítást vezettek be 2006 nyarán is – a Heathrow repülőtéren terrorfenyegetettséggel összefüggő riasztás után –, amikor szigorították a repülőgépek fedélzetére vihető tárgyak, élelmiszerek, italok körét, csomagolását és mennyiségét.¹³ Az ún. Chicagói Egyezmény 17. számú mellékletével kapcsolatban a repülés biztonsága érdekében alapvető követelményként jelenik meg, hogy az abban foglalt előírások napjainkban és a jövőben is igazodjanak a repülésbiztonsági elvárásokhoz és a terrorfenyegetettség szintjéhez.

A szabályok a repülőgépekre és a repülőterekre egyaránt vonatkoznak. Nem szabad elfeledkeznünk arról sem, hogy milyen fontos a repülőtereken az utasok poggyászaik és az egyéb küldemények ellenőrzése. A nemzetközi előírásokkal összhangban készültek el Magyarországon is polgári repülés védelméről szóló jogszabályok. (Szabó. M. 2007)

Folyamatosan szem előtt kell tartani azt a jogászok körében közhelynek számító megállapítást, hogy önmagukban a szabályok csak akkor érnek valamit, ha azokat be is tartják. A nemzeti hatóságoknak és a nemzetközi szervezeteknek időről-időre gondoskodniuk kell a biztonsági előírások betartásának szigorú ellenőrzéséről. A különböző szervezetek által végzett vizsgálatok egyaránt az utasok, repülőtéri üzemeltetők és a légitársaságok érdekeit szolgálják.

Következtetések

A repülőterek biztonságának problematikája messze túlmutat a közlekedés biztonsági kérdésén. A légikikötők és légijárművek elleni sikeres terrorakciók az áldozatok nagy számán és az okozott tetemes anyagi káron kívül szimbolikus jelentőséggel is bírnak. A terroriszervezetek a saját „erejükét” fejezhetik ki, miközben rámutathatnak az államok, a légitársaságok, légügyi szervezetek, repülőtéri üzemeltetők gyengeségére.

Mit lehet tenni a légiközlekedés terrorfenyegetettségének csökkentése érdekében? A kritikus infrastruktúra védelemmel foglalkozó szakértők a legfontosabb teendők közé sorolják, hogy a biztonsági előírások preventív jellegűek legyenek és ne a már megtörtént eseményekhez, terrortámadásokhoz igazodjanak. (Szabó. M. 2007) Ennek a követelménynek nem könnyű megfelelni, a komplex megközelítési és megoldási módok keresése nélkül a sikeres megelőzésre nincs esély. Azt is tudomásul kell venni, hogy a biztonság növelése nem csupán rendvédelmi és műszaki probléma. A különböző szakterületek kutatóinak és az utasok bevonása nélkül nem csökkenhet a repülőterek terrorfenyegetettsége.

Felhasznált irodalom

1971. évi 25. törvényerejű rendelet a nemzetközi polgári repülésről Chicagóban, az 1944. évi december hó 7. napján aláírt Egyezmény és az annak módosításáról szóló jegyzőkönyvek kihirdetéséről. CompLex DVD jogtár, KJK KERSZÖV Jogi és Üzleti Kiadó Kft., Budapest, 2005.

¹³ A nemzetközi szakirodalomban ún. Transz-atlanti Összeesküvésnek nevezett esemény légiforgalomra gyakorolt hatásáról lásd bővebben: Szabó M. 2007: Terrorcselekmények elhárításának időszerű kérdései, különös figyelemmel a polgári repülésvédelemre. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest. A pontos URL címet lásd az irodalomjegyzékben.

20/1997. (X.21) KHVM rendelet: A nemzetközi repülésről Chicagóban, az 1944 évi december hó 7. napján aláírt Egyezmény függelékének a kihirdetéséről. CompLex DVD jogtár, KJK KERSZÖV Jogi és Üzleti Kiadó Kft., Budapest, 2005.

D. Stevens, T. Hamilton, M. Schaffer, D. Dunham-Scott, J.J. Medby, E. W. Chan, J. Gibson, M. Eisman, R. Mesic, C. T. Kelley, Jr., J. Kim, T. LaTourrette, K. J. Riley: Implementing Security Improvement Options at Los Angeles International Airport. Published 2006 by the RAND Corporation. United States, Santa Monica. URL cím: <http://www.rand.org/>. p. 68.

Havas P 2004: Közlekedéstechnológiai rendszerek. In.: Kövesné dr. Gilicze Éva (szerk). Közlekedési rendszerek. A Budapesti Műszaki és Gazdaságtudományi Egyetem Közlekedésüzemi Tanszék kiadványa. pp. 27-67.

Horváth A. 2009: The terror-threat characteristics of critical ground traffic infrastructure. Tudományos Mozaik. 6. kötet. A Tomori Pál Főiskola lektorált tudományos kiadványa. Kalocsa, 2009. pp. 269-177. ISBN 978-963-88162-3-8.

Horváth A. 2008/a: A polgári repülőgépek elleni terrortámadások tapasztalatai. Repüléstudományi Közlemények. A Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Repülő és Légvédelmi Intézet on-line folyóirata. Szolnok, 2008. pp.: 14. URL cím: <http://www.szrfk.hu/rtk/>

Horváth A. 2008/b: The Experience of Terrorist Attacks Against the Civil Airports. Review of the Air Force Academy. The Scientific Informative Review. Brasov, Romania. No 2/2008. pp. 113-1178 Number of ISSN 1842 - 9238

J. D. Moteff. 2008: Critical Infrastructures: Background, Policy, and Implementation. United States Congressional Research Service. Washington DC. p. 45.

Joint Homeland Security Assessment 2007: Glasgow Airport Illustrates Varied Terrorist Tactics to Attack Transportation Infrastructure. United States, Washington DC. URL cím:

Kovács L., Krasznay Cs. 2009: Digitális Mohács. (kézirat). Hacktivity Felhasználóbarát IT Biztonsági Konferencián elhangzott előadás írásos változata.

Szabó M. 2007: Terrorcselekmények elhárításának időszerű kérdései, különös figyelemmel a polgári repülésvédelemre. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest.

URL cím: http://193.224.76.4/download/konyvtar/digitgy/phd/2009/szabo_miklos.pdf

Szabó M. 1999: Terrorizmus a polgári légiközlekedésben. A Belügyminisztérium Szakmai, Tudományos Folyóirata. Budapest, 1999. 12. szám.

The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks Upon the United States. Official Government Edition. United States, Washington DC ISBN 0-16-072304-3 p. 589.

Pap Andrea

pap.andrea@zmne.hu

AZ E-LOGISZTIKA KAPCSOLATA A LOGISZTIKAI SZOLGÁLTATÓ KÖZPONTOKKAL

Absztrakt

Az elmúlt évtizedek során végbement technológiai fejlődés, valamint a társadalmi és gazdasági igények növekedése lehetővé tették az új kommunikációs lehetőségek megjelenését. Napjainkra már szinte elképzelhetetlen az élet az informatika újabb- és újabb találmányai, vívmányai nélkül. A megnövekedett igények, valamint a kezdeti számítógépes hálózatok létrehozása, illetve ezek továbbfejlesztése képezik a mai Internet alapjait, amelyek mostanra behálózzák az egész világot. Az elektronikus üzletvitel, az elektronikus kereskedelem és az elektronikus logisztika kialakulása is mind kapcsolatban áll az Internet kialakulásával, de nemcsak a külső, hanem a belső integrált információs rendszerek létrejöttével is.

The technological development and the increase in social and economic demands over the last few decades have facilitated the emergence of new communication possibilities. By now life has become unimaginable without the newer and newer developments and achievements in information technology. The growing demand and the establishment of the initial computer networks and their further development constitute the basis of today's Internet, which encompasses the whole world. The emergence of electronic business, electronic trade and electronic logistics is also closely related to the invention of the Internet, but not only to the development of external but also of internal integrated communications systems.

Kulcsszavak: *technológiai fejlődés, kommunikáció, Internet, elektronikus logisztika ~ technological development, communication, Internet, electronic logistics*

Az Internet segítségével a termékek és a szolgáltatások egyaránt elérhetők, rövid idő alatt összehasonlíthatók a termékek, továbbá az áraik, illetve egyszerűen ellenőrizhetők a szállítási feltételek, nemcsak az internetes webáruházak oldalain, hanem a különböző vállalatok saját oldalain is, így egyszerűen megvásárolhatók vagy elérhetők az egyének számára a megfelelő termékek, vagy szolgáltatások. Tehát ez az újfajta kommunikációs és értékesítési csatorna sok lehetőséget nyújt a társadalom tagjai számára.

A fent említettek miatt az informatika területén az utóbbi évtizedben forradalmi változások következtek be, amelyek érintették mind az információs, mind a kommunikációs technológia valamennyi területét. Ezen forradalmi változások eredményeképpen nagyobb teljesítményű és üzembiztosabb számítógépek, gyorsabb és megbízhatóbb lokális hálózati és adatátviteli technológiák váltak elérhetővé a felhasználók számára, továbbá ehhez kapcsolódóan nagyot fejlődtek az operációs rendszerek, az adatbázis kezelő rendszerek, illetve a háttérrendszerek fejlesztésére alkalmas eszközök.¹

A fejlett és fejlődő eszközök, szoftverek és az Internet új teret nyitottak meg a gazdasági élet szereplői számára. Megjelent és elterjedt az elektronikus kereskedelem, amelynek segítségével a hagyományos üzleti tranzakciók elektronikus formában is lebonyolíthatók, valamint már országhatárokon átnyúló lehetőségeket biztosít az eladók és a vevők igényeinek kielégítésére helyváltoztatás nélkül, ezáltal költséget és időt megtakarítva. Azonban az Internet növekvő terjedése nemcsak a kereskedelem területén jelentkezik, hanem éppúgy megfigyelhető a közigazgatásban, az oktatásban, az egészségügy és a kultúra területén is.

AZ E-BUSINESS, AZ E-KERESKEDELEM ÉS AZ E-LOGISZTIKA LÉNYEGE

Az *e-business* (elektronikus üzletvitel) fogalmára napjainkban nagyon sok értelmezés létezik. Az elektronikus üzletvitel a vállalatok, szervezetek külső és belső folyamatainak integrált információs rendszerek segítségével történő támogatása a tervezés – végrehajtás – ellenőrzés fázisokon keresztül. Tehát minden olyan üzleti tranzakció, amely elektronikus úton zajlik le, felhasználva a különböző szükséges és fejlett technológiákat. Az *e-business* magában foglalja a *e-kereskedelmet*, és az ehhez a tevékenységhez kapcsolódó belső folyamatokat is, mint például: a gyártást, a termékfejlesztést, a pénzügyeket, a humán erőforrásokat és a kockázatkezelést. Ehhez azonban egy fejlett, integrált vállalatirányítási rendszerre van szükség.

Az *e-kereskedelem* olyan üzleti tevékenység végrehajtását jelenti, amely magába foglalja az adatok, termékek, szolgáltatások és az információ elektronikus vételét, eladását, feldolgozását és átvitelét a hálózaton keresztül. Azonban az *e-kereskedelem* részét képezi az elektronikus pénz átutalás, az elektronikus értékpapír kereskedelem, a különböző aukciók és az elektronikus fuvarlevelek kiállítása is.

Az *e-logisztika* minden olyan valós logisztikai tevékenységhez kapcsolódó információáramlás, amely a logisztikai vállalkozások, azok szerveződései (logisztikai központok, ipari parkok), a logisztikai szolgáltatásokat igénybe vevő vállalkozások között zajlik.²

Ezen rövid áttekintés után most áttérek a civil és a katonai Logisztikai Szolgáltató Központokra (továbbiakban: LSZK), illetve ezek kapcsolatára az *e-logisztikával*.

A LOGISZTIKAI SZOLGÁLTATÓ KÖZPONTOK SZEREPE A GAZDASÁGBAN

Az Európai Unió (továbbiakban: EU) ajánlásának megfelelően a 10 korridorból 4 fő korridor keresztezi hazánkat. Ezek mentén alakultak ki az LSZK-k, melyek ismertetése előtt kitérnék a hazánkat érintő korridorokra.

A Helsinki főkorridorok kialakítására 1997-ben került sor az úgynevezett III. Páneurópai Közlekedési értekezleten, Helsinkiben. Azonban az igények jelentkezése 1991-re vezethető

¹ Bóna Krisztián 2003., 2.o.

² http://www.klaszter.hu/tanulmanyok_cikkoldal.php?cikk_id=46

vissza, ekkor az Európai Parlamentben sürgetik az egységes európai közlekedési hálózatok és infrastruktúra kialakítását, amelynek hatására 1992. február 07-én aláírásra került, majd 1993. november 01-jén hatályba lépett a Maastrichti Szerződés, aminek eredményeképpen létrehozzák a Transzeurópai Hálózatot (továbbiakban: TEN). Eközben Prágában az I. Páneurópai Értekezleten és 1994-ben Krétán a II. Páneurópai Értekezleten lehetővé tették, hogy a kialakított európai közlekedési folyosók összekössék az EU tagállamait harmadik országok területeivel, olyanokkal amelyek az EU gazdasági érdekei számára fontosak, így került rögzítésre az ún. „Páneurópai Hálózat” (továbbiakban: PEN). Ezek a PEN korridorok kerültek kiegészítésre Helsinkiben, ahonnan az elnevezés is származik. A hazánkat is érintő folyosók a IV-es, az V., V/B, V/C, a VII-es és a X/B, amelyek közúti, vasúti és vízi útvonalakat foglalnak magukba grafikusan az 1. számú ábrán megjelenítve.

Ezen korridorok mellett jött létre a 13 országos jelentőségű Logisztikai Szolgáltató Központ, melyből Budapest környékén található három – Soroksáron a BILK, Nagytétényben a Harbor Park és a Csepeli Szabadkikötő –, továbbá Sopronban, Győr-Gönyű kikötő, Székesfehérvár, Nagykanizsa, Baja, Szolnok, Miskolc, Debrecen, Záhony, Kecskemét városokban. Az országos logisztikai szolgáltató központok mellett a VPOP-val közösen kijelölésre kerültek a regionális logisztikai központok is, melyek elsősorban megyeszékhelyeken létesültek, úgy mint Kecskemét, Békéscsaba, Nyíregyháza.³



1. számú ábra. Az országos logisztikai szolgáltató központok hálózata (KTI)⁴

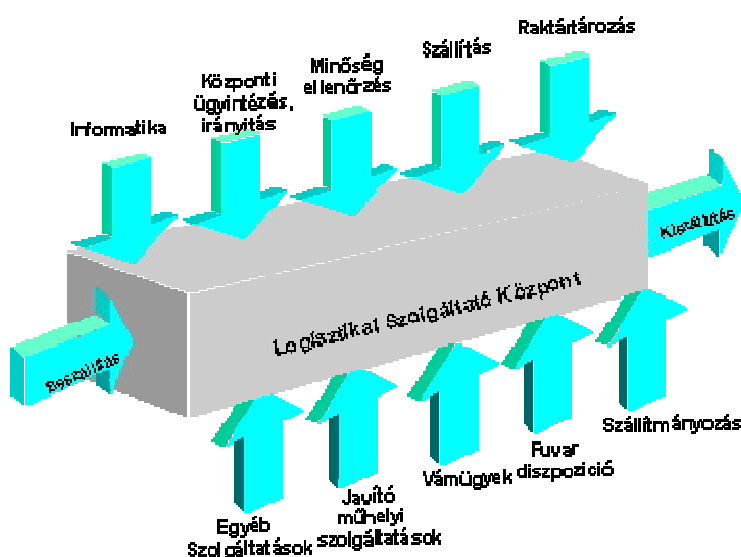
³ Magyar intermodális logisztikai fejlesztési koncepció 2006.

⁴ Forrás: Magyar intermodális logisztikai fejlesztési koncepció 2006.

A CIVIL ÉS A KATONAI LOGISZTIKAI SZOLGÁLTATÓK FELADATA, TEVÉKENYSÉGE

Egy vállalatnál a logisztikai tevékenységek végrehajtása többféle formában valósulhat meg. Történhet úgy, hogy a vállalat saját maga végzi minden logisztikai tevékenységét, vagy egy részét, illetve teljes egészét ki is helyezheti, az ezen feladatok ellátására létrejött szolgáltatókhoz. A logisztikai tevékenységek elvégzésére szakosodott vállalatokat nevezzük logisztikai szolgáltatóknak.

Az LSZK-k olyan zárt teletszerűen elhelyezkedő, a szolgáltató vállalkozások illetve szervezetek összessége, amelyek közös infrastruktúrára és információs hálózatra épülnek, ahol az áruforgalmi szolgáltatásokon túlmenően a beszerzés és értékesítés, valamint értéknövelő tevékenységek történnek.⁵(2. számú ábra)



2. számú ábra. A Logisztikai Szolgáltató Központok egyszerűsített működése⁶

A logisztikai szolgáltatók igénybevételét több ok indokolhatja, melyek közül a legfontosabbak:

- költségcsökkentés, ezzel egyidejűleg,
- a logisztikai kiszolgálás színvonalának növelése, tehát minőségi szolgáltatás nyújtása,
- alaptevékenységre való koncentráció,
- a logisztika komplexé válása.

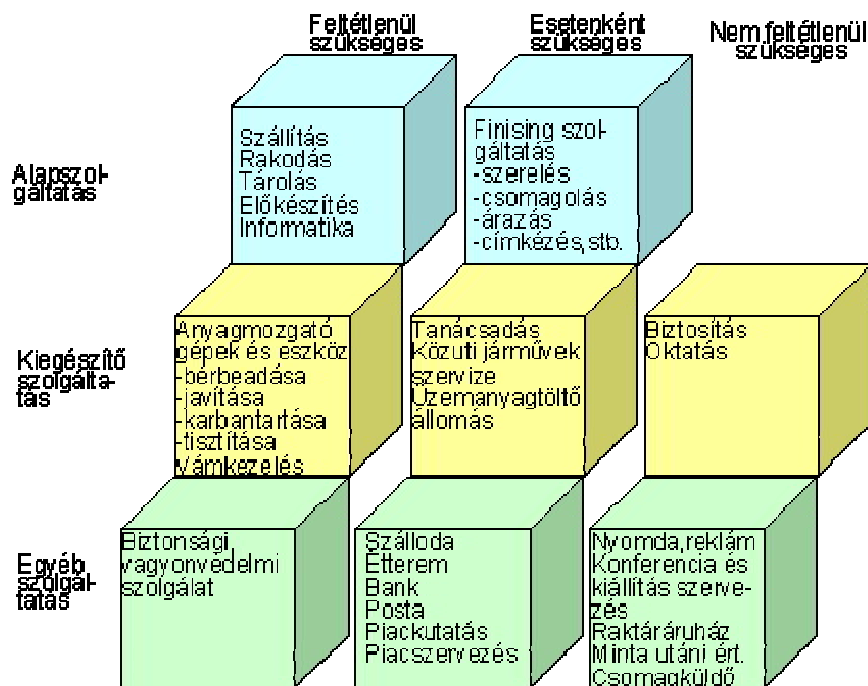
Az alábbiakban ismertetem a logisztikai szolgáltatók tevékenységeit, melyek általában két csoportba sorolhatók, illetve grafikusan a 3. számú ábrában:

- Alapszolgáltatások:
 - raktározás,
 - szállítmányozás,

⁵ <http://www.logsped.hu/lshk.htm>

⁶ Forrás: <http://www.logsped.hu/lshk.htm>

- rakodás,
- elosztás,
- információs rendszerek működtetése.
- Hozzáadott érték szolgáltatások:
 - selejt kezelése,
 - csomagolás, esetlegesen újracsomagolás,
 - készletgazdálkodás,
 - címkézés,
 - visszáru és hulladékkezelés,
 - kommissiózás,
 - tanácsadás.



3. számú ábra. A Logisztikai Szolgáltató Központok szolgáltatásai⁷

Most, a civil Logisztikai Szolgáltató Központok feladatának ismertetése után bemutatom a katonai ellátó központok tevékenységét. Jelenleg a Magyar Honvédség két ellátó központtal rendelkezik, a Logisztikai Ellátó Központ Mátyásföldön, míg a Veszélyesanyag Ellátó Központ Pusztavacson települ.

Az MH Logisztikai Ellátó Központ 2007-ben alakult, két ellátó központ jogutódjaként, feladatai közé sorolható többek között:

- a katonai szervezetek ellátása az előírt szakanyagokkal;
- megszervezi és végzi az anyagok tárolását, karbantartását;
- inkurrensé vált anyagokkal kapcsolatos mindennemű feladatok végrehajtása;
- központi beszerzésű anyagok átvétele;
- nyilvántartja szállítók szerint a megrendeléseket és teljesítéseket;
- a NATO és nemzetközi missziók ellátásával kapcsolatos szakmai feladatok;
- részt vesz az MH háborús logisztikai biztosításának megszervezésében, stb.⁸

⁷ Forrás: <http://www.logsped.hu/lisz.htm>

⁸ http://www.hm.gov.hu/honvedseg/mh_logisztikai_ellato_kozpont

Ezen feladatok ellátását a központ 5 raktárbázissal, egy kijelölt állandó raktárral és öt inkurrencia tároló raktárral látja el, amely raktárak az ország egész területén több mint 14 helyőrségben helyezkednek el. Ez a széttagoltság megnehezíti a központ munkáját, és a feladatok végrehajtását.

Az MH *Veszélyesanyag Ellátó Központ* 2005-ben jött létre. Fő feladatai közé sorolható:

- ellátja a honvédelmi szervezeteket az előírt szakanyagokkal, végzi a szaktechnikai eszközök szervizelésének, javításának koordinálását;
- megszervezi és végrehajtja a központi beszerzésű lőszer, rakéták, műszaki harcanyagok, üzem- és kenőanyagok átvételét és a raktárak közötti elosztását;
- külön rendelkezés alapján végzi a különféle NATO és nemzetközi missziók ellátásával kapcsolatos szakmai feladatokat;
- megszervezi a központi anyagkészletek nyilvántartását, tárolását, karbantartását, szavatossági időn belüli cseréjét, a központilag előírt szinten tartja az anyagi készletek és a tartalékokat, stb.⁹

Mind a civil, mind pedig a katonai szolgáltató központok esetében a felsorolt tevékenységek hatékony összehangolásához, végrehajtásához szükséges egy fejlett információs technológia.

AZ E-LOGISZTIKA

Az e-logisztika létrejött egy hosszú folyamat eredménye, amely az információs technológia fejlődésével párhuzamosan alakult. Az informatika fejlődését kihasználva hazánkban is felgyorsult mind az online, mind az Internetes üzleti kapcsolat. Ezt szem előtt tartva a vállalatok logisztikai rendszerét is úgy kellett kialakítani, hogy képes legyen végrehajtani az elektronikus beszerzést és az értékesítési folyamatokat. Az e-logisztika az anyagoknak, termékeknek, szolgáltatásoknak és információknak az áramlását elősegítő és irányító funkcióit foglalja magába, amelyek hatékonyan veszik igénybe az Internetet és az elektronikus hálózat adta lehetőségeket. Az e-logisztika előnyei közé sorolható, hogy a gyors vevőkiszolgálás mellett, képes csökkenteni az elosztási csatornában felhalmozódott készleteket. A logisztika optimális működéséhez, működtetéséhez és az elfogadható költségek kialakításához, meg kell határozni a megfelelő vevő-kiszolgálási szintet.

Az e-logisztika nem összekeverendő az e-kereskedelem logisztikájával, azonban most mégis erről ejtenék néhány szót, hiszen az elektronikus kereskedelemnek egy megfelelő logisztikai rendszerrel összekapcsolt alkalmazása önmagában is növeli a vevő-kiszolgálási szintet és csökkenti a költségeket a következők miatt:

- az Interneten vagy az on-line rendszeren keresztül könnyen hozzáférhetővé válik a vevő számára a vevő-kiszolgálási politika;
- a vevő gyorsabban értesül az őt érdeklő vásárlói akciókról, változásokról, eseményekről;
- növekszik a megrendelési kényelem;
- a számítógépes feldolgozás segítségével kiszűrhetők a megrendeléskor vétett hibák;
- az elektronikus formában kapott ajánlatkérések és megrendelések egyszerűsítik az adatfeldolgozást, így rövidebb lesz a megrendelési ciklusidő;
- a vevő gyorsan és pontosan tájékozódhat arról, hogy mit tudnak neki azonnal szállítani, esetleg milyen helyettesítő termékeket tudnak ajánlani;
- a vevő követheti az általa megrendelt árucikkek útját, értesülhet a várható kézbesítési időpontról;

⁹ http://www.hm.gov.hu/honvedseg/mh_veszelyesanyag_ellato_kozpont

- az elektronikus adatfeldolgozás és ellenőrzés segítségével a rendszerben elkövetett hibák nullára csökkenthetők;
- egyszerűbb lesz a vásárlói panaszok kezelése;
- a panaszok elektronikus beérkezése által természetes módon előáll a vásárlói követelések, panaszok, visszatérítések adatbázisa;
- a vevő-kiszolgálási mutatók egy részét az elektronikus kereskedelmi rendszer is rögzíti, stb.¹⁰

A logisztikai műveletek az üzletkötési folyamatokkal szemben háttérben maradnak, mégis végigkísérik a teljes folyamatrendszert. Hazánkra jellemző, hogy a nagyvállalatok kihelyezik logisztikai tevékenységeiket vagy azok egy részét külső, erre a feladatra szakosodott szolgáltatókhoz, amelynek okai már ismertetésre kerültek.

A logisztikai szolgáltatók igénybevétele és a jó információáramlás eredményezheti az ellátási lánc lerövidülését – a klasszikus ellátási lánc (beszállító – termelő – nagykereskedő – kiskereskedő - fogyasztó) módosul – ezáltal a költségek csökkenését és a folyamatok felgyorsulását.

A logisztikai folyamatok irányítása, valamint a központi adatfeldolgozás az együttműködő vállalatok számítógépes rendszerén és a meglévő kommunikációs hálózaton alapul. Az irányításhoz az adatok rendelkezésre bocsátása, továbbá rendszerezett feldolgozása szükséges.¹¹

A Logisztikai Szolgáltató Központok tevékenységeiből adódóan az információs rendszerek technikai eszközeinek a logisztikai irányítás alapfolyamatait követve kell az anyagok, termékek, eszközök, járművek stb. különböző azonosítóit az RST folyamatok változásait a rendszerben összegyűjteni, feldolgozni és az irányítás számára biztosítani.¹² A feldolgozási folyamat végrehajtásához a következő technikai eszközök szükségesek:

- termékazonosító eszközök;
- adatfelvételi eszközök;
- adatfeldolgozási eszközök;
- adatátviteli rendszerek, eszközök,
- árukövető rendszerek, eszközök stb.

Az adatátviteli rendszerek esetében olyan eszközökre van szükség, amelyek egy egységes adatkommunikációs rendszerben továbbítják a szükséges információkat a felhasználók felé, ennek egyik eszköze az elektronikus adatcsere (EDI=Electronic Data Interchange).

Az árukövető rendszerek segítségével pedig folyamatosan nyomon lehet követni az áru útját minden időpontban a feladótól a vevőig, esetlegesen módosítva az útvonalat (visszaküldés, átirányítás stb.).

A LSZK-k rendelkeznek ezen eszközökkel, tehát a logisztikai folyamat legelejétől végig tudják kíséni a velük szerződött partnerek anyagainak minden lépését, a termékazonosítás, a raktározás, a készletgazdálkodás, a járattervezés, az útvonal kiválasztás, a járműkövetés feladatain keresztül a vevőnek történő átadásig.

A katonai ellátó központok esetében már – a speciális feladatoknak köszönhetően – bonyolultabb a helyzet, hiszen az alegységek nemcsak honi, de külföldi területen is települnek. A feladatok sikeres végrehajtását szolgálja az ADAMS. Ez egy Szövetséges Felvonulási és Mozgatási Rendszer, amelyben megtervezhető, elemezhető és vezethető a csapatok tevékenysége hazai és missziós feladatok végrehajtása során is. Hiszen olyan adatbázissal rendelkezik, amely lehetővé teszi az érintettek számára bármilyen eszköz, anyag,

¹⁰ <http://www.miau.gau.hu/miau/60/fanclub/szegedi.doc> 4-5.o.

¹¹ Bóna Krisztián 2003., 18.o.

¹² Bóna Krisztián 2003.

alegység mozgatóját, nyomon követését, a feladat végrehajtását az elképzeléstől, a követelmények meghatározásán át egészen a nemzeti mozgatói tervek elkészítéséig.

ÖSSZEGZÉS

Az e-logisztika kialakulásával a vállalatok sokkal több információt tesznek hozzáférhetővé a velük kapcsolatban álló érintettek számára. Összességében ezen újfajta logisztika megjelenésével a szervezeti hatékonyság növekszik, illetve különböző racionalizálási folyamatok zajlanak le a vállalkozásoknál, valamint a szállító és a vevő közötti lépések száma csökken, hiszen a klasszikus ellátási lánc lerövidül a fent említett okok miatt. A hagyományos logisztikai funkciók kihelyezése (outsourcing) miatt a vállalatnál a belső folyamatok és tevékenységek egyszerűbbé válnak, mert az adott cégnek esetlegesen csak az alaptevékenységére kell koncentrálnia, azonban az e-logisztika és informatikai háttere összetettebbé válik ennek következtében. Ez igaz a honvédségre is, hiszen a csapatoknak nem kell a különböző több területet is érintő beszerzésekre koncentrálni, vagy az egyes anyagok tárolásával foglalkozni, mert ezek központosítva lettek a ellátó központok feladatai közé.

Felhasznált irodalom

- Bóna Krisztián (2003): Logisztika II. Internetes segédanyag az „Elektronikus üzletvitel logisztikája” című témakörhöz, Heller Farkas Gazdasági és Turisztikai Szolgáltatások Főiskolája
- Magyar intermodális logisztikai fejlesztési koncepció (2006), Gazdasági és Közlekedési Minisztérium, Közlekedési Főosztály, Budapest
- http://www.hm.gov.hu/honvedseg/mh_logisztikai_ellato_kozpont
- http://www.hm.gov.hu/honvedsef/mh_veszelyesanyag_ellato_kozpont
- http://www.klaszter.hu/tanulmanyok_cikkoldal.php?cikk_id=46
- <http://www.logsped.hu/l Szk.htm>
- <http://www.miau.gau.hu/miau/60/fanclub/szegedi.doc>

Tóth Attila

tothattila.bp@gmail.com

Tóth Bálint

tothbalintdr@mail.datanet.hu

A NAGYVÁROSOK FELSZÍNI KÖZLEKEDÉSI RENDSZEREINEK VIZSGÁLATA A TERRORFENYEGETETTSÉG TÜKRÉBEN

Absztrakt

Egy város szerkezetének és közlekedési hálózatának kialakulása és fejlődése meghatározó jelentőségű a városlakók közlekedési szükségleteinek kielégítésében és a közösségi közlekedés feltételrendszerének biztosításában. A közlekedési rendszerek működőképességének bármely okból eredő zavara, vagy kiesése, részbeni kapacitáscsökkenése jelentősen befolyásolja a társadalom mindennapi életét, a szolgáltatások biztosítását, a gazdaság működőképességét, a lakosság létszükségleteinek kielégítését. Ebben a cikkben azokat a fővárosi közlekedési objektumokat (csomópontokat, hálózatokat) kívánjuk bemutatni, amelyek célpontjai lehetnek a közlekedési rendszerek elleni terrorcselekményeknek, valamint ezen objektumok működésének bármely okból keletkező zavara miként hat a nagyváros egészének mindennapos közlekedésére.

The formation and the development of a city's organisation and transportation system have determinant importance of fulfilling the habitants' needs and ensuring the transportation conditions. The disturbances or interruptions of the transportation systems' working order (by any causes) and partly decreasing capacities have influenced the everyday life of society, the provision of services, the economic working order, the satisfaction of essentials of population's life. In this article we would like to introduce those transportation objects (like junctions and networks) at the capital which might be possible targets of terror attacks against transportation systems. As well as how the disturbances of those objects' operation effect the daily transportation of a whole town.

Kulcsszavak: városi közlekedés, közösségi közlekedés, terrorizmus, terrorizmus célpontjai ~ city transportation, public transportation, terrorism, targets of terrorism

BEVEZETÉS

Egy város közlekedési hálózatának kialakítását és fejlődését számtalan tényező határozza meg. A város területi kiterjedésén és lakosainak számán kívül döntő fontossággal bír, milyenek a közlekedés-földrajzi adottságai, milyen szerepet tölt be a társadalom közigazgatási, kulturális és nem utolsósorban gazdasági életében nemzetközi, országos és regionális vonatkozásban. E szempontokon túl, meghatározó jelentőségű még a város szerkezeti felépítésének jellege, az egyes városrészek funkcióinak szerepe is. Utóbbiak alapvetően befolyásolják az ott élő városlakók életvitelét, szokásait, a munkájukkal (hivatásukkal) és a különböző szolgáltatások igénybevételével, ügyeik intézésével, valamint személyes mozgásukkal kapcsolatos közlekedési szükségleteiket.

Napjainkban szinte mindenki számára természetes, hogy a saját egyéni közlekedési szükségletei kielégítéséhez bármely időpontban rendelkezésre állnak a – többé-kevésbé elfogadható állapotú – a közel 150 ezer km hosszú országos közúti hálózat, a mintegy 6500 km-en üzemelő un. nagyvasúti (Magyar Államvasutak Rt, Győr-Sopron-Ebenfurti Vasutak Rt.) közlekedés, továbbá a nagyvárosokban működő közösségi közlekedési rendszerek [felszínalatti (metró)- és helyiérdekű vasutak (HÉV), közúti villamos- és trolibusz hálózatok, valamint a helyi és helyközi közlekedést biztosító autóbuszjáratok]. Az is elfogadott, hogy a közösségi közlekedési rendszerek alkalmankénti igénybevételéért fizetni kell (menetjegy), azonban ennek ellenében az igénybevevő az üzemeltetőtől kifogástalan kiszolgálást és gyors eljutást vár el. Mindaddig, amíg ez az összetett, és hazánkban közel kétszázézer fővel üzemeltetett közösségi közlekedési rendszer az előírásoknak megfelelően működik, szinte "észre sem vesszük" meglétét, azonban tervezett üzemszünete (pl. felújítás, vagy bejelentett sztrájk), illetve nem tervezett kiesése (üzemzavar, baleset, katasztrófaesemény, terrorcselekmény) miatt fellépő néhány órás hiánya is „felbecsülhetetlen károkat” okozhat, mind az egyéneknek, mind a termelésnek, szolgáltatásnak stb., összességében az egész társadalomnak. Az ilyen esetek miatt keletkező (társadalmi és gazdasági jellegű) károk elkerüléséhez, illetve gyakoriságának és költségkihatásának csökkentése érdekében elkerülhetetlen a közlekedési (köztük a közösségi közlekedési) szolgáltatások színvonalának és megbízhatóságának növelése, infrastruktúrája (hálózat, jármű, személyzet, létesítmények, erőforrások) működőképességének fenntartása, életképességének (védelmi képességeinek) biztosítása, tartalékok képzése. Mindezek természetesen a jelenleginél sokkal több költségvetési ráfordítást igényel(né)nek.

Ebben a cikkben a nagyvárosok felszíni közösségi közlekedésének kapcsolatrendszerét kívánjuk bemutatni, abból az aspektusból, hogy az egyes közösségi közlekedési alágazatok működésének bármilyen zavara miként hat a nagyváros egészének mindennapos közlekedési szükségletei kielégítésére.

VÁROSI KÖZLEKEDÉSI KAPCSOLATOK KIALAKULÁSA

A fontosabb települések közlekedési hálózatát a különböző funkcionális feladatai ellátásához szükséges útvonalak alkotják, amelyek azokon rendszerint áthaladnak, vagy a közelükben lévő – nemzetközi és országos kapcsolatokat biztosító közúti és vasúti – hálózatról bevezetnek, illetve a települések, városrészek közötti „belső” közlekedési szükségleteket elégítenek ki. Míg korábban az országos (nemzetközi) kapcsolatokat biztosító útvonalak a fontosabb településeket közvetlenül érintették (áthaladtak rajta), napjainkban a fejlődés iránya – a növekvő forgalom kedvezőtlen hatása (balesetveszély, zaj- és környezetszennyezés) miatt – a településeket elkerülő útvonalak kiépítését tartja szem előtt.

A városokon átmenő tranzit forgalmat akkor sem lehet teljesen „kizárni”, ha kiépülnek az elkerülő közúti körgyűrűk és vasútvonalak. Az urbanizáció egyes szakaszai meghatározták a városi közlekedés alakulását is (Mándoki P. 20009). Az elmúlt évtizedekben országszerte a városokba bevezető autópályák és főútvonalak mellé különféle logisztika (bevásárló- és szolgáltató központok) és ipari létesítmények épültek, ennek következtében az itt kiépült területekre helyezte át tevékenységét a szolgáltató szféra meghatározó része is. Mindez hozzájárult ahhoz, hogy a városi közlekedés forgalmi irányában is jelentős változások történjenek. A városokból a város környéki településekre való kiköltözés is jelentősen növelte a nagyvárosok és városkörnyéki települések közötti forgalmat.

Általánosan elfogadott szakmai álláspont, hogy a városi közlekedést már nem lehet csupán a város határán belül értelmezni. Nemcsak azért, mert Magyarország lakosságának közel kétharmada él városokban, hanem azért mert a közlekedési problémák fokozottan jelentkeznek városi és elővárosi területeken, ahol a lakó- és munkahelyek halmozódnak, illetve a helyváltoztatási és szállítási igények koncentrálnak. A városok és agglomerációs térségeik közlekedés- és területfejlesztése között – a közlekedési igények közigazgatási határtól független megjelenése miatt – célszerű összhangot biztosítani, a helyi, környéki, regionális, országos és nemzetközi közlekedési rendszerek közötti átjárhatóság biztosítása érdekében, a hálózatok hierarchikus egymásba illeszkedése szükségessé teszi, hogy a részrendszerek fejlesztését a magasabb szintű rendszerekhez (hálózatokhoz) igazítsuk. A városi közlekedés szervezése, működtetése és fejlesztése során figyelembe kell venni a városok határán kívülre települt raktárak, bevásárló és szórakoztató központok és szolgáltató vállalkozások, valamint a város vonzáskörzetében, az ún. „szuburbanizációs” térségekben lakók közlekedési igényét is.

A fentiek alapján megállapíthatjuk, hogy a befolyásoló tényezők sokasága, az adott városra jellemző adottságok mellett a lakosság közlekedési igényeinek kielégítését csak jól szervezett és gazdaságosan működtetett közlekedési rendszerekkel (infrastrukturákkal) és megfelelő minőségű közlekedési szolgáltatásokkal (közösségi közlekedéssel) lehet biztosítani. A nagyvárosok fejlődésére jellemző, hogy a minél nagyobb „társadalmi, gazdasági potenciál” megszerzése érdekében a városok közötti verseny is egyre inkább felgyorsult. Ebben a folyamatban a közlekedési rendszer fejlettségi színvonala a városok versenyképességének egyik fontos elemévé vált. A közlekedési rendszer minőségét számtalan tényező határozza meg, ezek közül a városi közlekedés biztonsága egyre inkább fontos összetevővé válik. A városokban közlekedő járművek, a közlekedés infrastrukturális elemei ellen elkövetett terrortámadások éppen ezt a biztonságot veszélyeztetik és kérdőjelezik meg.

A városi közlekedéspolitikai fő prioritása olyan városi közlekedésfejlesztési stratégia, amely a fenntartható mobilitás érdekében a személyközlekedésben nem az egyéni gépjármű közlekedést, hanem a közforgalmú közlekedést részesíti előnyben, valamint az áruszállításban határozottabban támaszkodik a city-logisztika megvalósítására.

A személyforgalom döntő része természeténél fogva - a nagyobb lélekszámú településeken élők közlekedési igényeit tekintve – a városokból indul ki. Éppen ezért ezeken a településeken haladnak át, vagy végződnek az elővárosi, a helyközi, az országos és a nemzetközi forgalmat lebonyolító vasút- és autóbuszvonalak. A nemzetközi, országos vagy regionális jelentőséggel bíró városokban nagyobb vasúti és autóbusz-pályaudvarok épültek, és általában ezekhez kapcsolódnak a városi közlekedést bonyolító közösségi közlekedési eszközök útvonalai, állomásai is. Napjainkban a modern metropoliszok - az elővárosokkal együtt - bonyolult rendszert alkotnak. Ebben a rendszerben a városi közlekedés színvonala a

városi élet minőségének egyik döntően meghatározó, számszerűen jól elemezhető és kifejezhető elemévé vált (Kövesné G. É. 2000).

A NAGYVÁROSOK ÉS KÖZLEKEDÉSI RENDSZEREIK FENYEGETETTSÉGE

Napjainkban szinte nem telik el olyan hét, hogy a hírügynökségek ne tudósítanak a világ valamelyik nagyvárosából - emberi áldozatokat is követelő - terrortámadásokról. Óhatatlanul felvetődik a kérdés: a terrrorszervezetek vezetői miért pont a metropoliszokban választanak ki célpontot maguknak. A válasz a magas népsűrűségben és a városi tér funkcióiban keresendő. A metropoliszokban található politikai, közigazgatási, pénzügyi és gazdasági, energetikai, közösségi közlekedési, kulturális, valamint turisztikai infrastruktúra alkalmas arra, hogy viszonylag kis erővel nagy pusztítást lehessen végrehajtani. Könnyebb a kiválasztott és lehetséges célpontokról pontos információkat szerezni, a helyszíneket bejárni, és ezért általában a terrortámadásokat megszervezni és egy terrorakciót követően a helyszínt gyorsan elhagyni (Horváth A 2006/a). Nem szabad figyelmen kívül hagyni a terrorizmus céljait sem. A terroristáknak – gyakorlatilag annak a szervezetnek a jellegétől és típusától függetlenül, amelynek a tagjai – alapvető céljai közé tartozik az állandó bizonytalanság keltése és a politikai intézményrendszer működésének befolyásolása.

A XX. század utolsó évtizedeiben – az addig a legnagyobb biztonsági kockázatot jelentő „hidegháborús” korszak helyére - az egyre szélesebb méreteket öltő nemzetközi terrorizmus lépett, amely ma is korunk legnagyobb kihívásai közé tartozik. A terrorizmus veszélyét egyetlen társadalom sem kezelheti „rutinszerűen”, mivel megjelenési formái, céljai, és potenciális helyszínei merőben különböznek a korábbi évtizedekben „megszokottaktól” (Barker 2003). Terroristátámadások gyakran a legváratlanabb helyeken, különböző politikai beállítottsággal és gazdasági körülményekkel rendelkező országokban történnek, és rendszerint függetlenül egymástól. Az eddigi tapasztalatok alapján a támadások okai és célpontjai nehezen prognosztizálhatók, így helyszínei, módjai és időpontjai előre kiszámíthatatlanok.

Korunkban a terrorizmus veszélyét különösen növeli, hogy a mindennapos tevékenységünk hatékonyságát segítő eszközök – az információs technikai forradalom vívmányai – ugyanolyan jól felhasználhatók a terrorcselekmények előkészítésére és végrehajtására is. Az elmúlt évtizedekben az információs technika és technológia olyan látványos minőségi és mennyiségi fejlődésen ment (és megy) keresztül, amely korábban elképzelhetetlen változásokat eredményezett mind a médiában, mind az információk tárolásban és információ-továbbítás (átvitel) technológiájában. A média által biztosított nyilvánosság jó lehetőséget teremt a terroristák számára (Sükösd M. 1999). Az információ áramlása és a széleskörű hozzáférés könnyebbé teszi a potenciális célpontokról az adatgyűjtést, a felderítést. Az informatika látványos fejlődése és az Internet elterjedése is megkönnyíti a terrorakciók szervezését és előkészítését.

A terrorizmus célja valójában a biztonság aláásával csökkenteni az állam tekintélyét és a kormányzatok legitimációját, továbbá olyan légkör teremtése, hogy az emberek ne tudjanak félelem nélkül, szabadságban élni. Éppen ezért a terrorizmus elleni küzdelem legfőbb gondját az jelenti, hogy nem, vagy nehezen számítható ki a terrrorszervezetek működése, mivel támadásaikat időben és térben jelentős eltérésekkel hajtják végre. A terrorakciókat nem lehet a hagyományos értelemben vett módszerekkel megelőzni és elhárítani. Ráadásul a kormányzatoknak folyamatosan „láthatatlan” ellenséggel kell küzdeni. Az eddigi terrortámadások kapcsán az egyes országok, kormányok által kidolgozott és bevezetett biztonsági intézkedéseknek köszönhetően ma már a terroristák egyre inkább a „puhább”

célpontok ellen terveznek és hajtanak végre támadásokat (Németh J. 2004). A terrorista csoportok a könnyebben pusztítható célok közé sorolják a nyilvános helyeket. Ezek közé tartoznak a turisztikai látványosságok, közintézmények, templomok, a közlekedési létesítmények, műtárgyak és járművek. Az ún. „puhább” célpontok ellen elkövetett, halálos áldozatokkal járó merényletek kisebb kockázattal járnak, mint a „klasszikusnak” számító politikai gyilkosságok. Ugyanakkor ezek az akciók is felkeltik a média és közvélemény érdeklődését, így alkalmasak terroristák a céljainak megvalósítására.

Az ezredforduló több mint két évtizedes időszakában (1980-as évek elejétől napjainkig) gyökeresen megváltoztak a kor biztonsági kihívásai is. A háborús kockázatok enyhülése mellett, egyre inkább fokozódott a társadalmi- és gazdasági változásokkal összefüggésbe hozható, valamint a közvetlenül nem katonai természetű – pl. a terrorizmus – erőszakos cselekmények száma, amelyek egyre inkább a városi és a közlekedési infrastruktúra működésének akadályozására (rongálás, robbantás, stb.) irányult. Ebből eredően a városi és a közlekedési infrastruktúra veszélyeztetettsége jelentősen megváltozott, és mértéke is megnőtt. (Léder F., Tóth B., 1998)

A NAGYVÁROS, TERRORTÁMADÁSOK LEHETSÉGES CÉLPONTJAI

A nagyvárosok terrorfenyegetettségét csak abban az esetben tudjuk reálisan megítélni, ha elkülönülten vizsgáljuk a város térszerkezetéből eredő helyi kockázatokat, a városi forgalommal összefüggő hálózati kockázatoktól. Ezt a megkülönböztetést arra lehet alapozni, hogy más jellegű veszélyforrásokat rejtjenek a város egyes területeinek beépítettségéből, az ott folyó tevékenység jellegéből, az adott objektum befogadó-képességéből stb. adódó kockázatok, mint az infrastruktúrákra, így a közlekedési rendszerekre, hálózatokra vonatkozó. A hálózati jellegű infrastruktúrákra, így a közösségi közlekedési rendszerekre (városi közlekedési rendszerekre) is jellemző, hogy működésük nemcsak a saját rendszerük megbízhatóságától, hanem annak üzemeltetéséhez szükséges egyéb feltételek meglététől is függ. Ezért a közösségi közlekedési rendszer – mint infrastruktúra – csak abban az esetben képes megbízhatóan működni, ha nemcsak a saját rendszere, hanem annak üzemeltetéséhez szükséges egyéb infrastruktúrák (pl. villamos-energiaellátás, hír- és távközlés, közműszolgáltatás, közút-fenntartás!) is működőképesek.

A nagyvárosok nem véletlenül váltak a terrorizmus kedvelt célpontjaivá. A magas népsűrűség, a metropoliszokban található politikai, közigazgatási, pénzügyi és gazdasági, energetikai, városi tömegközlekedési, valamint turisztikai infrastruktúra alkalmas arra, hogy viszonylag kis erővel (létszámmal) nagy pusztítást lehessen végrehajtani. A városokban elkövetett terrortámadások (különösen az emberi áldozatokkal és nagy anyagi kárral járók) alkalmasak arra is, hogy felhívják a médián keresztül a figyelmet a terrorszervezetre (és céljaira), és nem utolsósorban félelmet keltve csökkentsék a társadalom biztonság érzetét. A nagyváros fejlettebb településszerkezete és infrastruktúrája ráadásul „segítséget is nyújt” a terroristáknak, mind a célpont felderítésében, megközelítésében, mind a támadást követően a helyszín elhagyásához is (Horváth A. 2006/c). (A terroristák a nagyvárosokban könnyebben válnak „láthatatlanná” mint kisebb lélekszámú, kisforgalmú településeken).

A nagyváros térszerkezetének és infrastruktúrája sebezhetőségének vizsgálata, elemzése ad(hat) alapot az illetékes szerveknek az objektumok védelmének és az azok ellen irányuló terrorcselekmények elhárításának megszervezéséhez. Természetesen – a terrorizmus sajátosságaiból eredően – az egyes városok, vagy infrastruktúra rendszerek terrortámadások elleni védelmének megszervezését célszerű azonos alapelveken (egységes szemléletben) kezelni, de csak a helyi sajátosságok szigorú figyelembe vételével (Horváth A. 2006/b).

A NAGYVÁROSI KÖZLEKEDÉSI RENDSZER TERRORFENYEGETETTSÉGE

A közlekedési rendszerek működőképességének biztosítása mindenkor, minden társadalomban és minden országban alapvető feladat. Már az ókori történelem is tesz említést a szállítási utak elleni támadásokról, a középkor és az újkor kezdetén elszaporodott tengeri kalózokról, később a postakocsi rablásokról. A modernkori terrorizmus kialakulása is a közlekedéshez, elsősorban a repülőgépek jogellenes hatalomba kerítéséhez és a légi közlekedés elleni szabotázs akciókhoz köthető. Napjainkban a légi közlekedésen kívül a többi közlekedési ágazat pályái, útvonalai, műtárgyai, objektumai és járművei is a terrorizmus célpontjaiként szerepelnek.

Az infrastruktúrák egészének veszélyeztetettségét rendszerint csak általánosságban lehet megállapítani: Konkrét intézkedések megtételéhez elengedhetetlen az egyes objektumok (résztevékenységet, területek) valós fenyegetettségének – az adott objektum jellegére, feladatára és területére vonatkoztatva – meghatározása. Az egyes objektumokra (részterületekre) számított eredmények adnak alapot a teljes (városi, vagy közlekedési) infrastruktúra működőképességének fenntartásához szükséges feltételek, erőforrások, kapacitások és tartalékok tervezéséhez. (Léder F., Tóth B., 1998)

A közlekedési rendszerek elleni lehetséges terrortámadások – az emberi áldozatokon és anyagi károkon kívül – főként a kedvezőtlen közlekedési hálózattal rendelkező országokat érinthetik súlyosabban. Magyarország felszíni közlekedési hálózata erősen sugaras szerkezetű, és alapvetően egy (Budapest) központú, ami egy-egy kritikus műtárgyánál bekövetkező „folyamatossági hiány” (pl. rombolás, baleset, hóakadály, sztrájk) komoly forgalom kiesést eredményezhet. Sok esetben még más (alternatív) útvonalakra tereléssel sem oldható meg a szokásos forgalom nagyságának fenntartása.

Feltétlenül meg kell említeni, hogy a közlekedési rendszer pálya (út, vasút, felső-vezeték rendszer) és jármű (vontató és szállító) elemeinek védelmét sok tekintetben nehezebb megoldani a terrortámadásokkal szemben, mint annak állandó jellegű objektumait (vasútállomások, pályaudvarok, hidak). A vasúti és autóbusz pályaudvarokat és az áruszállítás létesítményeit az utazó közönség és az áruforgalom lebonyolításának igényei szerint alakították ki. Ezek nélkülözik ugyan a hatékony védelmet szolgáló technikai ellenőrző rendszereket és védelmi berendezéseket, de a technikai fejlettség már lehetővé teszi, hogy a járműveket, járműszerelvényeket menetközben ellenőrizni lehessen. Ugyanakkor az állomásokról elindult járművek, szerelvények jogellenes hatalomba kerítését és a járművek ellen elkövetett robbantás merényleteket technikailag még nem lehet megakadályozni.

A terrorszervezetek számára a városi közlekedés és ezen belül a személyközlekedés járművei és létesítményei könnyen felderíthetőek, és támadható célpontot jelenthetnek. A közlekedési hálózat összetettsége ellenére a városokban viszonylag jól kiszámítható a forgalom nagysága, ciklikussága és iránya. A közlekedési eszközöket egyidejűleg sokan veszik igénybe, az utasok tömeges jelenléte rendszerint az adott viszonylat csúcsidejéhez köthető. A tömeges igénybevétel miatt a pályaudvarokat, és a megállókat ezért általában úgy alakítják ki, hogy megközelítésük ne okozzon különösebb nehézséget. A városi közösségi közlekedést igénybe vevőket napjainkban korszerű informatikai eszközök és rendszerek segítik a járatok és járművek kiválasztásában. A technikai fejlettség ma már ott tart, hogy akár egy forgalmasabb csomópontban arról tájékozódhat az utas, hogy a következő autóbuszjárat mikor érkezik a megállóba. Az utas- információs rendszer eszközei azonban nem csak az utasoknak szolgáltatnak hasznosítható információkat, hanem sajnálatos módon hathatós segítséget nyújthatnak a terrorszervezetek vezetőinek is a terrortámadások előkészítéséhez és

végrehajtásához (Horváth A. 2006/a). A fentiek mellett a városi közlekedés elleni terrorakciókat megkönnyíti, hogy a közösségi közlekedési eszközök igénybevétele nemcsak nyilvános, hanem tömeges is. Így könnyebben juthatnak be a terroristák a célobjektumokba (állomás, jármű) és „pontosan tervezhető” a cselekmény eredményessége, a lehetséges áldozatok száma, a károk mértéke. Ez az alapvető oka annak, hogy a terrrorszervezetek egyre gyakrabban jelölik ki támadásaik célpontjául a városi közlekedés járműveit és infrastrukturális létesítményeit.

A városi közlekedés mindennapos működésének egyik fontos jellemzője, hogy a város jellegének és adottságainak figyelembe vételével kialakított (a város-szerkezetéhez és a lakosságának közlekedési szükségleteihez és szokásaihoz igazított) közlekedési hálózaton, milyen eljutási sebességet tudunk elérni. Az is ismert tény, hogy az eljutási sebesség mértéke nagymértékben függ, az utak műszaki jellemzőitől és az adott időszakban jelentkező forgalmi terheltségtől. Ezeket a tényezőket rendszerint a műszaki állapotok javításával és a „beépített kapacitások” növelésével lehet befolyásolni. Az adott útvonal átbocsátóképességének (kapacitásának) növekedésével arányosan emelkedik a forgalom sebessége (sok esetben az átbocsátott járművek mennyisége is), ezáltal csökken az eljutási idő is. Tekintettel arra, hogy a városi közlekedési hálózatot veszik igénybe a nem kötöttpályás közösségi közlekedés járművei mellett esetenként a közúti villamosok és a trolibuszok is, ezért a városi közúthálózat terhelése jelentősen megnövekedhet (lassul a forgalmi áramlat sebessége), így a közösségi közlekedési eszközökön utazók eljutási időszükséglete is emelkedik, hosszabb időt töltenek el a járművek utasterében. Reményeink szerint az eddig tárgyaltakból világosan kitűnt, hogy a közösségi közlekedés járművei potenciálisan célpontjai lehetnek a terrortámadásoknak, ezért az utasok biztonsága azt követeli, hogy minél rövidebb időt töltsenek veszélyeztetett helyen. Ez csak úgy érhető el, ha a közlekedési hálózaton e járművek számára megfelelő feltételeket, illetve előnyöket biztosítunk. A városi közlekedési hálózat forgalmának rendszeres vizsgálatával megállapíthatók azok az útszakaszok, objektumok és csomópontok, ahol ezeket a feltételeket, előnyöket biztosítani szükséges. A vizsgálat elvégzésére számos módszert lehet alkalmazni, azonban a veszélyeztetettség szempontjából az lehet az egyik járható út, hogy a városi közlekedési hálózat közösségi közlekedési útvonalai mentén vizsgáljuk a legnagyobb forgalmi intenzitású csomópontokat és objektumokat (vasút-, metró-, HÉV- és autóbusz állomásokat, az átszálló-helyeket és nagyobb forgalmú megállóhelyeket) és azok kapcsolatrendszeit. (Tóth A. 2008.) A vizsgálatból levont következtetésekből prioritásokat állapíthatunk meg, és javaslatokat fogalmazhatunk meg a szükséges intézkedésekre.

A FELSZÍNI KÖZÖSSÉGI KÖZLEKEDÉSI RENDSZEREK TERRORFENYEGETETTSÉGE

A felszíni közösségi közlekedési rendszerek (és eszközeik) terrorfenyegetettségét nagymértékben befolyásolják azok a körülmények, amelyek az üzemeltetésükkel függnek össze. Nyilvánvaló, hogy a kötöttpályás közlekedési rendszerek csak több feltétel együttes megléte esetén működőképesek, ezért lényegesen több lehetőség van arra, hogy üzemét megzavarhassák (Tóth A. 2006). Ezek közé tartoznak az egynél több pályaszerkezetet igénylő közösségi közlekedési eszközök, így:

- a kettő pályaszerkezetet – közúti hálózat és felső-tápvezeték rendszer – igénylő trolibusz-, valamint a vasúti vágány mellett a biztosító és jelzőrendszert igénylő autonóm vontatású vasúti hálózat, továbbá

- a három pályaszerkezetet – vasúti vágány, felső-, vagy alsó tápvezeték rendszer, biztosító- és jelzőrendszer – igénylő Metró, HÉV, közúti villamos és villamosított vontatású vasúti hálózat.

Szerencsésebb helyzetben vannak a nem kötőtpályás közösségi közlekedési rendszerek (autóbuszok), mivel működésük kevésbé függ más infrastruktúrák szolgáltatásainak állandó meglététől, az egyes problémás helyeket viszonylag egyszerűbben megkerülhetik, így folyamatos üzemük is könnyebben fenntartható.

KÖTÖTTPÁLYÁS KÖZLEKEDÉSI RENDSZEREK

A kötőtpályás közlekedési rendszerek – megnevezésükből is következik – rendszerint egy sajátos jellemzőkkel kialakított, általában nem mozgatható pályához kötődnek. Ebből eredően a térben (itt a városi teret kell érteni) való elhelyezésük „állandónak” tekinthető, paraméterei nem, vagy csak jelentősebb idő és anyagi ráfordítások után változnak. Ebből eredően a kötött pályás közlekedési rendszerek szinte valamennyi eleme könnyen és részletesebb felderíthető, megismerhető. (Ideális terep a terrorista hírszerzés számára!). A közösségi közlekedési rendszerekről tudható, hogy funkciójuk ellátásához szükséges rendszerelemek elhelyezése között gyakran jelentős távolságok vannak, illetve a szállítóeszközök (járművek) mozgásához szükséges „pályát” térben elnyújtva több km-es távolságokra kell kiépíteni. Ily módon az egyes vonalak sokaságából felépülő hálózat adott esetben több-tíz, vagy több-száz km-es építményláncot (pályatestet, energia-ellátási, és hír- távközlési vezetékrendszereket), keresztezési és elágazási csomópontot, valamint az energia-ellátás szempontjából több „betáplálási” helyet is jelenthet. Amennyiben a kötőtpályás közösségi közlekedési rendszer a már meglévő közúti infrastruktúrára épül, akkor a fentiekben túl még biztosítania kell azt is, hogy üzele lehetőleg ne zavarja a közúti forgalmat, az ott haladók biztonságát. Belátható, hogy a kötőtpályás közösségi közlekedési rendszereknek a városi szerkezetébe történő beépítése és annak infrastruktúrájához való kapcsolódása bonyolult és hosszú távú gondolkodást igénylő feladat, melynek megoldása nagyon sok, egymással összefüggő feltétel megteremtése árán jöhet létre.

A kötőtpályás közlekedési rendszerek terrorfenyegetettségének mértéke alapvetően attól függ, hogy az adott ágazatnak milyen szerepe van a város mindennapi közlekedési szükségletei bonyolításában. Gyakorlati tapasztalatokból tudjuk, hogy a nagyvárosok közösségi közlekedési szükségleteinek kielégítése csak különböző kapacitású (óránkénti utasszámban meghatározható szállítóképességű) rendszerek komplex alkalmazásával oldható meg. Nyilvánvaló, hogy néhány tízezres lélekszámú településen jelentkező városi közlekedési igények kielégítésére nem lehet gazdaságosan metrót építeni, de a lényegesen kisebb beruházással járó autóbusz közlekedés megszervezése megfelelő kapacitású és kultúrált megoldást jelenthet. Villamos-vonalak építése is csak ott gazdaságos, ha az adott irányban rendszeresen egyidejűleg tömegesen (és tartósan) jelentkezik a szállítási igény. Amennyiben a felmért szállítási szükségletek azt indokolják, hogy az adott helyen kötőtpályás közösségi közlekedés üzemeltetése lenne gazdaságos, célszerű tovább vizsgálni a külső feltételeket is.

Ennek során figyelembe kell venni, az adott eszközrendszer (jármű) szállítóképességét, az üzemi helyek (vonalak, megálló- és átszállóhelyek, állomások, pályaudvarok, egyéb létesítmények) kapacitásait, kieséséből eredő zavarok elhárításának lehetőségét, továbbá a vonali létesítmények sérülékenységét (szükség szerint őrzésére fordítandó kiadásokat) stb., valamint az üzemeltetéshez szükséges egyéb erőforrások (pl. energia, járulékos beruházási igények terület és szakember igénye) meglétét, illetve megteremtésének lehetőségét. (Tóth B. 1998.)

A kötőtpályás közlekedési rendszerek létesítésének, üzemeltetésének fentiekben – vázlatosan – bemutatott alapelemei szolgálnak kiindulópontként a meglévő rendszerek terrorfenyegetettségének vizsgálatához is. Mivel az ismert kötőtpályás rendszerek felépítése

elemeikben alapvetően nem különböznek, így az általánosan valamennyire vonatkozó felsorolásnál, csak a kivételeket fogom az adott közlekedési eszközre külön nevesíteni.

A kötöttpályás közösségi közlekedési rendszerek (metró, HÉV, villamos, trolis) mindegyike magába foglalja a hálózatot, a járműállományt, a működést biztosító létesítmény rendszert, a teljes rendszer működését biztosító egyéb ellátási rendszerekhez való csatlakozási pontokat, valamint a működést biztosító szakállományt.

A kötöttpályás közösségi közlekedési rendszer (ebben a felsorolásban, továbbiakban: rendszer) a terrorfenyegetésnek kitett elemei:

a) A közlekedési hálózat, ez a rendszer legnagyobb kiterjedésű része, amely magába foglalja:

- azokat a közlekedési utakat (pályákat), amelyek a közlekedési igény források keletkezési és végpontjait kötik össze egymással, kapcsolódnak a külső környezethez, valamint egymáshoz. A pályák (a trolis kivételével) rendszerint különböző típusú – de azonos nyomtávolságra elhelyezett – vasúti sínek, amelyek kialakítása és rögzítése a rajta közlekedő járművek tömegétől és sebességétől függő. A felszínalatti közösségi közlekedésnél a pálya fogalmába beleértendő az alagútrendszer is, függetlenül attól milyen mélységben és milyen technológiával épült. A villamos vasúti sínek egy része olyan megoldással van lefektetve és rögzítve, hogy rajta a közúti forgalom akadálymentesen bonyolódhasson. A trolibusz mozgása során pályaként a közutat használja, amelyen viszonylag „szabadon” közlekedik.
- a pályák azonos szintű keresztezési, csatlakozási (elágazási) pontjait, amelyek lehetőséget teremtenek más vonalakra, történő átjárásra. Az elágazási (csatlakozási) pontokon a vasúti rendszerhez kialakított, de az alkalmazott sínhez megfelelő váltószerkezeteket alkalmaznak, amelyek többsége elektromosan vagy távvezérléssel állítható. A trolibuszok esetében az elágazásokat biztosító váltószerkezetek nem a pályán, hanem a munkavezetékeken vannak elhelyezve. Állításuk a jármű mozgása által elektronikusan történik;
- a pályák nyomvonalában épült olyan létesítményeket, amelyek a terepakadályok (árok, patak, folyó, völgy, keresztező útvonal, közműalagút stb.) áthidalására szolgálnak és ezen létesítményre rögzített pályán történik a jármű közlekedése. Ugyancsak e kategóriába sorolhatók azok a létesítmények, amelyek a pályát külön szinten (rendszerint felette) keresztezik. Nem tartoznak ezen rendszerhez azok az áthidalások, amelyek más infrastruktúrák (gáz, víz, elektromos energia, stb.) kiépítésével jöttek létre, és közvetlenül nem tartoznak a közösségi közlekedési rendszert támogató infrastruktúrák köréhez;
- a hálózat részét képezik azok az utasforgalom számára létesített megállóhelyek, állomások is, amelyek egyben a szállítási folyamat ideiglenes megállítását is szolgálják. A megállóhelyek többsége a villamos és trolibusz közlekedésnél egyszerű kialakítású (leginkább az utasok tájékoztatására és esetenként biztonságérzetének fokozására alkalmasak). A HÉV és a metró (ideértve a földalatti vasutat is) állomásai és megállóhelyei jelentősebb építmények, amelyek az utasok le- és felszállásán kívül számos forgalomtechnikai feladatokra és egyéb szolgáltatásokra is alkalmasak;
- ugyancsak hálózati elemként kezelendő a járművek mozgatásához alkalmazott vontatási energia-ellátó vezetérendszer, a munkavezetékekkel (a metrónál –

vezetősín) és azok rögzítését szolgáló tartószerkezetekkel és tartósodronyokkal. A tartószerkezet legalább olyan fontos része a rendszernek, mint a munkavezeték!

- önálló elemként kell kezelni a kötőtpályás járművek biztonságos közlekedését elősegítő és ellenőrző jelző és biztonsági berendezéseket. A villamos és troli közlekedésnél a sajátos jelző és biztonsági rendszerek mellett kötelezően figyelembe kell venni a közúti forgalom irányítás jelzőrendszerét is. (Tóth A. 2008.)

b) Járműállomány

A közösségi közlekedés járművei a rendszer olyan elemei, amelyek működésük folyamán – térben és időben – önállóan (vagy kis csoportokba rögzítetten) mozognak a hálózaton, ezzel egyedülálló – sebezhető – pontot képeznek a rendszer biztonságában. A járművek az utasforgalom lebonyolításának eszköze. Típusuktól, kialakításuktól függően legkevesebb 30 – legfeljebb 300 utas (Metró és HÉV szerelvények esetében maximum 800 - 1000 utas) egyidejű, egyirányú helyváltoztatására alkalmasak. Közlekedhetnek önállóan (trolik), vagy zárt szerelvényként (kettő - hat jármű egy szerelvényben). A járművek menetközben zárt ajtókkal közlekednek, ezért bármilyen esemény hatására (pl. gyors fékezés) előfordulhat, hogy az utasok közül valakinél „menekülési kényszerhelyzet” lép fel, melynek hatása több utastársra is kiterjedhet, így a járművön pánikot okozhat. Különösen élessé válhat ez a helyzet, ha ez a jelenség a földalatti közlekedés járművein történik. Ezekből egyenesen következik, hogy a kötött pályás közlekedés járművein utazókat akár végtelenül is meglehet „ijeszteni” –, a „zárt hely” pedig alkalmat adhat arra, hogy az utasokat szándékosan megfélemlíthessék, illetve túszul ejtsék. Minél kisebb a jármű belső tere, annál inkább valószínű a „végtelen pánik esemény okozásának” lehetősége, míg a nagyobb utaslétszámot befogadó járműveknél a „szándékos” cselekményeknek nagyobb a valószínűsége. E tekintetben a trolibuszok és a villamosok „előnyösebb” helyzetben vannak, mivel az utasok „elengedése” egyszerűbb, mint a metró, vagy HÉV szerelvények esetében.

c) A közösség közlekedési rendszerek működését biztosító létesítmények

- A kötőtpályás közösségi közlekedési rendszerek működéséhez – a pályák és a járművek működtetéséhez szükségeseken túl – még számos technikai feltételnek kell rendelkezésre állni. Ezek közé sorolhatók azok az üzemi létesítmények, amelyek a hálózatok működésének felügyeletével, üzemvitelük irányításával foglalkozó szakállomány elhelyezésére és tevékenységükhöz szükséges technikai feltételek biztosítására szolgálnak. Mivel ezek a „vezérlő-központok” – funkcionálisan a hálózat egészére, vagy egy-egy jelentősebb részére kiterjedő hatáskörűek lehetnek – az adott közösségi közlekedési alágazat üzemeltetésében meghatározó irányító és koordináló feladatot látnak el (pl. a metró központi forgalomirányító diszpécshatszolgálat), így működőképességük megzavarása, a felügyeletük alá tartozó hálózaton (vagy egy részén) jelentős üzemzavart okozhatnak. Ebből eredően e létesítmények kétség kívül veszélyeztetettek, illetve terrortámadások lehetséges célpontjai lehetnek.
- Ebbe a kategóriába tartoznak továbbá azok a létesítmények, amelyek a szállítóeszközök (járművek) mindennapos forgalomba bocsátásának, rendszeres ellenőrzésének, szükség szerinti javításának és tisztításának technikai feltételeit biztosítják. Ezek a létesítmények az ún. garázsok, vagy kocsiszínok. Tekintettel arra, hogy ezekben a létesítményekben, a forgalommentes időszakban (általában a késő esti óráktól a hajnali órákig) egyidejűleg nagyon sok jármű tartózkodik, ezért a járművek „koncentrációja” már eleve veszélyforrásnak tekinthető. Amennyiben azt is figyelembe vesszük, hogy e létesítményekből (többnyire csak egy ellenőrzött kijáraton át)

indulnak mindennap a hálózat meghatározott vonalaira a járművek, megállapítható ezen létesítmények olyan szintű veszélyeztetettsége, amely esetenként hosszabb ideig is kihatással lehet a hálózat egészének üzemére.

- A földalatti közösségi közlekedési rendszerek üzemeltetésével kapcsolatban ki kell emelni az alagutak (állomások, megállók) levegő ellátását, szolgáló berendezéseket, és építményeket. Tekintettel arra, hogy a kéreg alatti, illetve a mélyvezetésű vasutak (metrók) pályája rendszerint egy „csőben” halad, így a vonatok mozgásuk közben (mint egy dugattyú) maguk előtt tolják az előttük lévő levegőtömeget, ezzel meghatározott nagyságú túlnyomást okoznak a vonat előtti térben, és vákuumot létesítenek a mögöttük lévőben. A túlnyomás, illetve a vákuum kiegyenlítése céljából (és a friss levegő beáramlása érdekében is) az alagutakat megfelelő távolságokban szellőzőaknákkal kell ellátni. A szellőző nyílások felszínén lévő végeit lehetőleg a közforgalomtól elzárt területeken célszerű kialakítani és megfelelő őrzéssel, fizikai védelemmel kell ellátni. Ezen létesítmények az egyik legkritikusabb (legvesélyeztetettebb) pontjai a földalatti közlekedésnek (Tóth B. 1998), mivel a szellőztető rendszeren keresztül az egész alagútrendszer (beleértve az állomásokat is) levegője rövid időn belül (néhány perc alatt) szennyezhető, illetve mérgezhető. A létesítmények a kiemelten terrorfenyegetettek közé tartoznak.

d) Egyéb ellátási rendszerek csatlakozási pontjai

- A korábbiakban már említettük, hogy a közösségi közlekedési rendszerek üzemeltetéséhez szükséges feltételek egy részét – így az energiaszolgáltatást, a közművekkel való ellátást – az országos rendszerekhez való csatlakozások útján lehet (kell) biztosítani. Ebből, és a közlekedési rendszerek térbeli kiterjedtségéből adódóan az ellátórendszerekhez való csatlakozási pontok rendszerint nem egy helyre koncentrálnak, hanem a hálózat több pontján kerülnek kialakításra. Ezzel jelentősen javul a közlekedési rendszer üzemvitelének megbízhatósága. A több ponton történő „betáplálásnak” az üzemvitelnél tapasztalt előnye mellett azonban több feladatot is jelent, egyrészt az elosztórendszerek kialakításánál (bonyolultabb), másrészt az egymástól távoli betáplálási pontok megfelelő védelmének biztosításában. Ezen pontok védelméért a felhasználó – azaz a közlekedési üzemet irányító szervezet – felelős.
- Az üzemvitelre közvetlenül nem ható, de a szakszemélyzet munkaképességén keresztül igen jelentősnek számító veszélyforrásként kezelendő a létesítmények ivóvíz-ellátási rendszere. Függetlenül attól, hogy ebben az esetben is elsősorban az országos (területi) közműrendszerekhez csatlakoznak a létesítmények, azonban a csatlakozási pontok őrzésének, felügyeletének biztosítása itt is az adott közlekedési szervezet feladata.

NEM KÖTÖTTPÁLYÁS KÖZÖSSÉGI KÖZLEKEDÉSI RENDSZEREK

A közösségi közlekedési rendszer legattraktívabb rendszerét az autóbusz-közlekedés képezi, amely a közúti hálózat igénybevételével bármilyen (megfelelő kiépítettséggel rendelkező) közúton – a közúti közlekedés valamennyi résztvevőjére vonatkozó szabályok és jelzésrendszer alapján – előre meghatározott útvonalon és menetrend alapján végzi az utasok szállítását. A terrorszervezetek számára az autóbusz-közlekedés korábban és napjainkban is könnyen sebezhető célpontnak számít. Ennek okát abban kell keresni, hogy akár városi közösségi közlekedésben, akár városokon átmenő ún. közösségi távolsági forgalomban az autóbuszok meghatározott útvonalakon közlekednek, ezek mentén épülnek ki a megállóhelyeik és az autóbusz-pályaudvarok is. Így egy terrortámadás előkészítésekor nem

jelent különösebb nehézséget meghatározni az autóbuszok útvonalát, a járművek típusát, menetrendjét, és ezek alapján az egyes napszakokban, vagy akár meghatározott járatokon megközelítő pontossággal megbecsülni az utasok számát (Tóth A. 2008). A lehetséges áldozatok szempontjából az autóbusz-közlekedés elleni merényletek egyaránt fenyegethetik a viszonylag könnyen kiszámítható (pl a „hivatásforgalomban” résztvevők) és a szinte teljesen véletlenszerűen kiválasztott áldozatok csoportját. Az eddigi terrorakciók tapasztalatai azt bizonyítják, hogy a terrorcsoportok célpontjai között elsősorban a menetrendszerinti, közösségi közlekedésben használt autóbuszok szerepelnek.

Az előzőekben említett terrorfenyegetettsége és annak lehetséges támadási célpontja ellenére, ennek a közösségi közlekedési ágazatnak kisebb a veszélyeztetettsége, mivel a támadás célja is lokálisabb, üzeme kevésbé zavarható, emellett az eredeti menetrendszerinti közlekedés is gyorsan helyreállítható.

A FELSZÍNI KÖZÖSSÉGI KÖZLEKEDÉS ELLEN IRÁNYULÓ TERRORTÁMADÁSOK

Azt, hogy vasúti közlekedés elleni támadások súlyos következményekkel járhatnak már a II. világháború partizánakciói és az '50-60-as években kialakult gerilla hadviselés tapasztalatai bizonyították. A partizán harcmóddal szemben a terrorcsoportok nem csak a nyíltvonali pályaszakaszokat fenyegetik, hanem a városokban levő vonalakat és vasúti építményeket is. A vasúti pályaudvarok elleni merényletek veszélyességét már az 1980. augusztus 2-án történt un. „bolognai mészárlás” is bizonyította, de a nagyvárosi vasúti közlekedés sebezhetőségére a 2004. március 11-én végrehajtott madridi merénylet világosan rámutatott (Horváth A. 2006/b). A spanyol fővárosban és elővárosaiban, a reggeli órákban a csúcsforgalom idejére időzítve, külföldi származású, vagy külföldi terroristák egy jól előkészített és összehangolt akció során tíz (hátizsákba rejtett pokolgépet) bombát robbantottak fel négy különböző helyszínen, a városközpontba tartó vasútvonalakon, illetve a madridi pályaudvarokon (Tóth B, Horváth A. 2006). A merényletsorozatban 199-en vesztették életüket, csaknem 1500-an megsérültek. A madridi merényletek súlyosságához fogható robbantás sorozatra került sor 2006. július 11-én az Mumbai-ban is. A kontinensnyi ország és a térség pénzügyi központjának számító pénzügyi központban, a délutáni csúcsforgalomban az elővárosi vasúti hálózat ellen elkövetett terrortámadás-sorozatnak 179 halálos áldozata és 774 sérültje volt (Horváth A. 2009). Mumbai-t gazdasági és pénzügyi súlyánál, a lakosság nagyságánál fogva az utóbbi évtizedben rendre éri súlyos terrorakció, amelynek nagysége éppen a közösségi közlekedési rendszer elemei ellen irányulnak (Horváth A. 2009).

Az elmúlt évtizedekben, hazánkban vasúti közlekedésében a fenti példához hasonló jellegű, és nagyságrendű terrortámadások szerencsére, nem voltak. Ez nem jelenti azt, hogy a hazai közösségi közlekedési rendszer objektumait nem érik, illetve nem érhetik támadások. Komolyan kell venni a bűncselekményeket és szabotázsakciókat is. Közel másfél évtizede országosan „divattá vált”, hogy bizonyos személyek különböző szándékkal rendszerint vasúti pályaudvarokon elhelyezett robbanószerkezettel fenyegette meg az adott intézmény vezetőit, illetve „bejelentést” tett a az elhelyezett „bomba” robbanásáról. Mivel minden ilyen esetben a Rendőrség köteles az esemény bejelentését követően a helyszínt lezárni, a bent lévő személyeket a lehető leghamarabb a helyszínről eltávolítani és az objektumot teljes egészében átvizsgálni. Ez azt jelenti, hogy a fenyegetett objektumban a szokásos munkarend több órára megszakad, és az átvizsgálás időtartama alatt semmiféle tevékenységet, szolgáltatást vagy termelést nem végeznek. Gyakorlati tapasztalatok azt igazolták, hogy a riasztások néhány eset kivételével teljesen alaptalanok voltak, mindösszesen a pánik és a működési zavar keltését szolgálták. Az ilyen esetek pénzügyi és gazdasági kihatásai az állami szerveknek

(Rendőrségnek, MH tűzszerészeinek) is jelentős többletkiadást okoznak. Ezen eseteket nem sorolhatjuk a terrortámadások közé, azonban jellegét, célját és tendenciáját tekintve közelítenek a terrorizmus legfőbb céljaihoz.

A vasútállomások, illetve iskolák, bevásárlóközpontok, intézmények elleni „bombatámadással” fenyegető bejelentésekhez képest valamivel ritkábban fordulnak elő terrorfenyegetésnek tekinthető incidensek a közúti villamosok és a nem kötöttpályás közösségi közlekedési rendszer járművei ellen.

Bár nem a terrorfenyegetés „kategóriájába” tartozik, mégis meg kell említeni azt a nem kívánatos jelenséget, hogy az utóbbi években egyre gyakrabban fordulnak elő a késő esti, éjszakai járatokon – rendszerint csoportosan – elkövetett, a garázdaságot kimerítő és gyakran a súlyos testi sérülést okozó erőszakos cselekedetek a közösségi közlekedés járművezetőivel és/vagy a járműveken utazókkal szemben. Ezek az esetek – túl az anyagi károkozásokon – jelentős mértékben rontják az utazók (és a járművezetők) biztonságérzetét, ezáltal a közösségi közlekedés iránti bizalmat (Léder., Tóth B. 1998).

KÖVETKEZTETÉSEK

A modernkori terrorizmus eddigi történelme során a városi közösségi közlekedés ellen elkövetett akcióival világszerte komoly károkat okozott emberéletben és anyagi veszteségekben egyaránt. A károk nemcsak a városi személyközlekedés létesítményeire korlátozódnak és a következmények felszámolása sem fejeződik be a forgalom helyreállításával. Ezért hasonlóan az eltérő jellegű terrortámadásokhoz a következmények felszámolása komplex problémát jelent. Az ezzel kapcsolatos feladatokban a közigazgatási, társadalmi, gazdasági, katasztrófa- védelmi, illetve biztonsági szféra minden szervezete valamilyen szinten és formában érintett.

Egy, a városi közösségi közlekedési rendszer ellen elkövetett súlyos következményekkel járó terrorakció nemcsak a nagyváros és környékének közlekedési rendszerét érinti. Az elhunytak családjáról gondoskodni kell, a sérültek fizikai és pszichikai rehabilitációját meg kell szervezni. Az ilyen támadásokat a gazdasági élet is azonnal megérzi. A nagyobb merényletek hírére az áru- és értéktőzsdék szinte pillanatok alatt reagálnak, a nyersanyagok ára néhány perc alatt emelkedik, az üzleti élet szereplői szinte azonnal biztosabb befektetéseket keresnek. A bizonytalan részvényeiket, műkincsekbe, illetve aranyba kívánják fektetni. A tőzsdei árfolyamok stabilizálódása után egy-egy nagyobb terrortámadás gazdasági következményei nem múlnak el azonnal, hatásukat néhány gazdasági szektorban, – pl. a turizmus és a vendéglátóipar – hónapokig, esetleg évekig érezni lehet. A terrorcselekmények bekövetkezése után célszerű újra gondolni a biztonsági intézkedéseket, a lehetséges megelőzés eszközeit és módszereit (Horváth A 2006/c). Már maguknak a szigorító intézkedéseknek a bevezetése és későbbi fenntartása tetemes pénzösszegeket emésztene fel, de a korszerűbb figyelő és megelőző berendezések beépítése, a korábbi eszközök cseréje csak újabb jelentős anyagi ráfordításokkal valósítható meg. Ezért nem túlzás azt kijelenteni, hogy a városi személyközlekedés elleni terrortámadások hatásai akár évekig tartó súlyos következményekkel járhatnak.

Irodalomjegyzék

Barker J. (2003): A terrorizmus. HVG Kiadói Rt. Budapest

Horváth A, (2009) : A vasúti közlekedés terrorfenyegetettségének jellemzői a városokban. Hadmérnök. A Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar és a Katonai Műszaki Doktori Iskola on-line tudományos folyóirata. Budapest, IV. évfolyam 3. szám. pp. 180-189.

Horváth A. (2006/a): A városi személyközlekedés terrorfenyegetettsége. Új Honvédségi Szemle, a Magyar Honvédség Központi Folyóirata. LX évfolyam 4. szám Budapest, 2006. április. pp. 114-126.

Horváth A. (2006/b): A közúti, vasúti és vízi közlekedés terrorfenyegetettségének jellemzői. In: Tóth Péter (szerk), Válaszok a terrorizmusra II. A politikai marketing csapdájában. Mágustúdió. Budapest, pp 321-336.

Horváth A. (2006/c): Terrorfenyegetettség: célpontok, nagyvárosok közlekedés. Nemzetvédelmi Egyetemi Közlemények. A Zrínyi Miklós Nemzetvédelmi Egyetem Tudományos Lapja. 10. évfolyam 3. (tematikus) szám. Budapest, pp. 136-152.

Kövesné G. É. (2000): A városi közlekedési infrastruktúra és a minőség kapcsolatrendszer. In: Glatz Ferenc (szerk), összeállította: Magyar István. Közlekedési rendszerek infrastruktúráik. Megjelent: Magyarország az ezredfordulón Stratégiai kutatások a Magyar Tudományos Akadémián VI. A közlekedés és technikai infrastruktúrája. Magyar Tudományos Akadémia. Budapest, pp 121–142. o.

Mándoki P.(2000): A térségi személyközlekedés-fejlesztés infrastrukturális hatásai. In: Glatz Ferenc (szerk.), összeállította: Magyar István. Városi és térségi közlekedés. Megjelent: Magyarország az ezredfordulón Stratégiai kutatások a Magyar Tudományos Akadémián. MTA helytanulmányok. Magyar Tudományos Akadémia. Budapest. 2000. pp. 37-55.

Németh J. (2004): A veszély, amivel együtt kell élnünk – a terrorizmus. Szakmai Tudományos Közlemények. A Katonai Biztonsági Hivatal és a Magyar Honvédség Térképész Szolgálat kiadványa. Budapest, 2004. pp. 107–112.

Sükösd M. (1999): A terror színháza, avagy a publicitás oxigénje. Terrorizmus és a média. Belügyi Szemle. Belügyminisztérium Szakmai, Tudományos Folyóirata. 1999. 12. szám pp 54–65. o.

Tóth Attila: A fővárosi közösségi közlekedés és a vasúti közlekedés kapcsolatrendszerének vizsgálata, különös tekintettel a kritikus infrastruktúrák elleni terrorfenyegetettségre. Szakdolgozat, ZMNE BJKMK Katonai Logisztikai Intézet Közlekedésmérnöki Tanszék Budapest, 2008. 13-22, 95-101. oldal

Tóth B., Horváth A. (2006): Az infrastruktúrák veszélyeztetettsége In: Tóth Bálint (szerk), A kritikus infrastruktúrák védelmének hazai és nemzetközi szabályozása, lehetséges veszélyforrások azonosítása. Gazdasági és Közlekedési Minisztérium Védelemkoordinációs Főosztály, Szakmai vitaanyag, Budapest, pp 25-32.

Tóth B. (1998): A közlekedési infrastruktúra veszélyeztettségének vizsgálata az ország biztonságát befolyásoló kockázati tényezők tükrében. Közlekedési, Hírközlési és Vízügyi Minisztérium Szervezési Főosztály, 1998. (Belső használatra készített tanulmány.) pp. 41-85.

Léder F., Tóth B. (1998): Az új biztonsági kihívások kezelése a közlekedési, hírközlési és vízügyi tárca felelősségi területén In: Matus János és Pataki G. Zsolt: Biztonságunk az ezredfordulón, Megjelent: Zrínyi Miklós Nemzetvédelmi Egyetem Civil-Katonai-Kapcsolatok Központja CKK Könyvek 2. szám, Budapest, 1998. pp. 51-55

Deák Ferenc

deak@nct.hu

LÉTRADIAGRAM FORDÍTÓK ELMÉLETE PLC VEZÉRLÉSEK SZÁMÁRA I.

Absztrakt

A létradiagram egyszerű, programozási képzettséggel nem rendelkező szakemberek számára is érthető nyelv, ennek köszönhető, hogy az elmúlt 20-25 évben az egyik legnépszerűbb ipari programozási formává vált. Bár létradiagramos PLC (Programmable Logic Controller) rengeteg létezik a piacon, az ezeket feldolgozó fordítóprogramok irodalma meglehetősen szegényes. Az alábbi cikk az NCT új vezérléscsaládja számára kidolgozott PLC fordító elméleti hátterét mutatja be. Ez az algoritmus szakít az irodalom által ismertetett megközelítéssel, és gráfelméleti oldalról közelíti meg a kérdést, ami egy jól áttekinthető, szemléletes többlépcsős megoldást eredményez.

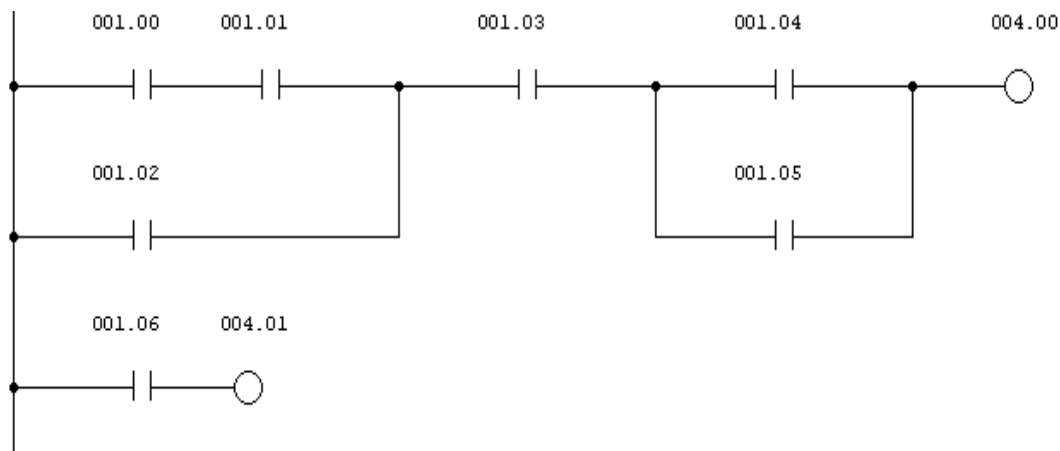
Relay ladder logic has become one of the most popular discrete control programming systems in the last 20-25 years. Programmable Logic Controllers (PLCs) usually can be programmed by wiring up relay contacts and coils on screen. This virtual circuit is transformed into a list of instructions in sequence. In this paper, the translation theory of relay ladder logic for new generation NCT controllers is examined. In contrast to solutions accessible in the literature this algorithm is multiphase, expressive and based on graph theory.

Kulcsszavak: PLC, Létradiagramm, fordító ~ PLC, Programmable logic controllers, relay ladder logic, compiler

BEVEZETÉS

Az NCT Kft. – akkor még gazdasági munkaközösségként – 1982-ben alakult. Munkatársai kezdetben az Elektronikus Mérőműszerek Gyára által gyártott Hunor vezérlők fejlesztésével foglalkoztak. A cég a kilencvenes évek elején NCT90 néven saját 16 bites eszterga-, majd pár évvel később maróvezérlővel lépett a piacra, majd szervomotorok és szervohajtások, CNC gépek fejlesztésével és gyártásával bővült a paletta. Az esztergavezérlők NC programnyelve

még a Hunor vezérlőkével egyezett meg, a maróvezérlők programozása azonban már Fanuc-kompatibilis volt.



1. ábra. Létradiagram

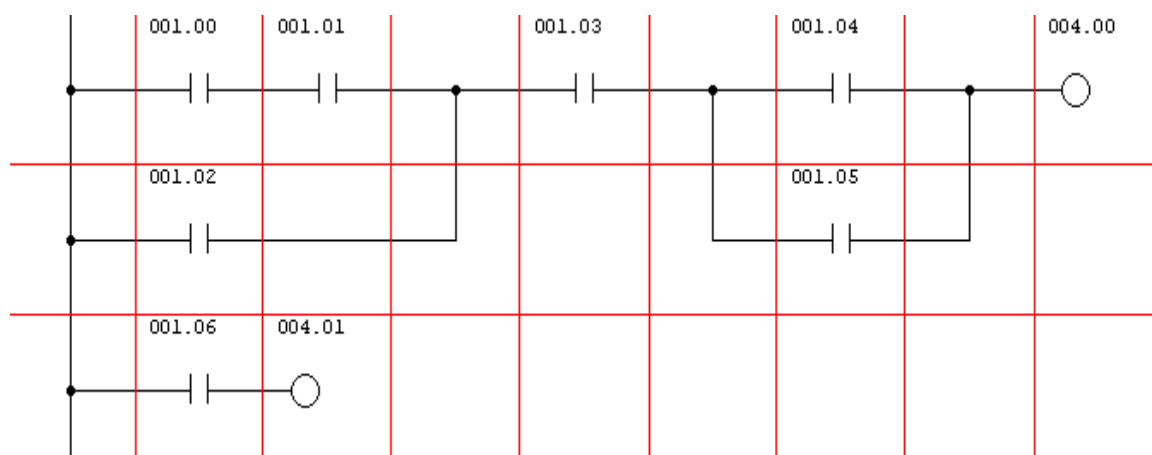
A következő generációváltás a kilencvenes évek végén történt a 32-bites NCT99 megjelenésével, melynél mind a maró- mind az esztergavezérlők programozása és jelentős részben a kezelése is Fanuc kompatibilissé vált.

```

LD 001.00
AND 001.01
OR 001.02
AND 001.03
LD 001.04
OR 001.05
AND LD
OUT 004.00
  
```

1. mnemonic kód: Az 1. ábrán lévő létradiagram mnemonic kódja

Tíz évvel később újabb nagyszabású termékmegújítás előtt állunk. A vezérlő többek között preemptív ütemezésű valós idejű operációs rendszert, a korábbinál lényegesen gyorsabb buszrendszert (EtherCAT [10]) kap.



2. ábra. Létradiagram mátrixos felépítése

Az NCT vezérlők a kezdetektől fogva integrált PLC-vel rendelkeztek, vagyis a programozható logikai vezérlő nem önálló hardver egység, hanem csak egy szoftver modul. Egy szerszámgép esetében a PLC feladata, hogy az általános célú eszterga vagy maró vezérlőt egy konkrét gép működési környezetébe illessze: irányítja a szerszám- és munkadarabcserét, pneumatikus munkahengereket működtet, induktív jeladók jeleit fogadja, illetve kommunikál a vezérlő CNC moduljával, ami a szervohajtások irányítását végzi.

Az NCT vezérlők PLC nyelve [3] jelenleg a Hunor vezérlőktől megörökölt alacsonyszintű szöveges kód, amit azonban nagyon kevesen ismernek. Mivel az NCT eladásaiiban egyre nagyobb súllyal van jelen az „OEM” (original equipment manufacturer) cégek (szerszámgépgyártók, szerszámgép-felújító vállalkozások) részére történő értékesítés, ezért szükségessé vált, hogy itt is a Fanuc vezérlőkhöz hasonló rendszert vezessünk be: ez a ma már többé-kevésbé szabványossá vált létradiagram.

A szabvány [1] ötféle programozási módot különböztet meg: utasításlista (mnemonickód), strukturált szöveg, létradiagram, funkcióblokk diagram és a sorrendi folyamatra [5]. Az állapotdiagramon [6, 7] és Petri-hálón [8,9] alapuló PLC programozási módok nem terjedtek el széleskörűen.

A létradiagram egyszerű, programozási képzettséggel nem rendelkező szakemberek számára is érthető nyelv, ennek köszönhető, hogy az elmúlt 20-25 évben az egyik legnépszerűbb ipari programozási formává vált.

Bár létradiagramos PLC rengeteg létezik a piacon, az ezeket feldolgozó fordítóprogramok irodalma meglehetősen szegényes. A témában született publikációk többsége azt tárgyalja, hogyan lehet egy megadott szabályrendszerből létradiagramot generálni [4]. Ennek további feldolgozásáról értekezik John T. Welch professzor cikke [2]. Az általa ismertetett algoritmus [2] csupán az alapelemek (kontaktusok, tekercsek) fordítását mutatja be, nem írja le a mai PLC-kben elterjedt bonyolult „soklábú” elemek számlálók, szubrutinok valamint ideiglenes relék kifejtését.

Az alábbi cikk az NCT új vezérléscsaládja számára kidolgozott PLC fordító elméleti hátterét mutatja be. Ez az algoritmus szakít az irodalom által ismertetett megközelítéssel, és gráfelméleti oldalról közelíti meg a kérdést, ami egy jól áttekinthető, szemléletes többlépcsős megoldást eredményez.

A cikksorozat három részből áll: az alábbi cikk ismerteti a létradiagram létrafokokra bontását, a második rész foglalkozik magával a fordítással, a harmadik rész pedig a speciális eseteket és az ipari alkalmazásokat mutatja be.

A LÉTRADIAGRAM

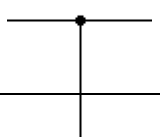
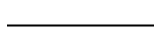
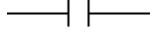
A PLC programot létradiagram formájában kell megírni, ami a hagyományos villamos áramút-tervek szoftveres megfelelője.

Kód	Magyarázat	A verem tartalma, az utasítás végrehajtása után
LD 001.00	A 001.00 bit tartalmát betöltjük a verembe	001.00
AND 001.01	- Kivesszük a verem tetején levő értéket - Elvégezzük a logikai ÉS műveletet a 001.01 tartalmával - Az eredményt betesszük a verembe	001.00 ÉS 001.01
OR 001.02	- Kivesszük a verem tetején levő értéket - Elvégezzük a logikai VAGY műveletet a 001.02 bit tartalmával - Az eredményt betesszük a verembe	001.00 ÉS 001.01 VAGY 001.02
AND 001.03	- Kivesszük a verem tetején levő értéket - Elvégezzük a logikai ÉS műveletet a 001.03 bit tartalmával - Az eredményt betesszük a verembe	(001.00 ÉS 001.01 VAGY 001.02) ÉS 001.03
LD 001.04	A verem tetejére betöltjük a 001.04 bit tartalmát	001.04 ----- (001.00 ÉS 001.01 VAGY 001.02) ÉS 001.03
OR 001.05	- Kivesszük a verem tetején levő értéket - Hozzávagyoljuk a 001.05 bit tartalmát - Az eredményt betesszük a verembe	001.04 VAGY 001.05 ----- (001.00 ÉS 001.01 VAGY 001.02) ÉS 001.03
AND LD	- Kivesszük a verem tetején található két értéket - Összeeszeljük őket - Az eredményt betesszük a verembe	(001.04 VAGY 001.05) ÉS ((001.00 ÉS 001.01 VAGY 001.02) ÉS 001.03)
OUT 004.00	Kivesszük a verem tetején található értéket, és beírjuk a 004.00 bitbe	üres

1. táblázat. A mnemonickód értelmezése

A PLC program fordítása a következő lépésekből áll:

1. A létradiagramot létrafokokra bontjuk.
2. Az egyes létrafokokat gráffá alakítjuk.
3. Kifejtjük az ideiglenes reléket.

Vezeték darabok		Engedélyezett szomszéd: főt, jobbra, lent
		Engedélyezett szomszéd: jobbra, lent, balra
		Engedélyezett szomszéd: főt, jobbra
		Engedélyezett szomszéd: jobbra, balra
Érintkező		Engedélyezett szomszéd: jobbra, balra
Kimenet		Engedélyezett szomszéd: balra

2. táblázat. Néhány létradiagram elem

A piacon léteznek olyan berendezések, amelyeket létradiagramban nem, hanem csak mnemonickódban lehet programozni. Ez esetben általában azt tanácsolják a leírások, hogy a PLC programozó rajzolja meg kézzel a létradiagramot. Ekkor a létradiagram lefordítása mnemonickóddá a PLC programozó feladata. A létradiagram és a mnemonickód között nincsen egyik irányban sem egyértelmű megfeleltetés. Az 1. ábrán szereplő létradiagram fordítása látható az 1. mnemonickód mezőben.

Az 1. táblázatban foglalt kód némi magyarázatot érdemel.

A mnemonic-kódra fordítást a PLC leírások intuitív folyamatként tárgyalják számos példával illusztrálva. A PLC programozók átlátva a létradiagramban levő kapcsolatokat „kisakkozzák” a megoldást. Ma már a létradiagram fordítók elvégzik ezt a munkát. Az alábbi cikk ennek a folyamatnak egy új módszerét ismerteti.

Ebben a leírásban létradiagram *vezeték darabokból*, *feltételekből* (*érintkezőkből*), és *kimenetekből* állnak. A vezeték darabok segítségével a feltételek között logikai (és/vagy) kapcsolatokat hozhatunk létre. A feltételeknek két fajtája van: az alaphelyzetben nyitott és az alaphelyzetben zárt érintkező. Kimenetből nagyon sokféle van, amelyektől jobbra már nem állhat más elem ezeket *jobboldali elemnek* is szokás nevezni. A létradiagram *létrafokokból* áll, melyek a baloldali alapvonalból indulnak ki, és jobboldalon pedig egy *kimenet* zárja őket. Lényegében az egy kimenethez tartozó létradiagram elemeket nevezzük *létrafoknak*.

A létradiagram elemek egymáshoz tehát vezetékekkel kapcsolódnak. Ha egy adott létradiagram elem és szomszédja között van vezetékes kapcsolat, akkor azt mondjuk, hogy a létradiagram-elem számára ez a szomszéd engedélyezett. Az 1. ábrán használt létradiagram elemek engedélyezett szomszédait a 2. táblázat mutatja.

```

minden (K kimenet típusú elemre)
{
    Választunk egy eddig nem használt C színt
    LétraFokokraBontás( K, C )
}

LétraFokokraBontás(Létradiagram-elem E, Szín C )
{
    ha ( E már a jobboldali alapvonal vagy E már be van színezve) akkor
        nem csinálunk semmit
    különben
    {
        E-t beszínezzük C színűre

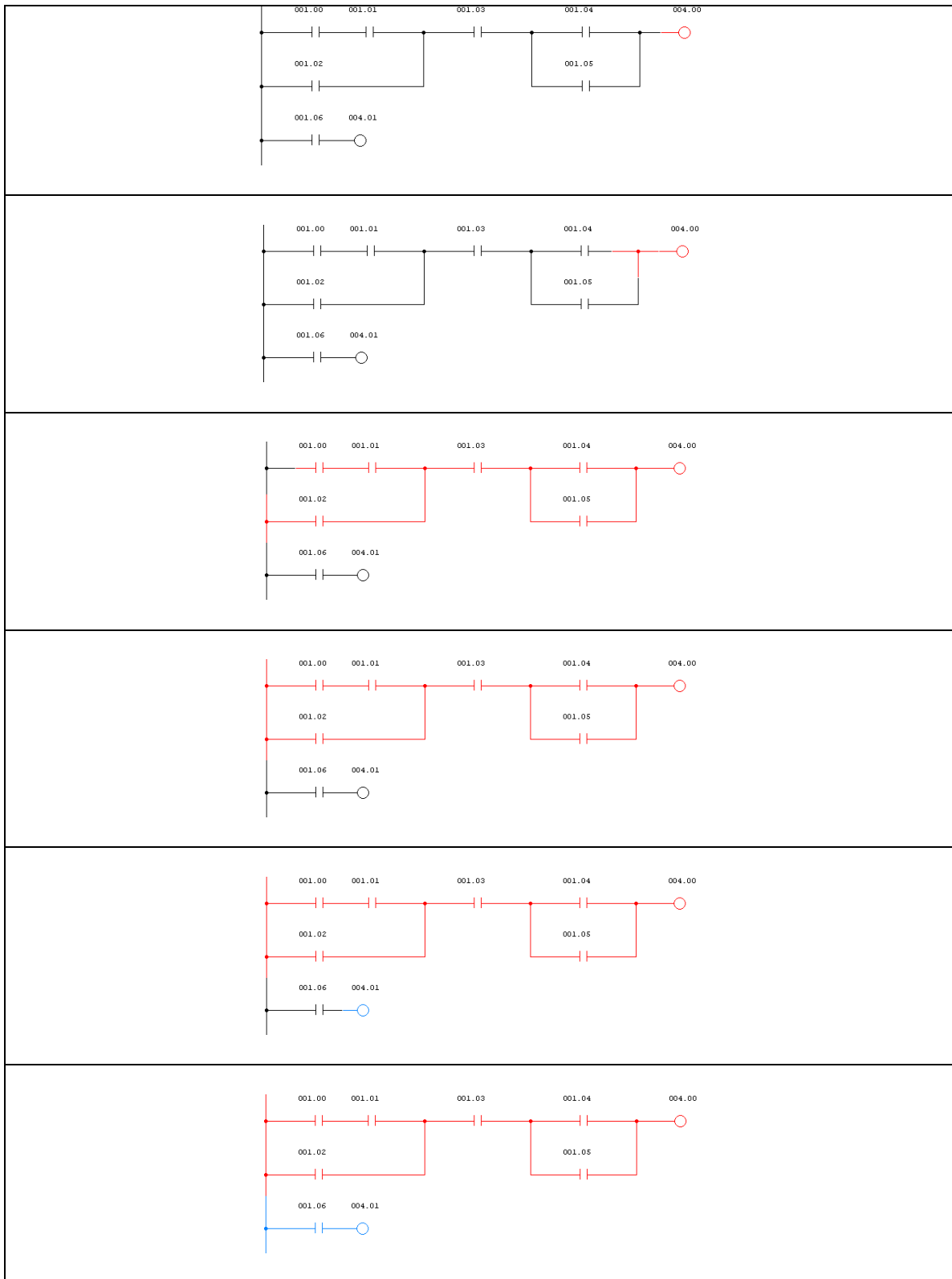
        minden ( S engedélyezett szomszédra )
        {
            LétraFokokraBontás( S, C )
        }
    }
}

```

1. Pszeudó kód: A létrafokokra bontás

Létradiagram mátrixos felépítése

A létradiagram elemeit egy kétdimenziós tömbben tároljuk a 2. ábrán látható módon. Az alábbi leírás nem tér ki minden részletre, a fordítási folyamatot a könnyebb érthetőség kedvéért csak fő vonalaiban ismerteti. A feldolgozás első lépése, hogy a létradiagramot felbontjuk olyan létradiagramok sorozatára, melyek mindegyike csak egyetlen létrafokot tartalmaz.



3. táblázat. A létrafokokra bontás néhány lépése egy példán

A LÉTRAFOKOKRA BONTÁS

A létrafokokra bontás célja, hogy független szegmensekre bontsuk a feladatot, melyeket önállóan lehet feldolgozni.

A kimeneteket a mátrixban balról jobbra és fentről lefele haladva keressük. A fentiek szerint végigmegyünk a mátrix összes elemén, és ha az adott elem kimenetnek számít, akkor választunk egy még nem használt szint és végrehajtjuk rajta a *LétreFokokraBontás* nevű eljárást. Az művelet algoritmusát 1. Pszeudó kód mutatja

Ebben az eljárásban az óramutató járásának megfelelően bejárjuk az adott elem összes szomszédját, és ha az engedélyezett, akkor rekurzív módon elvégezzük azon is a *LétraFokokraBontás* eljárást. A rekurzív hívásoknak akkor van vége, ha elértük a baloldali alapvonalat, vagy ha egy korábban színezett elemre lépünk. Ezt a bejárési módot *mélységi keresésnek* (*depth first search, DFS algoritmus*) hívják. Erre mutat egy példát a 3. táblázat

Az azonos színűre színezett létradiagram elemek jelentenek egy lépcsőfokot. A továbbiakban a lépcsőfokokat egymástól elkülönítve dolgozzuk fel.

ÖSSZEFOGLALÁS

A cikksorozat első részében a PLC program létrafokokra bontása került bemutatásra. A következő rész ezeknek az önálló programként értelmezhető programrészeknek végrehajtható szöveges kóddá alakítását fogja majd ismertetni. A harmadik rész tárgyalja, hogy a fordítási algoritmus kidolgozása után a létradiagram szerkesztő kényelmesebbé tétele a fejlesztés fő iránya. Hangsúlyozni kell, hogy a cikkben ismertetett elmélet alapján kialakított szoftver alkalmazásaként már egyre több termelő berendezés működik, főleg a járműiparban.

Felhasznált Irodalom

- [1] IEC 61131-3 Programmable controllers - Part 3: Programming languages International Standard, International Electrotechnical Commission, 2003
- [2] John T. Welch: Translating unrestricted relay ladder logic into Boolean form. Computers in Industry, 20 (1992) 45-61
- [3] NCT szerszámgép vezérlések PLC programozási leírása
http://www.nct.hu/pdf/NC_Documents/Magyar/Telepites/magplc.pdf
- [4] H. A. Barker, J. Song, P. Townsend: A rule based procedure for generating programmable logic controller code from graphical input in the form of ladder diagrams, Eng. Appli. of AI, 1989, Vol. 2, December
- [5] R. Wareham, Ladder diagram and sequential function chart languages in programmable controllers, Can. Mach. Metalwork., December 1988, pp. 25-26.

- [6] R. Devanathan, "Computer aided design of relay ladder diagram from functional specification" Int. Conf. on Industrial Electronics, Control and Instrumentation – IECON, 1990, pp. 527-531.
- [7] D. Harel, "Statecharts: a visual formalism for complex systems," *Sci. Comput. Programming* Vol. 8, 1987, pp. 231-274.
- [8] M. Courvoisier, R. Valette, J. Bigou and P. Esteban, "A programmable controller based on a high level specification tool," *IECON* 1983, pp. 174-179.
- [9] T. Murata, N. Komoda, K. Matsumoto and K. Haruna, "A Petri-net based controller for flexible and maintainable sequence control and its applications in factory automation," *IEEE Trans. Ind. Electron.*, Vol. IE-33, No. 1, February 1986, pp. 1-8.
- [10] IEC PAS 62407 Real-time Ethernet control automation technology (ETHERCAT™), International Electrotechnical Commission, 2005

Fleiner Rita

fleiner.rita@nik.bmf.hu

ADATBÁZISOK ELLENI FENYEGETÉSEK RENDSZEREZÉSE

Absztrakt

A publikáció az adatbázisok biztonságát fenyegető támadások rendszerezésével foglalkozik. Az adatbázis-biztonság alapfogalmainak értelmezése után különböző rendszerezési kategóriák kerülnek ismertetésre, majd a támadási pontok szerint jellegzetes adatbázis fenyegetések bemutatása történik meg.

The publication studies the taxonomies of the database security threats. After discussing the basic terms of database security, we present different methods for the classification of the database security threats, then according to the point of the attack we present typical database attack methods.

Kulcsszavak: *adatbázis-kezelő rendszer, adatbázis fenyegetés, adatbázis-biztonság ~ database management system, database security threat, database security*

Bevezetés

Napjainkban az informatikai rendszerek jelentős részének működésében lényeges szerepet játszanak különböző adatbázisok. Az adatbázis adatoknak számítógépekben tárolt, valamely adatmodell szerint strukturált gyűjteménye. Az adatbázisokban tárolt adatok kezelését speciális alkalmazások, az úgynevezett adatbázis-kezelő rendszerek biztosítják, melyek több felhasználós, hálózatos környezetben működnek. Adatbázis szervernek nevezzük az egy vagy több adatbázis-kezelő rendszert futtató számítógépet.

Az adatbázisok biztonságának megsértése (működésképtelenné tétele, meghamisítása, a tárolt adatok jogtalan megismerése) az adott informatikai rendszer és az általa nyújtott szolgáltatás

biztonságát fenyegeti. Ebből következően lényeges kérdés az adatbázisok megfelelő védelme, melyhez ismernünk kell az adatbázisok biztonságát veszélyeztető fenyegetések különböző formáit.

Jelen publikáció értelmezi az adatbázis-biztonság alapfogalmait, különböző kategorizálási szempontrendszer ad meg az adatbázis fenyegetéseinek osztályozásához, majd a támadási pontok szerint jellegzetes adatbázis fenyegetéseket gyűjt össze.

Adatbázis-biztonság alapfogalmai

Általános értelemben a fenyegetés olyan potenciálisan káros, vagy meg nem engedett hatás, amely a védendő objektumot károsan, egy megengedett mértéknél jobban befolyásolja. A fenyegetés érintheti a védendő objektum létét, érdekeit, állapotát, működését, vagy valamely tulajdonságát. A fenyegetések bekövetkezését a különböző sebezhetőségek teszik lehetővé. A sebezhetőség a biztonság alanyának egy olyan tulajdonsága, hiányossága, vagy gyengesége, amely lehetőséget teremt egy fenyegetés megvalósulására. [1]

A publikációban az adatbázisok információs jellegű fenyegetését vizsgáljuk. Ehhez szükséges az adatbázis-biztonság fogalmának tisztázása, ezen belül az adatbázis-biztonság alanyának és ennek védendő tulajdonságainak meghatározása. Az adatbázis-biztonságot az informatikai biztonság részének tekintjük.

Az adatbázis-biztonság fogalmának nincs széleskörűen elfogadott értelmezése. Az egyik típusú értelmezés szerint az adatbázis-biztonságot a tárolt adatok biztonsága jelenti, ezen belül az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, az adatbázis-kezelő rendszerekről ez a hozzáállás nem tesz említést. Ezt a szemléletmódot tükrözik a több kiadást megélt, felsőoktatásban is használt adatbázis témájú szakkönyvek [2, 3]. A másik típusú értelmezés a tárolt adatokat és az ezeket kezelő adatbázis-kezelő rendszert tekinti a biztonság védendő objektumának, ezt a hozzáállást megtalálhatjuk például az USA Védelmi Minisztériuma által kiadott Adatbázis-biztonság Technikai Megvalósítási Útmutatóban [4]. Mivel a témát a kritikus infrastruktúra védelem, illetve az informatika biztonság megvalósítása oldaláról is tanulmányozom, az adatbázis-biztonság fogalmába mind a tárolt adatok, mind az azokat kezelő adatbázis-kezelő rendszerek biztonságát beleérttem.

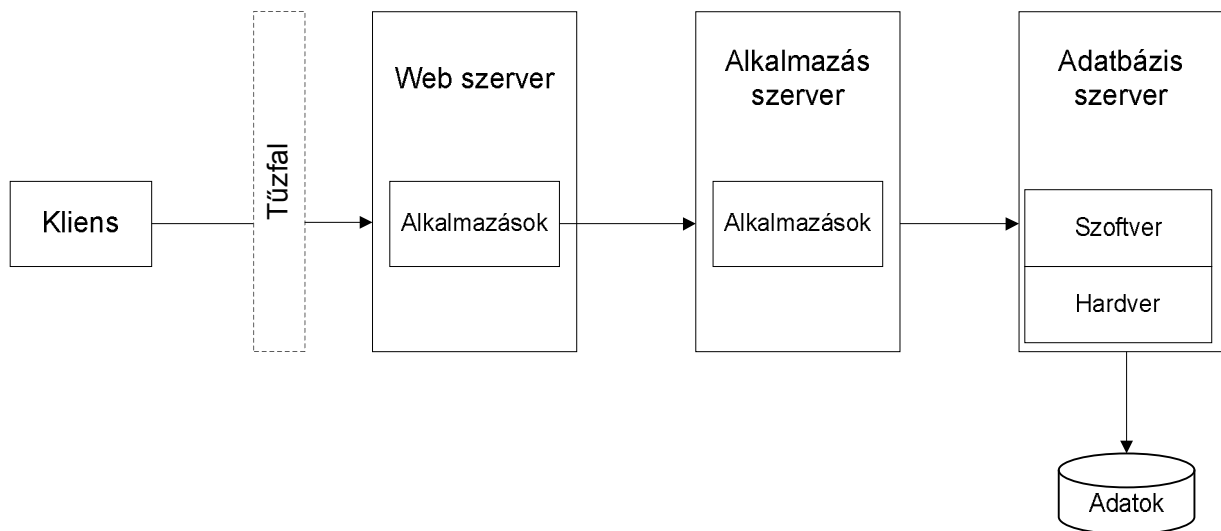
A biztonság alanyának meghatározása mellett szólni kell a védendő tulajdonságok halmazáról is, amik természetesen konkrét alkalmazások és környezetek esetén eltérőek lehetnek. Az adatbázisok védelme szempontjából a bizalmasság, sértetlenség és rendelkezésre állás biztosításának követelménye jelenhet meg. [5]

Adatbázisok nézőpontjából a bizalmasság: annak biztosítása, hogy az adatok csak az arra jogosultak számára legyenek elérhetőek, a bizalmasság elvesztése az információ illetéktelenek általi hozzáférését, megismerését jelenti. A sértetlenség azt jelenti, hogy a tárolt adatot, illetve az adatbázis-kezelő rendszert csak az arra jogosultak változtathatják meg, azok észrevétlenül nem módosulhatnak és nem törölhetők. A rendelkezésre állás annak biztosítása, hogy a felhatalmazott felhasználók hozzáférjenek a szükséges adatokhoz. A rendelkezésre állás megsértése azt jelenti, hogy az adatokhoz, illetve az adatbázis-kezelő rendszerhez való hozzáférés egy adott időtartamra

nézve ellehetetlenül vagy teljes mértékben megszűnik.

A letagadhatatlanság és a hitelesség biztonsági kritériumait adatbázisokkal kapcsolatban ritkán említik, ezek a sértetlenség biztonsági tulajdonság részének tekinthetők. A letagadhatatlanság az a biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az adatbázis-kezelő rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően, ezt auditálhatóságnak is szokták hívni. A hitelesség az adat forrásának, eredetének a valóságát jelenti.

Az adatbázisokat tartalmazó rendszerek felépítése nagyon összetett és változatos lehet. Az alábbi ábra egy olyan részstruktúrát mutat be, mely bonyolultabb rendszerekben is építő elem lehet. Ezt a struktúrát is szem előtt tartva fogjuk a fenyegetések rendszerezését elvégezni.



1. ábra: Adatbázisokat tartalmazó rendszerek architektúrája

Az architektúrában a kliens nem közvetlenül fordul az adatbázis-kezelő rendszerhez, hanem egy alkalmazást használ, ami az adatbázis adataihoz való hozzáférést is elvégzi. Az ábrán egy tűzfal látható a web szerver előtt, a gyakorlatban azonban az architektúra több pontján is előfordulhat. Gyakran az adatbázis-kezelő rendszereket futtató számítógépeket is tűzfal védelemmel látják el. A kliens tehát a web szerveren, alkalmazás szerveren és adatbázis szerveren keresztül éri el az adatokat. Az adatbázis szerver esetén berajzoltuk a hozzá tartozó platformot is, amit hardver és szoftver részekre osztottunk fel. Ezt persze a többi komponensre is bejelölhetnénk, de az adatbázis támadások szempontjából ennek van különösebb jelentősége.

A struktúra persze módosulhat, ha például több adatbázis szerver kommunikál egymással, gondoljunk az osztott adatbázis rendszerekre, vagy a magas rendelkezésre állás biztosítására kiépített fürtözött vagy tükrözött struktúrákra.

Szempontrendszerek az adatbázis fenyegetések osztályozásához

Mivel az adatbázisokban koncentráltan található érzékeny, kritikus információ, az adatbázisok védelme fontos feladattá vált. Az adatbázisok az architektúra legutolsó pontján, tűzfalak védelmével ellátva helyezkednek el, ezért sokáig ezek védelme az informatika biztonsági feladatok között nem szerepelt prioritásként. Mára a helyzet megváltozott. Egyrészt a webes alkalmazások elterjedtével támadásuk könnyebbé vált, a behatolók ellen kevésbé vannak elrejtve, másrészt integritásuk megsértése bizonyos esetekben helyreállíthatatlan vagy nagyon problémásan helyreállítható helyzetet teremtenek, illetve törvényi előírások is létrejöttek az adatok védelme érdekében. Egyre elterjedtebb igény, szükség jelentkezik vállalati szinten adatbázis biztonsági terv készítésére az adatvagyon védelme érdekében. A védelem megtervezéséhez fontos ismerni, hogy milyen veszélyek ellen lehetnek az adatbázisokat kitéve.

Az adatbázis fenyegetések rendszerezésével a célunk olyan rendszerezési kategóriák felállítása, melyek segítségével számbavehetők, áttekinthetők az általunk vizsgált fenyegetések. Olyan kategorizálási szempontokat keresünk, melyek egyértelmű besorolást tesznek lehetővé.

Osztályozni lehet a fenyegetéseket a támadó adatbázishoz való viszonya szerint. Adatbázis fenyegetések esetén vizsgálható, hogy külső vagy belső támadás zajlott-e le. Komoly felmérések, tanulmányok készültek annak kimutatására, hogy ezek közül melyik a gyakoribb probléma egy szervezet esetében. Több tanulmány egész magas százalékot hoz ki a belső fenyegetések javára. A belső-külső kategóriák jelentésének meghatározása nem is olyan egyszerű, mint első ránézésre hinnénk. Belső támadásnak definiálhatjuk az adatbázist üzemeltető személyek által elkövetett támadást, melyben a támadó a számára megadott jogosultsággal él vissza, azokat nem rendeltetésszerűen használja.

Kategorizálhatunk egy támadást az elkövető indíttatása szerint, azaz a kivitelezője elkövetheti ezt szándékosan vagy véletlen folytán.

A támadásokat kategorizálhatjuk aszerint, hogy mely biztonsági tulajdonság sérülését okozhatja. Azaz a bizalmasság, a sértetlenség vagy a rendelkezésre állás biztonságát veszélyezteti-e. A sértetlenség és rendelkezésre állás esetén megvizsgálható, hogy az adatokon történt meg a negatív kölcsönhatás vagy pedig az adatbázis-kezelő rendszert érintette. Például a rendelkezésre állás megsértése esetén az adatok megsemmisítése miatt vagy pedig az adatbázis-kezelő rendszer megváltoztatása miatt vált az adatbázis elérhetetlenné. A sértetlenség megsértésekor szintén megvizsgálható, hogy az adatokon vagy az informatikai rendszerben történt meg az illetéktelen módosítás. Egy fenyegetés több biztonsági tulajdonság megsértését kiválthatja, így egyszerre több kategóriához is hozzárendelhető.

Végül vizsgálhatjuk az adatbázis fenyegetéseket a lehetséges támadás architektúrában elfoglalt helye szerint is. Szem előtt kell tartanunk, hogy csak azokat a fenyegetéseket rendszerezzük, vesszük számba, melyek az adatbázisban tárolt adatokat vagy az adatbázis-kezelő rendszer működését veszélyeztetik.

Az adatbázis-biztonság helyzetét mérő kockázat elemzések egyik célja annak azonosítása, hogy a szervezet adatvagyonát hol veszélyeztetik a támadások leginkább. Ebből a nézőpontból tekintve ennek a csoportosításnak a jelentősége nagy. Az adatbázisokat veszélyeztető fenyegetések az architektúra négy pontjáról indulhatnak. Ennek alapján megkülönböztethetők a

hálózat, az alkalmazások, a platform és az adatbázisok sérülékenységeire építő fenyegetések.

Hálózati fenyegetésének tekintjük azokat a lehetséges támadási módokat, melyek az adatbázis szerverek, illetve adatbázis állományokat tartalmazó háttértárak közötti kommunikáció támadására alapulnak, vagy pedig a hálózat tetszőleges pontján lépnek fel és az adatbázisok rendelkezésre állását vagy sértetlenségét támadják meg. Az adatok bizalmasságának hálózati úton való támadása már nem tartozik a rendszerezésünk tárgyába.

Az alkalmazásokban rejlő sebezhetőségek, programozási hiányosságok az adatbázis fenyegetések egy fontos csoportját jelentik, ebbe a kategóriába eső támadások különös tekintettel a webes alkalmazások használatának elterjedésével váltak gyakorivá.

A platform fenyegetései alatt a hálózatba kötött szerverek és felhasználói számítógépek hardver és szoftver komponenseinek sebezhetőségeit értjük. Mivel csak az információs úton történő támadásokat vizsgáljuk, az operációs rendszer és egyéb rendszerprogramok hibáit kihasználó fenyegetések tartoznak ebbe a kategóriába, különös tekintettel az adatbázis szervereket futtató platformok sebezhetőségeire.

Az adatbázisok felőli támadási pont az adatbázis-kezelő rendszerben, illetve a tárolt adatokban rejlő sérülékenységeket kihasználó fenyegetések induló pontja. A következő fejezetben a támadási pontok szerinti jellegzetes fenyegetéseket vizsgáljuk meg.

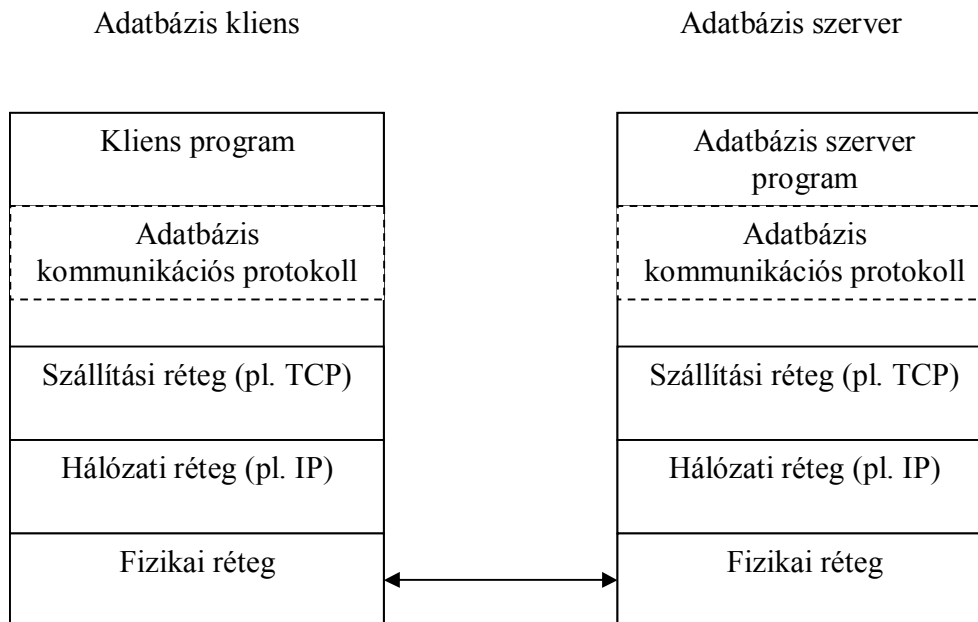
Jellegzetes adatbázis fenyegetések a támadás pontja szerint

Hálózati infrastruktúra sebezhetőségei

A hálózati fenyegetések kategóriájába tartoznak az OSI modell szerinti hálózati-szállítási réteg lehetséges támadásai, illetve az adatbázis-kezelő rendszer hálózati protokolljának támadásai. A támadások technikai épülhetnek a hálózati adatforgalom lehallgatására, beékelődéses (man in the middle) támadási módszerre (melyet például a forráscím meghamisításával lehet megvalósítani), szolgáltatás megtagadása típusú támadásra (például a SYN csomagok elárasztásának módszerével), de akár a puffer túlsordulásos hiba kihasználására is.

A hálózati adatforgalom lehallgatásának veszélye megjelenik az adatbázisok magas rendelkezésre állásának megvalósításánál (adatbázis tükrözés, fürtözés), ahol adatbázis szerverek kapcsolódnak hálózaton keresztül. Az adatbázis szerverek közötti adatforgalom titkosítás nélkül (vagy gyenge titkosítással) áramlása esetén az adatok lehallgathatóak, ezzel pedig adatbázisok tartalma kerülhet illetéktelenül támadók birtokába.

Pár évvel ezelőtt az adatbázis szerverek elleni új támadási vektor jelent meg, méghozzá az adatbázisok kommunikációs protokolljában rejlő sebezhetőségekre építve [6]. A támadás mindhárom biztonsági tulajdonság megsértését okozhatja. Az adatbázisok kommunikációs (vagy más néven hálózati) protokolljai az OSI modellben a hálózati-szállítási réteg és az alkalmazás réteg között helyezkednek el az alábbi ábra szerint:



2. ábra: Az adatbázis kommunikációs protokoll elhelyezkedése

Az SQL adatbázis lekérdező nyelv a kliens-szerver kommunikációhoz szükséges folyamatokat nem definiálja, ezeket az adatbázis-kezelő rendszer hálózati protokollja látja el. Például a kliens kapcsolat (client session) létrehozása, a parancsok (autentikációs, lekérdezés, kontroll információ) klientszól szerverhez való eljuttatása, az adatok és a lekérdezés státuszának klientshez való eljuttatása az adatbázis hálózati szoftverének a feladata.

Az adatbázisok hálózati szoftvereit (nem szükségszerűen, de a gyakorlat alapján) az adatbázis-kezelő rendszerek gyártói fejlesztik (például Oracle esetében Oracle Net-nek hívják), kódjaik általában nem nyilvánosak és számos sebezhetőséget hordoznak magukban. Bejelentett kommunikációs protokoll sebezhetőségek alapultak az üzenet struktúrájának elrontására, mező méret megváltoztatására, mező tartalmának manipulálására, illetve üzenet sorszámának meghamisítására.

A támadás kivitelezéséhez a támadónak vagy egy saját programot kell írnia, amivel a manipulált üzeneteit elküldi a szervernek és feldolgozza a kapott választ addig a pontig, amíg a káros hatás bekövetkezik vagy pedig egy TCP proxy segítségével be kell ékelődni a kliens és a szerver közé, és ebben a pozícióban az elkapott üzeneteket megfelelően módosítva kell továbbítani. TCP proxy: a kliens-szerver kommunikációba ékelődik be, a TCP csomagokat megjeleníti, változtatás nélkül továbbítja, illetve szükség esetén módosítva küldi tovább.

Alkalmazások sebezhetőségei

Az alkalmazásokban rejlő sebezhetőségek, programozási hiányosságok az adatbázis támadások egy fontos csoportját jelentik, melyek mögött elsősorban a felhasználói inputok ellenőrzésének hiánya áll. Sérülékenységet jelent még a hibaüzenetek nem megfelelő kezelése, az adatbázis elérések nem megfelelő megvalósítása és a naplózás hiánya is.

A felhasználói inputok ellenőrzésének hiánya puffer túlcsordulásos, SQL injekciós, illetve XSS (cross-site scripting) támadásra adhat lehetőséget. Mindhárom támadási módszerrel kiváltható a rendelkezésre állás, a sértetlenség illetve a bizalmasság megsértése.

Alkalmazások a felhasználók számára megjelenített hibaüzeneteikben adatbázisra, illetve az adatbázis szerverre jellemző információkat fedhetnek fel, ami támadások felépítéséhez ad segítséget, ezáltal sérülékenységi pontot jelent.

Egy adott alkalmazás az adatbázis szervert mindig egy (esetleg több) adatbázis felhasználó nevében éri el. Ha az alkalmazás tulajdonosként vagy superuserként csatlakozik az adatbázishoz, sérülékenységet jelent, mivel bármilyen utasítást és lekérdezést lefuttathat, pl. a szerkezeti módosítást (táblák megszüntetése) vagy táblák komplett törlése. Mindig a lehető legkevesebb jogosultsággal rendelkező, az alkalmazás számára önálló és testreszabott felhasználókat kell használni. Ekkor, ha a behatoló meg is szerez valamilyen jogosultságot (hitelesítési információt), akkor is csak akkora változást tud okozni, mint az alkalmazás maga.

Az alkalmazás szintjén történő adatbázis lekérdezések, hozzáférések naplózásának hiánya szintén sérülékenységet okozhat a rendszerben, hisz az adatbázis szerver naplóiban az alkalmazás számára az adatbázis elérésre létrehozott felhasználók jelennek csak meg (általában ezek száma a tényleges felhasználók számának töredéke). Nyilvánvalóan a naplózás nem tud megakadályozni egyetlen ártalmas próbálkozást sem, de segítséget nyújthat annak felderítésében, hogy melyik alkalmazás és ki által lett kijátszva.

A puffer túlcsordulásnál a program egy fix hosszúságú tömböt (puffert) foglal le a memóriában, majd a tömb írásakor nem ellenőrzi annak határait. A támadó a lefoglalt tömböt túlírva (túl hosszú bemenet segítségével) felülírhat a program működése szempontjából lényeges memóriarészeket, így kártékony kódokat futtathat le. Puffer túlcsordulást kiváltó sérülékenység felléphet az alkalmazás szintjén például az SQL kérések túlméretezésével, vagy a dinamikus SQL lekérdezés számára túlméretezett input megadásával.[7]

Az adatbázisokat érintő fenyegetések közül az SQL injekciós technika mindenképp az egyik vezető helyet foglalja el. A támadásnál az alkalmazás által előállítandó, tervezett tartalmú, dinamikusan szerkesztett SQL utasításba illesztenek káros tevékenységeket megvalósító kódot. Az alkalmazás a felhasználótól bekért paraméterek segítségével állítja elő az SQL szerverhez eljuttatandó lekérdezést. A támadó a paraméter értékének olyan kártékony karaktersorozatot ad meg, ami megváltoztatja az eredeti lekérdezés szintaktikáját, ezáltal az egészen más feladatot valósít meg, mint az eredeti elképzelés. [8]

XSS támadás jelenti napjainkban a webes alkalmazások leggyakoribb megsértését. A támadó a felhasználó böngészőjében futtathat le tetszőleges kódot (például javaskriptet), miközben a felhasználó egy megbízható webhelyhez kapcsolódik. Igazából a felhasználót sebzi meg a támadás, a web alkalmazás, mint közvetítő közeg segítségével. A támadó munkafolyamat (session) azonosítókat tud a felhasználó gépéről megszerezni, ezáltal a felhasználó nevében be tud lépni az alkalmazáson keresztül az adatbázis rendszerbe. A session azonosítók megszerzésére építő támadást munkamenet-eltérítésnek (session hijacking) nevezik. Az XSS támadás különösen veszélyes az adatbázis rétegre nézve, ha a támadáshoz használt web alkalmazás a felhasználó által megadott adatokat az adatbázis rétegen belül tárolja, ekkor a támadó az adatbázisba tud illetéktelenül beleírni. [9]

Platformok sebezhetőségei

A platformok fenyegetéseihez hozzájárulnak a hálózatba kötött szerver és felhasználói számítógépek szoftver komponenseinek sebezhetőségei. Az adatbázisok biztonságára nézve az adatbázis-kezelő rendszert futtató számítógép operációs rendszerének és az itt található állományoknak a nem megfelelő védelme biztonsági rést jelent.

A Blaster féreg például a Windows XP, Windows 2000 operációs rendszerek puffer túlcsordulásra épülő sérülékenységet használta ki, amivel megfertőzött gépeket, köztük adatbázis szervereket is elérhetetlenné tett. [10]

Az adatbázis-kezelő rendszer gépén lévő állományok megfelelő védelméről is gondoskodni kell. Titkosítatlanul tárolt adatbázis mentések és futtatható állományok jogosulatlan hozzáférése is biztonsági rést jelent.

Gyakori példa, hogy felhasználók adatbázis-kezelő rendszerbe való belépésekor lefut egy login szkript, mely a rendszer szükséges beállításait elvégzi. Ha ezt a login fájlt illetéktelenek elérik és módosítani tudják, akkor teljes hozzáférést szerezhetnek az adatbázishoz, amit az alábbi példa szemléltet:

```
-----login.sql-----  
  
set term off  
  
create user hacker identified by hacker;  
  
grant dba to hacker;  
  
set term on  
  
-----login.sql-----
```

Adatbázisok sebezhetőségei

Az adatbázis-kezelő rendszer szoftverei és a tárolt adatok is hordozhatnak sérülékenységeket. A biztonságos működéshez elsődleges feladat az adatbázis-kezelő rendszer biztonságos telepítése, megerősítése és folyamatos felügyelete, ezt angolul „database hardening”-nek nevezik. Az adatbázis-kezelő rendszerek telepítésekor gyakran, automatikus módon, ismert nevű felhasználók jönnek létre, mely a támadás számára egy jó kiindulási pont. Ugyanis a felhasználónév birtokában a támadónak „csak” a jelszót kell kitalálnia (ami gyakorta nem erős, azaz könnyen megfejtendő). A telepítéskor automatikusan létrejövő táblák, tárolt eljárások is sérülékenységi pontot jelenthetnek. Célszerű ezeket törölni, és szükség esetén más névvel magunknak létrehozni.

A szerverekre vagy anonim kapcsolattal vagy autentikáció után lehet kapcsolódni. A támadó a hitelesítési mechanizmus és információk lehallgatásával, megszerzésével illetéktelenül tud az adatbázis szerverre bejutni.

Gyenge konfigurációs paraméterek használata, szoftver hibák, az adatbázis tárolt eljárásaiban található puffer túlcsordulásra, illetve SQL injekcióra épülő sérülékenységek, felhasználói hibák,

elavult verziójú programok használata és biztonsági frissítések feltöltésének hiánya kártékony kód lefuttatását, vírusok, trójaiak és férgek rendszerbe való bejutását eredményezheti, illetve szolgáltatás megtagadása típusú támadásra ad lehetőséget. Például az SQL Slammer féreg a Microsoft SQL szerverének puffer túlsordulásra épülő sérülékenységet használta ki és okozott az adatbázis-kezelő rendszer biztonságában rendelkezésre állás megsértést. A kártékony kód olyan rendszereket tudott megfertőzni, melyek a már bejelentett sérülékenységet javító biztonsági frissítést nem alkalmazták. [11]

Összefoglalás

A publikációban az adatbázisok fenyegetések különböző formáit mutattuk be. Először értelmeztük az adatbázis-biztonság alapfogalmait, többek közt az adatbázis-biztonság alanyát és a védendő tulajdonságait, majd különböző rendszerezési kategóriákat állítottunk fel az adatbázis fenyegetések rendszerezéséhez. A támadási pontok szerint négy csoportra osztottuk az adatbázis fenyegetéseket, ezek a hálózat, alkalmazások, platform és adatbázis rendszerek sebezhetőségeire épülő támadási lehetőségek. A támadási pontok kategóriái szerint jellegzetes adatbázis fenyegetéseket gyűjtöttünk össze. Egy szervezet adatbázisainak biztonságát mérő kockázat elemzések fő célja a veszélyek felvázolása és rangsorolása, ezt a folyamatot segíti az, ha ismerjük a lehetséges támadásokat és ezek megvalósulásának helyeit.

Felhasznált irodalom

- [1] MUNK Sándor: Információbiztonság vs. informatikai biztonság. – Robothadviselés 7 tudományos szakmai konferencia anyaga (2007.11.27.), Hadmérnök különszám
- [2] Ramez Elmasri , Shamkant B. Navathe: Fundamentals of Database Systems, 5th Edition, Addison Wesley 2007
- [3] C. J. Date: An Introduction to Database Systems, 8th Edition, Addison Wesley 2004
- [4] Database Security Technical Implementation Guide, Version 8, Release 1, 19 September 2007, Developed by DISA for the DoD
- [5] Útmutató az IT biztonsági szintek meghatározásához
http://www.ekk.gov.hu/hu/emo/ekozigkeretrendszer/ek3-itbiztonsag/EKK_ekozig_ITbiztonsagiszintekmeghatarozasa_080822_V101.doc
(2009.12.10.)
- [6] Amichai Shulman: Danger From Below: The Untold Tale of Database Communication Protocol Vulnerabilities http://www.imperva.com/resources/adc/db_comm_protocol.html
(2009. 12.10.)
- [7] Bucsay Balázs: MySQL and SQL Column Truncation Vulnerabilities
<http://rycon.hu/papers/02mysqlcolumntruncation.pdf> (2009.12.10.)
- [8] Fleiner Rita: SQL injekcióra épülő támadások és védekezési lehetőségek, Hadmérnök, 2008 (III.)/4. (117-128.o.) http://hadmernok.hu/archivum/2008/4/2008_4_fleiner.html
(2009.12.10.)

- [9] Simon Whatley: What is a SQL Injection Attack <http://www.simonwhatley.co.uk/what-is-a-sql-injection-attack> (2009.12.10.)
- [10] CERT® Advisory CA-2003-20 W32/Blaster worm <http://www.cert.org/advisories/CA-2003-20.html>
- [11] SQL slammer (computer worm)
http://en.wikipedia.org/wiki/Slammer_%28computer_worm%29 (2009.12.10.)

Fürjes János

furjes.janos@chello.hu

GRAPHICS CARDS IN RADIO RECONNAISSANCE: THE GPGPU TECHNOLOGY

Absztrakt/Abstract

Jelen írás egy modern technológiát elemez, amely költséghatékony módon képes a keskenysávú vevők jelfeldolgozását elvégezni. Az állandóan fejlődő felhasználó piac, az igények és az új technikák összehangolása, mind-mind felhasználható, így azok szakmai területen csökkentik a fejlesztési és a működési költségeket.

This paper examines an up to date technology, which is a cost effective way of processing narrowband receiver channels can be carried out. Techniques aligning to the demands of the permanently developing user's market can also be used in the professional field reducing the development and the operation costs.

Kulcsszavak/Keywords: GPGPU, rádiófelderítés ~ GPGPU radio reconnaissance

INTRODUCTION

Who has ever thought over how pixels are calculated by a three dimension featured graphics program? Probably only a few of us, as it is out of our interest. However, when purchasing computer parts, we usually consider carefully what to spend on our scraped and saved money. But those who want to keep abreast of the times are compelled to innovate their machine quite often. The most dynamically developing component in the IBM PC market is the field of the graphics cards. When a new card generation is born, their performance doubles. In the beginning, an alternative usage was already considered to utilize the card's capacity not only for specialized graphics routines but also for general computing tasks. Regarding the fast developing rate we can only make proper decision if we follow the technological progress.

HISTORICAL OVERVIEW- THE EVOLUTION OF GRAPHICS

The story started with the Hercules cards. Cards from the first generation could only display fix characters in monochrome mode. In the next step the four and the sixteen color CGA/EGA

graphics cards appeared, which were followed by the (S)VGA 256 color cards with 1024*768 pixel resolution. Finally the features of the top cards reached the 1280*1024 pixel resolution with 16 millions of colors. At that time the computer game industry emerged to transfer some of the hardware elements facilitating the CPU's job to the graphics card.

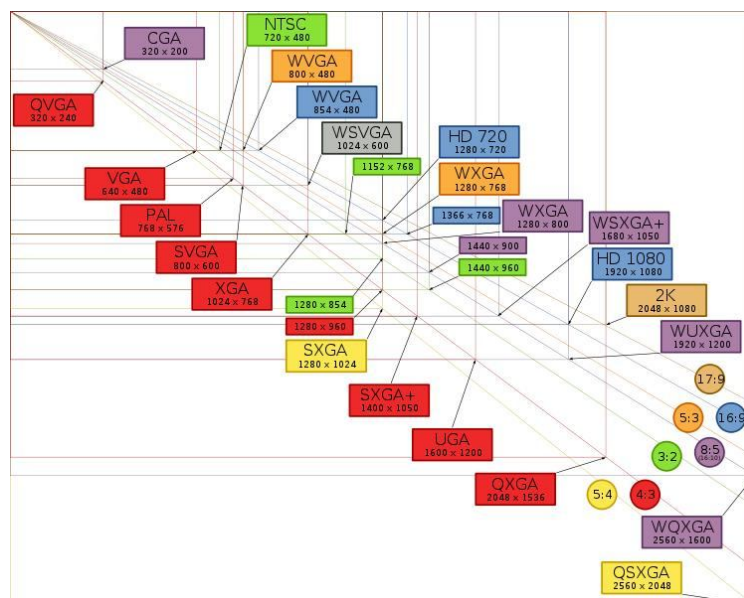


Figure1. The most commonly used resolutions [1]

Evolution of graphics chips

The 3dfx (in the beginning: 3Dfx), which already closed down, was a company that used to design 3D graphics processors. It is regarded as the originated producer of the 3D PC graphics processor. Although 3D technology had already existed, 3dfx made it wide known when introducing Voodoo 1 card. Its main trade partner was Quantum3D having share in military industry. At this moment a hardware device developed for this purpose of handling parallel graphics tasks appeared. In 2000 the company went down, and its technology was transferred by nVidia. In 2003 an engineering team separated from Cray Computing joined nVidia. That time onward events speeded up. They invented a cell structured processor which was able to cooperate with additional executing elements and to reach high computing accuracy.

The other relevant company called ATI (Array Technologies Incorporated) from Canada was established by three Chinese immigrants in 1985. At first ATI designed GPUs for the major manufacturers (IBM) being interested in computer science, but by 1987 it became an independent one producing EGA/VGA Wonder cards. In 2000 ATI launched its popular Radeon series. Besides, it went on cherishing its relations with other companies (Microsoft uses ATI chips in Xbox 360). In 2006 AMD purchased ATI for 5.4 billion dollars.

Recently ATI is the main rival of nVidia. In 1991 ATI created the Mach8 chip which was able to display graphics information without CPU. In 1992 it was followed by Mach32 and in 1994 by Mach64 as the harbinger of 3D acceleration (in 1999 ATI Rage 128). In 2000 the next step was the Radeon series with DirectX support whose developing process has been in progress from that time. Nowadays ATI's top quality graphics card is HD5970 containing 2GB DDR5 memory module and 2*RV870 chips consisting of 2.15 billion transistors with 40 nm technology. This configuration includes 2*1600 computing units at a clock rate of 725 MHz

executing 2320 billion floating point operations per second. The applied technology allows the clock rate to be set up to 1000 MHz meaning that the operations per second achieve 3200 billions. In order to utilize the huge computing capacity implemented in the card AMD issued ATI CAL developer environment which provides an effective way to exploit the embedded calculation capabilities. To promote the standardization Chronos group specified the general purpose completion of OpenGL¹ shader language, called OpenCL². Forming a standardized interface of the integration of general purpose calculations, OpenCL² makes programmers job easier, hiding the complicated methods of hardware handling. Naturally it leads to decrease in operation speed, but usually the accuracy of developing and testing processes have more importance.



Figure 2. ATI's top quality graphics card: HD5970 [2]

GRAPHICS CARD FUNCTIONS

First let's see what tasks are carried out in such a card in normal operation mode.

Scene calculations

The scene processing can be divided in many coherent steps as described below:

- Application tasks
- Scene level calculations
- Transform and Lighting
- Triangle Setup and Clipping
- Rendering

¹ OpenGL: Open Graphic Library,

² OpenCL: Open Computing Language,

Application tasks

The running program controls the movement of the stand point and the objects, and their interactions. This element is usually called application engine. The basis of each pixel is an extracted detail from the modeled state of the whole virtual domain. Having all these information the actual drawing could start but still there would not be any sense in lavishing resources for forming such objects which cannot be seen from the actual viewpoint. As the virtual field is regarded as to be modeled, only the stand point information is provided for the user.

Scene level calculations

In 3D computer graphics, Visible Surface Determination (VSD) is the process used to determine which surfaces and parts of surfaces are not visible from a certain viewpoint. A related area to VSD is *culling*, which usually happens before VSD in a rendering pipeline. Primitives or batches of primitives can be rejected in their entirety, which *usually* reduces the load on a well-designed system.

The advantage of culling early on the pipeline is that entire objects that are invisible do not have to be fetched, transformed rasterized or shaded.

Often, objects are so far away that they do not contribute significantly to the final image. These objects are thrown away if their screen projection is too small.

In computer graphics, accounting for level of detail involves decreasing the complexity of a 3D object representation as it moves away from the viewer or according other metrics such as object importance, eye-space speed or position. Level of detail techniques increases the efficiency of rendering by decreasing the workload on graphics pipeline stages, usually vertex transformations. The reduced visual quality of the model is often unnoticed because of the small effect on object appearance when distant or moving fast.

Although most of the time LOD is applied to geometry detail only, the basic concept can be generalized. Recently, LOD techniques included also shader management to keep control of pixel complexity. A form of level of detail management has been applied to textures for years, also providing higher rendering quality.

Transform and Lighting

On this level the desired geometry can be drawn. To do so, the vertexes positions must be specified by their spatial coordinates (x, y, z). Connecting all vertexes belonging to the same object leads to the frame of the actual model. Then models are transformed and lighting according to the selected viewpoint.

Triangle Setup and Clipping

On this level the necessary calculations for the efficient rendering process are done. Also, invisible vertexes are removed from and behind the models.

Rendering

Rendering is the process of generating an image from a model, by means of computer programs. The model is a description of three-dimensional objects in a strictly defined language or data structure. It would contain geometry, viewpoint, texture, lighting, and shading information. The image is a digital image or raster graphics image. The term may be by analogy with an "artist's rendering" of a scene. 'Rendering' is also used to describe the process of calculating effects in a video editing file to produce final video output

Scanline rendering and rasterization: A high-level representation of an image necessarily contains elements in a different domain from pixels. These elements are referred to as primitives. In a schematic drawing, for instance, line segments and curves might be primitives. In a graphical user interface, windows and buttons might be the primitives. In 3D rendering, triangles and polygons in space might be primitives. If a pixel-by-pixel (image order) approach to rendering is impractical or too slow for some task, then a primitive-by-primitive (object order) approach to rendering may prove useful. Here, one loops through each of the primitives, determines which pixels in the image it affects, and modifies those pixels accordingly. This is called rasterization, and is the rendering method used by all current graphics cards.

Rasterization is frequently faster than pixel-by-pixel rendering. First, large areas of the image may be empty of primitives; rasterization will ignore these areas, but pixel-by-pixel rendering must pass through them. Second, rasterization can improve cache coherency and reduce redundant work by taking advantage of the fact that the pixels occupied by a single primitive tend to be contiguous in the image. For these reasons, rasterization is usually the approach of choice when interactive rendering is required; however, the pixel-by-pixel approach can often produce higher-quality images and is more versatile because it does not depend on as many assumptions about the image as rasterization.

The older form of rasterization is characterized by rendering an entire face (primitive) as a single color. Alternatively, rasterization can be done in a more complicated manner by first rendering the vertices of a face and then rendering the pixels of that face as a blending of the vertex colors. This version of rasterization has overtaken the old method as it allows the graphics to flow without complicated textures (a rasterized image when used face by face tends to have a very block-like effect if not covered in complex textures; the faces aren't smooth because there is no gradual color change from one primitive to the next). This newer method of rasterization utilizes the graphics card's more taxing shading functions and still achieves better performance because the simpler textures stored in memory use less space. Sometimes designers will use one rasterization method on some faces and the other method on others based on the angle at which that face meets other joined faces, thus increasing speed and not hurting the overall effect.

As mentioned above scene calculation is made up of several steps and done by the CPU and the GPU. In the early times all tasks but rendering were carried out by the CPU. As graphics processors have been getting more and more sophisticated GPUs took this role over.

Application tasks	CPU	CPU	CPU	CPU	CPU
Scene level calculations	CPU	CPU	CPU	CPU	CPU
Transform and Lighting	CPU	CPU	GPU	GPU	GPU
Triangle Setup and Clipping	CPU	Graphics chip	GPU	GPU	GPU
Rendering	Graphics chip	Graphics chip	GPU	GPU	GPU
DirectX	5.0 (1997)	6.0 (1998)	7.0 (1999)	8.0 (2000)	9.0 (2002)

It is noticeable that from DirectX7 the hardware supported T&L function appeared in graphics chips so scene calculation steps are done by the GPU. The main disadvantage of this approach was the fact that GPU used a fix algorithm for transformation and lighting levels. However

developers were not able to utilize the GPU's full resources, they were happy with the innovations.

Multipurpose application

If graphics cards are intended to be utilized, a different approach - listed below - should be considered.

- Program preparing task
- Environment preparing task
- Program execution
- Waiting for execution
- Data storage

Program preparing task

During this phase the card capabilities are checked and also modules necessary for the handle of the graphics card are loaded (Access routines are initialized, memory and processors are allocated). Then the card's physical addresses are linked with the application's virtual addresses running on the PC. When accomplishing the program preparing tasks, the applied framework depending on the hardware structure is regarded to be initialized.

Environment preparing task

According to the received addresses an applicable code is generated from the source program. The translation can be carried out in real time, which increases the execution time, or a pre-translated one. Buffers used in the card's program are linked with the PC's address domain then are loaded with data. The data transfer is accomplished with hardware support. When moving data individually between the PC and the chip memory, the GPUs are able to reach considerably high operating speed (~GB/s). It is called direct memory access (DMA¹). The CPU is notified about the end of data transfer through a so called EVENT² object. A CPU's thread is listening to this object whether it is activated by the GPU or not. One of the main advantages of the multi tasking operating systems using preemptive timing is the fact that the listening thread is inactive during the waiting period so that the processor and other recourses are free for other tasks.

Program execution

The stream processors are started to execute the instruction threads. Parallel with this operation the control returns to the CPU so the main program execution is independent from the GPU. Providing synchronization between CPU and GPU is the programmer's task.

Waiting for execution

The synchronization of the stream and the application threads are accomplished during this phase. To make active these EVENT² objects is the task of the GPU (with direct hardware

¹ DMA: (Direct Memory Access) direct memory access through dedicated hardware unit.

² EVENT object: this object is used for waiting for an external event.

support), while checking these threads is carried out by one of the threads operating within the main program.

Data storage

Now data at the output of the stream processors is available so additional processing can be done. The transfer of the data is accomplished with DMA¹ operations through watching an EVENT² object.

STRUCTURE OF GRAPHICS CARDS

The next chapter will study the inner structure of the graphics cards so that it is easier to understand their capabilities.

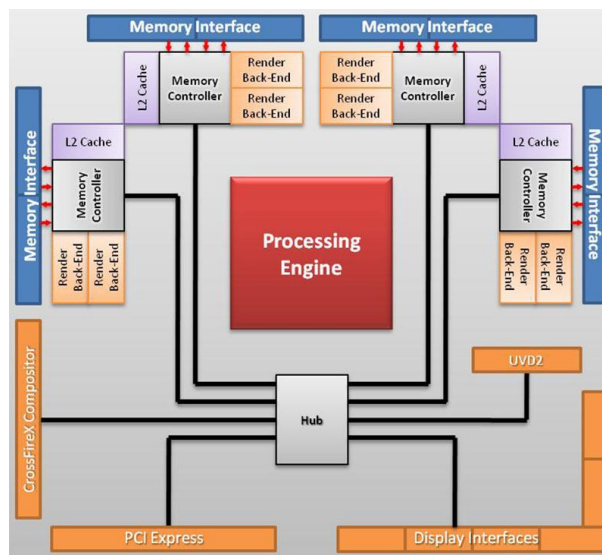


Figure 3. The structure of the AMD made RV700 GPU. [3]

Figure 3. clearly shows that the central HUB provides physical connection between the units inside the processor. Also it is responsible for communication and traffic control. The monitor is connected to the card through the display interface unit. The card communicates with the PC through PCIExpress interface. In multi-card applications, cards are connected to each other through CrossFireX interface. The memory blocks embedded on the card are connected to the GPU's processing engine through wideband (128-256 Bits) memory interface. Generally the memory is segmented by the processor so the processes competing with each other have parallel access to the memory. Also the processor contains the UVD2¹ unit which is responsible for coding-decoding high resolution video streams.

¹ UVD2: Unified Video Decoder version 2, general purpose video decoder unit

The structure of the processor unit (GPU)

The GPU is specially designed and developed for executing multithread processes running parallel. Its structure contributes the principle of SIMD (single command-multidata). The GPU is controlled by the command processor which is responsible for dispatching the threads, for accomplishing memory operations (DMA), and for signing the events. The processor consists of several SIMD engines (the number of the engines depends on the version of the processor). SIMD engines are the master unit of program execution. Each of them executes different programs. Data share between SIMDs is carried out through the global and the local data share memory blocks. Accessing local memory is considerably faster than the global one as it is divided between the units, but the global memory is available for all SIMD units. The next picture shows the GPU containing the most SIMD engines so far.

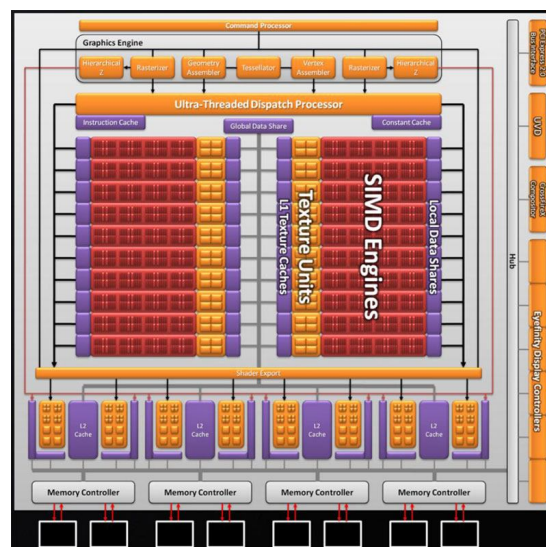


Figure 4. GPU RV870 produced by AMD. [4]

The structure of the SIMD engines

Thread processors inside the SIMD unit executes the programs. Sixteen of them are embedded in a SIMD unit. All of the thread processors execute the same code with different data. The main advantage of this is the fact that an operation on a parallel data source (matrix multiplication) is accomplished in one sixteenth times less. On the other hand, its disadvantage is the request of the 16 threads multi memory access at a time. A thread processor is made up of 4 simple and one double point stream core. It means that in one clock cycle it can execute 4 floating point operations or one double point operation. Every one of the stream cores consists of 1024 pcs of general purpose registers which can be accessed according to the clock cycle. All of them are a 128 bit wide one that can store four of 32 bit floating point or **integer type** data. Coupling the sub-registers (marked with x, y, z, w) double floating point or **integer type** operations are achievable. But during these operations there is no possibility for 4 times rate execution.

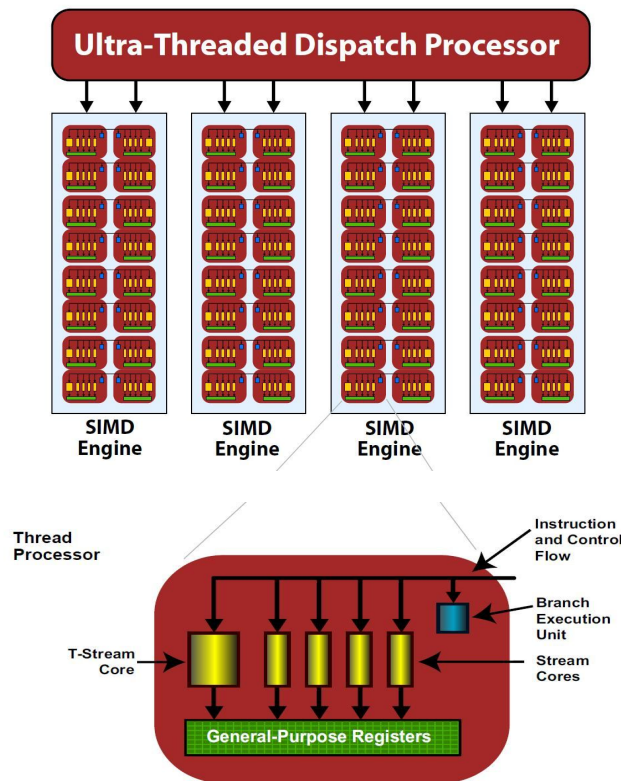


Figure 5. The structure of the SIMD engines and the thread processors [5]

The picture above shows the structure of the SIMD engines and the thread processors. In fact, these units execute the calculating operations and store their results. To produce very effective codes it is essential to take into consideration the number of the registers and the operating units in the executing cores.

The operation of the video cards, the shaders [6]

The programs created directly for running on graphics cards are called shaders.

The Direct3D and OpenGL graphic libraries use three types of shaders.

Vertex shaders are run once for each vertex given to the graphics processor. The purpose is to transform each vertex's 3D position in virtual space to the 2D coordinate at which it appears on the screen (as well as a depth value for the Z-buffer). Vertex shaders can manipulate properties such as position, color, and texture coordinate, but cannot create new vertices. The output of the vertex shader goes to the next stage in the pipeline, which is either a geometry shader if present or the rasterizer otherwise.

Geometry shaders can add and remove vertices from a mesh. Geometry shaders can be used to generate geometry procedurally or to add volumetric detail to existing meshes that would be too costly to process on the CPU. If geometry shaders are being used, the output is then sent to the rasterizer.

Pixel shaders, also known as fragment shaders, calculate the color of individual pixels. The input to this stage comes from the rasterizer, which fills in the polygons being sent through the graphics pipeline. Pixel shaders are typically used for scene lighting and related effects such as bump mapping and color toning. (Direct3D uses the term "pixel shader," while OpenGL uses the term "fragment shader." The latter is arguably more correct, as there is not a one-to-one relationship between calls to the pixel shader and pixels on the screen. The most common

reason for this is that pixel shaders are often called many times per pixel for every object that is in the corresponding space, even if it is occluded; the Z-buffer sorts this out later.)

The unified shader model unifies the three aforementioned shaders in OpenGL and Direct3D 10.

As these shader types are processed within the GPU pipeline, the following gives an example how they are embedded in the pipeline:

Simplified graphic processing unit pipeline

The CPU sends instructions (compiled shading language programs) and geometry data to the graphics processing unit, located on the graphics card.

Within the vertex shader, the geometry is transformed and lighting calculations are performed.

If a geometry shader is in the graphic processing unit, some changes of the geometries in the scene are performed.

The calculated geometry is triangulated (subdivided into triangles).

Triangles are transformed into pixel quads (one pixel quad is a 2×2 pixel primitive).

General computing task

It is concluded from the Vertex structure that freely programmable graphics processors can not only be used for special rendering tasks but also for general purpose parallel operations.

It is only a step ahead to get contribution for the efforts to produce appropriate and effective developer environment as it can be realized in OpenCL and DirectX11.

Multichannel receiver

Regarding graphics chips during their general computing processes the most optimized operations are those which contains the same operations for the input stream with different data. The multichannel receiver accomplishes the same theory. It receives different carriers with the same bandwidth. On account of the relatively small bandwidth (max.: 9 kHz) and the high number of the channels it can be used the in the most effective ways in HF applications.

The structure of the receiver

The following figure shows the structure of the multichannel receiver.

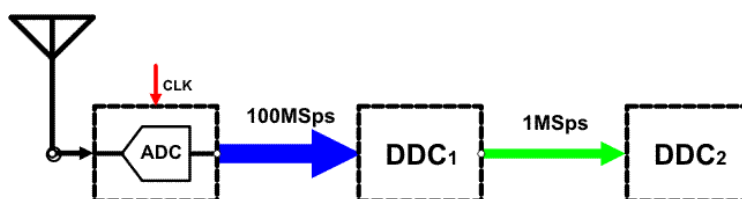


Figure 6. The block diagram of a multi channel receiver.

The incoming RF signal is digitized with a high speed ADC. From the full HF band (0-30 MHz) 500 kHz sub bands are extracted with a DDC unit. The DDC allows us to select the interested band, and to shift its frequency down to base band reducing the sampling rate. In the above case, the initial sampling rate is reduced from 100 MSps to 1 MSps. These amounts of data can be handled by video cards¹.

¹ Based on real tests, the number of the processable samples is a maximum of 4 million/second.

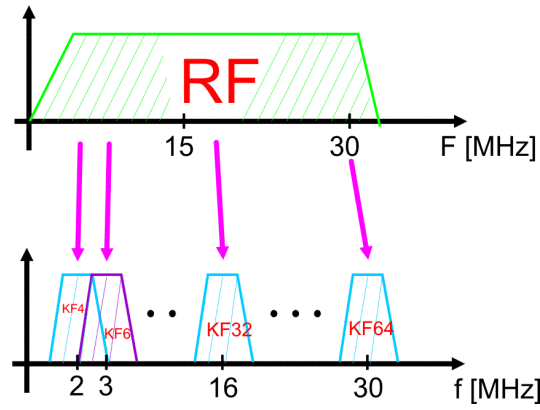


Figure 3. Sub-band forming

The first DDC unit processes the high input data rate. Its output data is put in a 2 dimensional array where the columns represent the time domain and the rows represent the frequency domain. So it is easy to implement the shift between the frequency bands. The task of the second DDC unit is to simultaneously receive narrow band channels from the 500 kHz bands. This is carried out by the software applied in the video card so its output represents only the selected channel. With this method the single sideband super heterodyne receiver can be implemented. Of course the solution of demodulation and decoding process is accomplished by a different unit which works in an out of real time environment.

Mathematical description

Figure 7. shows the structure of a DDC unit.

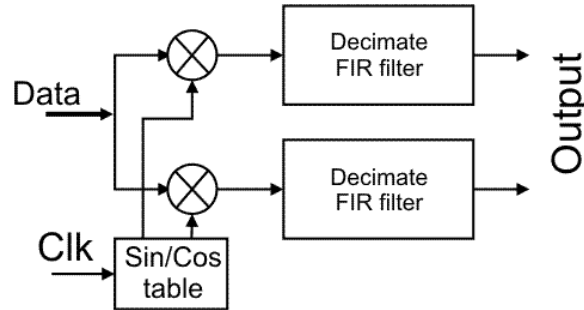


Figure 7. The structur of the DDC [7]

The picture above shows that the input data is multiplied at a time by sine and cosine having increasing arguments so that the received frequency is converted down to 0 Hz.

$$I_{out}[t] = D_{in}[t] * \sin(\omega_c * t)$$

Where,

I: the output data,

D: the input data

ω_c : the interested carrier.

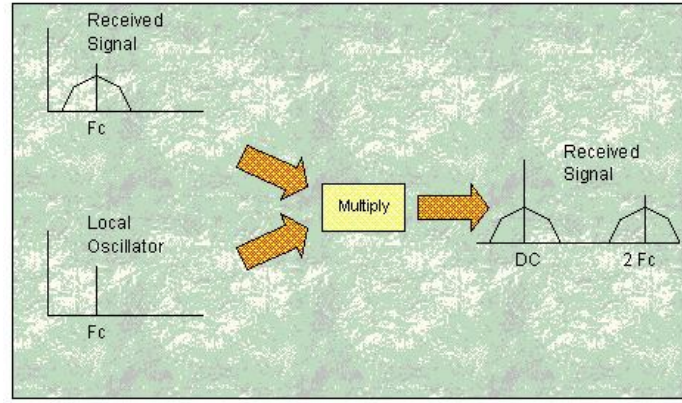


Figure 4. The result of multiplication [8]

According to the formula it is obvious that the high accurate sine and cosine values required for the multiplication of the incoming data cannot be derived from a table due to the high number of the values. During the multiplication process along with the base band signal a double frequency component also appears. This component must be eliminated with the FIR filter right after the multiplication unit. The FIR output data has to be calculated in the case when the sample of the pre set bandwidth is requested. Saving considerable resources the FIR routines have to be applied at only every n^{th} sample.

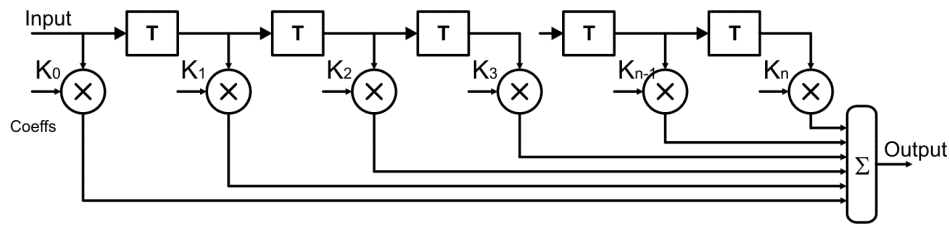


Figure 5. The structure of a FIR unit

It is concluded that the number of multiplying and adding operations done on every single multiplied data depends on the goodness of filtering. [9]

$$D_{out}[t] = \sum_{k=0}^K I[t-k] * K_k$$

Where:

D: the output data,

I: the input data,

K: the coefficient values for filtering

Capabilities

According to the above mentioned structure, a video card can process approximately 320 narrowband channels in the full HF (0-30 MHz) band. Implementing more cards in the system, the number of the channels also increases up to 512 as the limit of channels processed due to the computer capacity.

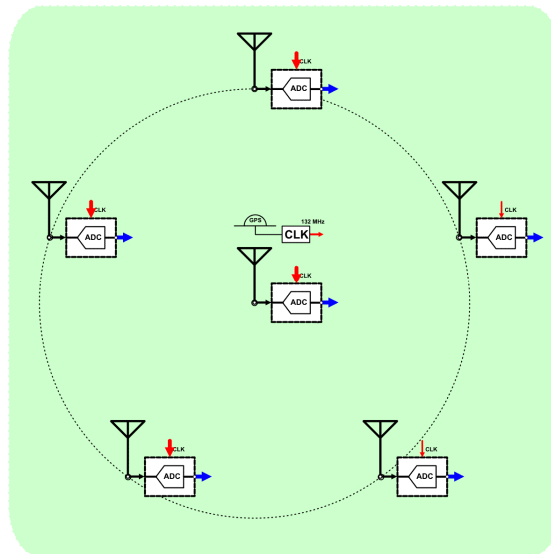


Figure 6. Direction finding antenna system

Figure 10. shows the structure of a real time direction finding system in which many parallel receiver channels are processed. The decrease of the number of the processed channels is directly proportional to the number of the antennas working parallel. In case of a 6 antenna system, 50 channels can be processed simultaneously. Using phase accurate adding up, digital beamforming can also be accomplished at a higher signal to noise ratio.

References

-
- [1] Display resolution
http://en.wikipedia.org/wiki/Display_resolution, Downloaded: 2009.12.01.
 - [2] Radeon HD5970: Egy kártya mind felett,
http://www.ipon.hu/_userfiles/Image/Svindler/5970/Sapphire_box_big.jpg,
Downloaded: 2009.12.03.
 - [3] Pintér Gábor: ATI Radeon HD 5870 - beköszönt a DirectX 11-es korszak,
<http://www.hoc.hu/teszt/548-ati-radeon-hd-5870--bekoszon-a-directx-11-es-korszak/2-technologia-felepites.html>, Downloaded: 2009.12.04.
 - [4] Pintér Gábor: ATI Radeon HD 5870 - beköszönt a DirectX 11-es korszak,
<http://www.hoc.hu/teszt/548-ati-radeon-hd-5870--bekoszon-a-directx-11-es-korszak/2-technologia-felepites.html>, Downloaded: 2009.12.04.
 - [5] ATI Stream Computing - AMD Corp.
http://developer.amd.com/gpu_assets/Stream_Computing_User_Guide.pdf, p 15.
Downloaded: 2009.12.01.
 - [6] Shader, <http://en.wikipedia.org/wiki/Shader>, Downloaded: 2009.12.01.
 - [7] Tony J. Roupheal: RF and Digital Sigal Processing for Software-Defined Radio, Elsevier 2009, p.65.
 - [8] HUNT ENGINEERING: Digital Down Conversion theory,
<http://www.hunt-dsp.com/pdfs/tech/ddctheory.pdf>, Downloaded: 2009.12.01.
 - [9] Tony J. Roupheal: RF and Digital Sigal Processing for Software-Defined Radio, Elsevier 2009, p.73.

Fürjes János

furjes.janos@chello.hu

FIZIKAI HOZZÁFÉRÉST NEHEZÍTŐ TECHNOLOGIA A MŰHOLDAS TÁVKÖZLÉSBEN

Absztrakt

Jelen írás a digitális műholdas kommunikációban alkalmazott újfajta megoldásokat mutat be, amelyek megnehezítik a kommunikációs csatornához való hozzáférést.

This paper shows new technologies which makes more difficult to access to the communication channel.

Kulcsszavak: *DoubleTalk, Carrier-in-Carrier technológia, Műholdas kommunikáció, Digitális jelfeldolgozás ~ DoubleTalk, Carrier-in-Carrier technology, Satellite Communication, Signal Processing*

BEVEZETÉS

A legújabb hibajavító eljárásoknak, illetve a nagykapacitású és sebességű FPGA áramköröknek köszönhetően a műholdas hírközlésben is olyan, megbízható lehallgatás biztosítási rendszert sikerült kialakítani, amellyel a külső lehallgatók lehetőségei lekorlátozódtak. A nagy spektrum hatékonyság mellett, védett összeköttetések kialakítására nyílik lehetőség, költséghatékony módon.

A MŰHOLDAS TÁVKÖZLÉS TÖRTÉNETE

1945-ben Arthur C. Clarke angol író volt az első, aki felvetette mesterséges távközlési műholdak indítását. Három geostacionárius pályára állított hold az egész bolygót lefedte volna. 1946-tól az amerikai kutatók a II. világháború során megszerzett német V-2 rakétákkal és Aerobee rakétákkal végeztek felsőlégköri méréseket. Azelőtt az ionoszféra kutatására rádióhullámokat és 30 km magasságig eljutó ballonokat használtak. A rakétás kutatások során 200 km-ig mérték a légköri nyomást, sűrűséget és hőmérsékletet. Az első műhold a

Szputnyik-1 volt, amelyet a Szovjetunió indított 1957. október 4-én. Az eddigi legnagyobb, Föld körül keringő műhold a Nemzetközi Űrállomás.

A műholdak felhasználási területei szerint számos típusba sorolhatók:

- távközlési műholdak;
- csillagászati műholdak;
- Földfigyelő vagy távérzékelő műholdak;
- navigációs műholdak;
- felderítő műholdak;
- űrállomások;
- meteorológiai műholdak. [1]

Ezek közül a legfontosabb és nagy jelentőséggel bíró típusa a távközlési műholdak, amelyek rádió és mikrohullámú frekvenciát használva kommunikációs feladatokat látnak el. A legtöbb távközlési hold geoszinkron vagy közel geo stacionárius pályát használ, de vannak alacsony pályán is.



1. ábra Az Intelsat VIII. generációs műholdja [2]

TÁVKÖZLÉSI MESTERSÉGES HOLDAK [3]

A távközlési műholdak olyan műholdak, melyeknek célja a telekommunikáció segítése rádió- és mikrohullámú frekvenciákat használva. A legtöbb távközlési műhold geoszinkron vagy közeli geostacionárius pályán kering. Az utóbbi időben vannak alacsony Föld körüli pályát használó rendszerek is. A felszíni földi állomások parabolaantennákkal küldenek vagy fogadnak adatokat a műholdakról.

A távközlési műholdak az optikai kábelek és a tengeralatti kábelek kiegészítői. Az optikai kábeles kommunikációval ellentétben a műholdas kommunikációban fellép egy legkevesebb 270 milliszekundumos jelkésés, amely megfelel a rádiójel haladási idejének a 35800 km-re lévő műholdhoz és vissza. A műholdas internetes kapcsolat késése 600-800 milliszekundum, amely a földi internetes kapcsolatnak a 10-szerese.

ÜRTÁVKÖZLÉS [4]

Az űrtávközlés feladata az irányító központok, és az űreszközök közötti, vagy két földi állomás közötti kommunikáció műhold segítségével. A rendszer mindenképpen aszimmetrikus, mivel az űreszközök mérete, és tömege erősen korlátozott, a földi eszközök mérete jóval kevésbé korlátozott.

A rendszer földi szegmensre és űrszegmensre tagolandó.

Az űrszegmens része a földi irányító központ is. A földi vevőállomás különálló adó és vevő részre bontható, amely azonban egy egységbe épül. Egy ilyen állomás lehet fix, vagy mobil. A Földről a műholdra irányuló sugarat uplinknek, míg a visszafelé irányút down-linknek nevezik. A műhold szerkezete fogja egybe a tápegységet, a rakéta hajtóművet, a hőszabályzóegységet, a műholdat irányító egységet, valamint magát a hasznos terhet, amely az antennákat és a jeltovábbító egységet jelenti.

Az űrtávközlésben használt vivőfrekvenciákat nemzetközi szabványok írják elő, szokásos értékük 3..31GHz közötti mikrohullám.

Egy műhold antennája által lefedett terület lehet globális, zónás, pontszerű. A műholdpályák alapján elliptikus, cirkuláris, geostacionárius lehet a pálya. Az űrtávközlésben a geostacionárius műholdakat alkalmazzák főként, mivel ilyenkor a földi állomás a műholdat mindig az ég egy adott pontján "látja", valamint a műhold a Föld csaknem feléről látható.

A műhold elhelyezkedése miatt az űrtávközlés alkalmazásának a következő előnyei vannak:

- olcsó földi állomás (akár mobil is);
- egyszerre a Föld jelentős része belátható;
- ebből fakadóan egyszerre több vevőt is kiszolgálhat, amelyet többnyire frekvenciaosztással, vagy időosztással valósítanak meg.

Az űrtávközlés alkalmazásának hátrányai:

- lehallgathatóság;
- nagy késleltetési idő

Régóta folyik a küzdelem a műholdas távközlés lehallgathatóság elleni védelem érdekében. Itt nem csak az információ végzett titkosításról, hanem a lehallgatás elleni fizikai védelemről is szó van. A fizikai hozzáférés megnehezítése illetve lehetetlenné tétele az utóbbi időkig nem volt megvalósítható. Ezen a helyzeten próbált változtatni a ComTech cég 2002-ben. Ekkor szabadalmaztatták azt a technológiájukat, amely nem csak, hogy kisebb sáv szélesség felhasználása mellett nyújtott kétirányú állandó kapcsolatot, hanem a fizikai hozzáférést is lehetetlenné tette.

VIVŐ A VIVŐBEN ELJÁRÁS, „DOUBLE TALK” TECHNOLÓGIA

Egy műholdas kommunikációs szolgáltatás életképességét és realizálható pénzügyi hasznát nagyban meghatározza az űrszegmens igénybevétele díja. Az űrszegmens díja pedig az elfoglalt sáv szélesség és a kisugárzott teljesítmény arányában közel lineárisan nő. Optimális megoldás esetén a transzponderek (műholdas átjátszók) közel azonos sáv szélességű és teljesítménysűrűségű adásokat tartalmaznak. Hagyományosan, az alkalmazott modulációs és kódolási eljárások fixen meghatározzák az átvitel paramétereit. Az újabb előrevetett hibajavítási eljárások (FEC), mint a Turbó szorzatkód és az Alacsony eloszlású paritás ellenőrző kódok magasabb megbízhatóságú összeköttetést biztosítanak alacsonyabb teljesítmény sűrűség mellett, mint a régebbi Viterbi és Reed-Solomon kombinációt, vagy a pragmatikus Trellis kód modulációt alkalmazó eljárások. Különösen a magasabb rendű (16,32 QAM) modulációs eljárások, nagyobb átviteli kapacitás mellett, igen jelentős teljesítmény többlet igényvel bírnak. A teljesítmény növelésének lehetséges módja az adó-vevő antenna fizikai méretének növelésével a felhasznált energia csökkenthető, azonos ekvivalens

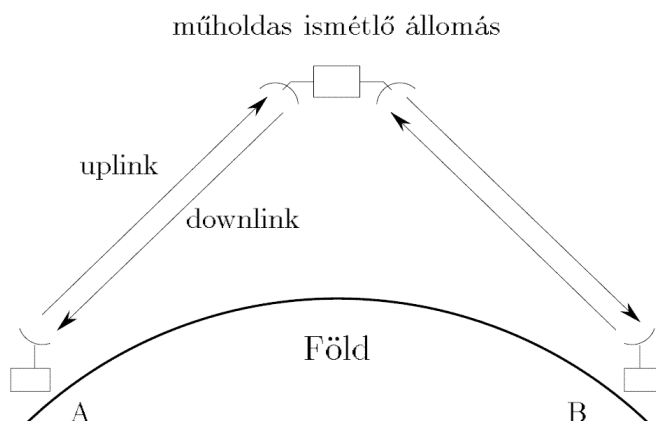
kisugárzott teljesítmény sűrűség mellett. Természetesen az antenna fizikai méretének növelése nem költséghatékony megoldása a teljesítmény sűrűség növelésének, illetve bizonyos helyeken nem kivitelezhető, például épületek tetején, vagy nagy szélterhelésnek kitett körzetekben.

A régebbi generációjú műholdak által vehető teljesítménysűrűség limitálva volt, a fedélzeten alkalmazott átjátszó erősítők nemlineáris tulajdonságai miatt, ami miatt az EIRP értéke limitálva van. A két rendszer együttes alkalmazása nagy differenciát okoz a sávszélesség kihasználtság és a realizálható haszon között, a az új technológiák javára.

A Comtech és a Applied Signal Technology cégek által közösen fejlesztett eszközzel drasztikus növelhető a spektrum kihasználtság, és az elérhető szolgáltatói pénzügyi haszon.

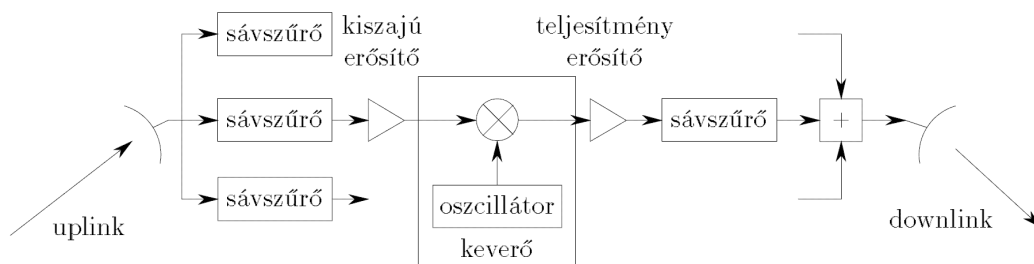
A technológia alapjai

A műholdas összeköttetések során a műhold, mint ismétlő állomás működik, az alábbi ábra szerint.



2. ábra Műholdas összeköttetések felépítése [5]

A műholdakon általában megkülönböztetnek uplink és downlink frekvenciákat. Az uplink frekvencián érkező jeleket veszi a fedélzeten lévő berendezés, majd ezt erősítve, frekvenciában áthelyezve sugározza vissza a Föld irányába.

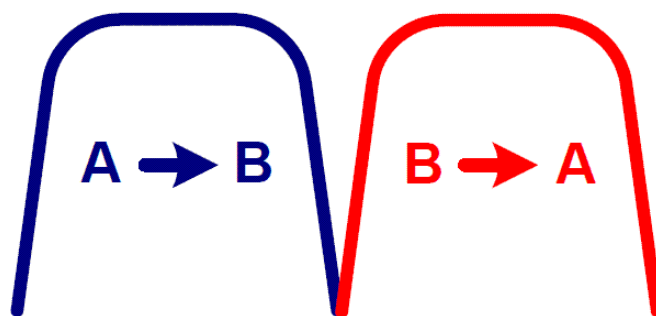


3. ábra Műholdas transzponder felépítése [6]

Amennyiben két-irányú¹ összeköttetést kell megvalósítani, akkor mindkét állomásnak más-más uplink és downlink frekvenciákkal dolgoznak.

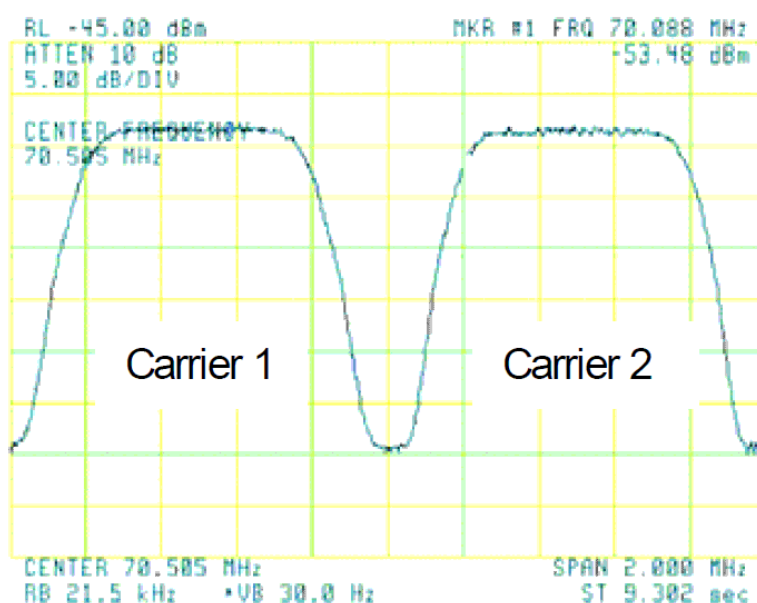
¹ Full-duplex teljes kétirányú összeköttetés

A spektrumban vizsgálva a hagyományos összeköttetéseket, a következő képek kapjuk.



4. ábra Full-duplex összeköttetés frekvencia viszonya

A hagyományos összeköttetések megbízhatóságát nagyban befolyásolja a két spektrum elválasztása, mivel ezek egymásba csúszása zavarként jelentkezik.

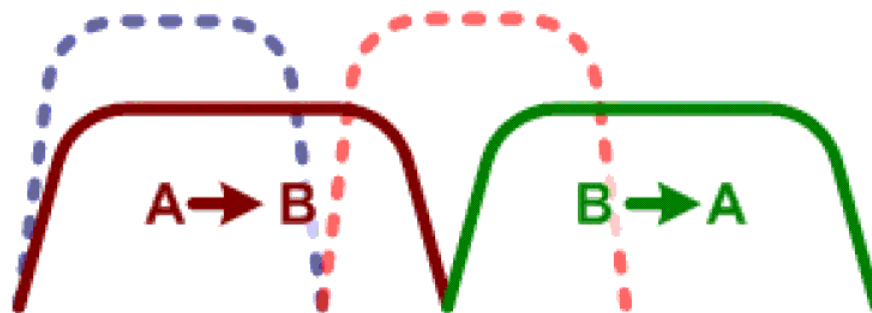


5. ábra Egy valós spektrum mérési eredménye [7]

Vivő a vivőben eljárás alapja

Az előző fejezetben az összeköttetés megbízhatóságát befolyásoló tényezőként a spektrumok egymástól történő elválasztását láthattuk. Amennyiben a két állomás azonos frekvencián működik, akkor elvben nem lehet összeköttetést megvalósítani.

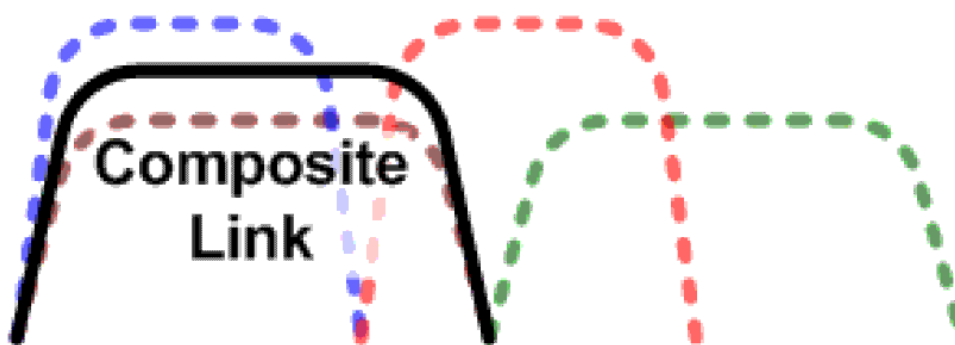
Ha a hagyományos konvolúciós és Reed-Solomon hibajavító eljárások helyett egy robosztusabb megoldást használunk, akkor az elfoglalt sávszélesség azonos adatsebesség mellett megnő, mint azt az alábbi ábra mutatja:



6. ábra Robosztusabb hibajavítás hatása az elfoglalt sáv szélességre

Ebben az esetben a kialakított rendszer kevésbé érzékeny a zavarokra, így megbízhatóbb összeköttetés alakítható ki.

A kifejlesztett új eljárás lényege az, hogy megtehető az adó és vevő frekvencia egymásra helyezése, úgynevezett kompozit eljárással egymásra tehető.

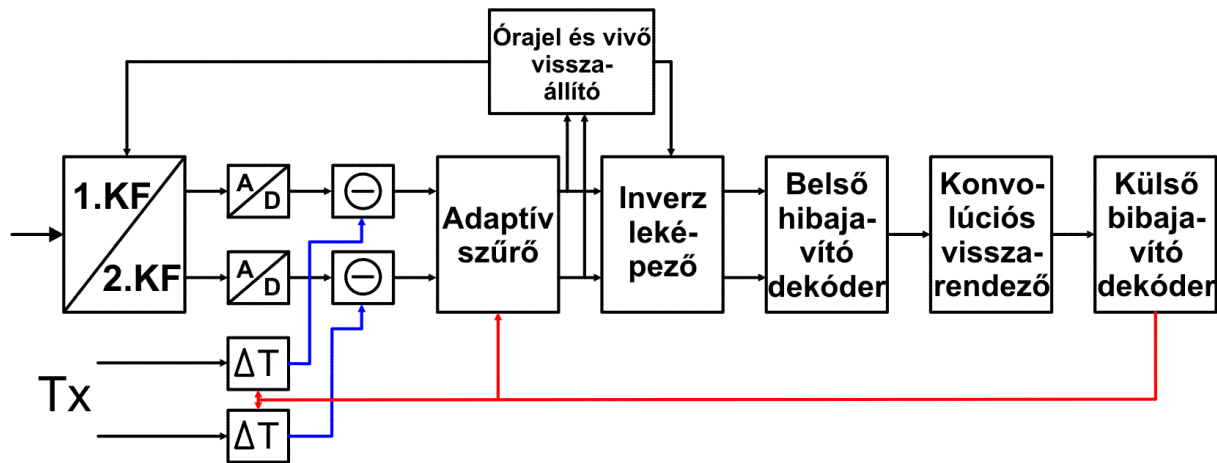


7. ábra Kompozit összeköttetés spektrum viszonya [8]

Ebben az esetben a műholdon a vett teljesítmény sűrűség megnő. Így a vevőkre mind a két jel összege kerül vissza sugárzásra.

Önmagában a megnövelt hibatűrő képesség még nem teszi lehetővé a két pont közötti full-duplex kapcsolat létesítését. Ehhez szükséges az úgynevezett „Adaptív elnyomó eljárás”.

Az eljárás lényege, hogy az adó oldalán tárolásra kerül a kisugárzott jel, és ez a műholdra történő oda és visszasugárzás késleltetésével, kivonásra kerül az eredeti jelből. A kivonáson kívül a legkorszerűbb FPGA elemeket felhasználva, olyan adaptív kiegyenlítő szűrő kerül alkalmazásra, amellyel a hibajavító megfelelő működéséhez szüksége jel-zaj viszony biztosíthatóvá válik. A kiegyenlítő szűrők folyamatosan követik és dinamikusan kompenzálják a vett jelből a késleltetett kisugárzott jelet.



8. ábra Adaptív kiegyenlítő eljárás a vevőben [9]

Mint a 8. ábrából látható, az adó (modulátor) kimenetén keletkező adatfolyamot egy átmeneti tárolóban kell elhelyezni. Az átmeneti tároló kimenetét változtatható késleltetéssel kinyerhető az eredetileg kisugárzott jel. A késleltetés mértékét (bizonyos határok között) a vevő elején elhelyezkedő adaptív szűrő szabályzó jele, illetve a külső hibajavító dekóder bithiba jele vezérli. E kettős szabályzó rendszerrel megbízhatóan elnyomható az eredetileg kisugárzott komponens. A technológia eddigi áttörését az adaptivitást biztosító FPGA áramkör sebessége és komplexitása korlátozta. A kiegyenlítő szűrőből párhuzamosan sokat kell futtatni, ahhoz, hogy a megfelelő eredmény megkapjuk.

Az így kialakított vevőben a kisugárzott jel kb. 30 dB-es csillapítással kerül a demodulátor egység bemenetére, amellyel nagy biztonságú összeköttetést lehet megvalósítani. [10]

Ezzel az eljárással csak egy irányban (viszonylatban) lehet full-duplex összeköttetést kialakítani. Ha több irányra van szükség, akkor páronként kell felépíteni a kapcsolatokat, különböző frekvenciákon. Ez az eljárás pont-multipont összeköttetésre nem alkalmas.

Figyelembe véve az adási és vételi teljesítmény sűrűséget, elmondható, hogy a 16QAM double-talk eljárás spektrum hatékonysága megfelel a 256 QAM adásának.

Lehallgatás elleni védelem

A double-talk technológia önmagában biztosítja a harmadik fél általi lehallgatás elleni védelmet. Amennyiben az adott helyen nem ismert a kisugárzott modulált jel, akkor nem állítható vissza egyik adás sem. A klasszikus hadászati rádiófelderítés nem képes saját eszközeivel ezt a problémát megoldani. A kisugárzás helyén telepített vevővel lehallgatható az adás, de ezt fedett módon hátszorból nem lehet kivitelezni.

Irodalomjegyzék

- [1] Wikipédia: Műhold - <http://hu.wikipedia.org/wiki/Műhold>
Letöltve: 2009. november 16.
- [2] <http://www.orbital.com/images/Low/Intelsat18.jpg>
Letöltve: 2009. november 19.
- [3] http://hu.wikipedia.org/wiki/Távközlési_műhold
Letöltve: 2009. november 20.
- [4] Dr. Mihály Zsigmond - A műholdas mobil hírközlés alapjai 1997 – egyetemi jegyzet – p10.
- [5] Dr. Mihály Zsigmond - A műholdas mobil hírközlés alapjai 1997 – egyetemi jegyzet – p12.
- [6] Dr. Mihály Zsigmond - A műholdas mobil hírközlés alapjai 1997 – egyetemi jegyzet – p13.
- [7] ComTech – CDM 625 User Guide, Comtech Corporation, 2008. p 2
- [8] ComTech – CDM 625 User Guide, Comtech Corporation, 2008. p 3
- [9] ComTech – DoubleTalk™ Carrier-in-Carrier™, , Comtech Corporation, 2004. p 5
- [10] ComTech – DoubleTalk™ Carrier-in-Carrier™, , Comtech Corporation, 2004. p 4

Illési Zsolt

illesi.zsolt@proteus.hu

SZÁMÍTÓGÉP HÁLÓZATOK KRIMINÁLTECHNIKAI VIZSGÁLATA

Absztrakt

Az infokommunikációs technológia (ICT) átítatja a mindennapokat a „virtuális” megoldások egyre több teret nyernek a hagyományos megoldásokkal szemben. Ezzel párhuzamosan nőtt az ICT szerepe a bűnözésben is. A bűncselekmények széles körének vizsgálatakor az ICT eszközök büntetőjogilag releváns információkat (bizonyítékokat) hordoznak, így bizonyítékforrásként célszerű ennek a szektornak a kriminálisztikai, krimináltechnikai vizsgálatával foglalkozni. Az ICT krimináltechnikai vizsgálata új kutatási módszereket és technikákat igényel. A cikk ennek a megközelítésére javasol egy módszert, amely Brian Carrier réteg megközelítésére épül, és amely alkalmas a szakmai kompetenciák meghatározására és az együttműködés interfészeinek azonosítására.

Infocommunication technology (ICT) is impregnated into the everyday life, and the “virtual” solutions are gaining around with traditional technologies. In parallel, increases the role of ICT in crime. Investigating the wide range of criminal activities the ICT equipments may provide relevant information from criminal law point of view (evidence), therefore it is practical to deal with criminal study and forensic analysis of this sector as a source of evidence. Forensic analysis of ICT requires new research methods and techniques. This paper proposes a method, based on Brian Carrier’s abstraction layer approach, to this analysis, and also suitable for professional competence and identifying the interfaces of cooperations.

Kulcsszavak: számítógép hálózatok, informatikai rendszerek vizsgálati rétegei, krimináltechnikai vizsgálatok ~ computer networks, investigation layers of information systems, forensics analysis

Bevezetés

Az informatika az infokommunikációs technológia a mindennapok megszokott részévé vált. Hazánkban 1,2¹ az egy főre eső mobiltelefonok száma; szinte minden háztartásban van már számítógép; valamennyi diák számára elérhető az internet. Sőt! A szélessávú internet hozzáférést néhány EU tagország már alapvető emberi jogként deklarálta.²

A számítógépek, az infokommunikáció jelen van a háztartásokban, az iskolákban, a kutatóhelyeken, a munkahelyeken. Az informatika, a telekommunikáció elmaradhatatlan részévé vált a mindennapjainknak.

Az infokommunikációs eszközök azonban nem egymástól elszigetelten működnek, hanem hálózatokba rendezve kapcsolódnak és megosztják egymással az erőforrásaikat, támogatják a beépített funkciókat, lehetővé teszi az alkalmazások távoli elérését és használatát.

Az intenzív használat, az „up-to-date” adatforrások és a hatékonyság és eredményesség növelő funkciók minden használó számára kívánatosak és hasznosak. Azonban a jogkövető felhasználók mellett az infokommunikációs eszközök és technológia magához vonzotta a bűnelkövetőket – köztük a terroristákat – is. Az egyedi számítógépek, hálózati eszközök, de maga a hálózat (függetlenül a kiterjedésétől) lehet:

- célpont,
- megvalósítási/ elkövetési tárgy/ környezet,
- elkövetés szimbóluma,
- elkövetés „tanúja”.

[2][6][9]

A fentiek miatt a számítógép hálózatok, mint az infokommunikációs technológia egyik működési területe, jó bizonyítékforrássá válhatnak, így tárgyai lehetnek a kriminalisztikának, azon belül a krimináltechnikai vizsgálatoknak.

Az infokommunikáció egy rendkívül gyorsan változó, bővülő tudományterület. A nyomfelderítést, a helyszíni nyomrögzítést, a titkos nyomozást a nyomozóhatóság képviselői látják el, akik véletlenszerű tartalmú és mélységű informatikai szakismerettel rendelkeznek és nincs napi rutinjuk, mély és formális ismeretük az informatikai és a telekommunikáció terén. A rögzített nyomok értékelését azonban – formális képzésben szerzett ismeretekkel, szakértelemmel és a speciális szakmai gyakorlattal rendelkező – igazságügyi szakértők végzik el, akiknek az ismeretei heterogének. Mindezek miatt célszerű a számítógép hálózatok, mint lehetséges bizonyítékforrásoknak a tudományos kutatása, a nyomfelkutatási, nyomrögzítési, esemény rekonstrukciós és elemzési tevékenységeit (a számítógép hálózat krimináltechnikai vizsgálat területét) tanulmányozni. A kutatás eredménye egy olyan megközelítés – módszerek és technikák együttese – lehet, amely alapul szolgálhat a nyomozóhatóság és az érintett igazságügyi szakértők kompetencia alapú professzionális feladatvégzésének és együttműködésük meghatározásának.

A cikkben ismertetni szeretnék egy, a számítógép hálózatok krimináltechnikai

¹ <http://portal.ksh.hu/pls/ksh/docs/hun/xftp/gyor/tav/tav20903.pdf>

² <http://ezinearticles.com/?Internet-Access-As-a-Human-Right&id=3243554>

<http://www.foxnews.com/story/0,2933,525993,00.html>

<http://www.csmonitor.com/2003/0701/p07s01-woeu.html>

<http://www.vouli.gr/politeuma/syntaxDetails.asp?ArthroID=6>

[http://translate.google.hu/translate?js=y&prev=_t&hl=hu&ie=UTF-](http://translate.google.hu/translate?js=y&prev=_t&hl=hu&ie=UTF-8&u=http%3A%2F%2Fwww.vouli.gr%2Fpoliteuma%2FsyntaxDetails.asp%3FArthroID%3D6&sl=el&tl=hu)

[8&u=http%3A%2F%2Fwww.vouli.gr%2Fpoliteuma%2FsyntaxDetails.asp%3FArthroID%3D6&sl=el&tl=hu](http://translate.google.hu/translate?js=y&prev=_t&hl=hu&ie=UTF-8&u=http%3A%2F%2Fwww.vouli.gr%2Fpoliteuma%2FsyntaxDetails.asp%3FArthroID%3D6&sl=el&tl=hu)

http://index.hu/tech/2009/10/19/allampolgari_jog_lett_a_szeles_sav_finnorszagban/

vizsgálati megközelítésére alkalmas modellt, amely kiindulópontja lehet egy igazságügyi módszertani levélnek.

1 Krimináltechnikai vizsgálatokról általában

1.1 A kriminalisztikai vizsgálatok célja

A kriminalisztikai vizsgálatoknak, ezen belül a krimináltechnikai vizsgálatok célja a törvényes forrásból származó, büntetőjogilag releváns tények szolgáltatása, amelyek összességükben alkalmasak büntetőjogilag releváns tényállás megállapítására. {[10] p. 79.} Ez a hétköznapi nyelvre lefordítva olyan folyamatot jelent, amely információt nyújt a(z)

- elkövető(k)ről (Ki?),
 - események valós természetével kapcsolatban (Mit?),
 - események helyszínével kapcsolatban (Hol?),
 - események sorrendjével kapcsolatban (Mikor?),
 - motivációs tényezőkkel kapcsolatban (Miért?),
 - elkövetés módjáról és a felhasznált eszközökről (Hogyan?).
- {[11] p. 58-59.}

A vizsgálatokat a fenti kérdésekre figyelemmel kell előkészíteni, hogy azok adekvát válaszokat adjanak és közvetett vagy közvetlen bizonyítékot szolgáltatassanak. [8][10]

1.2 A számítógép hálózat krimináltechnikai vizsgálati megközelítése

Az informatikai rendszerek vizsgálatakor lényeges szempont, hogy milyen körülmények között, milyen eszközökkel és mikor zajlik a vizsgálat.

A szakirodalomban elterjedt az élő-holt rendszer felosztás. Az élő rendszer e szerint a felosztás szerint azt jelenti, hogy a vizsgálatot a vizsgálni kívánt számítógépen, annak operációsrendszerét és segédprogramjait felhasználva végezzük. A holt rendszer, ezzel ellentétben azt jelenti, hogy a vizsgálatot saját megbízható eszközökkel, saját megbízható környezetben végezzük. Ez utóbbi megközelítés megbízhatóbb eredményt szolgáltat ugyan, de a valóságban sajnos nem mindig megvalósítható a gyakorlati életben (például egyedi eszközök és prototípusok vizsgálatánál, speciális vizsgálati környezet és segédeszköz hiányában, továbbá ha nagyon gyors, azonnali helyszíni elemzésre van szükség).

A számítógép hálózatok krimináltechnikai szakirodalma azonban nem ilyen módon osztja fel a vizsgálatokat, hanem a számítógép hálózatokból kinyerhető adatforrások szerint írja le a vizsgálati folyamatot:

- hálózati komponensek azonosítása
 - ISO/OSI modell vizsgálata
 - együttműködés rejtett hálózati ügynökökkel és szerverek kontrollja
 - hálózati adatok (forgalom) mentése
 - hálózati adattárolók keresése
 - folyamatok újraalkotása a forgalom alapján
- {[7] p. 241-263.}

A másik megoldás a számítógép hálózatok IP protokoll, vagy ISO/OSI réteg alapú megközelítése. {[4] p. 370-380.}

Véleményem szerint az élő-holt megközelítés kiegészítésre szorul, mivel nincs tekintettel az elkövetés és a vizsgálat időbeni kapcsolatára (egyidejű vagy követő vizsgálat), illetve nem eléggé pontosan határolja el a vizsgált eszköznek és környezetnek a vizsgálatra gyakorolt befolyását. A fenti felosztások közül a második a krimináltechnikai vizsgálatok leírására nem alkalmas mivel a fókuszban csak a hálózati rétegek állnak, a bizonyítékok megszerzésének módjáról és időzítéséről nem szól. Javaslok egy olyan megközelítést, amely az élő-holt felosztáshoz hasonlít leginkább, de javaslom azt tovább finomítani az alábbiak szerint:

- az elkövetés-vizsgálat időbenisége szerint:
 - az elkövetéssel egyidejű
 - az elkövetés után végzett
- vizsgált rendszer működési állapota szerint:
 - kikapcsolt (holt)
 - bekapcsolt (élő)
- a vizsgáló eszköz (program) kontrollja szerint:
 - a vizsgált rendszerbe integrált (a vizsgált rendszer kontrollja alatt álló)
 - a vizsgált rendszertől független (a vizsgált rendszernek nincs kontrollja a vizsgáló felett)

A cikkben a számítógép hálózatoknak az elkövetéssel egyidőben végzett krimináltechnikai vizsgálatával (nyomrögzítés és elemzés) foglalkozom, amikor is a vizsgálat tárgya (a hálózat) működik, függetlenül attól, hogy az adatgyűjtést végző eszköz a vizsgálati környezet kontrollja alatt áll-e vagy sem.

1.3 Locard anyagcsere és kölcsönös nyomhagyási szabálya

A számítógép hálózatok krimináltechnikai vizsgálatának meg kell felelnie a kriminalisztika általános követelményeinek és az infokommunikációs rendszerek sajátosságainak is.

Az elsődleges alapelv, amely a krimináltechnikai vizsgálatokat megalapozza Edmond Locardtól, az 1920-as évek kiemelkedő kriminalisztikai szakértőjétől származik. Alapelve (Locard Exchange Principle) szerint bárki, vagy bármi kerül kapcsolatba egy bűncselekmény helyszínével valamilyen nyomot hagy és valamilyen nyomot tovább visz magával, amikor elhagyja azt. Az elv következetes alkalmazása vezetett a traszológia (nyomtan) kifejlődéséhez, és ez alapján lehet az elkövetőt, a sértettet és a tetthelyet összekapcsolni és a kapcsolódásra utaló nyomokat a büntetőeljárásban felhasználni.

A kriminalisztika és a traszológia egyik alapfogalma a nyom, hiszen ez az, amit megfelelő szakértelemmel végzett elemzést követően a büntetőeljárásban büntetőjogilag releváns tényként valamilyen állítás igazolásához vagy cáfolatához bizonyítékként fel lehet használni. A nyom helyes kategorizálása az alapja annak, hogy azokat megfelelően azonosítani, konzerválni és elemezni lehessen.

A nyom a jelenlegi értelmezés szerint lehet lenyomat (valamilyen tárgy morfológiai sajátosságait magán viselő nyom, ilyen lehet például egy ujjnyom, törésnyom, lövedéken a huzagolás miatt keletkezett elváltozások), de lehet anyagmaradvány is (valamilyen anyag kémiai, biológiai sajátosságait magán viselő nyom, például vér, DNS, anyagmaradvány, amelynek az összetétele lényeges). A nyomok vizsgálata során sokszor előfordul, hogy ugyanaz a nyom mindkét fenti kategóriába beletartozik és csak a vizsgálati eljárás sajátosságai használják ki ezen nyomok lenyomat-anyagmaradvány természetét, például egy ajaklenyomat és a lenyomatról vett nyál/DNS minta kettős természetű vizsgálatakor.

Véleményem szerint a fenti két nyom-kategória az infokommunikációs rendszerekben keletkező nyomokra nem alkalmazható. Szükségesnek tartom egy harmadik kategória bevezetését, a digitális nyomét, vagy másként az „adatmaradvány”-ét. [5][8]

1.4 Az infokommunikációs rendszerből kinyert bizonyítékok osztályozása

Az infokommunikációs rendszerből (így a számítógép hálózataból) kinyert nyomok tehát bizonyítékforrások és mint bizonyíték a következő módon kategorizálhatók:

- eredeti vagy származékos,
- tárgyi jellegű,
- terhelő vagy mentő,
- közvetlen vagy közvetett (indíciium).

Az eredeti környezetben működő számítógép hálózat továbbá irreverzibilis bizonyítékforrás, mivel az azon áthaladó jelek csak egyszer léteznek, csak akkor és ott (ex tunc et allicundo) vizsgálhatók.

A számítógép hálózatokból kinyert bizonyítékokról megállapítható, hogy mind az elkövetés tárgyi oldaláról (in rem), mind pedig a személyi oldaláról (in personam) szolgáltat információkat. Meg kell azonban jegyezni, hogy a számítógép hálózatokból kinyert bizonyíték elsősorban in rem bizonyítékforrás, csak ritkán (például az elkövetésről készült jó minőségű on-line továbbított videó felvétel, vagy hálózaton keresztüli biometria azonosítás esetén a küldött/fogadott biometria adatok) szolgáltat in personam bizonyítékokat. Ez a sajátos hangsúlyeltolódás egyébként az infokommunikációs rendszerek krimináltechnikai vizsgálatainak egészére igaz, és sajátos többlet nyomozati feladatokat generál az in rem bizonyítékok természetes személyhez kötésénél³.

[8][10]

1.5 Daubert kritériumok

A bizonyítékgyűjtés nem lehet minden kontroll nélküli. Ha nincsenek korlátai a bizonyításnak, akkor az teret adhatna a korlátlan megfigyelésnek, az alaptalan bizonyítékok felhasználásának így az anyagi szabályok megkerülésével ártatlanok büntetőjogi felelősségre vonására vagy bűnösök felmentésére kerülhetne sor. A bizonyítékszerzésnek ezért jogszerűnek kell lennie, a jog által meghatározott forrásból kell származnia, illetve a Büntetőeljárás törvény (1998. évi XIX. törvény a büntetőeljárásról, a továbbiakban Be./ [1]) normáinak megfelelően kell begyűjteni, kezelni (tárolni) és értékelni.

Az egyik fontos szempont a bizonyítékok minőségének, megalapozottságának kérdése. Az egyik ilyen alapvető kontrollt az Amerikai Legfelsőbb Bíróság 1993-as a Daubert v. Merrell Dow Pharmaceuticals ügyben hozott precedens értékű ítélete jelenti a szakértők szakvéleményével (expert witness testimony) kapcsolatban. A döntés értelmében a bíróságnak ellenőriznie kell a bizonyítás során felhasznált új módszereknek a módszer által szolgáltatott bizonyíték tudományos megalapozottságát, garantálva a megfelelő alkalmazást és megbízhatóságot. Az ellenőrzés során a bíróságnak vizsgálnia kell, hogy az alkalmazott módszer

- mennyire állta ki a gyakorlat próbáját,
- hibaaránya ismert-e,
- a tudományban elismert módon publikált-e, mi a tudományos elemzésének eredménye (megmutatható-e a hamissága, tehát falszifikálható-e, cáfolhatóság, tesztelhetőség⁴), és a szakemberek közössége által elismert-e,
- keresztül ment-e alapvető gyakorlati teszteken. [6][8]

³ A felhasználói név nem azonos a felhasználóval magával. Azonos felhasználói név alatt többször több személy egymástól függetlenül is tevékenykedhet, még az sem biztos, hogy a jogosult felhasználó tudtával, vagy anélkül történik-e mindez. Tehát valamilyen felhasználói név alatt elkövetett cselekmény önmagában még nem alapozza meg a felróhatóságot. Bizonyítandó, hogy a terhelt használta az adott eszközt az elkövetés idején.

⁴ Ld. Karl Raimund Popper osztrák és Lakatos Péter magyar tudományfilozófusok munkáit.

A Daubert kritériumok megjelennek a szakértői vizsgálatokkal kapcsolatban a Be. 105. § (1) bekezdésében is:

„A szakértő szakértői vizsgálat alapján ad véleményt. A szakértő a vizsgálatot a tudomány állásának és a korszerű szakmai ismereteknek megfelelő eszközök, eljárások és módszerek felhasználásával köteles elvégezni.”

A Be. azonban nem említi meg a „tudományosság” kritériumát a nyomozóhatóság nyomozati feladataival kapcsolatban. Figyelembe véve azonban, hogy amatőr módon, megalapozatlan eljárásokkal végzett nyomrögzítés – ami a krimináltechnikai vizsgálatok kezdő lépése – nem szolgáltatathat szakszerű, tudományos szakvélemény alapjául. Ezért a Daubert kritériumok betartása kötelező érvényű a nyomozóhatóságok munkájára is, az általuk végzett nyomozati munka egészére, a nyomrögzítő eljárásokra és eszközökre mind a nyílt, mind a titkos adatszerzés során. [1]

1.6 Logikus érvelés és Occam borotvája

Az egyes bizonyíték elemek megszerzésének tehát ki kell állniuk a tudományosság próbáját. A bizonyítás során hangsúlyt kell helyezni a logikus érvelésre, az ok-okozati lánc fenntartására, kerülendő az inkonzekvens következtetés.

Az indíciumoknak a bizonyítandó feltételezést alátámasztó láncolatának azonban nem csak logikusnak, de egyszerűnek kell lennie. A lehetséges verziók felállításakor kerülni kell az oda nem való részletekkel való kiegészítést, használni kell Occam borotváját, hogy a rendelkezésre álló indíciumok alapján a legvalószínűbb magyarázattal szolgálhasson.

A bizonyítás során lényeges, hogy a bizonyíték a bizonyítandó feltevés alátámasztásán túl alkalmas legyen az alternatív feltevések kizárására. [5][6][8]

2 A számítógép hálózatok vizsgálati modellje

Számítógép hálózatnak azt a speciális infokommunikációs alrendszert tekintem, amely a számítógépek kommunikációs eszközök egymás közötti kommunikációját biztosítja. A számítógép hálózat kategorizálható a mérete, a funkcionális kapcsolatok, a topológiája, az adatátviteli sebesség szerint. [12]

A krimináltechnikai vizsgálatok szempontjából a számítógép hálózat egyszerűsített sémája a következő:



1. ábra – Számítógép hálózatok egyszerűsített sémája
[szerkesztette: Illési Zsolt]

A sémában szereplő

- hálózat az átviteli közeget, a csatorna kódolást, valamint a hálózati adatforgalomban szerepet játszó aktív hálózati eszközöket (jeltovábbítás esetén),
- végpont az adatforrásokat és nyelőket jelentik, amik szerverek, munkaállomások vagy aktív hálózati eszközöket („saját jogon” történő kommunikáció esetén).

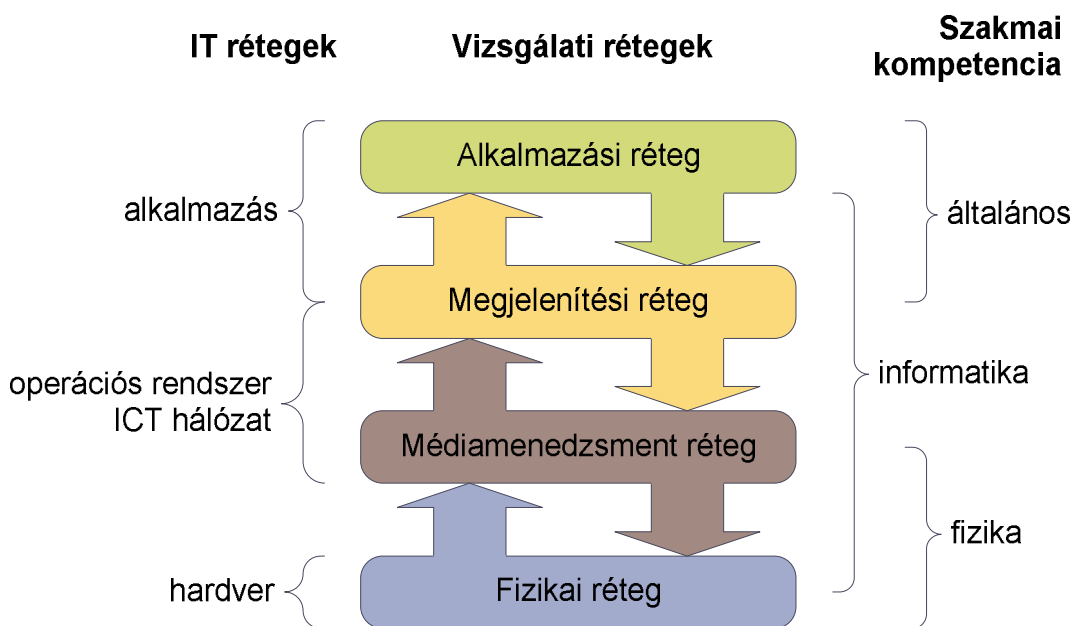
A cikkben nem foglalkozom a hálózati végpontokon és aktív hálózati eszközökön tárolt

adatokkal, naplóállományokkal, vezérlési logikák vizsgálatával, sem ezen eszközök és működési paramétereik felderítésének kérdéseivel; de nem foglalkozom az általános infokommunikációs eszközökről kriminalisztikai célból történő adatszerzéssel sem. Ezek a vizsgálatok nem tartoznak közvetlenül a számítógép hálózat – pontosabban a számítógép hálózati adatforgalom – vizsgálatának a tárgykörébe.

A fenti számítógép hálózati séma azonban még nem elegendő ahhoz, hogy az azon történő adatforgalom vizsgálatát modellezni lehessen, továbbá még nem ad kellő információt arról, hogy a krimináltechnikai vizsgálatok során milyen feladatokat kell ellátni és ezekhez milyen speciális szakértelem szükséges.

Brian Carry 2003-ban publikált egy réteg megközelítést, amelyet ő az adathordozók vizsgálatának elemzéséhez használt. [3] Az ő réteg-megközelítése a számítógép hálózatokra, mint a modellbe nem illeszkedő, attól eltérő entitásokra tekint. Véleményem szerint Brian Carry modellje megfelelő kiegészítésekkel alkalmassá tehető az infokommunikációs eszközök és rendszerek krimináltechnikai vizsgálatának általános leírására, illetve alapjául szolgálhat az egyes rétegekkel kapcsolatos kriminalisztikai funkciók meghatározására, továbbá e funkciók megvalósításához szükséges szakértelem és az egyes szakterületek közötti interdependencia azonosítására.

Brian Carry modellje az általam tett kiegészítésekkel a következő:



2. ábra – Informatikai rendszerek vizsgálati rétegei
[forrás: [3] alapján szerkesztette: Illési Zsolt]

2.1 Fizikai réteg

A fizikai réteggel kapcsolatos tevékenységek célja a számítógép hálózaton áthaladó valamennyi, az ügy szempontjából releváns jel érzékelése, rögzítése, a rögzített adatok időpecséttel, ellenőrző kóddal (hash), esetleg digitális aláírással való hitelesítése. A későbbi vizsgálati lépések (keresés és elemzés) szempontjából ez alapvető fontosságú. A hiányos bitminta gátja lehet az adatok rekonstrukálásának, mivel a számítógép hálózaton továbbított jelek irreverzibilis bizonyítékforrások. A hitelesítetlen adatforrás pedig a későbbiekben – a

tárolás vagy további szakértői vizsgálatok során szándékosan vagy véletlenül – módosítható, ezért szakmai alapon kétségbe vonható a valódisága, ezért bizonyítékként való felhasználhatósága jelentősen csökkenhet, vagy alkalmatlanná válhat.

A kódolás-dekódolás során felmerül a „tényleges” csatornakódolás és a nyomrögzítéskor használt „lehetséges” kódolásnak a kérdése. Egy hibás dekódoló alkalmazásával rögzített adatfolyam alkalmatlan lesz bizonyítékként való felhasználásra. A számítógép hálózat fizikai rétegének elemzéséhez, az ezen áthaladó bitfolyam rögzítéséhez tehát speciális szaktudásra van szükség a fizika, a villamosmérnöki, és az információ- és kódelmélet terén.

Az elkövetéssel egyidőben végzett hálózati adatforgalom rögzítése a jelenleg hatályos Be. 200.§ (1)/c szerint titkos adatgyűjtésnek minősül, ami csak a 201.§-ban felsorolt speciális esetekben végezhető és a 203.§ alapján bírói engedélyhez kötött az alkalmazhatósága. Az ilyen adatgyűjtést elsősorban a külön törvényben meghatározott szervek (Be. 204. §), a szakszolgálatok végzik, szükség esetén bevonva az adattovábbítást végző szervezet képviselőit. A jelenleg hatályos Be. nem szól a különleges szakértelemmel rendelkező személyek (nem szakszolgálati szakértők) szükséges szerepéről a titkos adatszerzés során. [1]

Mivel a szakszolgálatok és a nyomozóhatóságok alapvetően nem telekommunikációs, számítógép hálózati szakértők és nem kötelező – csak a Be. 182.§ alapján lehetséges – különleges szakértelemmel bíró személyek bevonása a nyomrögzítési tevékenységbe, ezért felmerül a fizikai réteg vizsgálatával kapcsolatos szakmai kompetencia kérdése, illetve az, hogy a szükséges kompetencia milyen technológiával biztosítható, mivel szakértő bevonásának hiányában a nyomozóhatóság (vagy a szakszolgálatok) feladata a nyomrögzítés szakmai szabályainak megkövetelése, az elvárható gondosság szintjének biztosítása. Ez egy igen sajátos probléma, mivel egy (telekommunikációs, számítógép hálózati) szakmai szempontból laikus szervezetnek kell egy általa csak részben vagy nem ismert terület szabályainak betartásáról, betartatásáról gondoskodnia.

Véleményem szerint ilyen esetekben a titkos adatgyűjtést végző szervezetnek igazságügyi szakértőt kellene kirendelnie szaktanácsadóként a nyomrögzítés elvégzésére, vagy a nyomrögzítés szakmai feltételeinek felügyeletére. A probléma részben kezelhető azonban, mivel a hálózati adatforgalom rögzítése elterjedt hálózati technológiák esetén alkalmas hardver és szoftver segítségével automatizálható. Sokat segítene ebben a kérdésben (is), ha ilyen típusú vizsgálatokkal, nyomrögzítéssel kapcsolatos módszertani levelek megszületnének és egységesen kiadásra kerülnének a nyomozóhatóságok, a szakszolgálatok és az igazságügyi szakértői kamara tagjai számára.

2.2 Médiamededsment réteg

A számítógép hálózat krimináltechnikai vizsgálatának második lépcsője során a cél a fizikai réteg elemzését, az azon áthaladó bitfolyam rögzítését követően az elsődleges adatkonténerek (a hálózati keretek) azonosítása és elkülönítése egymástól.

Az egyik szakmai problémát az jelenti, hogy a bitfolyam elvileg többféleképpen értelmezhető, az egységes (valamennyi kódolási eljárásban egységesen alkalmazott) irreducibilis kódok használata nem jellemző. Amennyiben a hálózati keretek nem különíthetők el egyértelműen egymástól, úgy az alkalmazott hálózati csomagok, hálózati protokollok, protokoll hierarchiák mélyebb ismeretére, illetve minta illesztő algoritmusok használatára is szükség lehet a legvalószínűbb keretfolyam előállításához.

Erre egy példa egy bitfolyam (hexadecimális formában) ARP csomaggént való 2 lehetséges értelmezése:

1. lehetséges ARP csomag kezdete

00 01 08 00 06 04 00 02 00 e0 00 10 80 00 60 4d 01 76 ff ff ff ff ff ff 9f 7d 03 55

2. lehetséges APR csomag kezdete

3. ábra – ARP csomag lehetséges értelmezése egy bitfolyamban
[szerkesztette: Illési Zsolt]

A médiamenedzsment rétegben kell először a csatorna-dekódolás esetleges hibáit, zavarait is figyelembe venni, ebben is a protokoll hierarchia mélyebb ismerete (alkalmazott hibafelismerő és hibajavító kódolás) szükséges.

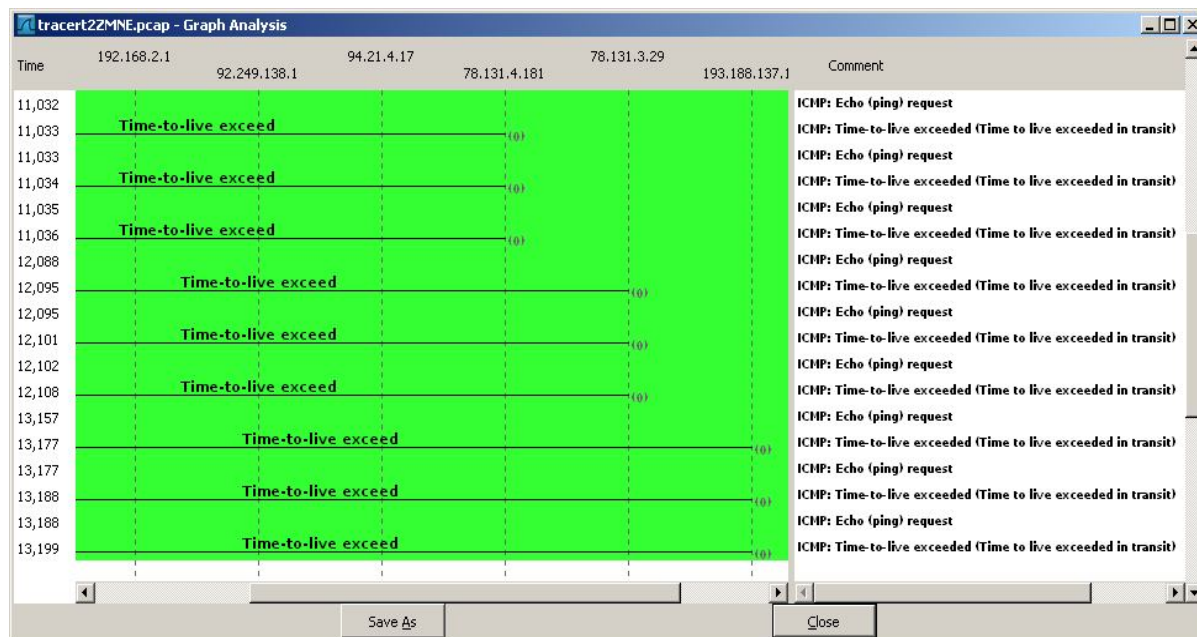
2.3 Megjelenítési réteg

A megjelenítési rétegbeli vizsgálatok célja az adatkeretek belső szerkezetének a feltárása, a protokoll információk dekódolása, a hálózati protokoll hierarchia „visszafejtése” és az átvitt adatok (email, dokumentumok, felkeresett weblapok, távoli rendszerekben kiadott parancsok, programok stb.) összeállítása, a hálózati események időbeli sorrendjének rekonstruálása.

Az adatkeretek azonosítása és szétválasztása során lehet az adatcsomagokra épülő protokoll keret információit (vezérlő információk, sorszámok, hibajelző és hibajavító kódokat, időbélyegeket, IP, MAC címeket stb.) értelmezni, és felhasználni azokat a hálózati adatforgalom dekódolására.

A médiamenedzsment rétegbeli tevékenységek eredményeként állnak elő:

- kapcsolat diagram (egymással kapcsolatban álló eszközök kapcsolathálója),
- esemény diagram (hálózati események és időzítésük),
- tevékenység diagram (felhasználói parancsok és időzítésük),
- protokoll lista és protokoll hierarchia,
- hálózati adatforgalmi statisztika,
- küldött fogadott adatok.



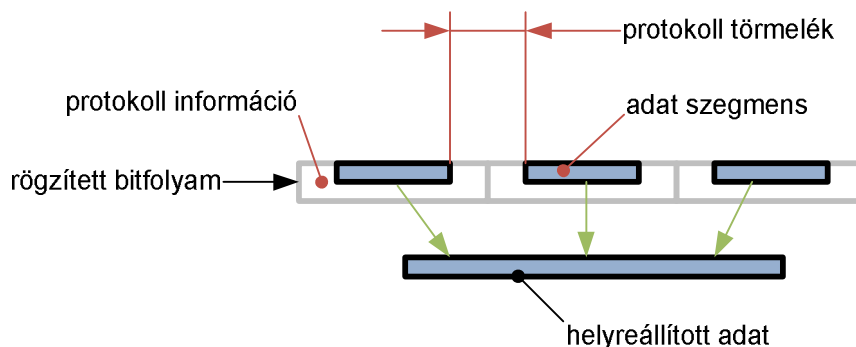
4. ábra – IP útválasztók sorozatát feltérképező traceroute parancs
ICMP csomagjainak folyamat diagramm részlete
[szerkesztette: Illési Zsolt]

Amennyiben a megjelenítési réteg vizsgálatakor a médiamenedzsment rétegből kinyert keretek magasabb szinten helytelen értelmezéshez vezetnek, úgy vissza kell térni az előző rétegben definiált feladatok elvégzéséhez valamilyen más megközelítést (például más protokoll bázist, más kezdőpontot) keresve új adatkeretek előállításához.

Előfordulhat az is, hogy többszörös kísérletezés ellenére sem állítható elő a bitfolyam alapján egy helyesen értelmezhető adatkeret-folyam. Ebben az esetben adatvésési (data carving vagy file carving) technikát lehet alkalmazni a protokoll információk, vagy küldött/fogadott adatok helyreállítására. Az adatvésési technika az adatok struktúrája, belső adatai (metaadatok), az egyes protokoll információkra, adatformátumokra jellemző kódolási sajátosságok alapján kísérli meg a helyreállítást. Ez a megközelítés az adattárolókon a partíciós táblák, a fájlrendszer-leírók (például FAT tábla, vagy inode) sérülése esetén, vagy egyszerű szteganográfia alkalmazásának gyanúja esetén, fájl töredékekből való helyreállításhoz használhatók.

Jó példa erre a JPEG képek kódolása¹, ahol a fájl „FF D8 ... FF D9” keretes szerkezetbe ágyazottak, ezek az értékek tetszőleges hexaeditorral kereshetők, így könnyen azonosíthatók és helyreállíthatók. A módszer következetes alkalmazásával az egymásba ágyazott képek is feltárhatók (például kép-indexkép reláció esetén).

A hálózati adatforgalom esetén a fenti technika sajátos nehézsége a hálózaton küldött-fogadott adatok keretinformációi miatti adattöredezettség, a protokoll törmelék azonosítása és eltávolítása az adatok helyreállítása során. Ezt szemlélteti a következő ábra:



5. ábra –Adatvésés hálózati adatfolyamból
[szerkesztette: Illési Zsolt]

A médiamenedzsment réteg egyik sajátos részterülete az azonosított adategységek (például fájlok) hitelességének, eredeti/ módosított/ hamis voltának vizsgálata. Kriptográfiai hitelesítő adatok hiányában ez információ és kódelméleti vizsgálatok alapján, a metaadatok és a fájl egyéb adatainak összevetésével, vagy a vizsgált adatfájl belső statisztikai elemzésével végezhető el.

Ide tartozik még az adatfájlok és a fájl belső jellemzőinek elemzése (a fájlok kiterjesztésének és a fájlok kódolásának összevetése), az adatfájlok entrópiájának vizsgálata, így a rejtett és a titkosított adatrészek azonosítása. Ezt, egymásba ágyazott adatrejtést feltételezve rekurzívan is el kell végezni.

A megjelenítési réteg elsősorban infokommunikációs (hálózati), másodsorban információ és kódelméleti és informatikai felkészültséget igényel, de speciális hálózati alkalmazások adatforgalmának elemzéséhez szükség lehet programozói vagy az alkalmazás működésével kapcsolatos egyedi szaktudásra.

¹ Ld. ISO/IEC 10918-1:1994.

2.4 Alkalmazási réteg

Az alkalmazási réteggel kapcsolatos feladatok célja (a hálózati és protokollinformációktól megtisztított) adatok értelmezése, büntetőjogilag releváns információ kinyerése. Az alkalmazási rétegbeli vizsgálatok tárgya lehet informatikai jellegű, például az adatfájlok metaadatainak kinyerése, az adatokban található SQL, shell stb. parancsok értelmezése, programok visszafejtése, a kód-logika értelmezése a vizsgált cselekménnyel kapcsolatban.

Ebben a vizsgálati rétegben azonban már olyan egyéb – nem informatikai, telekommunikációs jellegű – adat is megjelenik, ami meghaladja az informatikai igazságügyi szakértő kompetenciáját. Fénykép esetén megállapítani a fényképen szereplő személy életkorát igazságügyi orvosszakértői feladat, szerzői védelem alá eső adatok (például program, kép, hang és videó fájlok) esetén az okozott anyagi hátrány megállapítása, vagy egyes esetekben a szerző, előadó azonosítása speciális (nem informatikai) szakértelmet és szakértői jogosítványokat kíván; így az ilyen adatokat tartalmazó ügyeket érdemben együttes, vagy egymást követő kirendelésekkel lehet szakszerűen lefednie a nyomozóhatóságoknak. (Például az informatikai igazságügyi szakértő feltárja a küldött-fogadott képeket, amelyeket ezután igazságügyi orvosszakértő elemez.)

Összefoglalás

Az infokommunikációs technológia átítatja a mindennapokat, meghatározó elemévé vált az üzleti életnek, a műszaki-tudományos világnak, de az egyének mindennapi életében is jelentős szerepet játszik. A technológia fejlődésével és terjedésével a „virtuális” megoldások egyre több teret nyernek a hagyományos megoldásokkal szemben. A levelet felváltotta az email és az SMS, a hagyományos vonalas telefonokat a mobil és az IP telefonia, a banki ügyintézők helyett (mellett?) terjed az eBanking... De a háttérben is nő az infokommunikáció szerepe. A kritikus – vagy jobban mondva a létfontosságú – infrastruktúrák is infokommunikáció segítségével csökkentik a működési költségeiket, növelik a hatékonyságukat és az eredményességüket.

Az infokommunikáció fejlődése nem csak a „fehér gazdaságra” igaz, hanem ugyanilyen (de legalább is hasonló) léptékben ismeri fel és használja ezt a technológiát a „szürke” és a „fekete” gazdaság is. És itt most nem csak a bűnözői csoportok kezében lévő hatalmas botnet hálózatokról, kiterjedt internetes pedofil képcserélő hálózatokról, a pénzügyi szektort támadó adathalász és hitelkártya-adat vadász csoportokra gondolok.

Számítógépet, internetet, mobil telefont használ(hat)nak a fehérgalléros bűnözők a bennfentes kereskedelmi tranzakció részleteinek egyeztetésére, a fekete galléros bűnözők egy rablás előkészítésre vagy lebonyolításakor, illetve a bűnös úton szerzett javak értékesítésére. De igazságügyi szakértői praxisomban talákoztam olyan esettel is, ahol a terhelt

- mobiltelefonja kamerájával vette fel a fiatalkorú partnerével eltöltött pásztoróra intim részleteit,
- házi eszközeivel szkennelt, editált és nyomtatott valódinak tűnő hamispénzt,
- egy rendőri túlkapásra hivatkozó leveléhez digitális felvételeket készített és szerkesztett a sérüléseiről.

Kimondható tehát, hogy a bűncselekmények széles körének vizsgálatakor az infokommunikációs eszközök büntetőjogilag releváns információkat (bizonyítékokat) hordoznak, így bizonyítékforrásként célszerű ennek a szektornak a kriminálisztikai, krimináltechnikai vizsgálatával foglalkozni. Szükség van e terület kutatására már csak azért is, mert az infokommunikáció naponta hoz újdonságokat – új protokollok, eszközök, kódolások stb. jelennek meg. Ezek elemzése, vagyis annak kutatása, hogy

- miképp használható az infokommunikációs technológia bizonyítékok kinyerésére,
- a technológiában rejlő adatok kinyerésének vannak-e, ha igen, akkor hol, törvényes akadályai,
- a „Ki?”, „Mit?”, „Hol?”, „Mikor?”, „Miért?”, „Hogyan?” kérdésekre adnak-e és ha igen, akkor mennyire adekvát válaszokat

komoly fizikai, informatikai, telekommunikációs krimináltechnikai és kriminalisztikai, nyomozati probléma.

Ez az új – újszerű – terület új kutatási módszereket és technikákat igényel. A cikkben ennek a megközelítésére javaslok egy módszert, Brian Carrier réteg megközelítésének továbbgondolt verzióját, amely alkalmas a szakmai kompetenciák meghatározására és az együttműködés interfészeinek azonosítására. Véleményem szerint az általam javasolt megközelítés megkönnyíti a téma tudományos kutatását is.

Sajnos hazánkban ez a terület elhanyagolt. Nincs még olyan módszertani levél sem, ami a nyomozóhatóság nyomszerzési, nyomrögzítési tevékenységét és az ezt követő értékelő-elemző igazságügyi szakértői vizsgálatok általános szakmai szabályait, módszereit és technikáit rögzítené.

Véleményem szerint nagy szükség lenne egy ilyen módszertani levélre. Nem csak az igazságügyi szakértők, de a nyomozóhatóságok, sőt a jogászok (ügyészek, ügyvédek és bírák) is nagy hasznát vehetnék. Ugyanis a szakértő súlyos hibát követ el, ha nem a kirendelő határozatban megfogalmazott kérdésekre válaszol és úgy szolgáltat bármilyen bizonyítékot, hogy azt a kirendelő határozat nem kéri. {[10] p. 136.} Rossz, hiányos kérdésekre azonban csak rossz, hiányos válasz adható, a legnagyobb szakértői professzionalizmus mellett is elmaradhat a rögzített nyom szakszerű értékelése, így büntetőjogilag releváns tények maradhatnak „árnyékban” és a terhelt bűnösségének megállapításakor nem lehet figyelembe venni sem mentő, sem terhelő bizonyítékként.

A cikkben csak felületesen említettem egy olyan területet, amely szintén új kutatási feladatként kell, hogy megjelenjen a számítógépek krimináltechnikai vizsgálatában. Ez a kriptográfia. A magántitok, a bank és üzleti titok, a minősített adatok tárolása, továbbítása mellett a „rosszfiúk” is előszeretettel alkalmazzák ezt a jogellenes magatartásuk nyomainak elleplezésére. Amíg az általános kriptóanalízis teoretikusan közelíti meg a titkosítások megfejtésének kérdését, addig a bűnüldözőknek praktikus megoldások kellenek. A kérdés számukra az, hogy a terhelt által használt (pontosabban az általánosan is elterjedt és a leggyakrabban alkalmazott) kriptográfiai eszközöknek mi a gyengéje, hogyan férhetnek az elkövető titkaihoz, mivel és meddig érdemes próbálkozni, hogy korlátos idő- és pénzráfordítás mellett ésszerű határidőn belül eredményre lehessen jutni.

Remélem sikerült érzékeltetnem az információtechnológiai krimináltechnika előtt álló feladatokat és azok nehézségeit. A kutatások ezen a területen azonban önerőből, egy-egy szakértő önálló (sokszor egymástól elszigetelt) munkájával nem végezhető el. A tudományos alaposágú elemzéshez fejlesztéshez szükséges lenne szervezett kutatásra ami anyagi források nélkül elképzelhetetlen. Ehhez jelenleg azonban nincs olyan pályázat, vagy egyéb forrás, ami az igazságügyi szakértés kutatási, eszközpark bővítési problémáit megoldaná.

Egy a szakértői körökben forgó jogszabálytervezet a módszertani levelek elkészítését a Magyar Igazságügyi Szakértői Kamara feladatává tenné: „30/A. § (1) A MISZK elnöksége (a továbbiakban: elnökség) a szakértői tevékenység egységes és magas színvonalú ellátása érdekében módszertani levelet ad ki”. A tervezet azonban nem rendel forrást a feladathoz – de nem ad ehhez „pénzt, paripát, fegyvert” egyéb más jogszabály tervezet sem. Tudomásom szerint módszertani levelek elkészítésébe kezdett a Nemzeti Nyomozó Iroda Csúcstechnológiai Bűnözés Elleni Osztálya, de az igazságügyi szakértői kamarától függetlenül...

Úgy gondolom, hogy az általam vizsgált kérdéskörnek a koordinálását és

menedzselését az Igazságügyi és Rendészeti Minisztériumnak kellene felvállalnia, kutatóhelyek teremtésével és pályázatok kiírásával együtt. Így ez a most elhanyagolt terület fejlődésnek indulhatna és a krimináltechnikai vizsgálatok is megfelelnek a kor társadalmi-tudományos elvárásainak.

Irodalomjegyzék

- [1] 1998. évi XIX. törvény a büntetőeljárásról (Be.)
- [2] Balogh Zsolt György: Jogi informatika, Dialóg Campus Kiadó, Budapest-Pécs, 1998.
- [3] Brian Carrier: Defining Forensic Examination and Analysis Tools Using Abstraction Layers, International Journal of Digital Evidence, 2003. Volume 1 Issue 4., Economic Crime Institute (ECI) at Utica College, USA, 2003.
- [4] Eoghan Casey: Digital Evidence and Computer Crime – Forensics Science, Computers and the Internet, 2nd edition, Elsevier Academic Press, California, USA, 2004.
- [5] Illési Zsolt: Krimináltechnika Szerepe az Informatikai Védelem Területén, Hadmérnök, IV. Évfolyam 1. szám - 2009. március, Budapest, 2009. [IZs2]
- [6] Illési Zsolt: Open Source IT Forensics, avagy Nyílt Forráskódú Programok Felhasználása az Informatikai Igazságügyi Szakértésben, Bolyai Szemle 2008. XVII. évf. 4. szám, ZMNE Bolyai János Katonai Műszaki Kar, Budapest 2008. [IZs1]
- [7] Linda Volonino PhD, Reynaldo Anzaldúa: Computer Forensics for Dummies, Wiley Publishing, Inc., Indianapolis, USA, 2008.
- [8] Szerk.: Dr. Bócz Endre: Kriminálisztika, BM Kiadó, Budapest, 2004.
- [9] Szádeczky Tamás: Terrorizmus a kibertérben, Infokommunikáció és jog, 2008. V. évf. 6. sz. pp. 200-205.
- [10] Tremmel Flórián: Bizonyítékok a büntetőeljárásban, Dialóg Campus, Budapest-Pécs, 2006.
- [11] Wayne Jansen, Rick Ayers: Guidelines on Cell Phone Forensics (NIST 800-101), National Institute of Standards and Technology, USA, 2007.
- [12] <http://hu.wikipedia.org/wiki/Számítógép-hálózat>

Inkovics Ferenc

ferenc.inkovics@gmail.com

LEHETSÉGES KOMMUNIKÁCIÓS KAPCSOLATOK AZ EU ELNÖKSÉG ALATT A KÜLKÉPVISELETEKEN ÉS A KÜLÜGYMINISZTERIUMBAN

Absztrakt

Ez a cikk röviden bemutatja az EU főbb szervezeteit. Majd ismerteti a Külügyminisztériumban (KüM) levő aktuális helyzetet a különböző típusú kommunikációk vonatkozásában. É végül számba veszi a kihívásokat, amikkel szembe néz a KüM, és az ezekre való reagálásokat.

This article briefly introduces the main organizations of the EU. Then it presents the actual situation in the Ministry for Foreign Affairs (MfA) concerning the different types of the communication. And at last it enumerates the challenges, the MfA faces, and the reactions for them.

Kulcsszavak: soros EU elnökség, kommunikáció, kihívások ~ EU Presidency, communication, challenges

Az Európai Unió és a soros elnökség intézménye

Az Európai Unió egy olyan 27 tagországból álló politikai és gazdasági unió melynek nem tagja az összes európai állam (Pl.: Svájc, Norvégia, stb.), ugyanakkor földrajzilag Európa határain is túlnyúlik (Pl.: Kanári-szigetek, Francia Guyana, stb.). Főbb intézményei [1]:

- Az Európai Unió Tanácsa (röviden Tanács): Az EU elsődleges, de nem kizárólagos kormányközi alapon működő, döntéshozó, jogalkotó szerve. Szokták Miniszterek Tanácsaként is emlegetni. Nem keverendő az Európai Tanáccsal¹, és az Európa Tanáccsal²;

¹ Az Európai Tanács az EU állam- és kormányfőinek testülete, amely intézményileg nem része a Tanácsnak, ugyanakkor annak struktúrájába illeszkedik, és csúcsszerveként működik.

² Európa Tanács székhelye Strasbourg és célja a parlamentáris demokráciák valamint az emberi és alapvető szabadságjogok védelme.

- Európai Bizottság: az EU mindennapi munkáját végző döntés előkészítő, javaslattevő szerv, amely bizonyos esetekben ellenőrző, képviseleti, döntéshozó és végrehajtó feladatokat is ellát;
- Európai Parlament: az Unió állampolgárai által közvetlenül választott képviselőtestület, amelynek fő feladata, hogy a tagállami érdekeket megjelenítő Tanács és a közösségi érdekeket megtestesítő Bizottság mellett, az Unió állampolgárainak érdekeit képviselje a közösségi döntéshozatalban. A közösségi döntéshozatal nagy részében a Tanács melletti társdöntéshozó, társjogalkotó szerv;
- Európai bíróság: A Bíróság biztosítja, hogy a közösségi jogot egységesen értelmezzék és alkalmazzák minden tagállamban, felügyeli a közösségi jog betartását, továbbá ellenőrzi és biztosítja, hogy a különböző intézmények a Szerződésekben lefektetett hatásköreik szerint járjanak el;
- Európai számvevőszék: az európai közösségi pénzügyek revíziójával megbízott független testület;
- Gazdasági és szociális Bizottság: az EU egyik tanácsadó bizottsága, melynek célja, hogy a különféle gazdasági, szociális érdekcsoportokat bekapcsolják a közösségi ügyekbe, valamint bevonják a közösségi döntések előkészítésébe;
- Régiók Bizottsága: az EU másik tanácsadó bizottsága, melynek célja, hogy lehetővé tegyék a helyi és regionális szervek számára, hogy közvetlen beleszólást kapjanak a Közösségek munkájába;
- Európai Beruházási Bank: célja, hogy tőkeberuházások finanszírozásával elősegítse a Közösségek kiegyensúlyozott gazdasági fejlődését;
- Központi Bankok Európai Rendszere és Európai Központi Bank: a közös valuta, az EURO menedzseléséhez szükséges központi intézményrendszerek;
- Európai Ombudsman: ide fordulhatnak az EU állampolgárai, valamint az Unió területén bejelentett irodával rendelkező társadalmi szervezetek és vállalkozások, amennyiben nem megfelelő elbánásban részesültek, illetve sérelmet szenvedtek el az Unió intézményei által.

A Miniszterek Tanácsát megkülönböztetik az azon részt vevő miniszterek szerint. Két speciális tanács van a Külügyminiszterek Tanácsa és az úgynevezett Általános Ügyek Tanácsa. Ezek politikailag nagyobb jelentőségű, átfogóbb, horizontális jellegű kérdésekkel foglalkoznak. Míg a szektorális tanácsok a szakminiszterek testületei. Ilyen például a Gazdasági és Pénzügyminiszterek Tanácsa (az ECOFIN), a Mezőgazdasági Miniszterek Tanácsa vagy az Egészségügyi miniszterek tanácsa. Összességében a szakterületek szerint mintegy 15-féle Tanácsot különböztetnek meg. A különböző tanácsok havonta vagy ritkábban (pl.: évente 2-6 alkalommal) ülnek össze. Az egyes szektorális Tanácsok ritka, 1-2 napos ülései nem teszik lehetővé a döntések megfelelő előkészítését és alapos megtárgyalását. Ezért hozták létre az ún. COREPER-t³, az Állandó Képviselők Bizottságát. Ez a testület az első pillérben próbálja meg a különböző tagállami álláspontokat egymáshoz közelíteni, egyeztetni, ezzel előkészíti, koordinálja, illetve segíti a Tanács munkáját. A második pillérben a Politikai és Biztonsági Bizottság (Political and Security Committee), a harmadik pillérben pedig a Koordináló Bizottság (Coordinating Committee) végzi ezeket a feladatokat. Több kérdésben nehéz a megegyezés, ezért a Tanács és a COREPER munkáját kb. 250 állandó, illetve ad hoc jelleggel felállított tanácsi munkacsoport (Council working groups) segíti. A Tanács elnöki tisztségét félévenként felváltva adják a tagállamok. A soros elnök tagállam joga a Tanács összehívása. Ő elnököl a Miniszterek Tanácsában, az Európai Tanácsban, a COREPER-ben és

³ A COREPER a COMmittée des REprésentants PERmanents francia rövidítéséből származik

a munkacsoportokban is. Nagy szerepe van az elnökségi időszak alatt tárgyalásra kerülő ügyek döntésének befolyásolásában, és kulcsszerepet játszik az Unió külső képviselésében és külpolitikai álláspontjának megjelenítésében is. [1]

Adatkezelés kapcsán felmerülő kérdések

Az egyes tagállamoknak és magának az EU-nak is a napi működése során adatokat/információkat kell eljuttatni különböző helyszínekre. Mindez persze a meghatározott, előre definiált felhasználói követelmények, igények megléte mellett lehetséges. Legtöbbször a felhasználói igény az, hogy minden adat álljon korlátozás nélkül rendelkezésre. Az ilyen igények kielégítését akkor lehet maradéktalanul teljesíteni, ha megfelelően felkészültünk arra, hogy az adatok a kívánt helyen, időben és formában rendelkezésre álljanak. A különböző típusú adatokhoz ki kell választani a megfelelő adatközlítési eszközöket, és adathordozókat. Ezen eszközök és adathordozók kiválasztásának feltétele, hogy ismerjük az adat származási helyét és végcélját - vagyis, hogy honnan-hova kell eljuttatni - a típusát, a mennyiségét és természetesen az időkorlátokat is. Mindezt szigorú rendelkezésre állási, hibatűrési követelmények nehezítik.

A MK Külügyminisztériuma (továbbiakban: KÜM) területi, funkcionális és szakmai főosztályokra, és külképviseletekre tagozódik. Alapvetően a szakmai, területi főosztályok és külképviseletek (pl.: Amerikai Főosztály vagy Biztonságpolitikai és Non-proliferációs főosztály) támasztják az igényt és szabják a követelményeket az adatok tekintetében és a funkcionális főosztályok (mint pl.: a Biztonsági Informatikai és Távközlési Főosztály) elégítik ki az igényeket, biztosítják a működési feltételeket. Természetesen az igényeket, a lehetőségeket (ide értve a jogszabályoknak való megfelelést is) és ezek költségvonzatát, megvalósíthatóságát, valamint az ahhoz szükséges időt össze kell hangolni. Ehhez alaposan előregondolt tervezés szükséges. Az alábbi kérdésekre meg kell kapni a válaszokat, ahhoz, hogy megfelelően fel tudjunk készülni arra, hogy az adatok megfelelő helyen és kért időben történő rendelkezésre bocsátására:

1. Honnan hova kell eljuttatni? Vagyis mi a kiindulópont és mi a rendeltetési hely? Pl.: Budapest – Brüsszel; vagy Sydney – Kairó;
2. Milyen típusú az adat: hang, elektronikus adat, video vagy papír. Ennek függvényében tudjuk kiválasztani az adatátviteli jellegét. Pl.: egy email csatolmányának formátuma és karaktereinek kódkészlete is fontos, hogy a másik fél is gond nélkül tudja értelmezni.
3. Mekkora mennyiségű adatok továbbítására van szükség? Pl.: e-mailnél a méret korlát szabhat határokat.
4. Az adat minősítése milyen? Teljesen másként kell kezelni a nyilvános, nem nyilvános és minősített adatokat.
5. Mikor? A küldésnek a különböző lehetőségek választásakor időtényezője is van. Pl.: egy e-mail percek alatt célba érhet, de egy postai csomagnak, vagy futárnak már akár napokra is szüksége lehet.
6. Milyen hibahatárok, türések léteznek: az adat elvesztése az szinte minden esetben probléma, de előfordulhat olyan eset is, amikor a minimális késés sem megengedett. Van-e lehetőség ismételt próbálkozásra?

A KÜM szempontjából a soros EU elnökség főbb adatkezelési pontjai a következők:

1. EU tanácsának főtitkársága, Brüsszel;
2. Külügyminisztérium Központ, Budapest;
3. A Magyar Köztársaság Állandó Képviselete az EU mellett, Brüsszel;

4. Több mint 100 magyar külképviselet, több mint 80 országban, különböző kontinenseken;
5. Magyarország brüsszeli és luxemburgi EU Tanácsi delegációs szobái;
6. Magyarország strasbourg európai parlamenti szobája
7. stb.

A jelenlegi helyzet

A hang és video alapú adatok továbbítására telefonokat, mobiltelefonokat, VoIP telefonokat, műholdas telefonokat és videokonferencia készülékeket használnak a KÜM-ben. Ezekkel a berendezésekkel 2 vagy akár több tucat kolléga között is megoldott a hang és képinformációk megosztása. Mindegyik megoldásnak megvannak a hátrányai és előnyei is. A telefon szinte a világ minden pontján van, ugyanakkor helyhez kötött. Mobiltelefont használók nem kötöttek fix földrajzi pontokhoz, de a mobilhálózatok lefedettsége nem 100%-os. A VoIP telefonhoz internet hozzáférés szükséges, a beszélgetés viszont forgalmi díjmentes. A különböző műholdas telefon szolgáltatások szolgáltatóik szinte az egész világon lefedettséget nyújtanak, de a mobiltelefonok áraihoz képest csillagászati áron kínálják a szolgáltatásokat. A telefonkonferencia és videokonferencia szolgáltatással egyszerűen össze tudunk kapcsolni tárgyalópartnereket és utazás nélkül megoldható egy-egy tárgyalás lebonyolítása, ugyanakkor ennek technikai oldalára megfelelően fel kell készülni.

Elektronikus adat alapú információ továbbítására számos megoldás létezik. A KÜM az ilyen adatok továbbítására felhasználja a saját honlapját, az Intranetjét, a hivatalos pl. titkársági elektronikus postafiókokat, iratkezelési rendszerét (Scriptament) és a külképviseletek valamint a KÜM központ között kialakított hivatalos érintkezési formát az ATTR⁴ rendszert. A legfeljebb nemzeti, NATO vagy EU bizalmas szintű minősített adatok továbbítására pedig a VKH (Védett Külügyi Hálózat) nyújt megoldást. A KÜM munkatársai használják az EUDOK rendszert is, melynek alapvető célja, hogy segítse a kormányzati koordinációt az európai uniós ügyek intézésében, és biztosítsa az EU-s dokumentumok eljuttatását az illetékes szakértőkhöz és döntéshozókhoz. Ennek a rendszernek nagy szerepe van az EU döntéshozatali tevékenység során képviselendő magyar álláspont kialakításának folyamatában [2]. A KÜM kollégái a hivatalos formákon kívül informális csatornákat is felhasználnak adatok gyűjtésére és továbbítására. Ehhez felhasználnak azonnali üzenetküldő és email szolgáltatásokat is. Ebben segítséget nyújt, hogy a KÜM Budapesten és a brüsszeli állandó képviselten már megoldotta a kollégák a belső nyílt levelező rendszert távolról, akár otthonukból is elérik. Az EU részéről az EU Extranet-et, a CORTESY⁵ és az ESDP⁶ hálózatot szükséges megjegyezni, mint hivatalos adatkommunikációt megvalósító megoldásokat.

Az EU régi tagállamai és a Bizottság még ma is üzemeltetnek egy veszélyhelyzeti rövidhullámú rádiós hálózatot a Föld különböző országaiban. Korábban Külügyminisztériumnak is az egész világra kiterjedő rövidhullámú rádióhálózata volt, de az számítógépek és hálózatok fejlődésével az adatforgalmazás egyre inkább áttérrelődött az internetre.

⁴ ATTR: Automatikus Távirat Továbbító Rendszer: egy e-mail alapú adattovábbító mechanizmus

⁵ The CORTESY egy rejtjelzett forgalmat bonyolító hálózat az EU tagállamok külügyminisztériumai, az EU Bizottság és a Tanács főtitkársága között. Nagyon hasznos rendszer pl.: a multilaterális vagy harmadik államot érintő kérdések politikai elemzéseinek szaktanácskozásaihoz.

⁶ ESDP-Net:

Bár mai világunk egyre inkább hasonlít egy információs szupersztrádához, még mindig van igény papír alapú adatok továbbítására is. Ennek több oka is lehet: pl.: hagyományok őrzése, egyéb megoldásokhoz képest gazdaságosabb mivolta, alternatív megoldás hiánya stb. Képzeljünk el egy olyan helyzetet, mikor az egyik külképviseletünkön egy diplomata egy rendkívül érzékeny információt szeretne eljuttatni a központba, úgy hogy az adott információ biztosan ne kompromittálódjon. Ehhez egyéb okok miatt sajnos nem áll rendelkezésre megfelelő technikai eszköz, ezért papírra veti az információt és diplomáciai futárral juttatja el a központba, Budapestre. Papír alapú információ továbbítását faxkészülékkel, postai úton és/vagy diplomáciai futárral valósítja meg a KüM.

Az előttünk álló kihívások

A KüM ma is nagy mennyiségű elektronikus és papír alapú adatot kezel. A korábbi statisztikai adatok alapján az egyes tagországok a többihez képest nagyságrendileg kb. egyforma adatmennyiséget kezelnek, kivéve az elnökséget ellátó tagállam, mert az ő esetében az adatforgalom kb. a 10 szeresére növekedik. Kb. ilyen mértékű adatmennyiség növekedésre számít a Külügyminisztérium is. Ez igaz a minősített és a nyílt adatok tekintetében is.

Soron EU elnökként sokkal nagyobb felelősség is hárul országunkra, de ez egyszerre jelent felelősséget és lehetőséget is. Az aktuális világgazdasági, világpolitikai és egyéb helyzetek valamint a kidolgozott stratégia várhatóan az eddig megszokott időkorlátokhoz képest jelentősen lecsökkenthetik a reagálási időket. Ennek oka abban keresendő, hogy a Tanács elnökségének elsősorban stratégia-alkotó, szervezési és reprezentatív funkciói vannak.

Egyes ülések nem a megszokott munkaidőben vannak. Több esetben előfordul, hogy délután pl.: 17:00kor kezdődik egy ülés és elhúzódik éjjelig vagy még tovább is. Ez azt jelenti, hogy a különböző szolgáltatásokat nem csak 08:00 és 17:00 között szükséges nyújtani, hanem biztosítani kell az elnyújtott és/vagy elcsúsztatott napokon is. A KüM központ a képviselők földrajzi elhelyezkedése miatt már eleve 24 órás berendezkedésű (pl.: Canberrában már a hivatalos munkaidő után járunk, de Washingtonban ekkor még csak a munkaidő fog elkezdődni).

Az ülések nem korlátozódnak csak 1 vagy 2 helyszínre, amiatt emelt szintű szolgáltatások biztosítása szükséges nem csak Budapesten, Brüsszelben, de Luxemburgban és Strasbourban is. Mindemellett előfordulhatnak olyan egyéb (pl.: magyarországi vidéki) helyszínek, ahol kihelyezett ülések lesznek.

A soros EU elnökséget Magyarország az államigazgatásban több száz fős létszámbővítéssel tervezi ellátni, e személyek technikai ellátottságát is biztosítani szükséges. Az új kollégáknak szüksége lesz többek között új számítógépes munkaállomásokra, nyomtatókra, új irodákra stb. Őket be kell kapcsolni abba az információs folyamba, aminek a többi kolléga már része.

Ahhoz, hogy az előzőekben említetteknek eleget tudjunk tenni a rendszereink rendelkezésre állását is erősíteniünk szükséges. Ahogy ma is úgy az elnökség alatt is adódhat olyan helyzet, hogy 2 órán belül szükséges reagálni. És még nagyobb súlya van egy esetleges üzemzavarnak akkor, ha az adott ország éppen a soros elnök.

Reagálás a kihívásokra

Az informatikában és telekommunikációban felmerülő kihívásokkal és problémákkal a KüM saját kollégáival (helyi és regionális rendszergazdák, telekommunikációs és hálózati szakemberek) és szerződéses partnereivel együtt néz szembe. A megnövekedett feladatok, nagyobb létszámú és vagy modernebb eszközparkot is igényelnek. A jelentkező létszámihiány pótlására több megoldás is lehetséges. Az egyik ilyen pl.: újabb informatikai szakemberek felvétele, de bizonyos szolgáltatások kiszervezése is szóba jöhet. mindkét megoldásnak vannak hátulütői. Már több pályázót elriasztott a köztisztviselői bértábla szerinti besorolás szerint bér, ami egy képzett szakember versenyszférában ajánlott fizetésével sokszor össze sem hasonlítható. És a munka is viszonylag rövidtávú: 1,5 évről beszélünk. A szolgáltatások kiszervezése, pedig csak úgy hoz kellő eredményt, ha a felelősségi viszonyok kellő mértékben tisztázhatóak. Megfelelő részletességgel kidolgozott SLA-k (Serviser Level Agreement – szolgáltatási szint megállapodás) szükségesek, ahhoz, hogy a szolgáltatás még kritikus helyzetben se essen a kívánt szint alá. Ugyanakkor a kiszervezés költségesebb is lehet az előbbihez képest, hiszen a kiszervezés során a vállalkozó profitját és akár jóval magasabban megfizetett szakembereket kell megfizetnünk.

Az elavult kommunikációs vonalakat folyamatosan cserélt a KüM modernebbekre, ahol szükséges ott alternatív megoldásokat is megvizsgált. A leginkább érintett terület például Afrika és a Közel-Kelet. Ezeken a területeken sokszor a földi szolgáltatás minősége, sávszélessége, rendelkezésre állása és/vagy ára nem megfelelő. Az elmúlt évek során több képviselőn műholdas internet szolgáltatásra váltott át a KüM. Természetesen az egyéb területeken (Európa, Amerika stb.) kontinenseken is folyamatosan fejleszti a kommunikációs vonalakat a KüM. A kommunikációs vonalak fejlesztése mellett fejlesztve vannak a felhasználói munkaállomások és a szerver oldali hardverek is. Mindezek olyan konstrukcióval, hogy garancia minimum az EU soros elnökség végéig meg legyen. A bővítéseket úgy szükséges elvégeznünk, hogy közben a rendelkezésre állást megtartsuk és/vagy erősítjük.

Az alkalmazott rendszerek többsége e-mail vagy web alapú megoldás, ezért elsődleges fontosságú a SPAM és vírusvédelem erősítése, az ezeket érintő adattárolási kapacitások növelése. Pl.: e-mail méret korábban a KüM-ben 5 MB volt, azonban egyre gyakrabban kúldtek csatolmányokkal együtt 5-10 MB körüli e-maileket a Tanácsból is, melynek fogadása elengedhetetlen volt. A kapcsolódó teljes szerverpark fiatalítása, korszerűsítése is folyamatosan történik.

Külképviselői hangátviteli rendszerek korszerűsítése, egységesítése terjesztése szintén folyamatos feladata a KüM-nek. Az elmúlt években szinte kivétel nélkül minden képviselőre sikerült kiterjeszteni a VPN hálózatot. Ennek egyik nagy előnye a képviselők és a központ közötti VoIP hálózat biztosítása. További modernizációs lépések, hogy a külképviselőken található telefonközpontokat integráljuk a KüM központi telefonközpontba. Ezzel különböző szolgáltatás kiterjesztést és bővítést érünk el. Néhány példa: egységes hívószámok alakíthatóak ki a jövőben; költségcsökkentést lehet elérni, ha a nemzetközi és távolsági hívások helyett IP szintű telefonközponti kapcsolatokat és azokon végződött helyi hívásokat használunk, stb.

Az elmúlt években úgy lett átalakítva a teljes VPN hálózat, hogy a munkaállomások és szerverek távmenedzselhetőek, illetve idén elindult a rendszerfelügyeleti eszközök telepítése és széles körű alkalmazása. A VPN hálózat lehetőséget adott arra, hogy egységes KüM-i

levelezőrendszer legyen. Technikailag meg lett oldva annak a lehetősége, hogy egy külügyes kolléga magával vigye az e-mail címét, bárhova is kerül külszolgálatra.

Jelenleg a KüM központban és a Brüsszel EU melletti Állandó Képviseleten dolgozók élvezhetik a távoli levélelérés előnyét. Tervek szerint 2010 elejétől ez a többi külképviseleten is megoldott lesz. Ezen felül jelenleg a KüM központban már működik az elektronikus levelek távoli elérése okos telefonokkal, PDA-kal is. E megoldás több kollégára való kiterjesztése is folyamatban van.

A több száz új kolléga elhelyezése miatt új számítógépes munkaállomások, irodák és épületek biztosítása folyamatban van.

Az EU minősített adatok közül az EU Korlátozott Terjesztésű (KT) adatokat szükséges kijuttatni a külképviseletekre. Ennek kivitelezésére egy minden képviseletet magába foglaló EU KT minősítésű hálózat kialakítása van folyamatban.

Mindamellet, hogy a Külügyminisztériumnak fel kell/kellett nőnie e feladathoz, mindezt úgy kell véghezvinnie, hogy az egyéb alapfeladatainak ellátása ne sérüljön. A Konzuli Információs Rendszernek (Consular Information System - CIS) és a Válságkezelő Központnak e megnövekedett súlyú feladatok mellett is működniük kell. Ahhoz, hogy kellően felkészüljünk a soros EU elnökségre már jó néhány lépésen túl vagyunk, de még sok megoldandó feladat áll előttünk.

Hivatkozások:

[1] Horváth Zoltán, Dr. Bathó Ferenc, Dr. Mohay György, Dr. Tóth Judit, Horváth Péter:
Közigazgatási szakvizsga – Általános közigazgatási ismeretek 5. rész – Az Európai
Uniószervezete és jogrendszere. Magyar Közigazgatási Intézet, 2002.

[2] EU-s ügyek kezelése a Synergon segítségével.
http://www.terminal.hu/cikk.php?article_id=5565 letöltve: 2009-11-10

Kassai Károly

karoly.kassai@hm.gov.hu

A HONVÉDELMI TÁRCA BIZTONSÁGPOLITIKÁJÁBAN MEGHATÁROZOTT KÖVETELMÉNYEK, FELADATOK ÉS AZOK FONTOSABB HATÁSAI

Absztrakt

2010. január elsejétől hatályba lépett a honvédelmi miniszter által novemberben jóváhagyott honvédelmi tárca információbiztonság politikája (továbbiakban: politika) [1.]. A cikk a politika központi szabályozó szerepét mutatja be, ismerteti a fontosabb szabályozó elemeket, amelyek meghatározóak a honvédelmi szervezetek szervezeti típusú és rendszer-specifikus információbiztonsági követelményeinek, védelmi rendszabályainak kialakításakor.

From the 1st of January 2010 the Information Security Policy of MoD signed up in November of 2009 by the minister is valid. This article describes the central regulation position of the policy and introduces the key elements which have determining impact in creation of organisation type and system-specific type information security requirements and protection measurements at military organisations.

Keresőszavak: *biztonságpolitika, információbiztonság, információvédelem, informatika, elektronikus adatkezelés ~ security policy, information security, protection of information, IT, information handling*

1. A POLITIKA ALKALMAZÁSA

A honvédelmi tárcánál eddig még nem történt meg az információvédelmi szakterület átfogó szabályozása, így e szabályozó megjelenése új, központilag meghatározott követelményrendszerként jelent a honvédelmi tárca szervezetei számára. A belső rendelkezés alkalmazása a honvédelmi tárca szervezeteinél a hatályba lépéstől kötelező. Általános követelmény, hogy az egyéb szakterületeket átfogóan szabályozó, vagy specializált, az adatkezelést is érintő szabályozás csak a politika követelményeivel összhangban készülhet. Ez alapját teremti meg annak, hogy a különböző célú és felépítésű szervezeteknél azonos elvek szerint történjen az adatkezelés szabályozása.

A politika hatályon kívül helyezi a főleg szervezeti kérdéseket tisztázó, az elektronikus információvédelemre vonatkozó belső rendelkezést [2.], ami a végrehajtásra vonatkozó eljárások részletezése nélkül 2002-ben kísérletet tett a NATO és EU védelmi rendszabályok centralizálására. A politika a kompromittáló kisugárzás elleni védelem területén 2010-től az új elektronikus adatkezelő rendszereknél kötelezővé teszi a NATO követelmények közvetlen alkalmazását, ami jogszabályi kötelezettség hiányában is jelzi a honvédelmi tárcánál a nemzeti, NATO és EU minősített elektronikus adatkezelő rendszerek kompatibilitására és az adatmegosztásra vonatkozó kötelezettségek érvényesítési szándékát.

A biztonságpolitika a *biztonsági célok és alapelvek, a felelősségi rend, az információvédelmi tevékenység szabályai, az adatok osztályba sorolásának elvei, a kockázatok kezelése, a fizikai és környezeti biztonság, a személybiztonság, a dokumentum biztonság, és az elektronikus információbiztonság* területekre bontva határozza meg a legfontosabb követelményeket.

2. INFORMÁCIÓBIZTONSÁGI CÉL ÉS ALAPELVEK

Az *információbiztonsági célkijelölés* a tárcánál alkalmazott elektronikus adatkezelő rendszerek fejlettségének megfelelően, a NATO és EU biztonságpolitikák és a nemzeti információbiztonsági menedzsment szabvány ajánlása szerint történik a bizalmasság, sértetlenség és rendelkezésre állás azonosításával. E célkitűzések mellett az adatkezelésre vonatkozó követelmények szerint a hitelesség, számon kérhetőség, letagadhatatlanság és a megbízhatóság érdekében kockázattal arányos eljárásokat kell kialakítani.

A politika egyik legfontosabb feladata a biztonsági célok végrehajtását támogató *általános alapelvek meghatározása*.

A honvédelmi szervezetek adatkezelő képességeiket csak a jogszabályokban foglalt követelményeknek megfelelően alakíthatják ki. A rendszerek kialakítása és fenntartása során a teljes életciklust lefedő kockázatelemzéssel kell támogatni a védelmi rendszabályok megfelelőségét. A rendszerek kialakítása során a szolgáltatások és a hozzáférések tekintetében a minimalitás elvét teljes körűen kell alkalmazni (rendszerelemre, üzemeltető állományra, felhasználóra), illetve hozzáférés csak a megfelelő személyi feljogosítás alapján biztosítható. A rendszerek használatba vétele csak előre definiált engedélyezési eljárás alapján történhet, illetve az üzemeltetés során a változtatások is engedélykötelesek. A rendszerek kritikus funkcióit megvalósító hardver és szoftver elemek csak a rendszer besorolásának megfelelő tanúsított termékek lehetnek. A rendszer elemek, adatkezelési és üzemeltetési eljárások csak szabványos eljárások lehetnek; a külső csatlakozásokat védelmi mechanizmusokkal kell védeni. A fejlesztésre, tesztelésre és képzésre használt adatkezelő infrastruktúrákat, adatokat egymástól a szükséges mértékben el kell különíteni. A biztonságra hatással lévő eseteket ki kell vizsgálni és a szükséges változtatásokat el kell végezni (üzemeltetési és a biztonsági dokumentumok módosítása).

Az üzemeltetési helyszíntől, biztonsági környezettől és alkalmazott rendszer-specifikus jellemzőktől függetlenül meghatározott alapelvek célja a rendszerek kialakítása és üzemeltetése során a nyomon követhetőség, az átláthatóság, a rendszerek felügyeletének biztosítása, összefoglalóan a rendezettség, a szükséges szintű biztonsági szint garantálása. A fentiekben bemutatott eljárások normálisnak tekinthető üzemeltetési eljárások megléte esetén különleges követelményeket nem jelentenek, csak korlátozzák a rendszerek üzemeltetőinek és felhasználóinak biztonságra veszélyes öntevékenységet. Meghatározzák, hogy az adatkezelő rendszerek esetében az illetékes vezetők azonosítsák a használatbavétel szabályait, a

változásokat tartsák kézben, illetve ne történhessen meg az üzemeltetői, fejlesztői, vagy teszt feladatok erőforráshiány, időhiány vagy éppen szubjektív hiba miatti összemosása, és ez által a szervezetek üzemeltetéséhez és vezetéséhez szükséges adatok és adatkezelő képességek veszélyeztetése.

Elektronikus adatkezelő rendszerek esetében a rendszerek elfogadása különböző szintű és tartalmú eljárásokat jelent. A NATO, EU minősített elektronikus adatkezelő rendszerek használatba vétele a hatályos jogszabályok alapján hatósági eljárás (akkreditálás) alapján lehetséges. Említésre méltó, hogy az EU és NATO biztonsági követelmények akkreditálást BIZALMAS vagy magasabb minősítési szint esetén határoznak meg, hazánkban ez a kötelezettség már KORLÁTOZOTT TERJESZTÉSŰ minősítési szintnél is jelentkezik. A szigorítás eredménye, hogy egy önálló telepítésű számítógép rendszerbe állítása - ami meglévő rendszerekhez képest elenyésző szintű képesség -, egész napos elfoglaltságot jelenthet a Nemzet Biztonsági Felügyelet, a HM Informatikai és Információvédelmi Főosztály, az MH Összhaderőnemi Parancsnokság kijelölt ügyintézőjének, és természetesen visszatérő jellegű elfoglaltság a helyi biztonsági menedzsmentnek. Nemzeti minősített adatok kezelésére történő feljogosításhoz hasonló eljárást jogszabály jelenleg nem határoz meg, csak HM belső rendelkezés szerinti helyi eljárásra van szükség. Rejtjelző eszköz, eljárás esetén a vonatkozó jogszabály kétszintű hatósági eljárást határoz meg (rendszeresítés és használatbavétel) amely hatósági követelmény nem tesz különbséget nemzeti és NATO, EU eszköz, eljárás között, ami szintén elgondolkodtató, és egyben jövőben megoldandó feladatot jelent.

Nem minősített adatok védelmének kialakítása esetén helyi illetékességű használatbavételi eljárás mellett egyes rendszerek, vagy összekapcsolások esetében független szervezet auditálására van szükség. NATO és EU nem minősített adatkezelés esetében vélhetően hasonló eljárásra van szükség azzal a kiegészítéssel, hogy *ezen adatok esetében jogszabály nem határozza meg, hogy kinek, milyen felelőssége van az adatkezelés biztonsága érdekében.*

A kötelezően alkalmazandó irányelvek megfogalmazásának igénye először 2006-ban jelent meg az MH Informatikai Stratégia első változatának kialakításakor, így a Stratégia 2010-es változatának elkészítésekor *kötelezően jelentkező feladat a két szabályozó összehangolása.* A politika felülvizsgálatakor célszerű lesz az alapelvekre vonatkozóan Munk Sándor informatikai szakterületen az alapelvekre vonatkozó kutatásait figyelembe venni [3.].

3. FELELŐSSÉGEK

A *felelősségi rend* meghatározásának legfontosabb eleme a vezetői és a végrehajtói feladatok elhatárolása, valamint az adatkezelés érdekében szükséges együttműködés alapvető követelményeinek meghatározása.

A *vezetői feladatok* közé tartozik a jogszabályban rögzített titokvédelmi felügyelő illetve biztonsági megbízotti, rejtjelfelügyeleti, iratkezelés felügyeleti, adatvédelmi felelős feladatok azonosítása, valamint a nemzeti ajánlás szerinti elektronikus adatkezelésért felelős elektronikus információvédelmi felügyelői feladatkör. Kis szervezeteknél, áttekinthető homogén elektronikus adatkezelő rendszer alkalmazása esetén akár egy személy is elláthatja az elektronikus információvédelmi szakfeladatokat, de bonyolultabb esetben már rendszer-specifikus felelősségi köröket kell azonosítani. Az adatvédelmi felelős és az elektronikus információvédelmi szakfeladatokat ellátó személyek között együttműködést egyértelműen rögzíti a politika, mert meghatározza, hogy az adatvédelmi felelős követelményei szerint a

szükséges védelmi rendszabályok kialakítása és megvalósítása az elektronikus információvédelmi szakállomány feladata.

A fenti feladatok kapcsán megjegyzendő, hogy egységes, kötelező érvényű nemzeti követelmény nem áll rendelkezésre a fenti feladatokra történő személyi felkészítés érdekében.

A *végrehajtói feladatok* között az előbb említett rendszer-specifikus elektronikus információvédelmi feladatok között a rendszerbiztonsági felelősöket kell érteni. Új elem a BIZALMAS és magasabb minősítési szint esetén alkalmazandó kompromittáló kisugárzás elleni védelmi felelős feladatkört, amelyet más megbízás mellett, vagy önálló megbízásként kell kialakítani a honvédelmi szervezeteknél, az alkalmazott elektronikus adatkezelő rendszerek bonyolultságának, méreteinek megfelelően. A honvédelmi szervezeteknél a rejtjeltevékenységtől függően rejtjelző, vagy rejtjelző nyilvántartó beosztásokat kell kialakítani, vagy a feladatok ellátására alkalmas személyt kell megbízni.

A végrehajtói feladatok kijelölése során tervezési szempont, hogy az adatkezelő rendszereket, vagy nagyobb rendszer esetében az alrendszereket, végpontokat felügyelő szervezeti elemek, felelősök között felügyelet nélküli terület ne maradjon, illetve ne legyen átfedéses a szabályozás. Ezek a szervezési feladatok ott jelentenek kihívást, ahol több honvédelmi szervezet közösen használ egy-egy rendszert, illetve az üzemeltetés több szervezet feladata. Ilyen esetekben egy szervezet nem képes megoldani egy adatkezelő rendszer biztonságos üzemeltetését, *szervezetek közötti együttműködési megállapodásokra, a védelmi rendszabályok és felelősök tevékenységének összehangolására van szükség.*

A politika lehetőséget teremt a honvédelmi szervezeteknél a felelősségek és szakfeladatok összevonására (melyek előnyeit kis szervezetnél, vagy egyszerűnek tekinthető adatkezelés esetén célszerű kihasználni), csak a helyi sajátosságok szerinti összeférhetetlenségeket kell szakszerűen vizsgálni. Ez általában elektronikus adatkezelés esetén lehet bonyolultabb, amikor az üzemeltetői, felhasználói, információvédelmi, biztonsági felügyeleti és esetleg tervezői, fejlesztői feladatokat kell összehangolni, illetve elhatárolni. Ilyen esetekben segíthet az érintett adatkezelő feladatok pontos vizsgálata, a kockázatok elemzése, vagy létszámhiány, speciális üzemeltetői környezet esetén a kiegészítő védelmi rendszabályok alkalmazása.

A szakirányítási feladatok azonosítása mellett megtörténik a *középszintű katonai szerv* feladatának és a *honvédelmi szervezet szintű* feladatok azonosítása. *A középszintű katonai szervnek egyértelműen ráhatással kell lennie az alárendelt szervezetek szakmai tevékenységére*, ami a hadműveleti igényeken keresztül a fejlesztési irányok meghatározása-, a szervezetek felépítése és állománytáblája-, az ellenőrzési tevékenység során a rendellenességek feltárása-, a képzések és továbbképzések szervezése, erőforrások biztosítása területek mellett az adatkezelő rendszerek életciklusa során számtalan egyéb feladatot is tartalmaz.

A jogszabályok, egyéb követelmények szerint kialakított és üzemeltetett rendszerek biztonsága érdekében az ismertetett vezetői feladatokat ellátó személyeknek és végrehajtóknak kötelező az együttműködés, illetve a szolgáltatást nyújtó szervezet tevékenységén belül felelős a védelemért. *A szolgáltatást nyújtó és az alkalmazó szervezeteknek kötelező az együttműködés az adatkezelés biztonsága érdekében.*

4. SZABÁLYOZÁS

Az információvédelmi tevékenység szabályai részben a szabályozási rend azonosítása történik. Az iratkezelés, a minősített adatok védelme, az elektronikus adatkezelés védelme kétszintű szabályozáson alapul (*központi és helyi szabályozás*).

A jelenlegi szakmai álláspont szerint a rejtjeltevékenység szabályozása nem kétszintű, csak *központilag* szabályozott. Nyilvánvaló, hogy e szakterületnél is érvényes az a jelenség, hogy egy-egy szakfeladatot, folyamatot a szükséges részletezettséggel csak helyben lehet szabályozni. Az elektronikus adatkezelés fejlődésével, a hálózatok gyarapodásával párhuzamosan előre jelezhető, hogy a rejtjelzés területén is megjelenik a kétszintű szabályozásra vonatkozó igény.

Az elektronikus adatkezeléssel kapcsolatos védelem szabályozása területén a jelenlegi technológiai szinten szükség van a honvédelmi szervezetek esetében a *helyi hálózatok és egyedi eszközök tömegének szervezeti szintű szabályozására*. Rendszerek esetében *rendszer-specifikus szabályozást kell kialakítani* úgy, hogy a két szabályozás egymást ne korlátozza, illetve ne keletkezzen bürokratikus célú, használhatatlan, a napi életet megfojtó rendszabály halmaz.

5. AZ ADATOK BIZTONSÁGI OSZTÁLYBA SOROLÁSA

Az egyik legjobban félreértett, és egyben közigazgatási szinten központi szabályozás nélküli terület az adatok besorolási kötelezettsége, melynek célja a szükséges mértékű védelem kategorizálhatóságának megteremtése.

A jogszabályokban egymástól eltérő megfogalmazású besorolási rendszerek találhatók, illetve általánosságban kijelenthető, hogy keveredik a kárérték szerinti besorolás és a bizalmasság szintje szerinti besorolás. E két besorolási rendet az alkalmazó szervezeteknek egymás mellett kellene alkalmazni, mert a kizárólag kárérték szerinti megközelítés téves vezetői, üzemeltetői és felhasználói reakciókhoz vezethet. Az országos lefedettség igénye szerinti Egységes Digitális Rendszer esetében például egy kézi rádió érteke szerint alacsony besorolású, de egy katasztrófa helyzetben, vagy egy rendőri intézkedés során egy-egy eszköz által nyújtott adat vagy hang kommunikációs szolgáltatás - vagy annak hiánya - könnyen kritikussá válhat. A légi vezetés és irányítás támogatását szolgáló NATO elektronikus adatkezelő rendszerek esetében egy-egy számítógép vagy rádió távvezérlő által biztosított képesség megléte vagy hiánya (egy kiegészítő elem, vagy alacsony értékű alkatrész meghibásodása, kellékanyag hiánya) szintén olyan példák, amelyek rámutatnak, hogy a kizárólag érték alapú megközelítés a közigazgatásban vagy a honvédelem területén esetenként félrevezethető lehet.

Az honvédelmi tárca adatait a minősítési szintekhez igazított biztonsági osztályokba kell sorolni. A nem minősített adatok esetében az ALAP biztonsági osztály mellett megjelenik a FOKOZOTT biztonsági osztály. Ennek feladata, hogy lehetőség legyen a nem minősített, de funkció vagy halmozódási hatás miatt érzékeny adatok védelmi szintjének emelt szintű kialakítására. Így kell védeni az országos rendszerek központi üzemeltetési adatbázisait, címtárait, a nagymennyiségű üzleti vagy személyes adatokat, a különleges adatokat. Ez a védelem általában a fizikai védelem emelt szintű rendszabályaival (beléptetés, őrzésvédelem), egyedileg kialakított üzemeltetési környezettel, a személybiztonság egyedi szabályaival (nemzetbiztonsági ellenőrzés, általános és szakmai végzettségre, gyakorlatra vonatkozó követelmények) valósítható meg.

Az osztályba sorolással kapcsolatosan egységes közigazgatási követelmények-, illetve a pontosan összehangolt védelmi rendszabályokra vonatkozó követelmények hiányában nehéz annak eldöntése, hogy milyen egységes elgondolás szerint kell elképzelni a különböző célú rendszerek összekapcsolását, adatkezelő szolgáltatások rendelkezésre bocsátását más szervezet felhasználói számára, így előre jelezhető, hogy ezen a területen is valamilyen kormányzati szintű központi rendezés várható.

6. A KOCKÁZATOK KEZELÉSE

Jelenleg a minősített vagy a nem minősített adatokat kezeléséhez kialakított infrastruktúrákra kötelező jellegűen érvényes kockázatelemzési kötelezettség nincs. Hiányzik az egységes nemzeti módszertan (vagy nemzetközi szabványokra, esetleg ajánlásra épített módszertan). A kockázatkezelési tevékenység csak a pénzügyi szektorban kötelező; a közigazgatásnál a szervezeti kockázatok kezelésének rendjébe az adatkezelés ugyan beletartozik, de az alkalmazó szervezeteken múlik, hogy milyen mélységig foglalkoznak ezzel a témával.

A politika a honvédelmi szervezetek esetében a hagyományos vagy elektronikus adatkezelő rendszerekhez életciklusban rögzített feladatként hozzárendeli a kockázatelemzést és kezelést. Az életciklus említése azért fontos, mert összetett rendszer kialakításakor a hadműveleti (alkalmazói) követelmények, a műszaki követelmények és a részletes műszaki tervezés, a kivitelezés (bennel telepítés, tesztelés) és az üzembe helyezés más-más szervezetek hatáskörébe tartozik. A részletes műszaki tervezésnek reagálnia kell a kockázatelemzés során megállapított hiányosságokra és sebezhetőségekre, tehát a hadműveleti (alkalmazói) követelmények elemzése, a rendszer szintű kockázatfelmérés és értékelés kiegészítő adatokkal, követelményekkel pontosítja a műszaki tervezést. Ha a kockázatkezelés során szervezeti határokat kell átlépni, kiemelkedő szerepe van a szervezeti együttműködésnek, a vezetői szándék esetleges pontosításához, módosításához szükséges visszacsatolás működésének, illetve az adott műszaki megoldás ellenőrzése érdekében a többfokozatú biztonsági tesztelésnek, ami a műszaki követelményeket meghatározó szervezet felelősségét hangsúlyozza.

A politika minősített adatkezelés-, több szervezet által közösen üzemeltetett rendszer-, illetve MH szintű rendszer esetében kötelezővé teszi a kockázatkezelést, melynek felelősségét az adatkezelésért felelős honvédelmi szervezet vezetője viseli. A kockázatelemzés során két szintre tagolt eljárást kell alkalmazni, ki kell mutatni és jóvá kell hagyni a maradvány (vagy elfogadható) kockázatokat, illetve a rendszer életciklus állapota szerint szükségszerűen részletezetten, ismétlődő jelleggel kell végezni ezeket a szakfeladatokat. A kockázatelemzés során keletkezett adatokat a rendszer biztonsági dokumentumaihoz kell csatolni, és az időben következő biztonságot is érintő szakfeladatot (pl. akkreditálás, auditálás, rendszerfejlesztés vagy átalakítás) ezekre az adatokra kell építeni.

7. A FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

Adatkezelés az adatok biztonsági osztálya szerint kialakított környezetben engedélyezhető. Nagykerterjedésű rendszerek, érzékeny adatok esetében megjelenik a FOKOZOTT biztonsági osztály kialakítására vonatkozó követelmény, egyébként jól alkalmazható a NATO, EU adatkezelés során alkalmazott adminisztratív zóna, illetve a minősítési szinthez kötött I. vagy II. osztályú biztonsági terület szerinti szemléletmód.

NATO és EU minősített adatkezelés esetében hazánkban az illetékes hatóság kettős eljárást alkalmaz: külön hatósági eljárással dönt a fizikai-, személyi-, és dokumentumbiztonsági

megfelelőségéről, valamint az elektronikus információbiztonsági megfelelőségről. Nemzeti adatkezelés esetén jogszabály hasonló követelményt nem határoz meg. A rejtjeltevékenységre külön jogszabály határoz meg eljárásokat.

Előrelépést jelentene elektronikus adatkezelő rendszerek esetén a hatósági eljárások összevonása, illetve a nemzeti és egyéb adatkezelés egységes eljárásrendben történő rendezése, így ezen a területen is fejlődés várható.

A fizikai biztonsági szakterületen gyakorlati változás érzékelhető, mert az újabban kialakított üzemeltetési helyszíneken már pontosabban kerül mérlegelésre az adatkezelés típusa és az adatkezelés személyes felügyeletének védelmi elemként történő értékelése. Pozitív jelenség a NATO csatlakozás időszakában szigorú nemzeti - NATO elkülönítés átalakulása inkább funkcionális elkülönítéssé.

8. A SZEMÉLYI BIZTONSÁG

A hagyományosnak tekinthető nemzetbiztonsági ellenőrzés, titoktartási nyilatkozat, és NATO, EU minősített adatokat kezelő rendszer esetében a szükséges szintű személyi biztonsági tanúsítvány megléte mellett a politika meghatározza az *összeférhetetlenség vizsgálatára vonatkozó kötelezettséget*, rögzíti, hogy hozzáférési jogosultságok csak adott munkakör ellátásának idejére szólóan adhatók. Külső fél (szerződéses partner, együttműködő szervezet alkalmazottja) által történő üzemeltetési feladatok, vagy felhasználói hozzáférések esetében meghatározza a *kiegészítő védelmi rendszabályok meghatározásáért való felelősséget*.

9. A DOKUMENTUMBIZTONSÁG

Az évtizedeken keresztül formált, pontosított ügyviteli és dokumentumvédelmi rendszabályok megléte nem teszi szükségessé kiegészítő eljárások meghatározását, így a politika ezen a területen főleg az elektronikus adatkezelés sajátosságaira reagál.

Az adathordozók használatbavétele előtt kötelező a funkcionális és a vírusvédelmi ellenőrzés, kezelési jelzések feltüntetése és nyilvántartásba vétel. Az adatok törlése, illetve az adathordozó megsemmisítése a biztonsági osztálynak megfelelő eljárással történhet.

10. AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁG

Az elektronikus adatkezelés során a biztonsági célok elérése érdekében a jogszabályokban és egyéb szabályozókban meghatározott minimum védelmi rendszabályokat kell alkalmazni, melyeket a kockázatelemzés által kimutatott, veszélyesnek ítélt fenyegetések és sebezhetőségek ellensúlyozása érdekében meg kell erősíteni. Az adatkezelő képességek kialakítása és üzemeltetése során tudatos kontrollt kell alkalmazni az üzemeltetési és felhasználói tevékenységek felügyeletére, a rendszer állapotának figyelemmel kísérésére, illetve minden rendszer esetében ki kell alakítani azt a jelentési és tájékoztatási rendszert, ami a rendellenes működés vagy biztonsági incidensek mielőbbi felszámolásához szükséges.

A honvédelmi szervezetek működéséhez és irányításához szükséges elektronikus adatkezelő szolgáltatások védelmére - amennyire az lehetséges - azonos védelmi rendszabályokat kell kialakítani a különböző identitású (nemzeti, NATO, EU, két-, vagy többoldalú szerződésen alapuló) adatok védelme érdekében.

Az információvédelmi védelmi rendszabályokat kiegyensúlyozva, a teljes életciklus során kell alkalmazni. A katonai sajátosságok gyakori kihívást jelentenek a védelmet kialakítók, az üzemeltetők, a biztonsági menedzsment, illetve a különböző hatóságok számára. A mobilitás vagy hordozhatóság követelménye, a speciális alkalmazások, a hálózati kapcsolati-, a különböző identitású adatok együttes kezelésére vonatkozó igény gyakran jelent olyan kihívást, amikor *a jogszabályok szellemében önálló megoldásokat kell kialakítani és jóváhagyni*, mert átfogó jellegű kormányrendeletektől nem várható el a katonai sajátosságoknak megfelelő specialitások részletes szabályozása.

A katonai képességek szervezeti szintű védelme érdekében egyértelmű követelmény, hogy az egyre bonyolultabb elektronikus adatkezelő képességek kialakításához, teszteléséhez, fenntartásához, ellenőrzéséhez szükséges technikai műveleteket - amennyiben lehetséges -, honvédelmi szervezettel kell elvégeztetni, és csak a megfelelő képességek hiányában lehet külső erőforrásokat igénybe venni.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A hivatkozott, szakmai előzmény nélküli belső rendelkezés láthatóan szerteágazó jogszabályi és NATO, EU követelmények összehangolását végzi. Az információvédelem szakterületeire vonatkozó átfogó követelmények megfogalmazása alapot ad a szabályozási rend korszerűsítésére és az alacsonyabb szintű szabályozók megalapozására. Korszerűségének szükséges és nélkülözhetetlen feltétele: a szabályozásért felelős szervezeti elemnek legyen szakmai elkötelezettsége és erőforrása a jogszabályok és egyéb követelmények változása-, illetve az alkalmazás során tapasztalt hiányosságok észlelése esetén a politika felülvizsgálatára és a változások átvezetésére, szélsőséges esetben akár új szabályozó kiadására a technikai és technológiai változások felgyorsulása mellett több éves lemaradással rendelkező szabályozók „bennragadása” fenyegetettség elkerülése érdekében.

A 2010. április elsejétől hatályba lépő minősített adat védelméről rendelkező törvény [4.] és végrehajtási utasításai is vélhetően szükségessé teszik a felülvizsgálatot, ami jelzi, ezt a politikát a szakmának célszerű valóban „élő dokumentum”-ként kezelni. A felülvizsgálatnak célszerű lesz vizsgálnia azt a NATO csatlakozás óta nem pontosan rendezett kérdést is, hogy kinek, milyen szabályozás keretén belül kell meghatározni a honvédelmi tárcára kirótt NATO/NYEU Központi Rejtjelelosztó (National Distribution Authority; NDA) és a NATO/NYEU Központi Nyilvántartó (Central Registry; CR) országos hatáskörű nemzeti feladatokat.

Hivatkozások

- [1.]94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról
- [2.]33/2002. (HK 13.) HM utasítás az elektronikus információvédelemről
- [3.]Munk Sándor: A katonai informatika alapelvei a Magyar Honvédségben I. (alapok); Hadmérnök, IV. Évfolyam 3. szám, 2009, p. 333-340.
- [4.]2009. évi CLV. törvény a minősített adat védelméről

Kis László

lkis@iit.bme.hu

Lantos Béla

lantos@iit.bme.hu

SZENZORFÚZIÓ ALKALMAZÁSA BELTÉRI AUTONÓM NÉGYROTOROS HELIKOPTEREN

Absztrakt

A cikk egy beltéri repülésre alkalmas autonóm négyrotoros helikopter szenzor és aktuátor rendszerét mutatja be. A szenzor rendszer két különálló részből áll: az első egy inerciális mérőegység, a második egy külső látórendszer. A két rendszer közötti fúziót kiterjesztett Kalman-szűrők valósítják meg. Bemutatásra kerül az inerciális mérőegység kalibrációja különféle hibaforrásokot feltételezve. A szenzorhibák elemzéséből a mérési zajok statisztikája határozható meg, mely a Kalman-szűrőknél kerül felhasználásra. A helikopter beavatkozó szerveit négy kefe nélküli DC motor képezi. A cikk bemutatja a motorok alacsonyszintű fordulatszám szabályozásának tervezési lépéseit. Az állapotbecslés verifikációja valós körülmények között történt. A cikkben bemutatott rendszer egy jelenleg folyó projekt aktuális állapotát mutatja be, melynek végső célja több autonóm négyrotoros helikopter formációban haladásának irányítása.

This article presents the sensory and actuator system of an indoor autonomous quadrotor helicopter. The sensory system has two separate parts. The first is an inertial measurement unit, the second is an external vision system. The fusion between the two systems is solved by extended Kalman filters. The calibration for various types of error of the inertial measurement system is presented. From the analysis of the noises of sensors, correlation can be calculated which is used in the extended Kalman filters. The actuator system of the helicopter is four brushless DC motors. The design steps of the low level control of the motors are presented. Verifications of state estimation were done in real circumstances. The article presents the actual state of a recent project. The main goal is the formation control of a group of quadrotor helicopters.

Kulcsszavak: UAV, beltéri autonóm négyrotoros helikopter, szenzor rendszer, állapotbecslés, beavatkozó rendszer ~ UAV, indoor autonomous quadrotor helicopter, sensory system, state estimation, actuator system

Bevezetés

A kisméretű légi járművek irányítási lehetőségeinek vizsgálata régóta szerepel a tudományos kutatások célkitűzései között. A kisméretű repülőgépeknek szükségük van nagy terekre a felszálláshoz, repüléshez és leszálláshoz. A helikopterek viszont képesek helyből fel- és leszállni és egyhelyben lebegni. Ezen tulajdonságok lehetővé teszik, hogy beltérben alkalmazzuk őket. A helikoptereknek többféle lehetséges megoldása ismert. Ezek közül mechanikailag legegyszerűbb, legrobosztusabb felépítésű az ún. négyrotoros helikopter.

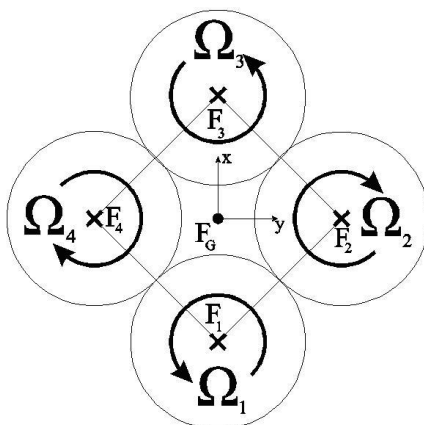
A négyrotoros helikopter koncepciója nem új keletű. Az első ilyen elrendezésű helikoptert 1907-ben készítette Jacques és Louis Breguet. A helikopter a gyors és instabil időállandói miatt nehezen volt irányítható, ezért a koncepció hosszú ideig feledésbe merült. A mai technológia lehetőséget ad elegendően gyors irányítási algoritmusok létrehozására, így az utóbbi időben számos ilyen irányú kutatás jelent meg. Az ezekről szóló leírások megtalálhatóak [1], [2], [3]-ban.

2006-ban a Budapesti Műszaki és Gazdaságtudományi Egyetem Irányítástechnika és Informatika Tanszéke és az MTA SZTAKI Rendszer és Irányításelméleti Kutatólaboratóriuma közös projektet indított, melynek célja egy beltéri autonóm működésre képes négyrotoros helikopter létrehozása. A projekt korábbi eredményei megtalálhatók [4],[5],[6]-ban.

A cikk felépítése a következő. A bevezető fejezet után a helikopter bemutatása következik. A harmadik fejezetben a gyorsulásmérő és szögsebességmérő kalibrációja kerül bemutatásra. A negyedik fejezet a képfeldolgozó rendszer ismertetését tartalmazza. Az ötödik fejezet rávilágít a szenzorok és az állapotbecslő kapcsolatára. A hatodik fejezet a beavatkozó szervekről szól. Végül a hetedik fejezet a tesztelés során kapott eredményeket mutatja be.

A helikopter bemutatása

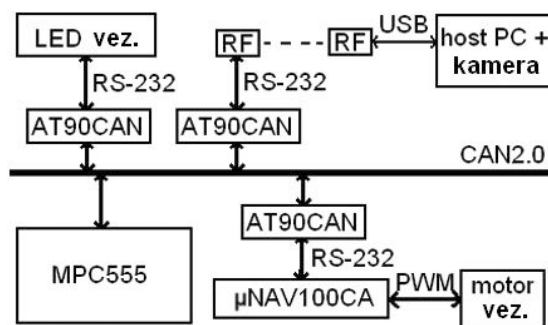
A négyrotoros helikopter működésének fizikai alapját a 1. ábra szemlélteti. Adott négy a helikopter síkjára merőleges tengelyű propeller egy négyzet négy csúcsában elhelyezve. Az egymás melletti propellerek forgásiránya egymással ellentétes, így azonos fordulatszám és felhajtóerő mellett a helikopteren keletkezett nyomatékok kiegyenlítik egymást.



1. ábra: A négyrotoros helikopter működésének fizikai alapja

A helikopter informatikai felépítése a 2. ábrán látható. A központi műveletvégző egység egy Freescale MPC555 típusú mikroszámítógép. Ez az egység futtatja az állapotbecsléshez,

pályaszámításhoz és szabályozáshoz szükséges algoritmusokat. A helikopter fedélzetén kapott helyet egy Crossbow mNAV100CA típusú inerciális mérőegység, melynek a gyorsulás- és szögsebességmérőjét használjuk. A teljes rendszer része egy külső kamera-alapú látórendszer, melynek az algoritmusai egy hoszt PC-n futnak. Ez a gép egy rádiófrekvenciás interfészen keresztül kommunikál a helikopterrel. A képfeldolgozó rendszer aktív markerek segítségével határozza meg a helikopter háromdimenziós pozícióját és orientációját. A markerek különböző színűek, a színeket RGB LED-ek állítják elő, ezért szükség van egy fedélzeti LED vezérlőre. A rendszer fő kommunikációs csatornája egy CAN busz. Azon egységeknél, melyeknél nincs beépített CAN interfész, Atmel AT90CAN128 mikrokontrollerek végzik az interfészek közötti fordítást.



2. ábra: A helikopter elvi felépítése

Az inerciális mérőegység

A helikopteren alkalmazott inerciális szenzorrendszer a Crossbow által gyártott mNAV100CA típusú mérőegység. A modult eredetileg kültéri kisméretű repülőknél alkalmazták. Ezért számos különféle önálló szenzort tartalmaz. Az inerciális mérőeszközök közül megtalálható rajta egy háromdimenziós gyorsulásmérő és egy háromdimenziós szögsebességmérő. További szenzorok: a háromdimenziós mágneses térerősségmérő, légnyomásmérő, légáramlásmérő és GPS.

A projekt során a helikopternek beltéri környezetben kell üzemelnie. Beltérben a mágneses térerősség iránya az épületek anyaga miatt erősen ingadozik, így a mágneses térerősségmérő nem alkalmazható. Az épületek árnyékolása miatt a GPS jele nem fogható. A légnyomásmérővel csupán néhány méteres pontossággal lehet a magasságot meghatározni, ami beltérben nem elegendő. A légáramlásmérő pedig a propellerek által keltett légáramlat miatt nem használható sebességmérésre.

A megmaradó szenzorok a gyorsulás- és szögsebességmérők. Az első vizsgálatok során kiderült, hogy a gyári beállítások mellett a mért adatok számos hibát tartalmaznak. Ezért egy kalibrációs folyamat került megvalósításra, melynek eredményeként a valós időben mért jelekből, különböző kompenzációk alkalmazásával a magasabb szintű szabályzás számára alkalmas adatok számíthatók.

Az egyes hibaforrások különféleképp osztályozhatók. Az állandó jellegű hibák kategóriába azok a hibaforrások tartoznak, melyek hosszabb időtartamon keresztül, esetleg a szenzor teljes élettartama alatt állandónak tekinthetők. Ilyen hibaforrások a gyorsulásmérő és szögsebességmérő esetén is a szenzorok tengelyi mérőlegességének hibája, a szenzorok

erősítéshibája és annak függése a hőmérséklettől. További állandó jellegű hiba a szögsebességmérő esetében, a különböző irányú gyorsulások által okozott ofszet hibák. Ezen hibaforrások mértékét elegendő egyszer, a szenzormodul felszerelése előtt kimérni és használat közben a mért értékek alapján végezni a kompenzációt.

A hibaforrások második kategóriája a változó jellegű hibák. Ezek a szenzor bekapcsolásakor ismeretlennek tekinthetők és a hibák nagyságának identifikálása után is legfeljebb a szenzor kikapcsolásig tekinthetők állandónak. A szögsebességmérő és gyorsulásmérő esetében ilyen hibák a tápfeszültség- és hőmérsékletfüggő ofszet hibák.

A harmadik kategória a repülés közben is változó hibaforrások. Ezek mindkét szenzor esetében ofszet jellegű hibának tekinthetők.

A hibaforrások osztályozására alapozva kétlépéses kalibráció került kidolgozásra. Az első lépés egy „offline” kalibráció. Ebben az esetben a szenzormodul nincs felszerelve a helikopterre. Lehetőség van a szenzor tetszőleges orientációba állítására és lehetséges hosszabb ideig tartó mérést végezni. Itt lehet meghatározni az állandó jellegű hibákat.

A második fázis az indítás előtti kalibráció. Ekkor a szenzor már a helikopter fedélzetére van szerelve, egyetlen orientációban lehet mérést végezni és csak rövid ideig tarthat a kalibrációs folyamat. Ekkor lehet kimérni a második kategóriába tartozó hibaforrásokat.

A repülés közben változó hibák mérésére nem készült kalibrációs folyamat, ezen hibaforrások meghatározása az állapotbecslés feladata.

A gyorsulásmérő kalibrációja

A gyorsulásmérő „offline” kalibrációja a következő elven alapul. Ha a szenzort egy alátámasztásra helyezzük és mozdulatlan állapotban mérünk, akkor a mért érték a gravitációs vektorral megegyező nagyságú és irányú vektor lesz. Mivel a gyorsulásmérő az értékeket G -ben adja vissza, így a mért érték egy egységvektor lesz. Ha a mérést megismétljük úgy, hogy a szenzort különböző orientációkba állítjuk, akkor a mért egységvektoroknak az egység sugarú, origó középpontú gömb felszínén kell mozognia. Ezek a megállapítások csak akkor igazak, ha a mért értékek nem tartalmazzak hibát. Figyelembe véve a gyorsulásmérő lehetséges hibáit, a bejárt felület egy tetszőleges helyzetű ellipszoidnak tekinthető. Egy ilyen ellipszoid leírható a következő egyenlettel:

$$[a_i^T \ 1]Q[a_i^T \ 1]^T = 0 \quad (1)$$

ahol a_i a mért háromdimenziós gyorsulásvektor és Q egy 4x4-es szimmetrikus, pozitív definit mátrix. A Q mátrixnak tíz független paramétere van. Kerüljenek ezek a paraméterek a p vektorba. Ekkor felírható a következő egyenlet:

$$a_{pi}^T p = 0 \quad (2)$$

ahol $a_{pi}^T = (a_x^2 \ a_y^2 \ a_z^2 \ a_x a_y \ a_x a_z \ a_y a_z \ a_x \ a_y \ a_z \ 1)$. A feladat a mérési adatok alapján a p vektor meghatározása. Mivel az egyenletnek a $p = 0$ triviális megoldása, ezért bevezetendő egy kényszer, mely szerint $p^T p = 1$. Ezt a kényszert betartva a probléma a „total least squares” módszerrel oldható meg.

A p vektor értékeiből a Q mátrix felépíthető. Ezután keressük azt a T transzformációt, mely az általános ellipszoidot az origó középpontú gömbbe transzformálja. Erre a T -re igaz:

$$Q = T^T T \quad (3)$$

Q -t értelmezzük a következő formában:

$$Q = \begin{bmatrix} M & v \\ v^T & c \end{bmatrix} \quad (4)$$

ahol, M egy 3x3-as szimmetrikus mátrix, v egy 3 elemű oszlopvektor és c skalár. Keressük T -t a következő formában:

$$T = \begin{bmatrix} N & -Np_e \\ 0^T & 1 \end{bmatrix} \quad (5)$$

ahol N ortogonális, p_e pedig az origóból az ellipszis középpontjába mutató helyvektor. Belátható, hogy (3) teljesüléséhez $M = N^T N$ teljesülése szükséges, mely probléma megoldható M sajátérték, sajátvektor felbontásával. Ekkor $p_e = -M^{-1}v$, mellyel megkaptuk a T mátrix összes elemét.

T mátrix N részmátrixa ortogonális, ami azt jelenti, hogy felbontható egy ortonormált $\tilde{N}$ ($\tilde{N}^{-1} = \tilde{N}^T$) és egy diagonális S mátrixra. Ekkor az S mátrix tartalmazza a gyorsulásmérő erősítéshibáját. Ez a hibaforrás hőmérsékletfüggő, azonban leírható egy lineáris összefüggéssel, és ezen összefüggés együtthatói állandónak tekinthetők.

Ha az eddig leírt kalibrációs algoritmust több hőmérsékleten elvégezzük és az S mátrix értékeit kiszámítjuk, a diagonális elemekre a legkisebb négyzetes hibák algoritmusával egy lineáris összefüggés illeszthető a következő módon:

$$\begin{bmatrix} s_x & s_y & s_z \end{bmatrix}^T = t_{pill} \begin{bmatrix} s_{mx} & s_{my} & s_{mz} \end{bmatrix} + \begin{bmatrix} s_{bx} & s_{by} & s_{bz} \end{bmatrix} \quad (6)$$

ahol s_x, s_y, s_z S diagonális elemei, t_{pill} az aktuális hőmérséklet és a többi változó a lineáris összefüggés konstansai. A (6) összefüggés alapján tetszőleges hőmérsékleten meghatározható az S mátrix.

A T mátrix a Q -val adott ellipszoidot transzformálja az origó középpontú egységgömbbe. Ez a gömb viszont forgatás invariáns, ezért a T transzformáció a mérési adatokat egy olyan koordináta-rendszerbe transzformálja, melynek a szenzorhoz képesti orientációja ismeretlen. Megtehető, hogy a szenzort olyan orientációba állítjuk, melyben a gravitációs vektor egy általunk kívánt koordináta-rendszer tengelyei irányába mutat. Az itt mért és transzformált adatokból felírható egy E ortonormált mátrix, mely minden mért és transzformált gyorsulást a kívánt koordináta-rendszerbe transzformál.

Ezek után a gyorsulásmérő kalibrációs folyamata a következő:

$$\begin{bmatrix} a_{kal} \\ 1 \end{bmatrix} = E \begin{bmatrix} \tilde{N}S & -\tilde{N}Sp_e \\ 0^T & 1 \end{bmatrix} \begin{bmatrix} a_{mért} \\ 1 \end{bmatrix} \quad (7)$$

A további levezetésekhez legyen:

$$T_s = E \begin{bmatrix} \tilde{N} & -\tilde{N}p_e \\ 0^T & 1 \end{bmatrix} \quad (8)$$

A szögsebességmérő kalibrációja

A szögsebességmérő kalibrációja két lépésből áll. Az első lépésben a szenzor statikus helyzetben áll és különböző orientációkban mérünk. Itt határozható meg a gyorsulás hatása a szögsebességmérőre. A második lépésben a szenzor elmozdulásából lehet következtetni az erősítéshibára.

Statikus állapotban a szenzor által mért adatra a következő egyenlet igaz:

$$\omega_{mért} = \omega_{valós} + \omega_{ofszet} + K^T a_{kal} \quad (9)$$

Az ω változók a megfelelő szögsebesség értékek, az a_{kal} pedig az előző fejezetben számolt kalibrált gyorsulás. Statikus helyzetben $\omega_{valós} = 0$ feltételezhető. A K 3x3 mátrix és a 3x1-es ω_{ofszet} elegendő számú (minimum 4db), különböző orientációban végzett mérésből a legkisebb négyzetes hibák módszerével számítható.

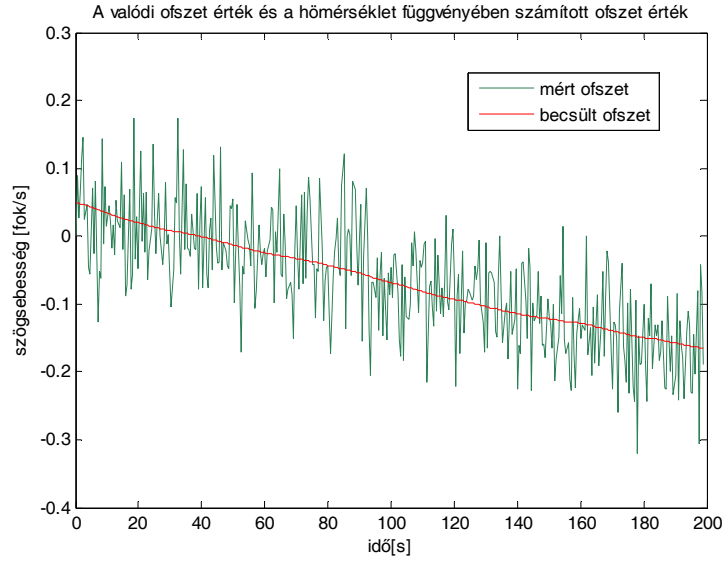
Az így keletkező szögsebességet át kell transzformálni abba a koordinátarendszerbe, melyben a kalibrált gyorsulások értelmezettek. Legyen a Γ T_s mátrix bal felső 3x3-as részmátrixa. A kalibráció második lépése számára legyen az átranszformált szögsebesség:

$$\tilde{\omega} = \Gamma(\omega_{mért} - \omega_{ofszet} - K^T a_{kal}) \quad (10)$$

A szögsebességmérő esetében az ofszet hiba tekinthető hőmérsékletfüggőnek, amelynek alakja

$$\omega_{ofszet} = t_{aktuális} \circ s_{\omega,m} + s_{\omega,b} \quad (11)$$

ahol $t_{aktuális}$ egy 3x1-es vektor, mely a három szögsebességmérő beépített hőmérsékletszenzorának az adatait tartalmazza. $s_{\omega,m}$ és $s_{\omega,b}$ a lineáris összefüggés 3x1-es vektorkonstansai, a $\circ$ szorzás a vektorok elemenkénti szorzását jelenti. Megfelelő számú hőmérsékleti értéken elvégezve a mérést, a konstansok a legkisebb négyzetes hiba módszerével meghatározhatóak. A 3. ábrán egy változó hőmérsékletű környezetben mért valódi és a hőmérséklet értékek alapján becsült ofszet látható.



3. ábra: Hőmérséklettől függő ofszet változása és a becsült ofszet értéke

A második lépésben tengelyenként határozható meg a szögsebességmérő erősítéshibája. Statikus helyzetből indítva a szenzort, forgassuk azt el a mérendő tengely körül, majd helyezzük újra statikus helyzetbe. A két statikus helyzetben számítható a kalibrált gyorsulás vektor. Ezen két vektor által bezárt szög adja az elforgatás szögét (pl. az X tengely esetében φ_{gyors}). Megjegyzendő, hogy a módszer akkor működik, ha a forgatás tengelye a gravitáció irányára merőleges síkban van. A forgatás közben rögzíthetők a mért szögsebesség értékek és (10) alapján transzformálhatók. A szögsebességmérő adataiból is meghatározható az elfordulás, az X tengely esetében pl:

$$\varphi_{szögseb} = \sum_i \tilde{\omega}_{xi} \Delta t \quad (12)$$

A két elfordulás arányából meghatározható a szögsebességmérő erősítéshibája:

$$s_{\varphi} = \frac{\varphi_{gyors}}{\varphi_{szögseb}} \quad (13)$$

A kalibrált szögsebesség a következő képlettel számítható:

$$\omega_{kal} = \text{diag}(s_{\varphi}, s_g, s_{\psi}) \tilde{\omega} \quad (14)$$

ahol ω_{ofszet} az aktuális hőmérséklet alapján számítható (11) szerint.

Indítás előtti kalibráció

Az eddigi kalibrációs folyamat után megmaradt hibák tekinthetők ofszet hibának. Az indítás előtti kalibrációs folyamat során összesen egy orientációban lehet mérni. A helikopter magasabb szintű irányításai számára fontos, hogy a helikopter vízszintes helyzetből induljon. Ezt felhasználva indulás előtt a szögsebesség értéke 0 és a gyorsulás értéke a $(0 \ 0 \ -1)^T$ vektor.

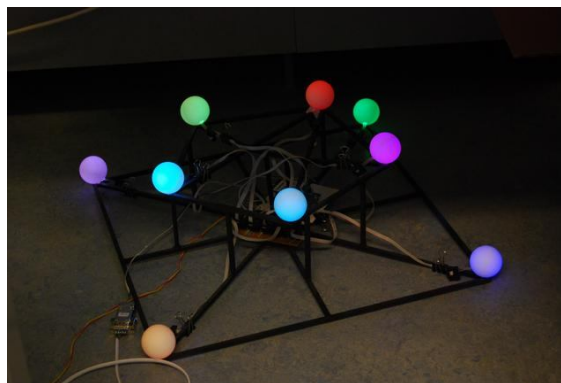
A kalibrációs lépés folyamata a következő: A gyorsulásmérővel és szögsebességmérővel rögzítendő egy néhány másodperces regisztrátum. Ezeken el kell végezni a korábban bemutatott kalibrációs folyamatokat, majd képezni kell a mérési értékek átlagát. Az átlagnak az eltérése a feltételezett értékektől fogja adni az ofszet értéket. Ezt az ofszet értéket a repülés során minden kalibrált értékből le kell vonni.

3D látórendszer

A beltéri repülés során a helikopter pozícióját és orientációját egy külső számítógépen futó képfeldolgozó algoritmus szolgáltatja. A látórendszer működésének alapja a mozgássztereoó elvén alapszik.

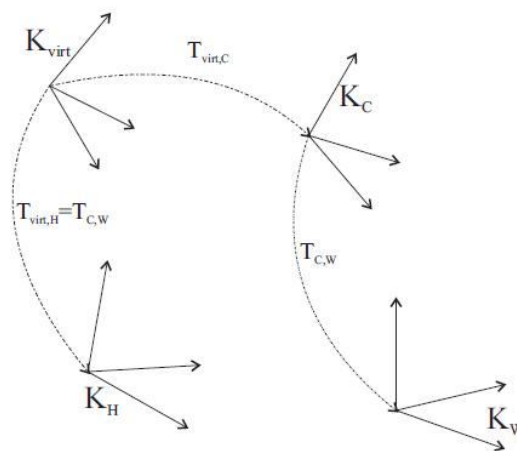
A rendszer központi része az ún. 7 pontos algoritmus [7]. Ez képes két kamera koordináta rendszere közti transzformációt megadni a kamerák képei alapján, amennyiben azokon azonosítható legalább 7 db összetartozó pontpár.

Ahhoz, hogy a pontárok könnyen meghatározhatóak legyenek, a helikopteren elhelyezésre került 9 db aktív marker. Elrendezésük olyan, hogy bármely irányból nézve a helikopter legfeljebb két markert takar ki. A 4. ábrán a kamera által készített kép látható.



4. ábra: A kamerák által látott kép

A képfeldolgozásnál használt koordinátarendszerek az 5. ábrán láthatóak.



5. ábra: A képfeldolgozó rendszerben használt koordinátarendszerek

A K_W keret a világkoordináta-rendszer, K_C az első kamera koordinátarendszere. Ennek a pozíciója és orientációja a világkoordináta-rendszerben nem változik, így $T_{C,W}$ állandónak tekinthető. K_H a helikopter koordinátarendszere. K_{virt} a második kamera koordinátarendszere. A második kamerát tekintjük a világkoordináta-rendszerben mozgó kamerának, mégpedig úgy, hogy K_{virt} és K_H relatív pozíciója és orientációja ne változzon, vagyis $T_{virt,H}$ állandó. A képfeldolgozás folyamata ezek után a következő. A két kamera képén fel kell ismerni a markereket, majd a $T_{virt,C}$ transzformációt a 7 pontos algoritmus kiszámítja.

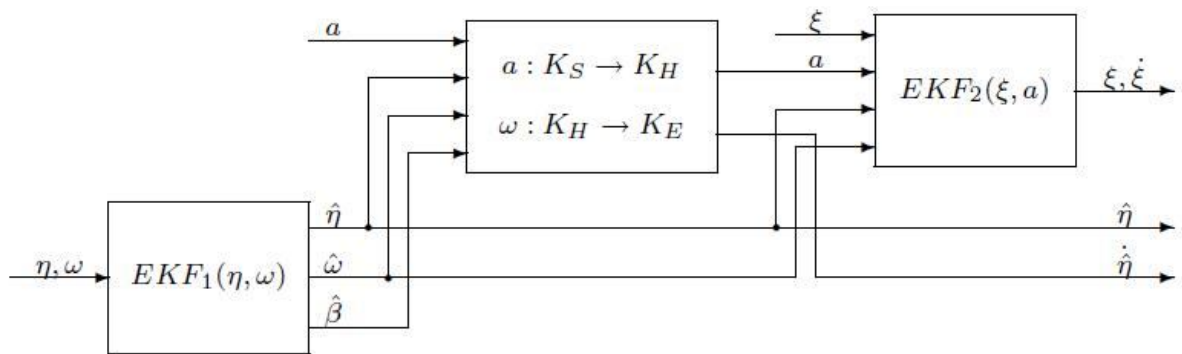
Mivel $T_{virt,H}$ állandó, ezért K_{virt} koordináta rendszerhez kötött kamera képén a markerek pozíciója is állandó. Ezért ez a kamera egy virtuális képpel helyettesíthető (innen a koordináta rendszer elnevezése). Ezt a virtuális képet a kezdeti inicializálás alatt az első kamerával rögzítjük. Ha a világkoordináta-rendszert úgy definiáljuk, hogy az inicializálás alatt megegyezik a helikopter koordináta rendszerével, akkor a $T_{virt,H} = T_{C,W}$ összefüggés igaz lesz. Ezek alapján a helikopter aktuális helyzetét és orientációját a

$$T_{W,H} = (T_{C,W})^{-1} (T_{virt,C})^{-1} T_{C,W} \quad (15)$$

transzformáció tartalmazza. Megjegyzendő, hogy a képfeldolgozás sebessége jelenleg nem elegendően gyors a magasszintű irányítás megvalósításához, ezért van szükség az inerciális szenzor használatára.

Állapotbecslés

Az érzékelés a magasabb szintű irányításokkal az állapotbecslőn keresztül áll kapcsolatban. Az állapotbecslő felépítése a 6. ábrán látható. Az állapotbecslés két lépésben, kiterjesztett Kalman-szűrőkkel történik. Az első blokk (EKF_1) a mért és kalibrált orientáció és szögsebesség alapján számít egy becsült orientációt, szögsebességet és szöggyorsulást. Ezen információk alapján a megfelelő koordináta transzformációk elvégezhetők. A második lépésben szintén egy kiterjesztett Kalman-szűrő (EKF_2) szerepel, mely a mért pozíció és transzformált gyorsulás alapján számítja ki a helikopter becsült pozícióját és sebességét.



6. ábra: Az állapotbecslő elvi felépítése

A Kalman-szűrők belső állapotként tartalmazzák a szögsebesség és gyorsulás szenzorok ofszet értékeit, melyek akár a repülés során is változhatnak. Ezt a változást a szűrők a képfeldolgozás adatai alapján tudják észlelni és pontosítani.

A kiterjesztett Kalman-szűrők állapotegyenletekkel írhatók le [5]. A belső állapotok az első szűrő esetében az orientáció állapota és a szögsebesség ofszet értéke. A második szűrőnél ezek a pozíció és sebesség állapotok és a gyorsulás ofszet értéke. A helyes működéshez szükséges az állapotok kezdőértékeinek helyes beállítása. Mivel a helikoptert a képfeldolgozásnál bemutatott módon a világkoordináta-rendszer origójából indítjuk és az indítás előtti kalibrációval az ofszet értékeket is kinullázzuk, így minden állapotot 0-ból kell indítani.

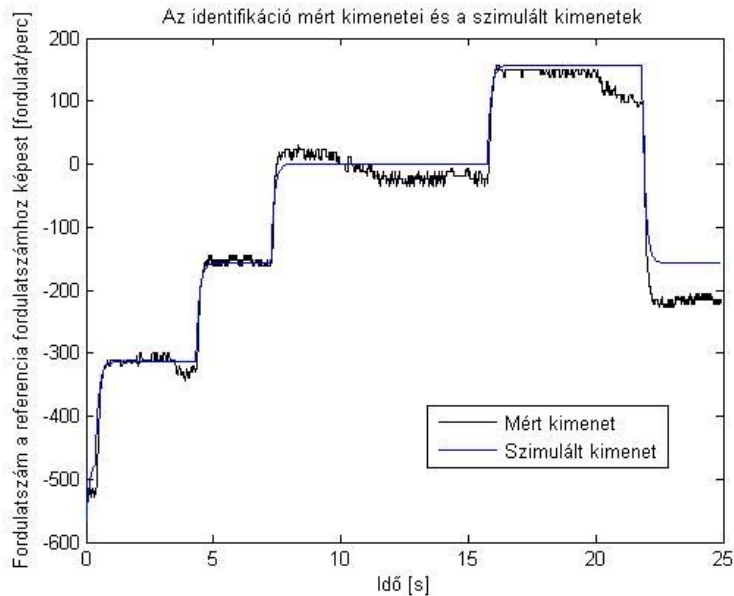
A kiterjesztett Kalman-szűrők azért képesek más állapotbecslésnél pontosabb értéket adni, mert figyelembe veszik a szenzor zajokat. Ezeket korrelációs mátrixokkal írják le, melyeket szintén inicializálni kell. Az indítás előtti kalibráció során rögzítésre kerül egy néhány másodperces regisztrátum, melyből ha levonjuk az ofszet értéket, csak zajt fog tartalmazni. Ezen a zajon végezhető variancia analízis, mellyel megadhatóak a zajok kezdeti korrelációs mátrixai.

Beavatkozó szervek: motorvezérlés

A beavatkozó szervek a helikopter fedélzetén elhelyezett négy darab rotor, melyeket háromfázisú BLDC motorok forgatnak. A magasabb szintű irányítás a motorok elvárt fordulatszámát számítja ki. Szükség van egy alacsony szintű mechanizmusra, mely biztosítja, hogy a motorok az előírt fordulatszámon forogjanak.

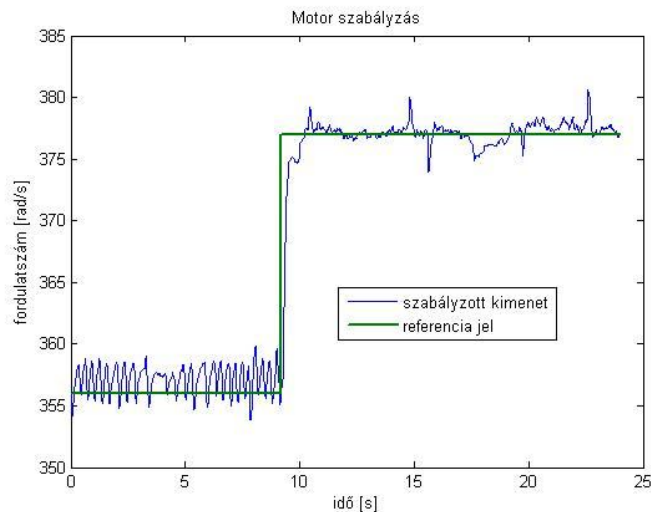
Ennek megvalósítására minden motor mellé beépítésre került egy optikai fordulatszám-mérő, valamint egy kereskedelmi forgalomban megvásárolható Dualsky gyártmányú teljesítményelektronika. Az így összeszerelt rendszer a propeller nemlineáris tulajdonságai és a teljesítményelektronika ismeretlen volta miatt egy „fekete doboznak” tekinthető.

A szabályzás megvalósításához elkészült ennek a rendszernek egy lineáris modellel történő identifikálása. 7. ábrán a linearizált modell és az eredeti rendszer válasza látható ugyanarra a bemenő jelre. A lineáris modell ebben az esetben elsőrendű. Azonban a magasabb rendű modellek sem adtak meggyőzően jobb eredményt. A rendszer tipikus hibái is leolvashatók a 7. ábráról. Látható, hogy a statikus szakaszokon a valós rendszer fordulatszáma nem állandó. Az is látható, hogy ha a bemenetnek egy adott értékét a bemenet növelésével, vagy csökkentésével érjük el a valódi rendszer két különböző fordulatszámra áll be.



7. ábra: Az eredeti és az identifikált modell viselkedése ugyanarra a bemenetre

Az identifikációnál tapasztalt jelenségek alapján és az egyszerűség megtartása érdekében a motorszabályozást egy PI szabályozó végzi. A szabályozott rendszer referencia jelét és kimenetét mutatja a 8. ábra. A megmaradt tipikus hibák jól láthatók ezen az ábrán. Abban az esetben, ha a rendszer elhagyja a linearizálásnál használt munkapontot, a nemlineáris hatások miatt oszcilláció lép fel. Ezen kívül még a munkapont körüli fordulatszámnál is vannak tüskék a jelben, melyet az ismeretlen teljesítményelektronika okoz. Ezeknek a hibáknak a nagyságrendje akkora, hogy a magasabb szintű szabályozások még képesek a helikopter irányítására.



8. ábra: A szabályozott motor viselkedése

A szabályozóval kapcsolatban megjegyzendő, hogy az integráló hatás miatt szükség van biztonsági protokollok alkalmazására. Kritikus pontja a rendszernek az optikai fordulatszám-mérő. Beépítésre került egy mechanizmus, mely abban az esetben, ha egy már forgó motor fordulatszámát 0-nak érzékeljük (vagyis tönkremegy a fordulatszám-mérő), lekapcsolja a szabályozást és a fordulatot egy előre beállított értékre vezérli. Ezen biztonsági

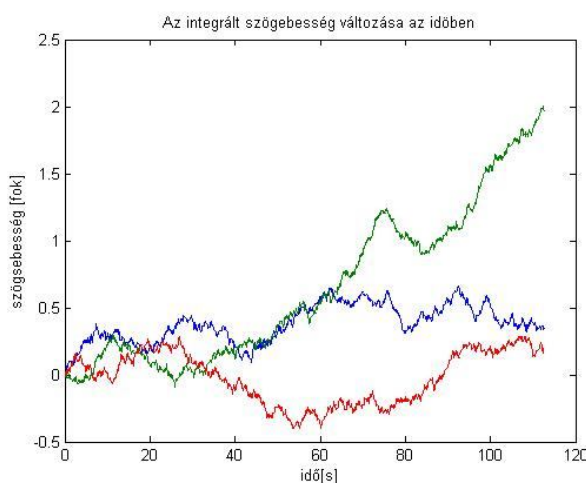
intézkedés nélkül az integrátor ilyen esetben folyamatosan növelné a motor fordulatszámát, ami megjósolhatatlan viselkedést eredményezne.

Eredmények

Kalibrációs eredmények

A gyorsulásmérő kalibrációja előtt a statikus helyzetben mért gravitációs vektor hossza 0.87G és 1.12G között változott. A gyorsulásmérő kalibrációját 18 különböző orientációra alapozva végeztük, melyek az egységgömb felületén egyenletesen voltak elosztva. Minden mérés során 50db regisztrátumnak az átlagát tekintettük egy mérési adatnak. A kalibráció után a különböző orientációkban mért gyorsulásvektorok hossza a [0.98 1.02]G tartományon belülre került. Ez az eredmény a regisztrátumok hosszának növelésével tovább javítható. Ezen kívül ha tudjuk, hogy a szenzort többnyire egy kis orientációs tartományban használjuk (pl. vízszintes helyzet környékén), akkor lehetséges, hogy a kalibrációnál használt orientációkat ebben a tartományban vegyük fel. Ezzel elérhető, hogy ebben a tartományban a szenzor pontossága nagyobb lesz.

A szögsebességmérő értékei a kalibráció előtt statikus helyzetben különböző orientációkban $\pm 2.5^\circ/s$ között mozogtak. A különböző irányú gyorsulásokat figyelembe véve ez az érték a $\pm 0.5^\circ/s$ -os tartományba került kalibrálás után. Az ebben a tartományban mért értékek már tekinthetők 0 középpontú fehérzajnak. Ezt demonstrálandó egy egyszerű orientációbecslést valósítottunk meg, pusztán a szögsebességmérő adatainak numerikus integrálásával. Egy körülbelül két perces futási eredmény látható a 9. ábrán.



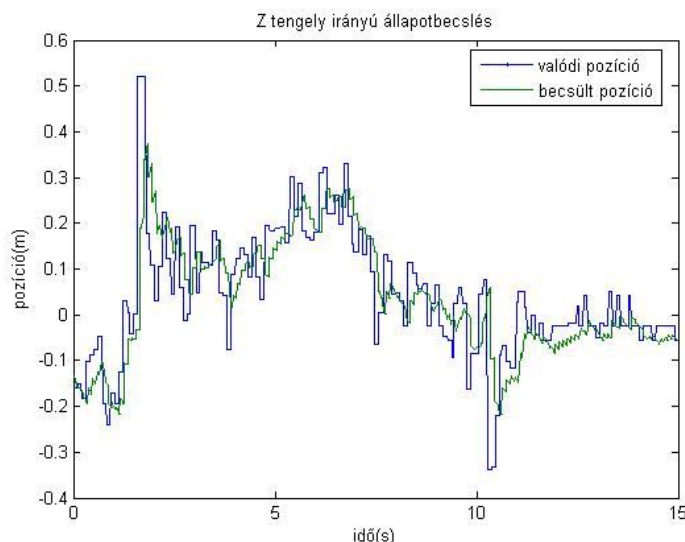
9. ábra: Az integrált szögsebesség változása az idő függvényében

A 9. ábrán megadott grafikon statikus helyzetben készült. Látható, hogy az akkumulálódott hiba két perc után körülbelül 2° . Visszafelé végezve a számításokat azt kapjuk, hogy a valódi ofszet és a becsült ofszet értéke nem különbözhet jobban, mint $0.0167^\circ/s$, ami nagyságrendileg a szenzor kvantálási szintjének kétszeresével egyezik meg.

Ez az eredmény mutatja, hogy a kamerás képfeldolgozás hibája esetén (kitakarás, stb.) pusztán a szögsebességmérő integrálása alapján elegendő idő van egy veszleszállás megvalósítására.

Az állapotbecslés eredménye

Az állapotbecslő megfelelő inicializálása után a helikopter mozgása közben végzett állapotbecslés eredménye a 10. ábrán látható.



10 ábra: A becsült és a valódi magasság a helikopter mozgása során

A helikopter valódi pozícióját a képfeldolgozás mérte. A 10. ábráról leolvasható, hogy az állapotbecslés értéke követi a valódi értéket. Az is látható, hogy a képfeldolgozás adatai jóval lassabbak, mint az állapotbecslés adatai. Az állapotbecslés az inerciális szenzorok adatai alapján képes a becsült állapotot két képfeldolgozási adat között is a jó irányba mozdítani.

Összegzés

A bemutatott eredmények alapján megállapítható, hogy az inerciális szenzorok, az ismertett kalibrációs algoritmusok alkalmazása mellett, kiegészítve a kamerás képfeldolgozó rendszerrel együttesen képes adatokat szolgáltatni az állapotbecslés számára. Ezek az adatok elegendően pontosak ahhoz, hogy az állapotbecslő kimenetén megfelelő sebességgel rendelkezésre álljon pozíció, sebesség, orientáció és szögsebesség információ a magasabb szintű irányítások számára.

A beavatkozó szervek irányításáról a kísérleti eredmények igazolták, hogy elegendő sebességgel és megfelelő pontossággal képes követni a magasabb szintű irányítások által számított alapjeleket.

A projekt folytatásának következő lépése az első összetettebb repülések megvalósítása. A tervek között szerepel számos magasabb szintű irányítás kipróbálása. A kutatás végső célja egy több egyedből álló helikopterraj formációban való haladásának megvalósítása.

Köszönetnyilvánítás

A bemutatott kutatás az Országos Tudományos Kutatási Alapprogramok OTKA K 71762 számú támogatásával készült.

Irodalomjegyzék

- [1] S. Boudallah, R.Siegwart: Backstepping and Sliding –mode Techniques Applied to an Indoor Micro Quadrotor. IEEE International Conference on Robotics and Automation 2005
- [2] G. Hoffmann, D.G.Rajnarayan, S.L. Waslander, D.Dostal, J. S. Jang, C. J. Tomlin: The Stanford Testbed of Autonomous Rotorcraft for Multi Agent Control (Starmac). Digital Avionics Systems Conference 2004
- [3] P. Pounds, R. Mahony, P.Hynes, J. Roberts: Design of a Four-Rotor Aerial Robot, Australian Conference on Robotics and Automation 2002
- [4] Soumelidis A., Gaspar P., Bauer P., Lantos B., Prohaszka Z.: Design o fan Embedded Microcomputer Based Mini Quadrotor UAV, European Control Conference 2007
- [5] Kis L., Regula G., Lantos B.: Design and Hardware-in-the-Loop Test of the Embedded Control System of an Indoor Quadrotor Helicopter. 6th Workshop of Intelligent Embedded Systems 2008
- [6] Kis L., Prohaszka Z., Regula G.: Calibration and Testing Issues of the Vision, Inertial Measurement and Control System of an Autonomous Indoor Quadrotor Helicopter. 17th International Workshop on Robotics in Alpe-Adria-Danube Region 2008
- [7] Hartley R. I., Zisserman A.: Multiple View Geometry in Computer Vision, Cambridge University Press, 2003

Koleszár Béla

koleszar@tele2.at

A FÖLDI ROBOTTECHNIKAI ESZKÖZÖK INFORMATIKAI RÉSZEGYSÉGEIVEL SZEMBEN TÁMASZTOTT SPECIÁLIS (TEREPI KIVITELT IGÉNYLŐ) KÖVETELMÉNYEK RENDSZEREZÉSE, ELEMZÉSE

Absztrakt

Egy fontos informatikai részegység kiesése/hibás működése megbéníthatja a robotot, veszélyeztetve ezzel a bevetés sikerét, biztonságát. Az autonóm robotok informatikai részegységeinek hibái, illetve hibásan kiértékelt információik az egyik legkomolyabb biztonsági veszélyforrást jelentik, hiszen nincs senki, aki ezeket a hibákat korrigálná.

A cikk fő kérdései: a földi robottechnikai eszközök sajátosságai, működésmódjai, a szárazföldi robotjárművekre és érzékelőikre leselkedő veszélyek felsorolása, az informatikai részegységeikkel szemben támasztott speciális (terepi kivitelű igénylő) követelmények rendszerezése, elemzése és az autonóm, a távirányított, illetve humán sofőrrel is vezethető robotok informatikai egységeivel szemben támasztott követelmények különbözőségei.

Failure or faulty function of informatics subunits can paralyze the robot, putting the overall goal at risk of deployment-success and safety. Informatics subunit-failures or incorrect evaluated information connote one of the primary security risks in the robots, because nobody is there, who can rectify the errors.

The main questions of this paper: properties and operating states of unmanned ground vehicles, particulars of the risks the unmanned ground vehicles and their sensors, the array and analyze of special requirements (field design) of informatics subunits and differentness of informatics subunits- requirements from autonomous, remote- controlled robots and robots with human driver.

Kulcsszavak: szárazföldi robot, informatikai részegységek, terepi kivitel, speciális követelmények rendszerezése ~ unmanned ground vehicle, informatics subunits, field design, the array of special requirements

Bevezetés

Egyre terjed a legkülönbözőbb rendszerek távolról történő, illetve autonóm vezérlése/irányítása. A távirányítható televíziók, autózárak, kertkapuk, garázsajtók, klímaberendezések, játékok, stb. mindennapossá váltak. Az iparban (pl. daruk), közlekedésben (közlekedési lámpák, vasúti váltók, sorompók, lámpák, stb.) szintén egyre gyakrabban találkozunk a távirányítással. A teljesen autonóm robotok elterjedése még nem ilyen tömeges, de a fejlődés itt is megállíthatatlan.

Logisztikai feladatokra két módon használják a robotokat: vagy emberek előtt zárt térben (pl. raktárakban), illetve emberek között (pl. kórházakban) óvatos, mindenre figyelő, „lassú, de biztos” üzemmódban. A háztartásban, a ház körüli munkák elvégzésére is egyre több robotot fejlesztenek ki, ezek között vannak autonómok is, mint például a medencetisztító, porszívó-, ill. a fűnyíró robotok. A vezető nélküli, síneken közlekedő szerelvények nem számítanak újdonságnak, a legújabban már leszállni is képes robotpilóták használata is közismert. Az emberek útját keresztező, nagyméretű, gyors, tehát nagy károkozó képességű, teljesen autonóm robotok ideje napjainkban még nem jött el. A robotok miatti problémák, az általuk esetelegesen okozott balesetek, veszteségek kérdésében úgy a civil, mint a katonai alkalmazók köre egyelőre aránylag kevés megértést mutat. Mindezt talán a vonat-, motoros-, ill. a légiközlekedés „hőskorában” fellépő ellenérzésekhez lehetne hasonlítani. A robotok informatikai részegységeinek hibái, illetve hibásan kiértékelt információik az egyik legkomolyabb biztonsági veszélyforrást jelentik, hiszen az autonóm robotnál nincs senki, aki ezeket a hibákat korrigálná. A katonai felhasználásnál természetesnek tekinthető terepi követelmények mellett megkülönböztetett figyelemmel kell e részegységeket kiválasztani, beépíteni és tesztelni, a lehető legkülönbözőbb feltételek mellett.

Cikkemben a harcjárművekkel szemben támasztott általános követelményekből kiindulva vizsgálom meg, rendszerezem az informatikai egységeikkel szemben támasztott követelményeket. Megvizsgálom a földi robottechnikai eszközök sajátosságait, működésmódjait, rámutatok a csak autonóm, a csak távirányított, illetve humán sofőrrel is vezethető robotok informatikai egységeivel szemben támasztott követelmények különbözőségeire. Végül a Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola doktoranduszaként kidolgozandó témám (*"Földi robottechnikai eszközök konstrukciós és alkalmazási kérdései, különös tekintettel a békefenntartó missziók biztonságának növelésére."*) első felére fókuszálva megvizsgálom a földi robotjárművek informatikai egységeivel szemben támasztott speciális követelményeket. Gyakorlati beállítottságuként, több mint 10 éves harcjárműtervezői gyakorlattal (Steyr - Pandur [1]) inkább a felhasználói oldalról közelítem meg a témát.

1. Harcjárművekkel és informatikai részegységeikkel szemben támasztott általános követelmények

A harcjárművek informatikai részegységei sokkal nagyobb igénybevételnek vannak kitéve, mint a civil rendszerek. A velük szemben támasztott minél kisebb meghibásodási arány szintén nagyon fontos kritérium.

Mivel az informatikai részegységek elévülési ideje nagyságrendekkel alatta van a járművek tervezett élettartamánál (kb. 40 év) [2], itt az informatika rohamos fejlődése által diktált rövidebb élettartam miatt inkább az egyszerű cserélhetőségre-bővíthetőségre, javíthatóságra kell helyezni a hangsúlyt.

Sok gyártó a költségek csökkentése érdekében a harcjárműveknél is megpróbálják a tömeg-autógyártás területéről felhasználni az egyes alkatrészeket, részegységeket. Ez például a kapcsolóknál, különböző lámpáknál, érzékelőknél, kameráknál, kijelzőknél, nyílászáróknál, tömítéseknél, kábeleknél, csatlakozóknál, a fűtés, szellőztetés részeinél figyelhető meg. Az

eredmény a legtöbbször kétséges, a csökkenő élettartam ugyan cserékkel orvosolható (még így is olcsóbb!), a kisebb megbízhatóság azonban nagy hiba!

Egy kitűnő kondícióban lévő, edzett katona hatalmas erő kifejtésére képes. Ha ezt az erőt a stressz miatt nem eléggé koordináltan használja, akkor bizony a „civil” alkatrészek egykettőre a kezében maradnak... Mindez akár a bevetés döntő szakaszában! Teljes felszereléssel (hátizsák, fegyver, védőruházat, golyóálló védőmellény, ~120 kg) csak egy hirtelen fordulattal is komolyan veszélyeztetni a nem eléggé védett részeket. Ezért is nagyon fontos, hogy a katonák a járművekben többpontos biztonsági övvel legyenek bekötve, a málháik, fegyvereik is megfelelően rögzítve legyenek. A nehéz terepen menet közben fellépő, állandóan változó (pozitív és negatív) gyorsulások komoly erőket jelentenek. Fontos biztonsági szempont az is, hogy az aránylag gyakori „könnyebb” baleseteknél (pl. árokba csúszás, terepakadályon való elakadás, oszlopmenetben történő ráfutás, gyalogsági akna robbanása, stb.) során fellépő gyorsulások sem okozhatnak olyan deformációkat, amelyek a katonák életét, egészségét veszélyeztetnék. Főleg a terepjárók elejének, aljának kell masszívnak lennie, de például a járművek tetejére szerelt berendezéseknél, alkatrészeknél is fontos a „taposás-állóság”.

Visszatérve a harcjárművek informatikai részegységeihez: rájuk a fentiek szintén érvényesek. A robosztus kivitel mellett védeni kell a mechanikus külső behatások ellen is. Használaton kívül, ha lehetséges, akkor javallott a további mechanikus védelem (lehajtható fedél, szállítóhelyzetbe történő billentés, betolható fiók, stb.) A kapcsolók, nyomógombok, billentyűzetek kivitele lehetővé kell tegye a kesztyűben való használatot is. Az áttekinthetőség is fontos, hogy álcafénynél, vagy akár sötétben, illetve nem oda nézve, csak tapintással egyértelműen azonosíthatóak legyenek. Nagy kihívást jelentenek a járművön kívül használt monitorok. Például a megemelt menethelyzetben, amikor a járművezető feje a szabadban van, akkor szüksége van legalább egy kisebb „műszerfalra”, ahol a fontosabb adatokat (sebesség, motorfordulat, hűtővíz-, olaj hőmérséklete, stb.) állandóan figyelemmel kísérheti. A kevésbé fontosakat is nyomógombok segítségével lekérdezheti, ill. a hibajelzések is itt jelennek meg automatikusan. Ennek a képernyőnek a biztonságos, vakításmentes olvashatósága a teljes sötétségtől kezdve a tűző napfényig, esőben, porban, különböző látószögek mellett bizony még mindig problémás.

Az informatikai egységek működésével szemben támasztott követelmények meghatározása nagy körütekintést igényel. A feleslegesen túlzott elvárások megfizethetetlen költségeket eredményeznek. Például a NATO szabvány szerint a legszélsőségesebb klimatikus zónák hőmérsékletei -57°C és $+71^{\circ}\text{C}$ között vannak [3]. Nem célszerű a harcjármű minden egyes alkatrészére megkövetelni az általánosan megadott $(-40) -35 \dots +50 \dots 60 \dots 63 \dots (80)^{\circ}\text{C}$ -os működési tartományt [4,5,6], ráadásul felfutási idő nélkül... Természetesen minden alkatrésznek tartósan állnia kell a megkövetelt szélsőségesebb hőmérséklettartományt, de a működőképességnél már „kedvezményeket” engedhetünk. Nagyon kicsi a valószínűsége annak, (részben lehetetlen) hogy a személyzet ilyen extrém belső hőmérsékletnél végezzen szerteágazó, hosszantartó, bonyolult feladatokat. A központi egységhez képest a perifériák szükség szerint csökkentett funkciókkal is rendelkezhetnek. Fontos még az energiaforrások kapacitása, minimális töltési ideje, illetve magasabb hőmérsékleteknél a rendszerek megfelelő hűtése, alacsony hőmérsékleteknél a fűtése, védettségi osztály (IP¹ [7]), rendszerben tarthatósági idő. Az elektronikai védelem, az elektromágneses impulzus bombák és nagy energiájú rádiófrekvenciás sugárforrások ellen árnyékolást sem szabad elhanyagolni. Itt a hagyományos, páncéllemezekből készült zárt járműszerkezetek Faraday kalitkaként működnek. Ha műanyagokat, kompozitokat használunk, akkor a belső informatikai egységek elektronikai védelmével külön kell foglalkoznunk.

¹ IP (Ingress Protection)

Újabban a szárazföldi harcjárműveknél is az informatikai hálózatot több, egymással együttműködő csomópontból irányítják, így kisebb a teljes kiesésnek a valószínűsége.

A harcjárművek passzív ballisztikai védelmét tovább már nem nagyon lehet emelni (súly, szállíthatóság, költségek, stb.), ezért egyre több aktív, SLID², „hard kill” [8] védelmi rendszert (pl. Arena [9], Drozd [10,11], Trophy [12], Iron Fist [13], stb.) állítanak hadrendbe. Ezeknél főleg az informatikai rendszerek gyorsasága fontos, hiszen pl. a közelről kilőtt páncéltörő rakétát érzékelni, értékelni, bemérni, időben hatástalanítani kell.

A fegyver-védelem, fegyver-ellenfegyver ösidők óta tartó párharcának újabb állomását jelentik a nemrég nyilvánosságra hozott, a fent említett aktív védelmeket hatékonyan áttörni képes páncéltörő orosz RPG-30-as rakéták. [14, 15]

Az egyre „intelligensebb” távirányított, több célt egyidejűleg is követni képes lövegtornyok informatikai részegységeivel jelen cikkben nem foglalkozom, itt az egyes követelmények még szigorúbbak.

2. Földi robottechnikai eszközök sajátosságai, működésmódjai

A Robothadviselés 8 konferencián [16] előadott értekezésem témájául a „Szárazföldi robottechnikai eszközök tervezésének és alkalmazásának biztonsági szempontjai”-t. Itt felsoroltam az egyes veszélyforrásokat: *„A „csak” két dimenzióban mozgó földi robottechnikai eszközöknél óriási előny a szilárd talaj, legalábbis addig, míg egy helyben áll a jármű. Amint elindul, változik a helyzet, a sebesség fokozásával egyre hasonlatosabb lesz egy éppen leszálló repülőgéphez. Sőt! Sokkal rosszabb a helyzete, mert nem rendelkezik egy / kijelölt / körbekerített / lezárt / egyenes / jó felületű pályával. A földi robotok „pályája” girbe-gurba, hepe-hupás, rosszul, vagy egyáltalán nem kijelölt, nyitott még a szembe- és keresztforgalomnak is! Az utakról letérve még bonyolódik a helyzet, számtalan terepakadály, házak, árkok, gödrök, folyók, fák, bokrok, kövek, veszélyes lejtők, víz, sár, mocsár, homok, hó-jég, köd, stb. leselkednek rá. Mindezeket a veszélyforrásokat menet közben érzékelni, értékelni lehetséges, de szinte „emberfeletti” feladat, sajnos ezt bizonyítják a közlekedési baleseti statisztikák is... Ha rendelkezünk is elegendő szenzorral, megfelelő információval, akkor is a végtelen felé konvergáló kombinációs lehetőségek kiértékelése miatt a valós idejű feldolgozás akadozhat. Hosszú évek szükségesek, míg a „tanuló” programok és maguk a programozók a különböző tereptípusokra szabott szoftvereket optimalizálják, majd a legkülönbözőbb terepeken tesztelik.*

A földi robotoknál, nehéz terepen menet közben fellépő, állandóan változó (pozitív és negatív) gyorsulások, ütések, rezgések, a külső mechanikai behatások (pl. ágak, szögesdrót), a szennyeződés lehetősége (eső, hó, dér, por, sár, harcanyagok jelenléte, stb.) a szenzorok terepi kivitelezésére is komoly, részben még megoldandó feladatokat rónak. A változatos, előre nem kiszámítható terep a meghajtás állandó változtatását (gyorsítás, fékezés, kormányzás) igényli, ez nagyon energiaigényes, a vezérlő egységek informatikai kapacitását is állandóan igénybe veszi.” [17]

Az érzékelők működése és az általuk szolgáltatott információk kiértékelése nagyon bonyolult feladat. Figyelembe kell venni a más járművek által okozott véletlen, illetve az ellenség által tudatosan sugárzott zavaró fények, rádióhullámok, lézersugárzások „vakító” ill. torzító, árnyékokat okozó hatását. Mindez nagyon leterhelheti a központi egység számítástechnikai kapacitását. Ezt a nagyon bonyolult rendszert gyakorlatilag lehetetlen matematikailag teljesen modellezni, mindig számítani kell váratlan eseményekre. Már ma is kijelenthetjük, hogy a robotok műszaki kivitelezése (hardver) mellett az egyes vezérlőprogramok (szoftverek) megalkotása, optimalizálása, tesztelése legalább ugyanilyen nagyságrendű kihívást jelent.

² SLID (small low-cost interceptor device – kis költségű elfogó eszköz)

Oszlopmenetnél - az út menti robbanó-csapdák aktiválását megakadályozandó - egyre gyakrabban alkalmaznak nagy teljesítményű, szélessávú zavaróadókat. A nagyon erős, „mindent elnyomó” elektromágneses terek a robotok működését-irányítását, ezzel megbízhatóságukat is negatívan befolyásolják, a védelem ellene nehéz.

A mély terep utáni tisztítás, illetve a harcanyagoktól való mentesítés (dekontamináció) lehetősége is fontos. Mivel autonóm robotjárművekről beszélünk, a távlati cél csak az lehet, hogy mindez a kezelőszemélyzet közvetlen jelenléte nélkül is megvalósítható legyen.

Tüntetéseknel mesterséges akadályok (barikádok), kőzápor, „molotov koktél”, vízágyú eltévedt vízszugara, a jármű felborításának veszélye jelenthet problémát.

2.1. Távirányított földi robottechnikai eszközök

Ezek a leggyakrabban használt robotok. A távműködtetésű rendszerek működhetnek teljes, illetve részleges távirányítással, a távirányító rendszere szerint lehetnek vezetékeselek, rádiófrekvenciás rendszerek, illetve internet alapú, hálózatos rendszerek.

Távirányított járműveknél az operátor hatékonyan tudja kiszűrni az éppen fontos információkat, nagy részben átveszi a központi egység véges funkcióit, tehermentesítve ezzel. *“A fedélzeti számítógépes rendszerre a robot bizonyos fokú autonómiájának megteremtése érdekében van szükség. Nagy értékű robot esetében még távvezérelt robot esetében is érdemes bizonyos biztonsági funkciókat a robot fedélzetén lévő intelligens eszközre bízni. A robottal való kommunikáció megszakadása esetén például a robot képessé tehető egy előre definiált helyre történő visszatérésre. Szélsőséges körülmények között a robotnak észlelni kell a rá veszélyt jelentő környezeti behatásokat (például túl meredek lejtő esetén a robot nem kockáztatja az esetleges zuhanást, hanem jelez a kezelőnek és új útvonalat kér).”*[18] Nagyon fontos a zavarmentes, alacsony zajszintű, lehetőleg kódolt, kétirányú információáramlás, ez csak jó minőségű rádióösszeköttetéssel lehetséges. A felderíthetőség és az energiafelhasználás szempontjából azonban a folyamatos jelkibocsátás hátrányos.

A távirányított járművek is kerülhetnek olyan (kényszer-) helyzetbe, amikor csak a saját rendszereikre hagyatkozhatnak – ha megszűnik, illetve akár csak rövid időre is kiesik az összeköttetés. Álló helyzetben ez jelentheti egyszerűen a kivárást. Gyors mozgás, illetve valamilyen veszélyes tevékenység közepette – például egy robbanóeszközzel való manipulálás/hatástalanítás közben a biztonságos nyugalmi helyzet elérését (autonóm módon) előre pontosan definiálni kell.

Ezt a biztonsági „rést” különösen fontosnak, eddig nem nagyon kutatottnak tartom. Tovább bővítik e biztonsági rést a Dr. Szabolcsi Róbert által leírt „robot-holtidők”. [19, 20]

2.2. Univerzális, sofőr által is vezethető földi robotjárművek

Ezeknél a járműveknél a távirányított, ill. az autonóm működés mellett a humán sofőr is átveheti az irányítást.

A hagyományos / direkt vezetésnél a nagyméretű robotjármű vezetőfülkével is rendelkezik, ekkor a szigorú ergonomiai követelményeknek is eleget kell tenni. A vezetőfülke kialakítása, műszerfal, periszkópok és/vagy képernyők, hagyományos kormány, fékek, stb. annyira megdrágítják a járművet, hogy valószínűleg csak kivételes esetekben lesznek ilyen irányú fejlesztések. Nyomós érv lehet ebbe az irányba az ún. „átmeneti” időszakban a biztonsági kérdések még nem eléggé alapos tisztása, kiértékelése, tesztelése. Az esetleges baleseteknél felmerülő jogi problémák – a katonai, ill. a civil forgalomban való engedélyezettetés elhúzódása befolyásolhatja a fejlesztéseket olyan irányba, hogy a nagyobb robotjárműveknél helyet szorítsanak egy humán sofőrnek is a fedélzeten. Így a közutakon hagyományos módon közlekedne a jármű. A már meglévő járművek robotjárművekké történő

alakításával/átépítésével szintén létrejöhetnek ilyen „mutánsok”. Erre már most is vannak példák, például M 48-as tankból építették át a német Keiler aknamekesítő járművet [21], ez teljesen távirányítható. A kisebb, szlovák gyártmányú Božena [22] aknamekesítő járművek fejlesztése eredetileg a Bobcat-ek [23] átépítésével kezdődött. Átalakított harcjármű példája a robot- Stryker [24], átalakított autonóm teherautó az Oshkosh cég járműve [25]. Hátrányuk, hogy az utólagos átépítések a konstrukciós megkötések (pl. a helyhiány) miatt mindig kompromisszumokat követelnek. Teljes értékű robotjárművekké nem válnak, de egyszerűbb feladatokra használhatók. Az említett aknamekesítés mellett például egy nem teljes biztonsággal megtisztított aknamezőn, veszélyes területen „felderítő-áldozatként”, illetve „csaliként” át lehet küldeni egy ilyen távirányíthatóvá átalakított járművet.

Valószínű, hogy a jövőben a személyzettel is rendelkező, univerzális robotjárműveket úgy alakítják majd ki, hogy a megfelelő nagyságú robotjármű „rakterében” helyezik el az operátor vezérlő-terminálját befogadó konténert és direkt módon (árnyékolt, vagy optikai kábelekkel) csatlakoztatják a jármű rendszereihez. A konténernek a bevetéshez elegendő védelemmel (ballisztikai, vegyi - sugár, IED³ [26], stb.) kell rendelkeznie, illetve eleget kell tennie az ergonómiai követelményeknek (elegendő tér, hűtés, fűtés, szellőztetés, megvilágítás, elégséges zaj- és rezgésvédelem, stb.)

Az informatikai egységeikkel szemben támasztott követelmények leginkább attól függenek, hogy a jármű személyzet nélkül csak távirányítottan, vagy teljesen autonóm módban is működhet.

2.3. Autonóm földi robottechnikai eszközök

„Az autonóm robot fedélzetén hordozza a működéséhez szükséges vezérlőberendezést, így működése nem függ semmilyen külső vezérlő számítógéptől, mivel a fedélzeti vezérlő képes a szükséges döntések meghozatalára” [27]

A szenzorok által küldött beérkező információáradatot valós időben kell feldolgozni, hogy még időben megfelelő ellenintézkedésekkel korrigálni lehessen az autonóm jármű tevékenységeit. Az informatikai egységeikkel szemben támasztott követelmények a legnagyobbak, hiszen óriási adatmennyiséget kell feldolgozni, minden várható és váratlan eseményre lehetőség szerint fel kell készülni.

A személyzettel ellátott járművek esetében maximum pár napi járőrözés után a személyzet szükségletei miatt meg kell szakítani az ellenséges területen való tartózkodást. Ezzel szemben a robotjárművek jól álcázva akár hónapokig (!) is kivárhatnak „alvó/hibernált” üzemmódban. Ez például csak az energiaforrások tartós, illetve hosszú „pihenő” idő után is jó terhelhetősége mellett lehetséges. Célrányos tervezés mellett víz alá is merülhetnek.

A robotjárművek rajokba, csapatokba való szervezése hasonlóan a természetben megfigyelhető csoportos létformáknál, minden bizonnyal előnyös. A terep feltérképezése több „kameraállásból” sokkal hatékonyabb, a veszélyhelyzetek jobban kiértékelhetők. Érzékelőik „szenzormezőt” alkotnak, így például a harcanyagok terjedéséről, az ellenség mozgásának sebességéről is közvetetten információkat tudnak szolgáltatni. A hibásan működő szenzorokat is jobban ki lehet szűrni. Az egyre inkább terjedő távirányítható lövegtoronyokat és a különböző, automatikusan működő fegyverrendszereket (aktív rakétaelhárító rendszerek, ködvetők) kitűnő felbontású és reakcióidejű érzékelőkkel rendelkeznek. Megtöbbszörözött funkcióként ezek adatait is fel lehetne használni a robotjármű biztonságosabb közlekedéséhez.

Az egyes terepakadályokat a (közös) digitális térképükön bejelölhetik, így a követő, vagy később áthaladó járművek ezekkel a területekkel csak felületesen foglalkoznak, egyszerűen kikerülik őket. Hasonlít egy kicsit a denevérek zegzugos barlangokban való repüléséhez, akik a megszokott „légifolyosóikon” repülnek és csak maguk előtt pásztázzák megkülönböztetett

³ IED (improvised explosive device – improvizált robbanó eszköz)

figyelemmel a "légteret". Ha egy fix akadályt helyezünk az újukba tartósan, akkor az egyes denevérek ezt természetesen észlelik és egy "vérszékezés" mellett, a jelkibocsátás frekvenciájának ugrásszerű emelésével "letapogatják", majd kikerülnek. Néhány óvatos "járőrözés" után a kényeserből megváltoztatott új folyosórész koordinátáit "égetik be" a memóriájukba. Később az akadályt eltávolítva a "félautomata" üzemmódban, gyorsan repülő denevérek még hosszú ideig "kopírozzák" a valójában már feleslegessé vált, hosszabb "elkerülő" utat. A szárazföldi robotoknál is hasonló módon lehet takarékoskodni a véges megfigyelő, kiértékelő és döntéshozó, illetve tápenergia kapacitással. A denevérekkel szemben van egy óriási előnyük, hogy az egyik egység által felderített akadály az egész „mátrix-autonóm” csapat számára ismert lesz. Ha tehát a menetoszlop közepén egy újonnan keletkezett aknátölcser megállásra készítet egy robotjárművet, akkor ez megvizsgálja, majd (esetleg az operátor segítségével) kikerüli, a kerülőutat bejelöli a digitális térképbe. Később az útakadályok elhárítása után az utászok „törlik” a kitérőt.

3. Földi robottechnikai eszközök informatikai részegységeivel szemben támasztott speciális követelmények

A robotjárműveknél az informatikai részegységek megbízhatósága még fontosabb, hiszen a személyzet hiánya miatt nem lehetséges a kézi beavatkozás, javítás, funkciók átvétele. Egy fontos informatikai részegység kiesése/hibás működése megbéníthatja a járművet, veszélyeztetve ezzel a bevetés sikerét, biztonságát. Az új, nem kiforrott, megfelelő csapatpróbákön át nem esett hardvereknek, szoftvereknek nincs helye a harci robotoknál. Egyszerű szavakkal úgy fogalmaznám meg, hogy az akció sikerességének szempontjából többet ér egy „hagyományos” katona, aki eljut a bevetési területre, mint egy „csúcstechnológiás”, aki útközben minduntalan elakad...

Ide kívánczik Molnár Zsolt értekezése az emberi felügyelet nélkül működő rendszerek öntesztelésének lehetőségeiről, ebből idézek néhány kiragadott mondatot: „*Egy terepi készülék tervezése esetében tehát törekedni kell arra, hogy ne legyen szükség külső eszközökre a teszteléshez, és a vizsgálatot a felhasználó, vagy a készülék saját maga képes legyen levezényelni. ... A terepi elektronikai eszközök beépített tesztelése számos előnyt biztosít. Ezek közül a legfontosabbként az említhető, hogy az önteszt lefutása vagy lefuttatása után pontos képet kapunk a készülék állapotáról: az esetleges meghibásodások felismerhetők, helyük azonosítható. ... az új készülékek esetében már a tervezéskor szem előtt kell tartani azokat a szempontokat, amelyek az öntesztelés megvalósítását lehetővé teszik, azaz a készülékeket (ön)tesztelhetőkre kell tervezni.*” [28]

A földi robottechnikai eszközök informatikai részegységeivel szembeni általános elvárások hasonlóak, mit az ember vezette járműveknél, vannak azonban eltérések. Ezen eltérések többsége a személyzet hiányából fakad, egy részük pozitív, de vannak negatívak is, egy külön alfejezetben részletesebben kitérek a nagy teljesítményű elektromos, ill. hibrid járművek problematikájára.

3.1. Pozitív hatások

A személyzet hiánya miatt a belső tér teljesen beépíthető, illetve a jármű kisebb, alacsonyabb lehet. Nem kell számolni a személyzet általi mechanikai túlterheléstől, nem kell figyelembe venni az egyre szigorúbb ergonómiai, tűzvédelmi (pl. megkötések az égéskor mérgező füstgázt kibocsátó anyagok választhatóságánál), stb. követelményeket, nem szükséges hermetikusan elválasztani a motorteret. Nem kell belső világítás, a messziről árulkodó reflektorok is elhagyhatók.

A hatékony tűzfelfojtás érdekében levegő- (oxigén-) mentes, zárt belső atmoszféra is kialakítható, itt a beépített rendszerek hűtésigényeit is figyelembe kell venni. Ennek az

említett zárt belső atmoszférának pozitív hatása lehet a céltudatos páramentesítés. A kondenzálódó vízcseppek negatív hatásai (optikai alkatrészek párásodása, villamos átvezetések, kisülés, kapacitáscsökkenés, korrózió, stb.) így hatékonyan kiküszöbölhetők.

Egy jól megtervezett, különböző szenzorokkal (a fordulát, forgatónyomaték, hőmérséklet, rezgések, stb. mérésére) felügyelt, teljesen automatikus hajtást nem kell feleslegesen „túlméretezni”. A célirányos szoftverekkel védve van a túlterhelések ellen. Például egy tengelykapcsoló hirtelen oldása, egy rossz kézi visszaváltás rövid ideig tartó, többszörös túlterhelést eredményezhetnek. A laza talaj után szilárd úttesten gyorsan haladó járműveknél a túl későn visszaállított kerék-nyomás a köpeny oldalfalainak a sérüléséhez vezethetnek, a sebesség függvényében akár 1-2 km-en belül!

A távol lévő irányítószemélyzet nincs olyan stressznek kitéve, mint a bevetésben fizikailag részt vevő katonák, csökkenthetők a személyi veszteségek.

A bármilyen okból (elakadás, meghibásodás, találat, robbanás, stb.) kieső, illetve taktikai okokból (pl. őrszemként) leállított jármű operátora tovább harcolhat/tevékenykedhet (egy másik robotot vezérelve).

3.2. Negatív hatások

A robotjárművek belsejében nincs szükség „emberi” körülményekre, ez a belső térben elhelyezett alkatrészekre, műszerekre, informatikai rendszerekre nagyobb megterhelést jelent. Tartósan extrém hőmérsékletek lehetnek, nagyobb lökések, vibrációk megengedettek, sugárzás, harcanyagok jelenléte lehetséges, stb.

A személyzet hiánya miatt egy máskor egyszerűnek történő hiba, pl. egy távirányítással nem aktiválható biztosíték kioldása, vagy pl. egy érzékelő bepárásodása is elakadáshoz, illetve átmeneti „vaksághoz” vezethet.

Jól képzett irányító- és karbantartó személyzetet igényel.

A távol lévő, közvetlen veszélynek nem kitett operátor hajlamosabb kockázatos akciókba bocsátkozni, mint a bevetésben fizikailag részt vevő katona.

Fel kell készülni olyan szituációkra, amikor az emberi felügyelet/védelem nélküli robot például a kíváncsi gyermekek ártatlan-, vagy a fegyvertelen civil lakosság rosszindulatú „érdeklődését” kelti fel. Ilyen helyzetekben, ha nem lehetséges a visszavonulás, illetve ha nincs a közelben élőerő- segítség, akkor a szituációhoz megfelelő, humánus, „non lethal” válaszlépés szükséges. Lehetőleg többlépcsős, kezdve a hanggal való figyelmeztetéstől a kellően hangsúlyos, elrettentő, fájdalmat okozó, akár időlegesen bénító fokozatokig. A robotok esetleges autonóm fegyverhasználatának hadijogi háttere még az ellenséges fegyveres támadás esetén sem tisztázott!

3.3. Nagy teljesítményű elektromos, illetve hibrid járművek problematikája

A sokak által a jövő trendjének kikiáltott hibrid járműknél, ill. az elektromos hajtásaiknál létrejövő, állandóan változó elektromágneses mezőket is figyelembe kell venni. Ezek egyáltalán nem elhanyagolhatók, ha már a 4x4-es járműkategóriánál is 1 MW-os tervezett teljesítményekről, ill. 100 km/h sebesség 5 s alatt való eléréséről olvashatunk [29]. Ilyen teljesítményfolyamok kapcsolása, vezérlése, csak megfelelően méretezett rendszerekkel lehetséges. Az esetleges hő- torlódások lehetőségére is ügyelni kell. Például a kerékagyba épített motoroknál, amikor a jármű kerekei mély talajban elmerülve, elakadva, maximális nyomatékok mellett nem teszik lehetővé a sugárzással, ill. a léghűtéssel történő hőleadást. A nagy teljesítményű áramfejlesztő(k), a meghajtó elektromotorok, a vezetékek, a teljesítmény-elektronikai részegységek megfelelő árnyékolása sem egyszerű feladat.

Az elektromos hajtások egyik előnye, hogy fékezéskor energiát juttathatnak vissza a rendszerbe, tehát a meghajtó villanymotorok generátorként működnek. Ehhez gyorsan és

hatékonyan tölthető energiatárolókra (akkumulátorokra) van szükség. A nagy kapacitás is fontos, hogy hosszabb lejtmenetben is legyen elegendő energiatárolási lehetőségünk. A töltést, ill. az energia-visszaadást vezérlő elektronika is bonyolítja-drágítja a rendszert.

A katonai, terepjáró járművek mindezen részegységénél a terepi kivitel is elengedhetetlen.

Összegzés, következtetések

A harcjárművek informatikai részegységei sokkal nagyobb igénybevételnek vannak kitéve, mint a civil rendszerek. A tömeg-autógyártás területéről csak a szigorú katonai feltételek teljesítése, tesztelése után lehet egyes alkatrészeket, részegységeket alkalmazni. A robosztus kivitel, ipari tokozások, mechanikai és elektronikai védelem nagyon fontos. Az időjárás viszontagságait a szélsőséges klímazónákban is állni kell. Az indokolatlanul szigorú elvárások teljesítése viszont többletköltségeket jelentenek.

Elemeztem a földi robottechnikai eszközök sajátosságait, működésmódjait, részleteztem a szárazföldi robotjárművekre és érzékelőikre leselkedő veszélyeket, rámutattam, hogy például a szenzorok elégséges terepi kivitelezése még kívánnivalókat hagy maga után.

Összehasonlítottam a járművek informatikai részegységeivel szemben támasztott követelményeket annak függvényében, hogy a fedélzeten tartózkodik-e személyzet, illetve jelenlétük kizárható (teljesen autonóm jármű).

Rámutattam arra a biztonsági „rés”-re, hogy összeköttetés bármilyen okból történő megszakadása után a távirányított jármű is átmeneti időre autonóm járművé válik! Ebből az következik, hogy ha egy nagyobb méretű, gyors, biztonságos, „egyszerű” távirányított robotot szeretnénk létrehozni, akkor is teljes mértékben foglalkoznunk kell az autonómítás problematikájával is.

Minden hadsereg arra törekszik, hogy katonáit a lehető legjobban védje az ellenséges csapásoktól. A személyi sérülések, veszteségek valószínűsége a legkülönbözőbb intézkedésekkel, új védelmi technikákkal-taktikákkal ugyan csökkenthető, de 100%-osan kizárni csak a robotok alkalmazásával lehet. Valószínűleg már ma ez a legmeggyőzőbb érv/szempont a robotok fejlesztésének szükségességét illetően. A földi robottechnikai eszközök informatikai részegységei állandó fejlődésben vannak. Részben a számítástechnika óriási fejlődése miatt, részben a robotokkal, robotjárművekkel szemben támasztott egyre szigorúbb követelmények miatt. Az egyre növekvő sebességek, az egyre rövidebb reakcióidők szükségessége, az egyre több beérkező információ feldolgozása, kiértékelése, majd valószínű időben történő döntések meghozatala óriási kihívást jelentenek a fejlesztőknek. Nem olcsók ezek a fejlesztések, akár meg is haladhatják a légi robotok informatikus részegységeinek a fejlesztési költségeit.

Távlatilag a robotok képességei egyre nagyobb mértékben haladják majd meg az emberek fiziológiailag behatárolt képességeit, ez lesz majd a további fejlődés hajtómotorja. Az informatikai részegységek minőségének, reakció-gyorsaságának, kapacitásának, felbontóképességének, ellenálló képességének, tartósságának, öntesztelő képességének, élettartamának, extrém körülmények melletti megbízhatóságának várható további rohamos fejlődése teszi ezt majd lehetővé.

Hivatkozott irodalom⁴

- [1] <http://www.steyr-ssf.com/>
- [2] Rolf Hilmes: Panzrentwicklung heute und morgen. Strategie und Technik Juli 2008, p. 23.
- [3] STANAG 2895 Annex A: A-1, A-2; Annex B: B-1
- [4] <http://www.army-technology.com/projects/pandurII/>
- [5] http://daten.bwb.org/AG-Bund/TL/daten/84700008_1.pdf
- [6] http://klein-gelenkwellen.de/tech/technische_hinweise_2.html
- [7] <http://www.incase.hu/index.php/Mobil-adatgyujto-valasztas/IP-vedettseg.html>
- [8] <http://www.defense-update.com/products/d/drozd-2.htm>
- [9] http://en.wikipedia.org/wiki/Arena_Active_Protection_System
- [10] <http://www.russianarmor.info/>
- [11] http://www.btvn.narod.ru/3/kaz_drozd.htm
- [12] <http://www.defense-update.com/products/t/trophy.htm>
- [13] http://de.wikipedia.org/wiki/Iron_Fist
- [14] <http://en.wikipedia.org/wiki/RPG-30>
- [15] <http://www.warandpeace.ru/ru/article/view/29715/>
- [16] <http://www.zmne.hu/tanszekek/ehc/konferencia/robot8.html>
- [17] Koleszár Béla: Szárazföldi robottechnikai eszközök tervezésének és alkalmazásának biztonsági szempontjai. Hadmérnök, IV. Évfolyam 2. szám – 2009. június, pp 385-397
Kiadó: ZMNE; ISSN 1788-1919; http://hadmernok.hu/2009_2_koleszar.pdf
- [18] Kucsera Péter: Moduláris felépítésű mobil robotikai alkalmazások kialakítási szempontjai. Hadmérnök, I. Évfolyam 3. szám - 2006. december, Kiadó: ZMNE; ISSN 1788-1919 http://hadmernok.hu/archivum/2006/3/2006_3_kucsera.html
- [19] Dr. habil. Szabolcsi Róbert: Handling time delay in control of unmanned robots. /A holtidő modellezése a távvezérelt robotok elméletében és gyakorlatában./ http://www.zmne.hu/tanszekek/ehc/konferencia/prezrw8/Szabolcsi_Robert.pdf
- [20] Dr. habil. Szabolcsi Róbert: Handling time delay in control of unmanned robots. http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/03_Szabolcsi_Robert.pdf
- [21] [http://de.wikipedia.org/wiki/Keiler_\(Panzer\)](http://de.wikipedia.org/wiki/Keiler_(Panzer))
- [22] <http://www.way-industry.sk/ger/index.php?b=products>
- [23] http://www.bobcat.com/?locale=EU_de
- [24] <http://64.202.120.86/upload/image/articles/2007/darpa-urban-challenge-2007/unmanned-stryker-dod.jpg>
- [25] http://www.spacedaily.com/reports/DARPA_Awards_Oshkosh_Truck_Contract_To_Advance_Its_UGV_Technology_999.html
- [26] http://en.wikipedia.org/wiki/Improvised_explosive_device

⁴ Az internetes hivatkozások esetében a letöltések időpontja egységesen 2009. október 20.

- [27] GIBILISCO S.: Concise Encyclopedia of Robotics. McGraw-Hill 2003; Kucsera Péter fordítása az „Autonóm működésű szárazföldi robotok védelmi célú alkalmazása“ című doktori (PhD) értekezés tervezetéből
- [28] Molnár Zsolt: A terepi elektronikai eszközök beépített öntesztelésének lehetőségei. Hadmérnök, III. Évfolyam 4. szám - 2008. december, Kiadó: ZMNE; ISSN 1788-1919 http://hadmernok.hu/archivum/2008/4/2008_4_molnarzs.pdf
- [29] Lukáš Visingr: Projekt Ultra / Technologie závodních vozů na bojišti. ATM 2008/11, pp 34-35, Aeromedia Praha, ISSN 1802-4823

Koleszár Béla

koleszar@tele2.at

A ROBOTHADVISELÉS ETIKAI KÉRDÉSEI¹ I. HARCI ROBOTOK

Absztrakt

A szerző rendszerezte és elemezte a világon jelenleg megkonstruált felfegyverzett robotokat, azok alkalmazásának elvi és gyakorlati lehetőségeit. Összehasonlította az embert a géppel, felsorolta az alapvető különbségeket az emberek és robotok között. Taglalta a robotok alkalmazásánál felmerülő problémákat, szemléltetve néhány robot-baleset kiértékelésével.

Rámutatott, hogy a robothadviselés, beleértve a robotok önálló fegyverhasználatát is, már elkezdődött.

The author systematized and analyzed the currently constructed, armed robots in the world and the possibilities of their theoretical and practical application. Man to machine was compared; the fundamental differences between humans and robots were listed. The problems arising from the application of robots, demonstrating with the evaluation of some robot-accidents were discussed.

It was pointed out that robot warfare including the autonomous weapon wearing of robots is already underway.

Kulcsszavak: robot, robothadviselés, harci robotok, robot balesetek, ~ robot, robot warfare, battle robots, robot accidents

Bevezetés

A téma terjedelmessége miatt írásomat két részre osztottam. A második részben taglalt robot-erkölcsi témák jobb érthetősége érdekében ezen első részben felvázolom a robottechnika mai állását, rámutatok a harctéri robotok alkalmazásának egyes problémáira.

A robotok tömeges katonai alkalmazásának a jelentőségét a lőfegyverek elterjedéséhez, a motorizált hadseregek, a repülőgépek megjelenéséhez lehet hasonlítani. A ma használt robotok döntő többsége még távvezérelt, ezek aránylag kicsik, illetve lassúk, tehát a (nem tudatos) károkozó képességük nem nagy. A képzeletbeli jéghegy csúcsán lévő (hordozóként bevethető) nagy robotrepülőgépek viszont már ma is harcászati jelentőséggel bírnak.

A robothadviselés korszaka már elkezdődött! Szeretném írásommal eloszlatni azt a még mindig gyakran hangoztatott téves nézetet, hogy ma még az összes fegyverhasználatnál

¹ A téma rövidített változatban, a Robothadviselés 9 [1] konferencián került előadásra

ember húzza meg a képzeletbeli elsütőbillentyűt, ill. nyomja meg a gombot... Mivel a robotok fegyverhasználata jogilag nincs rendezve, a robothadviselés etikai kérdéseivel nemzetközi szinteken kell foglalkozni!

A robotok civil felhasználása még gyerekcipőben jár, például a robotok nyílt területeken (pl. közlekedésben) való alkalmazása gyakorlatilag lehetetlen. Az ezekre vonatkozó legiszlatívák (irányelvek) kidolgozása is késik.

1. Mi a robot?

A **robot**² fogalom újkori jelentését 1922-ben alkották meg a cseh Čapek testvérek.[2]

Egy távirányított gép is robotnak tekinthető? Vagy inkább egy önállóan működő gép áll közelebb egy igazi robothoz? Kedvelt szemléltető példa a meleg vizet szolgáltatató bojler. **Önműködő szabályozóval** rendelkezik, tehát az autonóm működés egy alapsíráját tartalmazza (önműködő szabályozás). Ennek esetleges kiesése, meghibásodása miatt még biztonsági szeleppel is rendelkezik. Igaz, hogy nem egy „lángész”, nem tud sokat, de amit tud, azzal biztonságosan, hosszú éveken, évtizedeken keresztül szolgálja az embereket. A felvonóknak beépített, **fix logikájuk** van, ami nem mindig úgy működik, ahogy mi szeretnénk... Aránylagos egyszerűségük mellett is elég gyakori a meghibásodásuk. A fotocellás ajtók is önműködően nyitnak-zárnak, de itt is vannak (tudatos - nem tudatos?) korlátozások, pl. a gyerekekre nem nyílnak biztosan. Más esetekben akkor is nyitnak, amikor nem kellene, pl. egy, a járdán előtte elhaladó gyalogos miatt. Ezeket a kellemetlenségeket persze ki lehetne küszöbölni, de ez bonyolultabbá és drágábbá tenné a rendszert. A „konyhai robot” elnevezés túlzó, hiszen a régebbieknek még **mechanikus programjuk** (mint az automata mosógépeknek) sem volt. Dél-Afrikában a közlekedési lámpákat robotoknak hívják – mert „önműködők”... (1. kép)

A fejlettebb robotok legfőbb ismérve, hogy hosszabb-rövidebb ideig külső **vezérléstől függetlenül** (autonóm) tudnak tevékenykedni (a jobb porszívó-, ill. fűnyíró robotok is már ilyenek). Az emberi beavatkozás általában lehetséges, de nem minden esetben, illetve nem minden helyzetben. Interaktív kapcsolatban vannak a környezetükkel, annak változásaira reagálni képesek.

Egy szárazföldi mobil robot-definíció: „az UGV³ egy olyan hajtott, helyváltoztatásra képes mobil eszköz, amelyen nincs emberi személyzet a fedélzeten.” [3]

Kucsera Péter szerint „Ez a definíció feloldja a távvezérelt eszközök és a robot fogalmának ellentétét, mivel itt nem szerepelt a programozott automatikus működés kritériuma. Ember nélküli szárazföldi mobil robotok, azaz UGV-k katonai alkalmazása olyan környezetben különösen indokolt, amely ember számára valamilyen okból nem megközelíthető (pl.: harci gázzal vagy nukleáris sugárzással szennyezett), vagy nagyon kockázatosan megközelíthető, elaknásított vagy erősen őrzött terület. Nem háborús katonai – pl. békefenntartó, terrorellenes – műveletekben UGV-k alkalmazásával az emberáldozatok száma szintén jelentősen lecsökkenthető.” [4]

A **távműködtetésű rendszerek** működhetnek teljes, illetve részleges felületű távirányítással, a távirányító felületük szerint lehetnek vezetékesek, rádiófrekvenciás rendszerek, illetve internet alapú, hálózatos rendszerek. Távirányított járműveknél az operátor hatékonyan tudja kiszűrni az éppen fontos információkat, nagy részben átveszi a központi egység véges funkcióit, tehermentesítve ezzel.

Ma még leginkább távirányítottan, illetve emberektől elzárt (körbekerített) területeken közlekednek a robotok. A légi robotok ugyan szabadabban mozoghatnak a levegőben, de kevés kivételtől eltekintve az emberek által vezetett légi járművek számára zárt légtérben. Kis

² Az idézetekben található vastagon szedett kiemelések, ill. a magyar nyelvű fordítások a cikk szerzőjétől

³ UGV - Unmanned Ground Vehicle – ember nélküli földi jármű

szenzációként tálták a hírt, hogy a 2009-es párizsi repüléstechnikai vásáron az ausztriai Schiebel cég helikoptere (2. kép) volt az első robot-légialkalmatosság, amit repülés közben is bemutattak a légishow-n. [5]



1. kép. Dél-Afrikában...



2. kép. Camcopter

Korlátozza az UAV⁴-k gazdaságos működtetését, hogy az **ellenőrzött légtérben** való civil alkalmazásoknál az operátorok képzésének legalább olyanak kell lennie, mint a pilótákénak. Ennek az oka a **biztonság prioritása**.

2. Harci robotok

A harctéri robotok hasonlatosan a civil társaikhoz, az ún. „DDD⁵” feladatok elvégzésére, az emberek tehermentesítésére, védelmére szolgálnak... Olyan helyeken is, ahol az ember létezése sem biztosított: hideg, forráság, harcanyagok, radioaktivitás jelenléte, de ide lehet a világűrt is sorolni.

A robotokkal foglalkozó Noel Sharkey brit szakember szerint Irakban és Afganisztánban jelenleg 4 és 6 000 közé tehető a bevetett harci robotok száma. [6] Más források még nagyobb számokat említenek.

A széles nyilvánosság körében talán a legismertebbek az Öbölháborúban bevetett Tomahawk típusú **robotrepülőgépek**. Ezek a szárnyas „bombák” igazából nem is tekinthetők robotnak. Előre, nagy gonddal programozzák be a kijelölt célpontjaikhoz vezető útvonalat. Az észlelésüket, leküzdésüket megnehezítendő üzemmódban, a terepet pár 10 m magasságban, szinte „borotválják”. Elődjeknek tekinthetők a második világháborúban bevetett V-1 és V-2.

Az **automata fegyverek** (géppisztolyok, gépkarabélyok, géppuskák, stb.) ugyan „önműködőek”, de **nem autonóm** fegyverek.

Ha vízmelegítő bojler példáján megyünk tovább, a végletekig leegyszerűsítve, akkor akár a **taposóaknákat** is robotoknak tekinthetjük – az autonómia csíráját ugyanis magukban hordozzák. Ezek „**áldozat által iniciált** (elműködtetett)” robbanó szerkezetek nagyon buták, de éppen ezért olyan veszélyesek. Nem tesznek különbséget ellenséges, ill. saját katona között sem. Mindegy, ki aktiválja őket: idős, fiatal, nő, gyermek, állat, jármű, vagy bármi más. Teszik azt, amire „beprogramozták” őket, robbannak! A „programjuk” a lehető legprimitívebb, mindössze 1 bit⁶-ből („igen-nem”) áll. A legújabb fejlesztésű, nagyobb (pl. páncéltörő) aknáknak már többet tudnak. Elműködtetésükhöz több körülmény együttes bekövetkezése szükséges (pl. nagyobb nyomás és elektromágneses tér). Ugyan a fejlesztésük

⁴ UAV - Unmanned Aerial Vehicle = személyzet (pilóta) nélküli légi jármű (robot)

⁵ „DDD” - **d**ull, **d**irty, **d**angerous = unalmas, piszkos, veszélyes

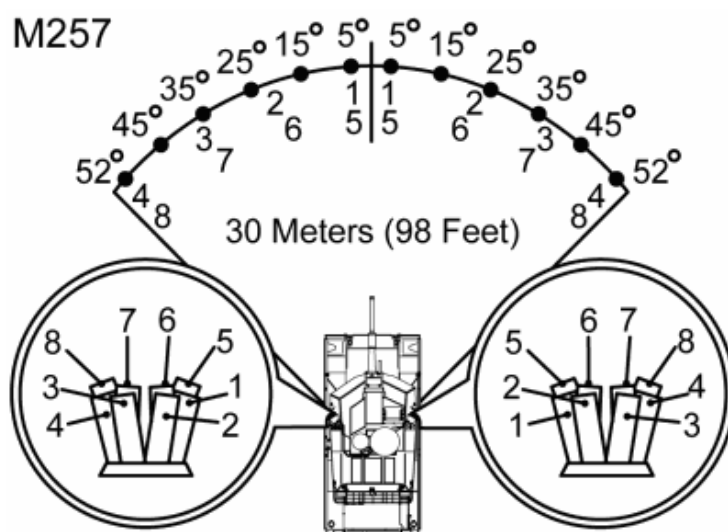
⁶ bit - információt hordozó közlemény. Lehetséges értékei: 0 (hamis), vagy 1 (igaz).

elsőrendű célja valószínűleg a lehető legnagyobb hatékonyság volt, de ezek a divatos szóval „intelligens” aknák a civil (főleg gyalogos) lakosságra jóval kisebb veszélyt jelentenek.



3. kép. Veszélyes aknák

Aránylagos olcsóságuk és utólagos szerelhetőségük miatt talán az **automata füstgránátvetők** a legelterjedtebb önműködő katonai védelmi rendszerek. Általában a lézerrel való megvilágításuk aktiválja őket, a gránátok robbanása a jármű és a lézerforrás közé (az időjárás függvényében) pár percig tartó füst-köd-függönyt állítanak elő. Ez idő alatt adott a fedezékbe vonulás lehetősége.



4. kép. Füstgránátvető-rendszer az egyes löszektorokkal

Ugyan védelmi eszközök, de **veszélyesek is lehetnek**, ha például épület mellett aktiválva a gránátok berepülnek az ablakokon... Ausztriában például egy gyakorlaton előállított füst-ködöt a szél a majd 300 m-re lévő autópályára fújta, a **gondatlanság** halálos balesetet idézett elő. [7] Tehát még az egyszerű, védelmi, „békésnek” tekinthető rendszereknél is marad kockázat, ha előre nem számított események történnek...

A terjedőben lévő „hard kill”⁷ védelmi rendszerek észlelik a közeledő lövedéket, illetve rakétát. A lokátorok munkáját segítik az infravörös érzékelők, amelyek az indítást (a

⁷ hard kill ~ “kemény típusú” fizikai megsemmisítés

felvillanást) érzékelik, aktiválják a rendszert, amely átveszi a követést. Ha veszélyesnek ítéli (a pálya irányától függően), a megsemmisítés kerül sorra. A védő muníció kilövése (állítólag) nem jár olyan fény, hang, tűz – hatással, hogy a közelben tartózkodó személyzetet, illetve más személyeket veszélyeztetné. Egy példa az izraeli fejlesztésű Iron Fist – kilövés után nem irányítható, a közeledő muníció melletti felrobbantásával (amikor éppen mellőzik egymást) keltett nyomáshullámával (keresztirányban) hatástalanítja (megrongálja, illetve eltöri). Egy másik iniciálási móddal (a találkozási pont előtt robbanva) hatékonyan téríti ki az eredeti pályájáról. [8]



5. kép. Iron Fist⁸ működés közben

A támaszpontok (bázisok) ellen intézett aknavető, illetve rakétatámadások ellen különböző csöves, illetve rakéta - védelmi rendszerek kerülnek rendszeresítésre. A célpontokként szolgáló kisméretű rakéták, illetve a gránátok felderítése, követése **emberi szemmel gyakorlatilag lehetetlen**. A lokátorokra, illetve elektrooptikai eszközökre bízák ezt az elengedhetetlenül valós idejű feladatot. A precíziós tűzvezetés automatikusan (tehát **robot – módban**) történik. Például a C-RAM rendszerek gépágyúi valóságos fémfelhőt (védőfüggönyt) képesek előállítani. Speciális lőszereik a cél előtt volfrámrepeszket terítenek. Az események lefolyása olyan gyors, hogy mire érzékeljük, már a válaszadásunk is megtörtént...[9] E fegyverrendszereknél az operátor csak annyit tehet, hogy kijelöli az egyes működési zónákat, be-ill. kikapcsolja a robotot. Beláthatjuk, hogy működés közben minden, a hatósugáron belüli lőszektorba kerülő (ellenséges, saját, ill. semleges) tárgy (pl. repülőgép), madár, stb. veszélyben van. Még akkor is, ha saját maguk nem tudják a rendszert aktiválni, például a kis sebességük miatt. Az átrepülésük alatt történő ellenséges belövés ezt megteheti!

Az operátor feladata az egyes zónák veszélyeztetettségének valószínűségét meghatározni, a felmerülő változások miatt a szektorok határait időben megváltoztatni.

A sokszor csak részben védett tetőlövész helyett egyre gyakrabban **távírányítású fegyverállványok** kerülnek rendszeresítésre. Az egyre „intelligensebb” távirányított lövegtornyok, több célt egyidejűleg is követni képes figyelő-célzó berendezések alkalmazása egyre gyakoribb. Itt is **csak az alkalmazott programoktól függ**, hogy távirányítottan, illetve önműködően (automatikus tűzvezetés) is használhatók-e?

A „**jövő tüzérsége**”- részben helyettesítheti a légi támogatást is – a rakéta-sorozatvetőkhöz hasonló mobil rendszerekből kilőhető: Fire Shadow – „kiváráó robotrepülőgépek”. A bevetési terület fölött órákon át körözve, önműködően képesek célt keresni, támadni. A kezelő az utolsó pillanatig megváltoztathatja a repülés pályáját, például ha váratlanul civilek jelennek meg a célterületen belül. Ez a MITL⁹, vagy OITL¹⁰ működési mód.

⁸ iron fist (ang.) = vas ököl

⁹ MITL - Man In The Loop ~ ember a (döntési) hurokban

¹⁰ OITL - Operator In The Loop ~ operátor a (döntési) hurokban

[10] Nagyobb tűzérési aknák is rendelkezhetnek végfázis (-ön) vezérléssel, ill. független célkiválasztással.

3. Emberek és robotok

Nézzünk magunkba: ha minden szabályt, szabályzatot, előírást, törvényt szó szerint (Švejk-szerűen) betartanánk, valószínűleg lebénulna a társadalmunk. Az „ésszerű” kompromisszumok, apró kihágásaink, föllentéseink, hiúságaink, gyengeségeink, hibáink, „bogaraink” életünk részei - **mi nem vagyunk robotok!** A robotokkal szemben nem vagyunk, nem lehetünk ilyen toleránsak. Éppen ezért sok helyen már most is biztonságosabb az esendő ember helyett robot-rendszereket alkalmazni – pl. egy atomerőmű vezérlésénél. Kevésbé veszélyes – ezzel etikusabb is robotokra bízni egyes bonyolult, ill. nagyon gyors rendszerek irányítását (pl. űrhajózás, léghárító rendszerek, stb.) **Az „emberi tényező” kiiktatása** más esetekben is **előnyös** lehet: Repülőgépeknél – az emberi szervezet számára elviselhetetlen gyorsulások miatt. Orvosi műveleteknél (pl. operálás) – több szabadsági fokozat a robotkarnál, mint az emberi kéznél, a szike nem remeg, egyszerűbben sterilizálható a gép, csírámentes a levegő. Szabad kézzel nem elérhető helyeken is lehet dolgozni, kicsik lehetnek a szükséges operáló nyílások. A beavatkozás sebességét változtatni lehet, tehát nagyobb kézmozdulathoz kisebb (pl. vágási) sebesség járul.

Alapvető különbségek emberek és robotok között:

Az ember társas lény, de „egyedi”, a robot egyenlőre az, aminek beprogramozzuk. A gép emóciók, félelem, „hezitálás” nélkül, gyorsan dönt. Gyűlölni nem képes, előítéletekkel is csak akkor rendelkezik, ha így programozták be őket. Nem ismeri a gyászt, a depresszió sem gyötri. Nem fogyaszt alkoholt, kábítószer. A robotoknak nem lanyhul a figyelmük, nem játszanak, nem korruptak, nem kialvatlanok, nem alszanak el szolgálatban. Nem hívják őket mobiltelefonon, stb.

A robot lelkiismeret furdalás nélkül cselekszik, határtalanul gépiesen-higgadtan. Nem ragadja magával a harc heve. Nem dühös, nem „kattan át”, nem kezd „állatian” viselkedni. Bár az állati jelző helyett inkább az „emberi” passzolna ide, hiszen az állatvilágban az okatlan, cél nélküli vérengzés nagyon ritkán fordul elő. A robotra tehát biztosan nem lehet ráhúzni a „hirtelen felindulásból” enyhítő körülményként alkalmazható (büntetést csökkentő) jogi köntöst.

Egy cseh cég nem szokványos gyakorló lőtábla- sorozatokat kínál. Például az egyiken egy szolid öltözetű, attraktív szőke hölgy látható, különféle „kiegészítőkkel”, az esernyőtől kezdve az automata géppisztolyig. *„Elit egységek szakemberei javaslatok alapján készült. Az ok az volt (a gyakorlatban bizonyítottan), hogy a fegyveres erők tagjai végzetesen tévóváznak, amikor egy gyönyörű nő ellen kell a fegyverüket használni. Néhány bevetés ugyanis alátámasztotta, hogy sok férfinak problémát jelent rálőni az ellenkező nem egy jól sikeredett példányára. Ez valahogy ellentétes az ő- természetükkel.*

*A pszichológusok szerint ez a zsigereinkben lévő **szexuális ösztönnel** magyarázható – a férfiak figyelmét először ugyanis a szép arc, a vonzerő foglalják le, általában csak sokkal később érzékelik a fehérrépet, mint komoly veszélyt. De még az után is, amikor felfogja (tudatosítja) a fegyvert (ami néha meglepően hosszú ideig tart), ilyen ellenségre lőni nem ritkán nehézkes, késedelmes, ami pedig a rendőr illetve a katona számára akár végzetes is lehet.” (az ESP cég „taktikai céltáblák” ismertetője alapján) [11]*



6. kép. „Vonzó veszély” (az Eurosecurity cég szíves engedelmével)

Bizonyos esetekben az egyes emberi hibákat tudatosan is kihasználják, pl. a figyelem elterelésére – ebből élnek a zsebmetszők is... A robotok a félrevezetésekkel, az ösztönökkel szemben immunisak, nem lehet őket érzelmekre ható praktikákkal befolyásolni: Ha megfelelő képfelismerési programmal és **megfelelő háttértárral** rendelkezik, egy szempillantásnyi idő alatt „kiszúrja” a fegyvert! A „riadó-alarm” után kezd csak villámgyorsan a fegyver gazdájával, illetve a környezettel, az esetleges válaszlépések lehetőségeivel, következményeivel foglalkozni. Az, hogy mi legyen a következő lépés, az előre beprogramozott „menetrendjétől” függ. Ha csak diszkréten felhívja a biztonsági személyzet figyelmét a veszélyforrásra, már ez is óriási segítség, hiszen az ellenséges kezdeményezés (pl. tűznyitás) meglepetésszerű hatását hiúsítja meg.

A **képfelismerő és kiértékelő programok** feladata a tárgyak (később emberek) lehetőleg egyértelmű felismerése. Itt segíthetnek a repülőtéri csomagvizsgáló rendszerek számára kidolgozott gazdag adattárak is. Járművek, repülőgépek, fegyverek típusának felismerésénél segíthet a kép, hőeloszlás (infra-kép), sebesség, forma, egyes részletek, stb. A **3D¹¹ szkenneléssel** kialakított és valós időben aktualizált virtuális térben kell tájékozódniuk, mozogniuk, a célt megkeresniük, identifikálniuk és esetleg leküzdeniük. Ezek a rendszerek képesek a környezet legkisebb eltéréseit is felismerni, ezért például kiválóan alkalmazhatók az **IED¹²-k elleni védekezésben**. Például a fontos útvonalak rendszeres (légi, földi) monitorozásával időben figyelmeztetnek a gyanús, átvizsgálandó változásokra.

A robot viszont még nem érzékeli az embereknek fellépő személyiségváltozásokat, viselkedési zavarokat, stb. Az arcmmimika felismerését, illetve mesterséges arcmmimika létrehozását viszont már kutatják.

A világhálón, a téma után böngészgetve tudatosítottam, hogy meglepően sok embert foglalkoztatnak az **ember – robot témák**:

Egy érdekes blog¹³ a közlekedéssel kapcsolatban:

„Azt gondolom, hogy a KRESZ szabályainak többsége azért született, mert felismerték azt az egyszerű jelenséget, hogy az ember nem hibátlan. Nem lát minden irányba, mert noha a feje

¹¹ 3D - három dimenziós

¹² IED - Improvised Explosive Devices = rögtönzött robbanóeszközök

¹³ blog - internetes napló (bejegyzés), általában kereszthivatkozásokkal

*forgatható, általában nem jó fele fordítja. De aki úgy tűnik, helyes fejmozgással él, annak is tehetetlen a lába, keze. Lassan mozdul a kívánt irányba, nehézkesen változtatja meg az autó mozgását. De még aki úgy mozog, mint a villám, az is nehézkesen dönt. Sőt, akár rosszul. **Kész katasztrófa vagyunk az úton. Ezért jött a KRESZ...***

*...minek álljon meg egy... robotjármű a stopvonalnál? Ha nem érzékeli pontosan, hogy a száz méteres körzetében centire pontosan ki merre mozog, akkor úgyis nekimegy valaminek majd. Ezért pont a **robotjármű** lehetne az, amelynél el lehetne kezdeni újraértelmezni a KRESZ-t. **Ne az legyen a feladata, hogy betartson minden, emberek számára készült szabályt, hanem az, hogy biztonságon legyen képes megtenni azt az útszakaszt. Felőlem befordulhat megállás nélkül oda, ahova ember nem lát be, ha ő igen.**” [12]*

Az emberekkel összevetve a **robotok számára nincs „nehéz” döntés.** Ők egy szempillantás alatt a bemenő adatok, illetve a programjaik alapján döntenek! Ha esetleg valami miatt túlterhelt a számítógépe, akkor a „homokóráján” ugyan egy ideig „pereg a homok”, de a döntés biztosan jön. Ha az inputok alapján önállóan „döntésképtelen”, akkor a döntése: „kivárni”!

4. A robotok alkalmazásánál felmerülő problémák

A „Szárazföldi robottechnikai eszközök tervezésének és alkalmazásának biztonsági szempontjai” c. cikkemben az etikai elvárások megvalósításának a műszaki/technikai korlátaival már foglalkoztam. [13]

Vicc: Két vak ló beszélget:

- Indulsz a holnapi versenyen?
- Nem látom semmi akadályát!

A vicc akár robotokról is szólhatna, lényege: **megfelelő inputok**¹⁴ nélkül a döntéseik rosszak! **Elegendő, és megfelelő információkra van szükségük.**

Kulcsár Béla: „...az információknak az előállítására szolgálnak a szenzorok. A szenzor által előállított információnak olyan tulajdonságokkal kell rendelkeznie, hogy azok a robot irányítórendszere számára értelmezhető és értékelhető legyen.

...Az utóbbi időben a mobil robot megnevezés a külső szenzorral vezetett autonóm járművekre vonatkozik. Egy mobil robotot akkor nevezünk autonómnak, ha azt a feladatot, amelyre készült külső energia felhasználás nélkül hajtja végre és döntési képességekkel van felruházva.” [14]

A robotok informatikai részegységeinél szükségünk van **hiba-visszajelző rendszerekre**, amelyek segítségével a meghibásodott robotok ön-vezérlésébe időben beavatkozhatunk. A biztonságot növelik a **többszörösen redundáns**¹⁵ **rendszerek.** A kétszeresen biztosított rendszernél eltérő értékeknél nem tudjuk eldönteni, melyik a hibás. A triplex rendszereknél, ha két érték egyezik, akkor a harmadikat ignorálni lehet. Sajnos a megbízhatóság és az elvárt alacsony ár – ellentétben állnak egymással.

Kommunikációs problémák:

Nagyon fontos a zavarmentes, alacsony zajszintű, lehetőleg kódolt, kétoldalú információáramlás, ez csak jó minőségű rádióösszeköttetéssel lehetséges. A felderíthetőség és az energiafelhasználás szempontjából ez az állandó jelkibocsátás viszont hátrányos! Ha a távolság, a terepviszonyok miatt műholdakon, ill. több (átjátszó) szatelliten, reléállomásként működő UAV-ken keresztül történik a parancsadás, a késedelem (time-lap) miatt eltűnhet a célpont (pl. egy gyors repülőgép).

¹⁴ input = bemenet - az az út, amelyen keresztül az adatok a robot „agyába” (számítógépébe) jutnak

¹⁵ redundancia - a működéshez szükségesnél több, egymástól független részegység léte

Ha valamit, valamilyen rendszert jól akarunk kezelni, működtetni, ellenőrizni, szerelni, stb., akkor azt értenünk, ismernünk kell. Ez a nagyon **bonyolult rendszereknél** már egyre nehezebb, egy ember számára teljességgel **lehetetlen**. Példaként hoz

„A kutatást vezető Dr. Patrick Lin szerint van egy olyan félreértés, miszerint az emberek azt hiszik, hogy a robotok csak azt teszik, amire készítők beprogramozták őket. A valóság az, hogy a robotokba több millió kódot programoztak, különféle fejlesztő csapatok, így a teljes programot senki sem ismeri. Így azt sem tudja senki megjósolni, hogy ezek a programok milyen hatással lesznek egymásra.” [15]

Colin Allen, az Indiana Egyetem filozófusa: *„Az a kérdés, hogy építhetők-e olyan automata harcosok, amelyek betartják a hadviselés szabályait?”* Ronald Arkin (a Georgia Tech Egyetem robotkutatója) szerint a robotok ténylegesen jobb küzdők (harcosok) lehetnek” [16]

Számomra a fentiekből levonható tanulság: harcjármű- tervezőként [17] az én felelősségem is eldönteni, hogy egyáltalán tudunk-e olyan harci robotokat (azok részegységeit), önműködő rendszereket építeni- programozni-„életre kelteni”, alkalmazni amelyekkel biztonságosan be tudjuk tarttatni a hadviselés írott és íratlan szabályait?

Aki számítástechnikával foglalkozik, azt tapasztalja, hogy az elkerülhetetlen **program-frissítések** (update) ugyan az eddigi problémákat általában korrigálják, de egyben új (megoldandó) problémákat is generálnak... - és ennek soha sincs vége! Az egyes programok kapcsolódása, logikája is más- és más. Közismert, hogy *„kész program nincs, csak olyan, aminek abbahagyták a fejlesztését”*...

„A modern fegyverrendszerek töménytelen alkatrészből állnak, a világ minden részéből, és a (fegyver-) piacot egyre inkább átláthatatlanná teszik”. [18]

A GlobalSecurity.org igazgatója, John Pike szerint *„van egy sejtés arról, hogy mi vár ránk a jövőben. Ezeknek a valamiknek nincs családjuk. Nem ismernek félelmet. Olyan feladatokkal is megbízhatók, amik a katonáktól nem várható el”* [19]

Egyre több hadsereg fog a (közel-) jövőben felfegyverzett robotokat csatasorba állítani. Ez a katonai logika kikerülhetetlen következménye, hogy a **tűzerő és a gyorsaság** a legfontosabb tényezők egyike.

Az önműködően tüzelő robotokról egyelőre senki nem akar tudni, de ez a tartózkodó hozzáállás elegendő lesz ilyen rendszerek jövőbeni létrehozásának a megakadályozására?

Ha a robotoknak nincs elegendő (megfelelő) érzékelőjük, akkor nem látják akadályát, hogy tüzeljenek (ha minden, számukra meghatározott követelmény ezt számukra lehetővé teszi, előírja / parancsolja)... Németországban tömegpszichikai okokból még a „robot” szót is kerülik, helyette az „unbemannte Systeme”¹⁶-t használják [20]

Ellenérzést válthat ki a döntéshozóknál, hogy a túlzott (pl. etikai) biztosítások miatt a robotok az esetek többségében nem tudnak majd dönteni, operátor segítségét kérik. Ha ezt több raj egyszerre teszi meg, az operátor túl lesz terhelve, lelassul az akció...

5. Robotok által (?) okozott balesetek

A monsturmokkal, szörnyekkel, gépemberekkel (Gólem, Frankenstein, Terminátor, stb.) kapcsolatos elképzeléseink-félelmeink valószínűleg még az ősi hitvilágokba vezethetők vissza... Sajnos, a (mindennapos) közlekedési balesetek híreivel szemben lassan immunisak leszünk! Ha viszont egy állat (cápa-hisztéria), vagy robot okoz halálos balesetet, arra mindenki felfigyel - a társadalmunk nagyon érzékeny ezekre a dolgokra.

„A bonyolult kérdések a mindennapokban egyszerű, jól leírható esetekben nyilvánulnak meg. Két évvel ezelőtt például egy dél-afrikai lögyakorlaton egy harctéri robot, pontosabban egy Oerlikon GDF-005 típusú, digitális tűzvezetési rendszerrel felszerelt

¹⁶ unbemannte Systeme = ember nélküli rendszerek

légelhárító ágyú megölt kilenc katonát, és tizennégyet megsebesített, valószínűleg szoftverhiba miatt. Ugyancsak 2007-ben egy Dvorak típusú robotfűnyíró végzett egy dán munkással, idén áprilisban pedig egy svéd céget ítélt 25 000 koronás pénzbüntetésre a bíróság, mert egy kőszedő robot majdnem letépte egy szerelő fejét. A szerelő megúsza bordatöréssel. Az ilyen esetekre még könnyű legyinteni azzal, hogy nem sok van belőlük, illetve hogy itt nem etikai, hanem pusztán technikai problémákról van szó. Hogyan is lehetne számon kérni egy szimpla szoftveren a morális tartást?” [21]



7. kép. Gyorstüzelésű automata légelhárító rendszer

A jugoszláviai háború keretén belül (1999. május 7) bombázták a kínai nagykövetséget. Az első hivatalos közleményekben véletlenről, „pontatlan” felderítésről, „hibás”, nem aktuális várostérképről beszéltek ... Az ilyen és hasonló álközlemények amellet, hogy a közvéleményt tudatosan félreinformálják, a hírszerzés, illetve a műszaki rendszerek megbízhatóságába vetett hitet is rombolják.

„A 2003-as iraki események első napjaiban egy brit Tornádó repülőgépet lőtt le a kuvaiti leszállása előtt egy Patriot rakéta. A szakemberek a Patriot rendszer szoftverének meghibásodására (kudarccára) gyanakodtak.



8. kép. Patriot rakéta indítása

Egy nappal később egy amerikai F16-ost mért be egy Patriot radar. A pilóta automatikusan (ösztönösen) reagálva kilőtt egy HARM¹⁷ rakétát, valószínűleg ezzel mentette meg az életét. A kivizsgálásnál az derült ki, hogy a Patriot kezelői gránát(vetős) támadás miatt fedezékbe vonultak. A rendszer automata üzemmódban maradt és aktiválta magát amikor a repülőgép berepült a felügyelt területébe. Mindkét esetben valószínűleg az automatikus barát-ellenség felismerő rendszer (IFF) mondott csődöt.” [22] (A „Truppendienst” cikke alapján)

Az UAV-s balesetek nagyobbik része vezethető vissza emberi hibákra, ill. a fel- és leszállás kritikus fázisára.

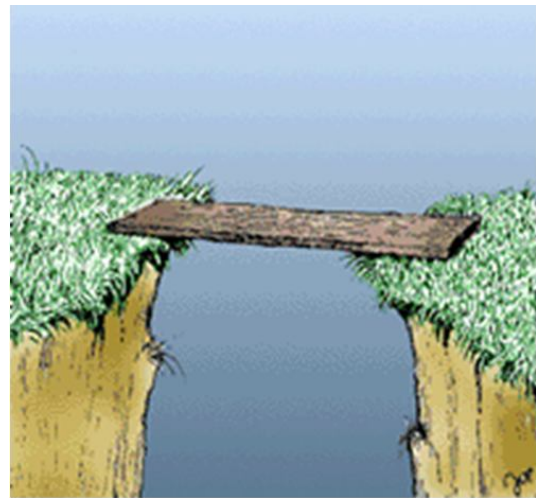
6. Robot, robot ellen?

A fejezet-cím nem vízió! Az előző fejezet egyik baleseténél ugyan akaratlanul „csapott össze” két magasan fejlett automata fegyverrendszer (a Patriot elhárító- és az F-16-os védőrendszere), de már ma is előfordul robotok tudatos bevetése robotok ellen. A Dél-Oszétiai konfliktusban egy orosz repülőgépről indított rakétával lőttek le egy grúziai UAV-t. Tehát a már „elengedett” rakéta robot-üzemmódban közelítette, ill. semmisítette meg a robotrepülőgépet, illetve ezzel együtt önmagát is.

Ma még a robotok az ilyen „megsemmisítő” találkozások mellett sokkal többre nem képesek, a harci robotok közötti együttműködés még gyerekcipőben jár... Mi történne például, ha a klasszikus népmese példáján a patak feletti pallón két robot találkozna? Ki engedne a másiknak, milyen alapon? Még csak nem is tanulnának az „összezőrrenésből”...



9. kép. „Big dog” robotok



10. kép. „A két kis kecske tudja már,
Hogyha nincs aki enged, végül bajjal jár.
Meeeeeeeeeeeeee.”¹⁸

Összegzés, következtetések

A robottechnika fejlődése megállíthatatlan. A cél az, hogy katonáink a jövőben a robotok segítségével, egymást kölcsönösen kiegészítve, kisebb hibaszázalékkal, kevesebb véráldozattal tudják a feladataikat ellátni. A több milliárd dolláros fejlesztések, sikeres (és sikertelen) bevetések sorozata után **az önműködő fegyverhasználatot megtiltani már**

¹⁷ HARM - High-speed Anti-Radar Missile = nagy sebességű lokátor elleni (radarromboló) rakéta

¹⁸ Psota Irén : Két kicsi kecske – dalszöveg (szövegíró Brand István)

bizonyosan nem lehet. Ezért a használatuk szabályozására kell törekednünk! Ne legyenek illúzióink, más (a „rossz oldal”) is fog (harci-, terrorista-) robotokat fejleszteni, illetve már fejlesztenek is. A gépeket sajnos, úgy is be lehet programozni, hogy „izmusokat” szolgáljanak, tüntetők ellen lépjenek fel, mindenre löjenek, ami mozog...

Minden robot egy potenciális fegyver? A gyorsabbak, nehezebbek már csak a mozgási energiájukkal is veszélyt jelentenek. A civil felhasználású autonóm robotok elterjedésének valószínűleg leginkább ez vet gátat.

Az írásom második részében részletesen térek ki a robothadviselés erkölcsi kérdéseire.

Hivatkozott irodalom

(Az internetes hivatkozások utolsó letöltési dátuma: 2009. 12. 09.)

- [1] http://robothadviseles.hu/eloadasok_rw9.html
- [2] Karel Čapek, Lidové noviny, 1933. 12. 24.; <http://capek.misto.cz/robot.html>
- [3] Várhegyi I. „Robotok és az információs hadviselés.” Hadtudományi Tájékoztató 2001/7. sz., II. rész, Budapest, 2001
- [4] Kucsera Péter: Autonóm működésű szárazföldi robotok védelmi célú alkalmazása Doktori (PhD) értekezés, 2009
http://193.224.76.4/download/konyvtar/digitgy/phd/2009/kucsera_peter.pdf
- [5] <http://www.nkth.gov.hu/nemzetkozi-tevekenysege/archivum/2009/szazeves-aeronautikai>
- [6] <http://www.dw-world.de/dw/article/0,,4108664,00.html>
- [7] Widersprüche um Unfall auf der A22
http://derstandard.at/fs/1231152924256?sap=2&_pid=11871583
- [8] http://de.wikipedia.org/wiki/Iron_Fist
- [9] <http://peoc3t.monmouth.army.mil/cram/cram.html>
- [10] Fire Shadow – ein loiterfähiges Wirkmittel <http://www.strategie-technik.de/02-09/spek.pdf>
- [11] Taktikai céltáblák az ESP cég honlapja
<http://www.eurosecurity.cz/eurosecurity.cz/index.php?link=cz/takticke-terce/takticke-terce.html&style=tactical-target>
- [12] <http://androidus.freeblog.hu/categories/kozlekedes/>
- [13] Koleszár Béla: Szárazföldi robottechnikai eszközök tervezésének és alkalmazásának biztonsági szempontjai. Hadmérnök, IV. Évfolyam 2. szám – 2009. június, pp 385-397
Kiadó: ZMNE; ISSN 1788-1919; http://hadmernok.hu/2009_2_koleszar.pdf
- [14] DR. habil Kulcsár Béla: Robottechnika, LSI Informatikai Oktatóközpont; Budapest, 2000; ISBN 963 577 243 2
- [15] http://renee.buzz.hu/archives/2009/10/02/Csak_azert_is_robotok/
- [16] <http://www.germancowboys.de/Business/2733>
- [17] <http://www.steyr-ssf.com/>
- [18] <http://reset.to/wissen/waffenhandel-0>

- [19] <http://www.spiegel.de/wissenschaft/mensch/0,1518,330745,00.html>
- [20] <http://www.heise.de/tp/r4/artikel/29/29720/1.html>
- [21] Újra kell írni a robotika három törvényét
http://index.hu/tudomany/2009/07/28/ujra_kell_irni_a_robotika_harom_torvenyet/
- [22] Friendly Fire - weiterhin ein Problem; Truppendienst 4/2003
<http://www.bmlv.gv.at/truppendienst/ausgaben/artikel.php?id=84>

Képek forrásai

1. kép http://1.bp.blogspot.com/_1WaO1OGuwzI/ShZRfRcvkRI/AAAAAAAAAJaI/WPE9xOZc7RU/s400/robot.jpg
2. kép <http://www.flightglobal.com/airspace/photos/farnboroughairshow2008/images/17554/500x375/schiebel-s100-camcopter.jpg>
3. kép http://www.dw-world.de/image/0,,2202610_4,00.jpg
4. kép http://www.inetres.com/gp/military/cv/tank/M1/M257_salvo.gif
5. kép http://defense-update.com/images/iron_fist1.jpg
6. kép a cseh Eurosecurity cég szíves engedelmével
7. kép http://www.rheinmetall-detec.de/img/skyguard_gr.jpg
8. kép http://www.raytheon.com/media/ausa08/Products/Patriot/PATRIOT_Missile.jpg
9. kép <http://www.thefutureisawesome.com/wp-content/uploads/2009/03/big-dog-robot-large.jpg>
10. kép http://lh5.ggpht.com/kartunboj/R8_izV-sCnI/AAAAAAAAAAvg/s7QFrHueWAw/anima3_thumb%5B2%5D

Koós Tamás

koos.tamas@zmne.hu

A GEOINFORMÁCIÓS TÁMOGATÁS KORSZERŰ ELEMEI, AVAGY ÚJ SZÍNFOLTOK A GEOINFORMÁCIÓS TÁMOGATÁS PALETTÁJÁN

Absztrakt

A szerző bemutatja a geoinformációs támogatás korszerű anyagait és termékeit a tervezett Magyar Honvédség geoinformációs támogatási doktrína tükrében.

The author reviews the up-to-date matters and products of geospatial support according to the draft Geospatial Support Doctrine of Hungarian Defence Forces.

Kulcsszavak: geoinformációs támogatás, távérzékelés, terepértékelés, térképészeti anyagok, geoinformációs termékek ~ geo-information support, remote sensing, terrain evaluation, cartographic materials, geo-information products

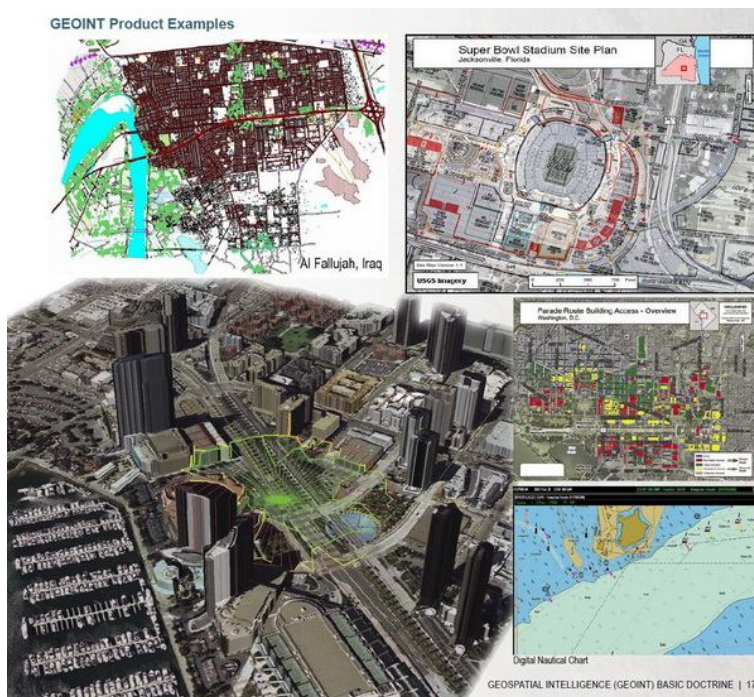
Bevezető

Napjainkban készítjük a geoinformációs támogatással kapcsolatos doktrínák új, modernizált kiadásait. A Magyar Honvédség Doktrinális Okmányok Fejlesztési Tervének (MH DOFT) megfelelően a Magyar Honvédség összhaderőnemi doktrína 2. kiadás (továbbiakban: ÖHD 2.) [1] felülvizsgálatának, módosításának, a Magyar Honvédség összhaderőnemi hadművelleti doktrína [2] és a Magyar Honvédség geoinformációs támogatási doktrína (továbbiakban: Geo) [3] kiadásának tervezett határideje 2010 tavasza.

A két felsőszintű doktrína (illetve tervezet) nem részletezi a geoinformációs támogatás tartalmát, de ismerteti a geoinformációs támogatással (ÖHD 2-ben még térképészeti és katonaföldrajzi támogatás néven) szembeni elvárásokat. (A térképészeti és katonaföldrajzi, illetve a geoinformációs támogatás fogalmának magyar és szövetséges értelmezésével a szerző egy korábbi [4] cikke foglalkozik.) A Geo tervezete tartalmazza a geoinformációs támogatás fogalmát, azonban az abban foglaltak a meteorológiai támogatásra vonatkozóan nem egyeznek NATO terminológiájával, mert a meteorológiai támogatás a NATO Térképészeti Politikája [5] szerint nem tartozik a geoinformációs támogatás feladatkörébe.

Ugyanakkor, véleményem szerint - mint ahogy a Magyar Honvédség térképészeti és katonaföldrajzi doktrína sem [6] - nem mutatja be kellő részletességgel a doktrínát alkalmazók részére, hogy mit is értenek a geoinformációs szakemberek a **távérzékelési-** és

egyéb térképészeti anyagok fogalma alatt. A hasonló célra készített amerikai GEOINT doktrína [7] (1. ábra) nem csak a szabatos és száraz megfogalmazásokat tartalmazza, hanem a nem szakemberek számára részletesen ki is fejtí azok fő tartalmi elemeit és egyszerű, szemléletes ábrákkal teszi azt még érthetőbbé.



1. ábra: Részlet a GEOINT doktrínából (Forrás: GEOINT doktrína)

A térképészeti anyagok és adatok (termékek) közül azért emelem ki e két témakört, mert ezek azok a „geoinformációs” anyagok, amelyek több, új típusú információt, ismeretet nyújtanak a felhasználóknak a terepről, mint az általuk már jól ismert és a mindennapi munkájuk során használt különböző topográfiai-, földrajzi és tematikus térképek, térképvázlatok és fototermékek (kontaktmásolatok, nagyítások, transzformátumok és ortofotók).

A geoinformációs termékek előállításának elsődleges célja a műveleti terület vizualizációja, a harcmező jellemzőinek realisztikus bemutatása minden szinten (hadászati, hadműveleti és harcászati) és minden térképi méretarányban. A speciális geoinformációs termékek jellemzője az informatikai eszközök és módszerek integrált alkalmazása az adatok előállítása, elemzések végrehajtása során, a fejlett technikájú érzékelők/szenzorok adatainak feldolgozása, a geoinformációs adatok széles skálájának használata, valamint a harmadik és a negyedik dimenzió szemléltetése, bemutatása.

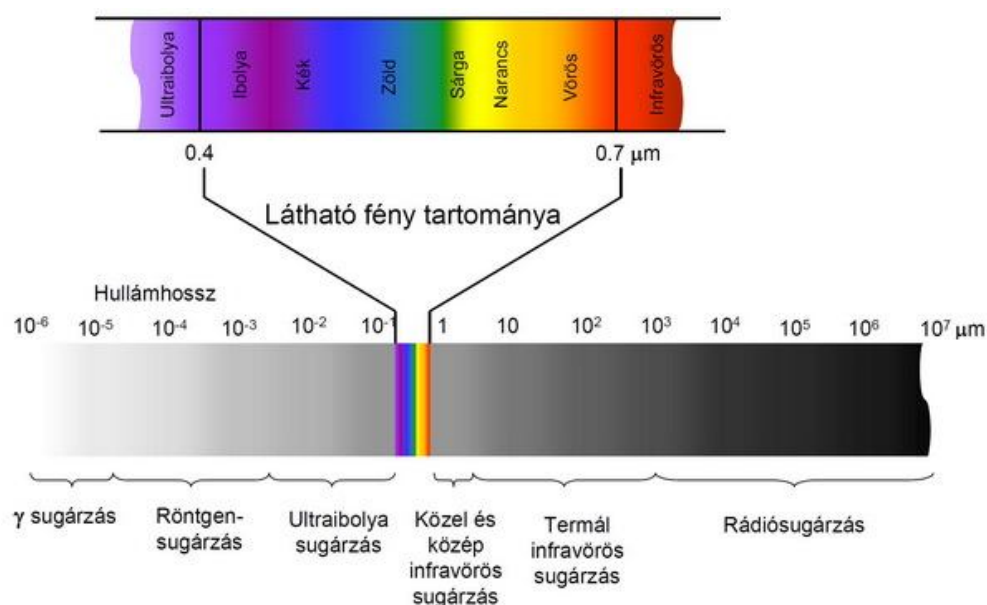
Távérzékelési anyagok

A távérzékelési anyagok fogalma a Geo alapján: „143. **A távérzékelési anyagok a terep felszínéről légifényképezéssel, űrfelvételek készítésével vagy más elektromágneses leképezési eljárás alkalmazásával készülnek.**”

E megfogalmazás alapján, az átlagfelhasználó számára nem egyértelmű, a Geo nem hangsúlyozza ki eléggé, hogy a fekete-fehér (pankromatikus) és színes képek mellett, ide

értjük a multi- és hiperspektrális képalkotó eszközökkel nyert anyagokat, a LIDAR¹, IFSAR² eszközökkel előállított digitális domborzat- (DDM³) és felület modelleket (DFM⁴) is.

A multi- és hiperspektrális képalkotó berendezések nem csak a látható fénytartományban (pankromatikus képek), illetve annak vörös-zöld-kék (RGB – Red-Green-Blue) hullámsávjában (band), hanem a szabad szemmel nem látható hullámhosszak zónájából is (2. ábra) képesek adatok gyűjtésére, akár több (multispektrális), vagy akár több tíz (hiperspektrális) szűk szektorban.



2. ábra: Az elektromágneses spektrum (Készítette a szerző)

A térinformatikában, hozzáférhetősége révén, a leggyakrabban alkalmazott Landsat műholdas képalkotó rendszerekkel (Multispectral Scanner –MSS, Thematic Mapper –TM és Enhanced Thematic Mapper Plus –ETM+) készített felvételek nem csak a térképezésben alkalmazhatóak, hanem a terep fedettségi jellemzőinek elemzésénél is (1. táblázat).

Hullámtartomány (Band)	Terepi felbontás		Spektrális felbontás	
	TM	ETM+	TM	ETM+
1 (kék - Blue)	30 m	30 m	0,45-0,52 μm	0,45-0,52 μm
2 (zöld – Green)	30 m	30 m	0,52-0,60 μm	0,53-0,61 μm
3 (vörös – Red)	30 m	30 m	0,63-0,69 μm	0,63-0,69 μm
4 (közel infra – NIR)	30 m	30 m	0,76-0,90 μm	0,78-0,90 μm
5 (közép infra – MIR)	30 m	30 m	1,55-1,75 μm	1,55-1,75 μm
6 (termál infra – TIR)	120 m	60 m	10,40-12,50 μm	10,40-12,50 μm
7 (közép infra – MIR)	30 m	30 m	2,08-2,35 μm	2,09-2,35 μm
8 (pankromatikus – PAN)	-	15 m	-	0,52-0,90 μm

1. táblázat: A Landsat TM és ETM+ szenzorok geometriai és spektrális jellemzői
(Forrás: http://landsat.usgs.gov/documents/ldcm_factsheet.pdf⁵ - 2009. 09. 27.)

¹ LIDAR (Light Detection and Ranging – fény érzékelés és távmérés)

² IFSAR (Interferometric Synthetic Aperture Radar – szintetikus nyílású interferencia radar)

³ Digitális Domborzat Modell: a magassági adatok a Föld felszínére - a talajszintre - vonatkoznak.

⁴ Digitális Felszín Modell: a magassági adatok a terep, a rajta lévő objektumok és tereptárgyak felülől látható felszínére vonatkoznak.

⁵ U.S. Geological Survey: Landsat Data Continuity Mission, Fact Sheet 2007–3093, 2007.

A több hullámsávban készített képek (3. ábra) felhasználásával különböző célokra állíthatók elő kompozit képek. A megszokott természetes színes képek a 3-2-1 csatornák keverékéből képezhetők.



Landsat TM - Band 1



Landsat TM - Band 2



Landsat TM Band - 3



Landsat TM - Band 4



Landsat TM - Band 5



Landsat TM Band - 6



Landsat TM - Band 7

3. ábra: A Landsat TM 7 érzékelési hullámsávjában készült képek (Várpalota és környéke)
(Készítette a szerző, alapanyagok a <http://glovis.usgs.gov> oldalról)

Mivel a különböző anyagok az elektromágneses hullámokat különböző intenzitással verik vissza (a képen világos területek), illetve nyelik el (sötét területek), az eltérő csatornák ötvözésével előállított képek (elsősorban az infra képek) alkalmasak a terep jellemzőinek (a felszint borító növényzet típusa, jellemzői, a talaj nedvességtartalma, az úthálózat és a felszíni vizek detektálása stb.) meghatározására (4. ábra).



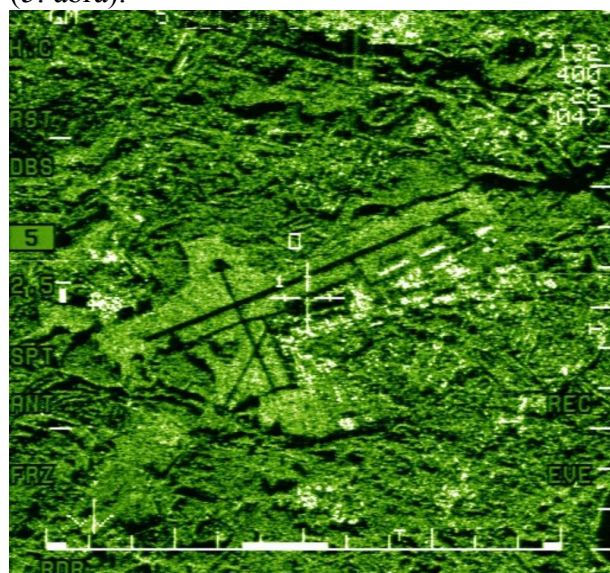
3-2-1 sávokból előállított természetes színes kép



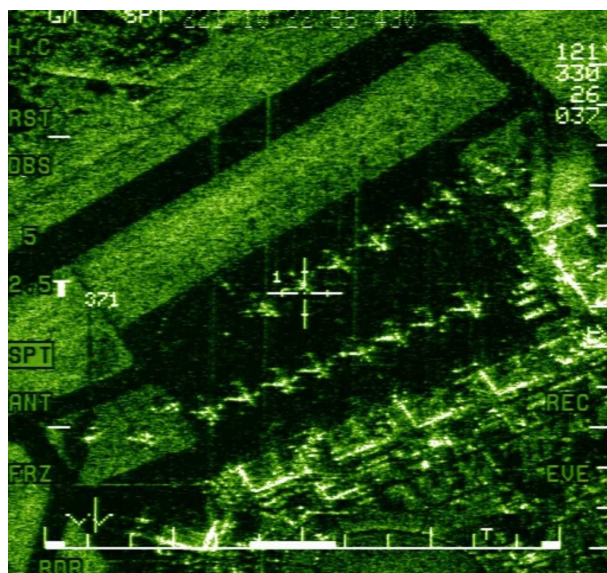
5-4-7 sávokból előállított hamisszínes kép

4. ábra: Landsat TM felvételeiből előállított kompozit képek
(Készítette a szerző, alapanyagok a <http://glovis.usgs.gov> oldalról)

Az egyéb elektro-optikai képalkotó és adatgyűjtő eszközökkel előállított távérzékelési termékek (infra- és termo képek, LIDAR és IFSAR adatok) digitális magasságmodellek, hőterképek előállítására alkalmasak, akár napszak és időjárási viszonyoktól függetlenül (5. ábra).



SAR



5. ábra: SAR⁶ képek

(Forrás: <http://www.airspace.net/TE-F-111-Upgrades-1998.html>⁷ - 2009. 09. 27.)

Katonai célokra természetesen a nagyobb terepi felbontású műholdképek, vagy a még jobb felbontású légifényképek, videofelvételek is alkalmazhatók (6. ábra).

⁶ SAR (Synthetic Aperture Radar – szintetikus apertúrájú radar).

⁷ Carlo Kopp: F-111 Upgrade Options, Australian Aviation, 2005.



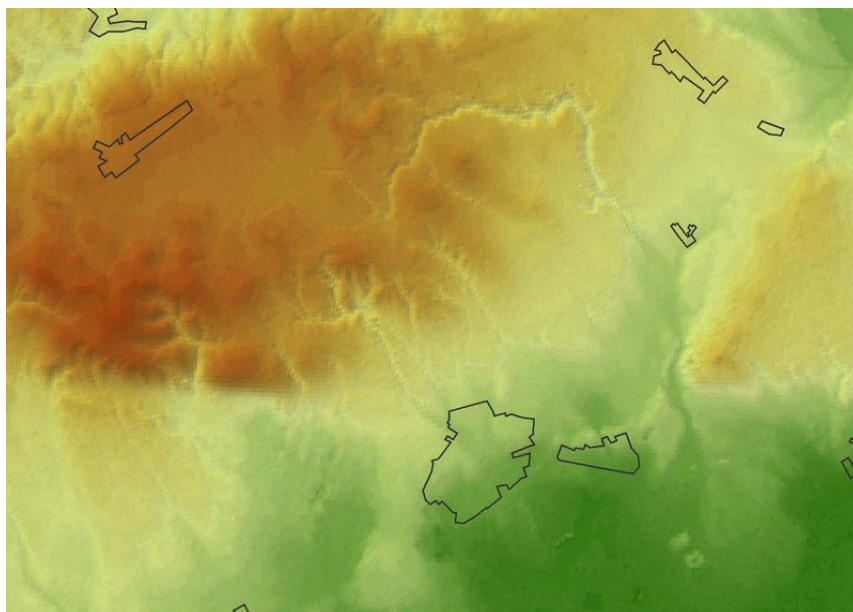
6. ábra: 0,125 méter felbontású ortofotó kivágat a ZMNE területéről
(Ortofotó: Telecopter Kft. 2007)

Egyéb térképészeti anyagok

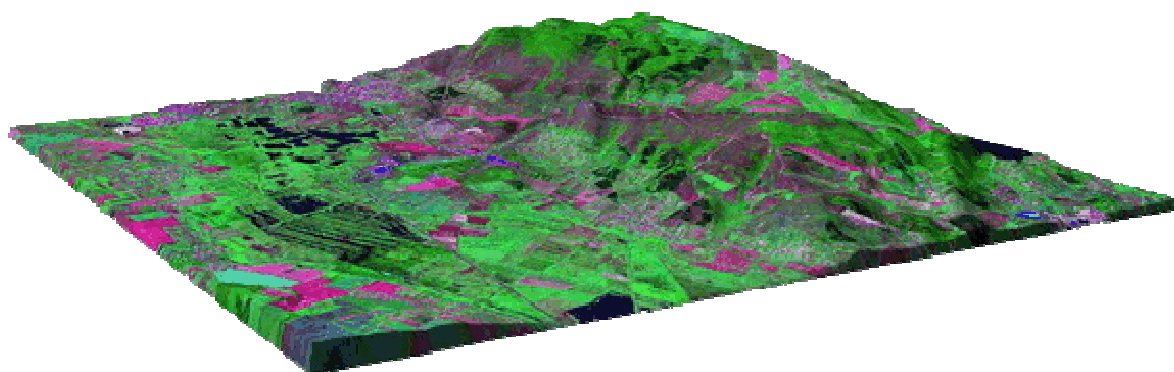
Az egyéb térképészeti anyagokat a Geo a következő képen definiálja: „145. **Egyéb térképészeti anyagok:** A térképészeti támogatás feladatainak végrehajtása során készített, a terepre vonatkozó vagy egyéb más információkat tartalmazó térképészeti anyagok. Általában egy-egy konkrét feladat végrehajtására sajátos igények kielégítésére, vagy oktatási célra készülnek.”

Az előző megfogalmazás hasonlóan - véleményem szerint - a Geo itt sem részletezi kellő mélységgel, hogy a „terepre vonatkozó vagy egyéb más információkat tartalmazó térképészeti anyagok”-hoz soroljuk a következő térbeli elemzések termékeit:

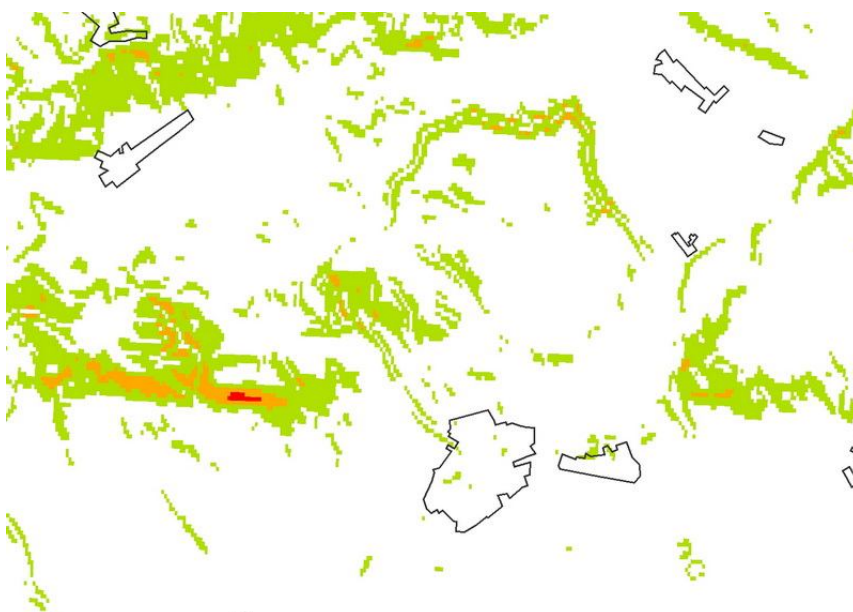
- katonai szempontból lényeges terepjellemzőket bemutató fedvényeket (lakott területek, növényzeti fedettség, közlekedési-, vízrajzi hálózat),
- domborzati viszonyokat szemléltető anyagokat (térképeket (7. ábra), anaglif- és perspektív képeket (8. ábra)),
- lejtőkategória térképeket (a lejtő meredekség szerinti osztályozása) (9. ábra),
- összeláthatósági vizsgálatokat (két pont közötti hosszmetset),
- láthatósági vizsgálatokat (egy pontból történő figyelés, beláthatóság) és a
- terepet bemutató videókat.



7. **ábra:** Terep domborzati viszonyai (Készítette a szerző, alapanyag a <http://srtm.csi.cgiar.org> oldalról)



8. **ábra:** Perspektív kép a terepről (Készítette a szerző alapanyag a fenti oldalakról)



9. **ábra:** A terep osztályozása lejtőkategória szerint (Készítette a szerző, alapanyag a <http://srtm.csi.cgiar.org> oldalról)

Ezen speciális geoinformációs termékek alkalmazása megkönnyíti és hatékonyabbá teheti a döntéshozatali rendszert.

Összegzés

Ahhoz, hogy a katonai műveleteket gyorsan és hatékonyan meg tudjuk tervezni, ma már nem nélkülözhetjük a geoinformációs támogatás különféle korszerű anyagainak és termékeinek (távérzékelési- és egyéb térképészeti anyagok) alkalmazását.

Ezeket a produktumokat a Magyar Honvédségben már nem csak központilag lehet legyártani, hanem a Terepelemző Munkaállomásokkal rendelkező csapatok, a sajátos céljaiknak megfelelő, kispéldányszámú tematikus térképeket elő is tudják állítani. Ennek egyik feltétele, hogy a végrehajtásban az adott területet és a geoinformációs támogatás speciális termékeit és azok előállítását is ismerő, kiképzett térinformatikus szakember, szakemberek vegyenek részt.

Felhasznált irodalom

1. Ált/27 - Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás, MH DSZOFT kód: 11313, 2007.
2. Magyar Honvédség Összhaderőnemi Hadművelési Doktrína (tervezet), MH DSZOFT kód: 15011, ZMNE, 2009.
3. Magyar Honvédség geoinformációs támogatási doktrína (tervezet), MH DSZOFT kód: 11516, MH GEOSZ, 2009.
4. Koós Tamás: Térképészeti és katonaföldrajzi támogatás - Geoinformációs támogatás, Kari tudományos találkozó „2008”, ZMNE KLHTK, 2008.
5. MC 296/1 (Final) - NATO Geospatial Policy, 03. February 2006.
6. Magyar Honvédség térképészeti és katonaföldrajzi doktrína, MH DSZOFT kód: 11431, MH TÉSZ, 2004.
7. Publication 1-0 – National System for Geospatial Intelligence, Geospatial Intelligence (GEOINT) Basic Doctrine, National Geospatial-Intelligence Agency NGA, September 2006.
8. Koós Tamás: A harcvezetési rendszerekben alkalmazható digitális magasságmodellek és azok jellemzői, Hadmérnök, III. Évfolyam 4. szám 2008. december

Krasznay Csaba

csaba@krasznay.hu

SZOFTVERFEJLESZTŐI KÖVETELMÉNYEK MINŐSÍTETT KÖRNYEZETBEN: ADMINISZTRATÍV KÖVETELMÉNYEK

Absztrakt

A közigazgatás elektronizálása korábban nem látott ütemű és kiterjedtségű szoftverfejlesztéseket tett szükségessé olyan környezetekben is, melyek a Magyar Köztársaság működése szempontjából közvetve vagy közvetlenül kritikusak. A kifejlesztésre kerülő rendszerek azonban a legtöbbször nem szigetyszerűen működnek, közvetlenül nem kezelnek állam- és szolgálati titkokat, így nem érvényesek rá a Titokvédelmi Törvény elvárásai. Jelen tanulmány bemutatja, hogy milyen személyi, szervezeti és szabályzati követelményeket kell szabni azon fejlesztőkkel és a fejlesztői környezettel szemben, akik ilyen, többnyire a 143/2004-es kormányrendelet keretében dolgoznak.

Electronization of public administration needs such enormous software developments as never before in high level security environments which are directly or indirectly critical for the normal operation of the Hungarian Republic. Most newly developed system doesn't operate alone, doesn't handle state secrets directly so the requirements of the State Secrets Protection Act are not valid for this area. The study, which is the first part of a two-part series, presents personnel, organizational and policy requirements for those developers and environments who work in the context of Edict 143/2004 about public procurement related to state secrets.

Kulcsszavak: közigazgatás, szoftver fejlesztés ~ public administration, software development

Bevezetés

Napjaink általános szoftverfejlesztéseiről – melyek közé a legtöbb e-közigazgatási projekt is tartozik – elmondható, hogy bár a biztonság erős kritériumként jelenik meg, ez elsősorban a fejlesztett funkciókra és nem a fejlesztői környezetre vonatkozik. Pedig gyakori, hogy a fejlesztők nem egy adott telephelyen dolgoznak, hanem otthonról, internetes kapcsolaton keresztül, nem kontrollált munkaállomásokon, hanem saját számítógépen, és olyan fejlesztést segítő eszközök felhasználásával, melyek a projekt általános biztonsági szintjének az elvárásait nem teljesítik. Ennek eredménye, hogy a kódok nem megfelelően kontrollált környezetben keletkeznek, továbbítódnak és tárolódnak, így komoly, akár egy-egy kritikus államigazgatási folyamatot is érintő bizalmassági és sértetlenségi kockázatok jelentkeznek.

A szoftverfejlesztési életciklus biztonsági vonatkozású része minden esetben egy kockázatelemzéssel kezdődik, melynek során fel kell mérni, hogy a kifejlesztésre kerülő termék pontosan milyen információs vagyont fog kezelni. Az életciklus során végig figyelembe kell venni az információs vagyron besorolását, tehát nem elégséges, hogy csak az élesüzemű működés során gondoskodunk a megfelelő védelemről. Már a tervezéstől kezdve folyamatosan biztosítani kell, hogy bármilyen, a rendszerrel kapcsolatos információ olyan védelmi szintű biztosítást kapjon, amelyet majd a végleges rendszer kap. A fejlesztői környezet kialakításánál tehát fő elvként az éles rendszerrel kell párhuzamot vonni. Azok az alkalmazások, melyeket köztisztviselők tízezrei használnak majd az interneten keresztül, egészen más fejlesztői környezetben alakulhatnak ki, mint azok, melyeket csak néhány száz felhasználó láthat szeparált, lokális hálózatról. A tanulmányban éppen ezért három védelmi szintet lehet meghatározni, mely megfelel a Közigazgatási Informatikai Bizottság (továbbiakban KIB) 25. [1] és 28. számú ajánlásában [2] leírt három szintnek: az államtitkot feldolgozó rendszerek (kiemelt), a belső használatú, bizalmas információkat kezelő rendszerek (fokozott), valamint a széles körben, interneten keresztül hozzáférést biztosító rendszerek (alap) fejlesztőire határozzuk meg követelményeket.

Jogsabályi követelmények

Az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 143/2004. kormányrendelet [143/2004. (IV. 29.) Korm. rendelet az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól] (a továbbiakban: Rendelet) hatálya azokra a Közbeszerzési törvény [2003. évi CXXIX. törvény a közbeszerzésekről] (a továbbiakban: Kbt.) szerinti egyszerű közbeszerzési eljárás mindenkorai értékhatárait elérő vagy azt meghaladó értékű beszerzésekre terjed ki, melyek – a Rendelet címének megfelelően – államtitkot, szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintenek, illetve különleges biztonsági intézkedést igényelnek.

A Rendelet értelmező részében kerül meghatározásra két, máshol nem definiált fogalom, az alapvető biztonsági érdeket érintő és a különleges biztonsági intézkedést igénylő beszerzés fogalma. Az ország alapvető biztonsági érdekével kapcsolatos a beszerzés, ha a beszerzés tárgya közvetlenül kapcsolódik az ország lakosságának fizikai, környezeti, egészségügyi, gazdasági, honvédelmi biztonságát befolyásolni képes építési beruházáshoz, árubeszerzéshez, illetőleg szolgáltatás megrendeléséhez. Különleges biztonsági intézkedést igényel a beszerzés, ha a beszerzés tárgyának előállításánál, az előállításához szükséges alapanyagok és termékek szállításánál, illetőleg a felhasználásnál, a beszerzés tárgyának szállításánál hatóság vagy

jogszabály különleges követelményt ír elő, illetve az általánostól eltérő előírás vagy technikai ellenőrzés szükséges. Azért is fontos ez a két fogalom, mert akkor is lehetővé teszi a Rendelet alkalmazását, ha a beszerzés tárgya államtitkot, szolgálati titkot, illetőleg nemzetbiztonsági érdeket nem érint.

A Rendelet nagyon részletesen szabályozza az ajánlattevők ellenőrzését, magát a beszerzési eljárást, de a beszerzési eljárás utáni, a teljesítés biztonsági követelményeire vonatkozó előírást, vagy elvárást nem ad. Persze erre nem is lenne szükség, ha ezek a követelmények máshol megjelennének. Nézzük részletesen a követelményekre vonatkozó előírásokat informatikai fejlesztések esetén.

Ha a beszerzés államtitkot, szolgálati titkot érint, akkor az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény (a továbbiakban: titoktörvény), továbbá a minősített adat kezelésének rendjéről szóló 79/1995. (VI. 30.) Korm. rendelet lenne a mérvadó. Jelenleg azonban ezek a jogszabályok nem jutnak érvényre, tudniillik a titoktörvény 30. §-ának (2) bekezdése előírja, hogy a “Kormány - az érintett állami szervek vezetőivel egyetértésben - a minősített adatot kezelő információs rendszerek létesítésének és működésének rendjét 1995. december 31-ig határozza meg”. Ez a nemzeti titkaink vonatkozásában a mai napig nem történt meg. A titoktörvény új változata 2002 óta parlament általi elfogadásra vár. Emiatt a kormány már nem kíván a régi titoktörvény szerinti szabályozással foglalkozni.

Ez viszont azt jelenti, hogy a nemzeti titkaink vonatkozásában nincs érvényes jogi előírás erre a területre vonatkozóan. Persze van azért ebben a témakörben – nem jogi, hanem logikai alapon – felhasználható előírás. A rejtjeltevékenységről szóló 43/1994. (III. 29.) Korm. rendelet 16. § (1) bekezdése például a rejtjelzőeszközök vonatkozásában előírja, hogy “fejlesztő, gyártó, javító munkahelyet ... megfelelően őrzött, illetve megfelelő biztonsági felszerelésekkel ellátott, elkülönített helyiségben kell elhelyezni, ahová az oda beosztottakon kívül csak az irányítási és ellenőrzési joggal rendelkezők léphetnek be”. A jelenleg hatályos magyar jogszabályokban a minősített adatot kezelő információs rendszerekre vonatkozóan más előírás nem található.

Ha a beszerzés alapvető biztonsági, nemzetbiztonsági érdeket érint, illetve különleges biztonsági intézkedést igényel, akkor sem találunk útmutatást a magyar jogszabályi rendszerben. Ugyanis az alapvető biztonsági, nemzetbiztonsági érdeket érintő beszerzések megvalósítása során követendő biztonsági elvárásokra nincs előírás. Tulajdonképpen a Rendelet szerinti valamennyi eljárásban a beszerzés tárgyának előállításánál, az előállításhoz szükséges alapanyagok és termékek szállításánál, illetőleg a felhasználásnál, a beszerzés tárgyának szállításánál az ajánlatkérőnek – esetleg az illetékes nemzetbiztonsági szolgálatnak – kellene különleges követelményt előírni. Ilyen követelményrendszernek azonban semmilyen nyilvános említése nem ismert.

Személyi és szervezeti követelmények

Mindhárom környezetben közös, hogy nem szabad a fejlesztőknek előzetes kontroll nélkül hozzáférést adni a fejlesztői környezethez, nem lehet őket felügyelet nélkül dolgozni hagyni, és ki kell találni, hogy milyen módon lehet hozzáférésüket megszüntetni. Ehhez fel kell állítani egy olyan belső biztonsági irányítási és ellenőrzési szervezetet, mely a fejlesztőket munkájuk során kontrollálni tudja. Erre a KIB 25. számú ajánlásának 1-2. kötete [1] ad ajánlást, mely szerint ki kell jelölni a Biztonsági Vezetőt, az Informatikai Biztonsági Vezetőt, az Informatikai Biztonsági Fórumot, valamint a szakterületi (fejlesztési és üzemeltetési)

vezetőt. Ezt a biztonsággal kapcsolatos szervezeti felépítést mindhárom területen érdemes betartani.

A fejlesztéssel megbízott szervezet vezetője, vagy kiemelt projekteknel a fejlesztés projektvezetője az Informatikai Biztonsági Fórum vezetője, azaz a biztonsági terület elsődlegesen neki tartozik beszámolóval.

Feladata:

- hatályba lépteti az Információbiztonsági Szabályzatot,
- értékeli a kockázatelemzést,
- felülvizsgálja az információk osztályozását,
- meghatározza a munkavégzés helyszíneit,
- utasítja a vállalkozókat információbiztonsági kérdésekben,
- kezdeményezi a felhasználói jogosultságok visszavonását, elrendeli az azonnali visszavonást,
- engedélyezi új eszközök beszerzését,
- értékeli az incidenseket.

Felelős:

- az adatvagyonleltár naprakészen tartásáért,
- az információbiztonsági tudatosság építéséért,
- a speciális információbiztonsági tudás megszerzésének biztosításáért,
- a képzések értékeléséért,
- a szankcionálásért,
- a belső auditok elrendeléséért és értékeléséért.

Az Informatikai Biztonsági Fórumot, és általában a fejlesztési projektet egy adminisztratív szervezet, a projektiroda támogatja, akiknek szerepet lehet adni a biztonsági keretrendszerben is.

Feladata:

- hardver- és szoftvereszközök nyilvántartása,
- a belépési naplók archiválása,
- a jogosultságok nyilvántartása,
- a forráskódok őrzése,
- az üzemeltetési feljegyzések őrzése.

Felelős:

- a jogosultságok kiadásáért és visszavonásáért.

A Biztonsági Vezető és az Informatikai Biztonsági Vezető szerepkört ugyanaz a személy is betöltheti az ajánlás szerint. A fejlesztési környezet biztonsági aspektusaiért elsősorban ő a felelős.

Feladata:

- az adatvagyonleltár elkészítésének támogatása,
- védelmi intézkedések megfogalmazása,
- az Informatikai Biztonsági Fórum és a fejlesztési/üzemeltetési vezető támogatása információbiztonsági kérdésekben,
- a vagyontárgyak kiadásának és visszavételének felügyelete,
- a kiemelt jogosultságok ellenőrzése,
- a karbantartási terv jóváhagyása.

Felelős

- az adatvagyonleltár rendszeres felülvizsgálataért,
- a kockázatelemzés elkészítéséért,
- a sebezhetőségvizsgálat elkészítéséért,
- a védelmi intézkedések bevezetéséért,
- a vállalkozók információbiztonsági szabályzatainak felülvizsgálataért,
- az Informatikai Felhasználói Szabályzat kidolgozásáért és karbantartásáért,
- az információbiztonsági oktatásokért,
- a belső auditok végrehajtásáért,
- a szabálysértések kivizsgálásáért,
- vállalkozók telephelyeinek ellenőrzéséért,
- az információbiztonsági eszközök karbantartásáért,
- a jogosultságok ellenőrzéséért,
- az üzemeltetés és a fejlesztés biztonsági ellenőrzéséért,
- az új rendszerek biztonságos üzembe állításáért,
- a megfelelő visszaállításért,
- az információbiztonsági incidensek kezeléséért,
- az üzletmenet-folytonossági intézkedések kialakításáért.

A fejlesztési vezető elsősorban az alkalmazás biztonságáért felelős, a fejlesztői környezet biztonságával kapcsolatban viszonylag kevés feladata van.

Feladata:

- A fejlesztés során keletkezett információk Információbiztonsági Szabályzat szerinti kezelése

- A Biztonsági Vezető és az Üzemeltetési Vezető támogatása az Információbiztonsági Szabályzatban leírtak teljesítésében.

Felelős:

- A fejlesztés során keletkezett információk minősítéséért,
- A fejlesztői jogosultságok kiosztásáért

Az Üzemeltetési Vezető az a személy, aki a fejlesztéshez használt eszközök üzemeltetéséért felelős. A Biztonsági Vezetővel közösen felel a biztonságos fejlesztői környezet kialakításáért.

Feladata:

- a projektiroda támogatása,
- új eszközök specifikálása,
- az erőforrás-kihasználás ellenőrzése,
- az incidensek értékelése.

Felelős:

- a kiemelt jogosultságokért,
- az üzemeltetési folyamatokért,
- a rendszerfejlesztés koordinálásáért,
- az üzemeltetési rend kialakításáért,
- a vírusvédelemért,
- a mentésekért,
- a visszaállítáért,
- a határvédelmi eszközök üzemeltetéséért,
- a karbantartásért,
- a hibabejelentések kezeléséért.

Fontos, hogy ezek a szerepkörök megfelelően megbízhatók legyenek, ezért a szerződéskötés során nevesíteni és ellenőrizni kell őket. A projektvezető a közigazgatási fejlesztések esetén mindenkor nemzetbiztonsági ellenőrzésen esik át, alap esetben A típusú, fokozott esetben B típusú, kiemelt esetben C típusú átvilágítást kell igazolnia. A projektiroda munkatársai, a Biztonsági, Fejlesztési és Üzemeltetési vezető alap esetben erkölcsi bizonyítvány benyújtására kötelezett, fokozott esetben A típusú, kiemelt esetben B típusú átvilágításon kell átesniük. A Biztonsági Vezetőnek emellett rendelkeznie kell az ISACA Certified Information System Manager (CISM) vizsgájával, mely nemzetközileg elfogadott biztosítékot ad arról, hogy képes feladatát teljesíteni. Kiemelt szinten a Biztonsági Vezető a felelős a titkos ügyiratkezelésért is, ezért Titkos ügykezelő bizonyítvánnyal kell rendelkeznie.

A fejlesztésben résztvevő, valamint a fejlesztői környezetet üzemeltető személyek ellenőrzése is kritikus. Alap és fokozott esetben minden érintettnek erkölcsi bizonyítvánnyal kell rendelkeznie, be kell nyújtania önéletrajzát és iskolai bizonyítványait. Fokozott esetben a

vállalkozónak háttérellenőrzéssel kell ezeket kiegészíteni, mely során meggyőződik a benyújtott iratok és információk hitelességéről, valamint nyílt források felhasználásával győződik meg az érintett megbízhatóságáról. Kiemelt esetben mind a fejlesztőknek, mind az üzemeltetőknek B típusú nemzetbiztonsági ellenőrzést kell teljesíteniük.

Szabályzati követelmények

Mivel a megrendelőnek érdemi beleszólása nincsen a fejlesztés folyamatába, így szerződéses feltételként kell megfogalmaznia azt az igényét, hogy a fejlesztés biztonságát ellenőrizhesse. Erre három lehetséges megoldás van.

- Előírhatja a Common Criteria vagy KIB 25. szerinti fejlesztést, melynek részeként a megrendelő által megbízott auditor ellenőrizheti a fejlesztés biztonsági környezetét. Hátránya, hogy a Common Criteria módszertan nem szab konkrét követelményeket, deklarálta az auditorra van bízva annak eldöntése, hogy a környezet megfelelően biztonságos vagy nem az, de azért a szabályozandó területeket meghatározza. Alap, közép és kiemelt szinten is kötelező lehet.
- Elrendelheti a fejlesztés nemzetbiztonsági ellenőrzését. Ilyenkor a teljes fejlesztési folyamat kontrollálható, hátránya viszont, hogy még annyi viszonyítási alapja sincs a fejlesztőnek a környezet kialakításához, mint a Common Criteria esetében. Fokozott szinten opcionális, kiemelt szinten kötelező lehet.
- Elvárhatja az ISO 27001-es tanúsítvány meglétét a fejlesztési folyamatra. Ekkor a megrendelő megbízza egy általa nem felkért harmadik személyben, és elfogadja, hogy a fejlesztő által benyújtott fejlesztés-biztonsági dokumentumok helytállóak. Ez a megoldás objektív, hiszen a szabvány konkrét védelmi intézkedéseket tartalmaz, melyek működésének ellenőrzése is szabvány szerint történik, hátránya viszont, hogy az értékelést végzővel semmilyen közvetlen kapcsolata nincs a megbízónak. Alap szinten opcionális, fokozott és kiemelt szinten kötelező lehet.

Mindhárom esetben elvárható az alkalmazás fejlesztőjétől, hogy biztonsági tevékenységeit megfelelően dokumentálja. A legkézenfekvőbb megoldás erre egy olyan szabályzati rendszer létrehozása, mely kielégíti mind a szabványok, mind a jogszabályok jelentette követelményeket. A KIB 25. ajánlás Informatikai Biztonsági Irányítási Rendszerrel foglalkozó része pontosan megnevezi, hogy milyen elemekből kell állnia egy szabályzati rendszernek, melyet három szintre lehet osztani.

- **Informatikai Biztonsági Politika (IBP):** „Az Informatikai Biztonsági Politika kinyilvánítja a menedzsment biztonság iránti elkötelezettségét, a biztonsági célt, valamint magas szintű biztonsági elvárásokat fogalmaz meg, amelyek a biztonsági cél elérését szolgálják, és amelyeket érvényesíteni kell a védelmi intézkedések specifikálása során.”
- **Informatikai Stratégia:** „Az Informatikai Biztonsági Stratégia célja, hogy a szervezet üzleti igényeinek jövőbeni változásaival összhangban meghatározza az információbiztonság fejlesztésének tervét (középtávú, hosszú távú).”
- **Informatikai Biztonsági Szabályzat (IBSZ):** „Az Informatikai Biztonsági Szabályzat rögzíti az IBIR működéséhez, működtetéséhez szükséges folyamatokat,

megadja az érintett szereplők (pl.: információbiztonsági vezető, üzemeltető, rendszergazda, fejlesztési vezető, adatgazda stb.) feladatait, felelősségeit, hatásköreit. Rögzíti az információfeldolgozó rendszer elemeivel (dolgozók, alkalmazások, technológiai elemek, helyiségek stb.) kapcsolatos biztonsági követelményeket. Az Informatikai Biztonsági Szabályzatot olyan mélységig kell elkészíteni, hogy technológiafüggetlen tudjon maradni.”

- **Informatikai Felhasználói Szabályzat (IFSZ):** „A dokumentum részletesen szabályozza a felhasználók kötelelességeit az informatikai eszközök használata során, meghatározza azokat a peremfeltételeket, melyek között a felhasználó kapcsolatot létesít az informatikai osztállyal, vagy az adatgazdákkal. A szabályzat részletesen kifejti a felhasználó által elvégezhető és tiltott tevékenységeket, megadja a számonkérés formáját és módját, rögzíti a biztonsági események jelentésével kapcsolatos kötelezettségeket.”
- **Eljárásrend gyűjtemény:** „Az eljárásrend gyűjteménybe tartozó végrehajtási utasítások olyan alacsony szintű szabályzatok, amelyek részletesen, rendszer specifikusan rögzítik azokat a tevékenységeket, melyeket az informatikai biztonsági szabályzat rendszerfüggetlenül megkövetel.”

Az IBP és a Stratégia alkotja a szabályzati rendszer első szintjét, az IBSZ és az IFSZ a másodikat, az eljárásrend pedig a harmadikat. Ezeknek koherens egésznek kell alkotniuk, nem szabad ellentmondásokat létrehozni, melyről a fejlesztőket értékelő szervezetnek is meg kell győződnie.

A gyakorlatban a fejlesztési folyamatot nem kizárólag egy szervezet fedi le, hanem egy fővállalkozó és több alvállalkozó együttesen. Ilyenkor különösen nehéz megállapítani, hogy ki, mennyire tudja betartani az elvárt biztonsági szintet. Alapelvként a megrendelőnek arról kell meggyőződnie, hogy a fővállalkozó, aki elsődlegesen felelős a projekt sikeres végrehajtásáért, megfelelő szabályzati rendszerrel dolgozik. Az alvállalkozóknak minden esetben minimálisan a fővállalkozó szabályzataiban foglalt elveket kell teljesíteniük, ezeknél alacsonyabb biztonsági szint nem megengedett. Ez a megoldás kellően rugalmas, mégis biztonságos lehet.

Az alvállalkozók ellenőrzése minden esetben a projekt Biztonsági Vezetőjének a feladata, aki ezt belső auditok során teszi meg. A belső auditokról készített feljegyzések, valamint a szűrőpróbaszerű ellenőrzés ad garanciát arra a megrendelő által megbízott külső auditornak, hogy a fejlesztésben részt vevő minden szervezet megfelelő biztonsági szinten dolgozik.

ÖSSZEFOGLALÁS

A tanulmányban bemutatásra került, hogy egy, a közigazgatás működése szempontjából fontos alkalmazás létrehozása során milyen szervezeti, személyi és szabályzati követelményeket kell betartania a fejlesztőknek. A cikk következő, második részében bemutatásra kerülnek azok a műszaki szabályok, melyekhez ebben a környezetben alkalmazkodni kell. Ehhez a jelenleg hatályos ajánlások szellemében kell szabályokat alkotni, ugyanis közvetlen előírások nincsenek ezen a területen.

Irodalomjegyzék

- [1] Berkes, Z., Déri, Z., Krasznay, Cs., Muha, L. (2008): Közigazgatási Informatikai Bizottság 25. számú ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA) 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR)
- [2] e-Közigazgatási Keretrendszer Kialakítása projekt (2008): A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár, IT biztonsági műszaki követelmények

Kucsera Péter

kucsera.peter@kvk.uni-obuda.hu

AUTONÓM KIÁLLÍTÁSI MOBILROBOT FEJLESZTÉSE

Absztrakt

A cikkben egy valóságban kivitelezett autonóm működésű mobil robot kerül bemutatásra. A robot kiállításokon, vásárokon, az emberek között mozogva képes magára felhívni a látogatók figyelmét, a rajta elhelyezett reklámfelületek segítségével pedig a megbízó cégeket reklámozni. A fejlesztés során ipari komponensek kerültek alkalmazásra, mivel fontos szempont volt a megbízható, stabil működés. Az automatizálási és hajtás komponensek a Phoenix Contact termékpalettájáról, míg a szenzorok a Sick Sensors eszközei kerültek kiválasztásra, a fejlesztést e két cég szponzorálta. A robot sikeresen megépítésre került a Kándó Kálmán Villamosmérnöki Kar Műszertechnikai Intézetében és első ízben nagy sikerrel mutathattuk be a Magyar Regula 2009 automatizálási szakkiallításán. A cikkben a robot fejlesztésének lépéseit, a szerzett tapasztalatokat ismertetem.

In this article an autonomous advertising mobile robot that has been realized in practice is going to be described. The whole development is based on industrial components. In the controlling and communication part, Phoenix Contact products were used, whereas the sensing was based on a Sick Laser Scanner. These two companies donated the whole project, and the final aim was to build up a working robot, which should advertise the companies on Hungarian and international exhibitions. The robot was successfully built up in the Process automation lab of the Budapest tech. Kando Kalman Faculty of Electrical Engineering and was exhibited with great success on Regula 2009, which is the biggest Hungarian automation exhibition.

Kulcsszavak: mobil robot, ipari komponensek, PLC, lézer szkennel, szenzor ~
mobile robots, industrial components, PLC, laser scanner, sensor

A fejlesztés célja egy olyan autonóm mobil robot megalkotása volt, amely képes sík terepen, alacsony sebességgel (max. 2 km/h) dinamikus környezetben, emberek között manőverezni. Elvárás volt a folyamatos legalább 1 órás működés. A robot a kiállítás területén haladva egy monitoron futó videó, vagy kép alapú reklámanyag segítségével képes magára vonni a

nézelődők figyelmét. A látogatók a robothoz lépve, a rajta elhelyezett reklámújságokból vehetnek.

Az elkészült robotrendszer alapvetően két fő részre osztható:

- mobil egység;
- telepített operátor és dokkoló egységek. (Esetünkben az operátorállomás egy hagyományos PC, a dokkolás pedig egy töltő csatlakoztatásával valósul meg.)

A mobil egység főbb komponensei:

- hordozó mechanika;
- meghajtó motorok és szervóhajtások;
- vezérlőrendszer;
- szenzorrendszer;
- kommunikációs eszközök;
- tápellátást biztosító eszközök;
- figyelemfelkeltést szolgáló eszközök.

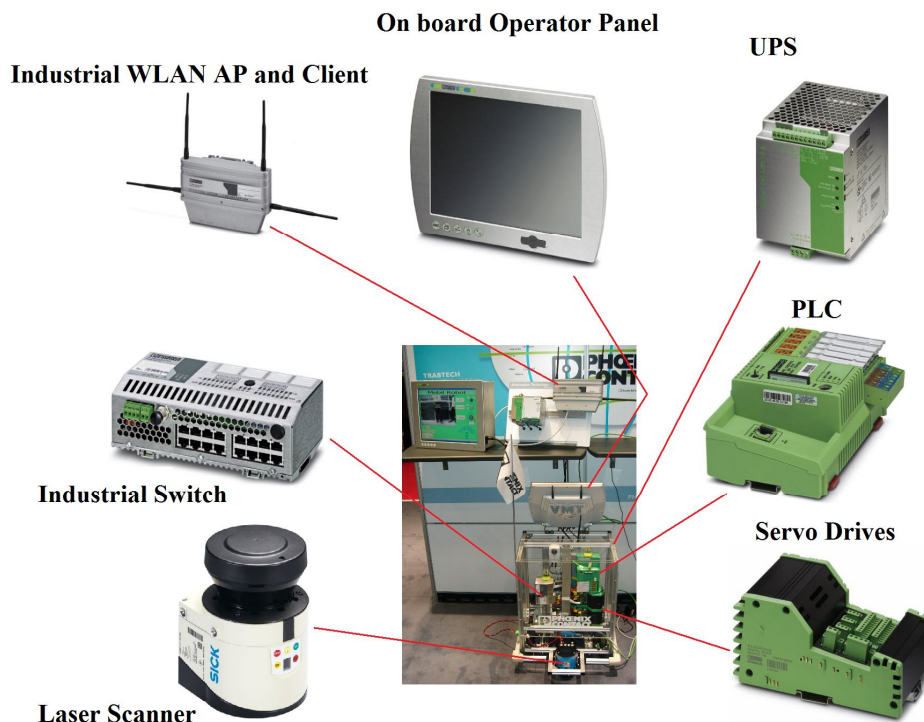
Az eszközök megválasztásánál fontos szempont volt a megbízható működés és a kompatibilitás, így a rendszer teljes egészében ipari komponensekből épül fel. A központi vezérlőegység egy, az iparban használt Phoenix Contact által gyártott ILC350PN típusú PLC (Programmable Logical Controller), melyhez ipari (InterBus) buszon keresztül csatlakoznak a szükséges perifériák és a hajtások. A rendszer moduláris kialakítású, így az esetleges bővítések újabb modulok csatlakoztatásával könnyen elvégezhetők. A PLC, a robot fedélzetén lévő egyéb eszközökkel Ethernet hálózaton kommunikál.

A navigációra és az akadály felismerésre egy SICK LMS100-típusú lézer szkennert használtunk. Ez a berendezés képes 270° -os nyílásszögben 0.25° -os felbontásban 20 m-es hatótávolságban távolság mérésére, maximálisan 50 Hz-es frissítési gyakorisággal. A szkennerekben szintén definiálhatók tetszőleges alakú védelmi zónák, melyek megsértése esetén a szkennerek képesek jelezni a vezérlőrendszernek. Esetleges ütközés esetén a robot rendelkezett egy olyan lökhárítóval, mely bármely irányból történő ütközés esetén ezt a vezérlőrendszernek képes volt jelezni egy kontaktus zárás segítségével.

A kommunikáció a már említett InterBus, Ethernet, valamint szabványos WLAN vezeték nélküli hálózaton zajlik. Csomóponti eszközként ipari switch-et alkalmaztunk.

A tápellátást szintén a Phoenix Contact által gyártott szünetmentes ipari tápegység biztosítja. Energiatárolóként 2 darab 12 V 12 Ah-ás gondozásmentes zselés akkumulátor szolgál, melyekkel biztosítható az egy órás folyamatos működés.

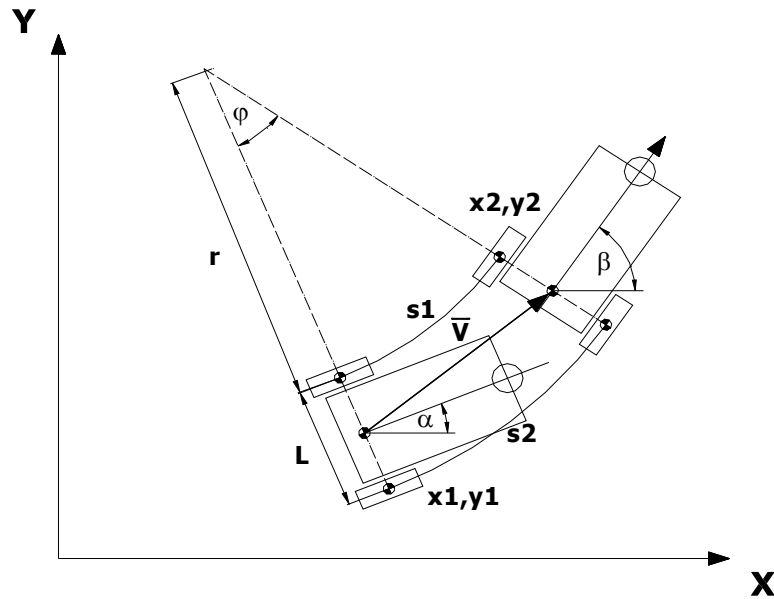
A reklámvideók lejátszására egy ipari IP65-ös védettségű panel PC szolgál, mely a további fejlesztések során elláthat vezérlési, adattárolási, vagy számítási feladatokat is. A panel PC szintén csatlakoztatva van a robot fedélzetén található Ethernet hálózathoz. A rendszer főbb komponensei az 1. ábrán láthatók.



1. ábra. A mobil robot rendszer főbb elemei

A fejlesztés során első feladat az eszközök összeintegrálás volt. Ezen belül a legnagyobb kihívást a LMS100-as szkenner által küldött TCP/IP csomagok PLC programban történő kezelése jelentette. A szkenner az általa mért szög és távolság adatokat, valamint a visszaérkező jel erősségét és egyéb technológiai paramétereket Ethernet TCP/IP csomagokban küldi, de mivel ez ~4-5 darab 1460 byte hosszúságú csomagot jelent, maximálisan 50 Hz gyakorisággal, és csomagonként szükséges a hasznos adatok kiválasztása és feldolgozása, ez komoly feladatot jelentett. A munkában nagy segítség volt az ipari switch-ek port tükrözési funkciója. A port tükrözéssel lehetőség nyílik két, a switch portjaira kapcsolódó, Ethernet hálózaton kommunikáló eszköz között zajló adatforgalom egy harmadik portra történő másolása, így a fejlesztő számítógépen egy protokoll analízátor program segítségével lehetőség nyílik a csomagok elemzésére.

A következő lépés a megfelelő navigáció és útvonaltervező eljárások kidolgozása volt. A cél az volt, hogy a robot egy előre definiált útvonalon haladjon, és, ha akadályt észlel a pályáján, az megpróbálja kikerülni. Korábbi robotfejlesztésekben alkalmaztuk a kerékelfordulás mérésének felhasználásával történő pozíciószámítást, mint inerciális navigációs módszert, kiegészítve egy kamerás pozícionálóval, mely felismerte a robotot és megadta annak pontos koordinátáit.



2. ábra. A modellen használt mechanikai elrendezés

Az adott mechanikai elrendezés figyelembe vételével a robot elmozdulása az 1. képlettel számítható. Az $s1$ és $s2$, a kerekek által megtett út hossza. Amennyiben a számítás gyakran elvégzésre kerül – azaz az $s1$ és $s2$ igen kis értékű az r - elfordulási ívhez képest –, akkor $s1$ és $s2$ köríven megtett úthosszak két egyenessel modellezhetők, így a számítás lényegesen egyszerűbbé válik.

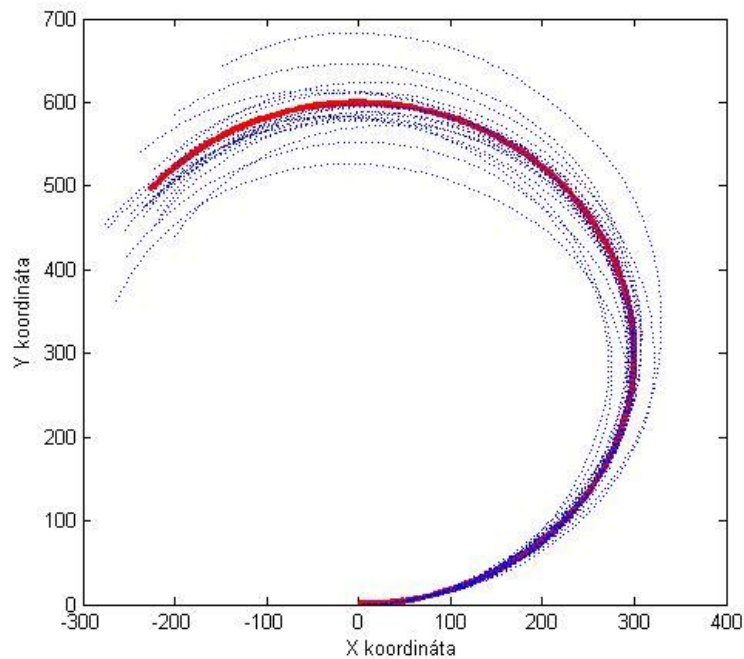
$$p' = f(x, y, \alpha, s1, s2) = \begin{bmatrix} x \\ y \\ \alpha \end{bmatrix} + \begin{bmatrix} \frac{s1+s2}{2} \cos\left(\frac{s1-s2}{2 \cdot L} + \alpha\right) \\ \frac{s1+s2}{2} \sin\left(\frac{s1-s2}{2 \cdot L} + \alpha\right) \\ \frac{s1-s2}{L} \end{bmatrix} \quad [1]$$

A számításhoz figyelembe kell venni a kerekek forgási irányát. Valamint eltérő képletek adódnak, amennyiben a kerekek forgási sebessége azonos. Azonos forgási sebesség, de ellentétes irány esetén a robot saját középvonala körül forog. Ha a kerekek sebessége azonos, valamint forgási irányuk is megegyezik, a robotok egyenes vonalú mozgást végeznek, a globális referencia koordináta-rendszerhez képest szögük nem változik.

A fent említett képletek programban történő megvalósítása, a kerékenkóderek jeleinek lehető legsűrűbben történő kiolvasásával, a számítások lefuttatásával történik. Amennyiben a számítások nem megfelelő sűrűséggel kerülnek elvégzésre, a körív egyenessel történő helyettesítése nagy hibákat eredményez. A túl gyakori lefuttatás esetén az enkóderekről csupán néhány impulzus érkezik, a kerekítések miatt itt is nagy hiba keletkezhet. Célszerű tehát a pontosság növelése érdekében nagy felbontású enkóderek alkalmazása is.

A fent említett számítások alkalmazhatóságát egy MATLAB szimuláció segítségével vizsgáltam (3. ábra). A modell megalkotásához a következő körülményeket vettem alapul:

- feltételeztem, hogy a kerekek elfordulásának mérése során a mért érték véletlenszerű hibával terhelt;
- feltételeztem, hogy a hiba arányos a számításhoz alapul vett megtett út nagyságával ($s1, s2$);
- feltételeztem továbbá, hogy a két hajtott kerék hibája független egymástól.

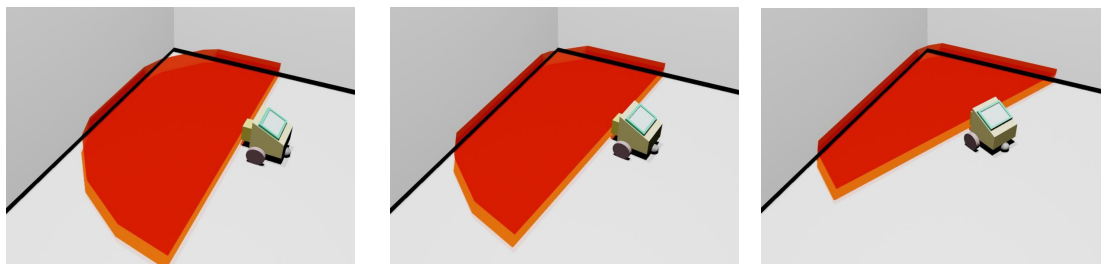


3. ábra. A kerékelfordulásból számított pozíció hibája.

Mivel egy kiállításon gyakori irányváltoztatás szükséges, valamint a robot viszonylag nagy területet jár be, az ismertetett módszer önmagában nem alkalmazható. Elvetettük a kamerás pozicionálás módszerét is, mivel tapasztalataink szerint a robot nem lenne képes még egy viszonylag nagy területet lefedő kamera látóterébe sem visszajutni csupán kerékelfordulásból számított helymeghatározás segítségével.

A megoldást véleményem szerint egy szenzorfüziós eljárás alkalmazása jelenti. Egy inerciális navigációs rendszer hatékony kiegészítője lehet egy abszolút helymeghatározó rendszernek. Beltéri navigációra megoldást jelent az inerciális navigációs rendszer kiegészítése egy lézeres lépáztázó (odometriás) rendszerrel (4. ábra).

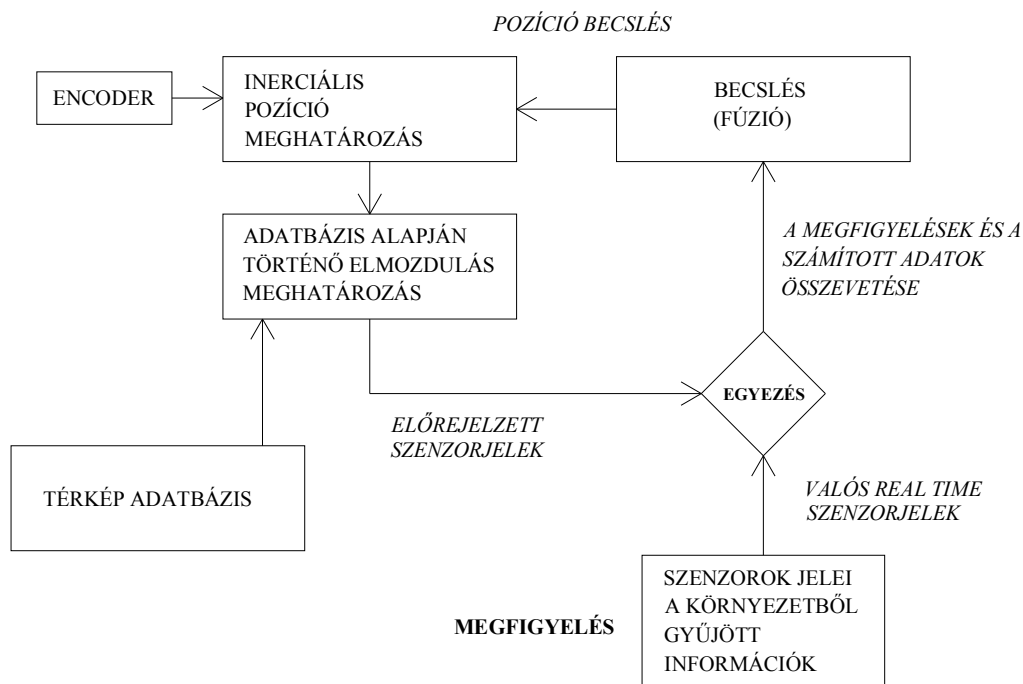
A lézeres letapogatás a már említett lézeres távolságmérésen alapul. A letapogatás során a mérő lézersugarat vízszintes irányban eltérítjük, így egy adott nyílásszögben mérhető egy adott távolságon belül található tereptárgyak távolsága. A letapogatást követően tehát egy térkép jellegű pontsorozathoz juthatunk, melyen a környező térben található tárgyak helye van feltüntetve. A robot elmozdulása esetén a környező tárgyak relatív pozíciója megváltozik, azonban az előző mérés eredményeit összevetve az újabb letapogatással, az elmozdulás és az elfordulás iránya és mértéke kiszámítható.



4. ábra. Beltéri navigáció megvalósítása Lézeres lépáztázás segítségével

Mivel a robot folyamatosan mozog, a pásztázás során ismerni kell a robot sebességét és irányát, és ezzel a szkennert által mért eredményeket korrigálni kell. A pozíció számítását

szintén nagyban megkönnyíti a kerekek elmozdulásának méréséből származó információ. Ebben az esetben tehát a lézeres letapogatás és a kerékelfordulást érzékelő enkóderek jeleinek fúziójából nyerhető a pontos pozíció (5. ábra).



5. ábra. Kálmán-szűrő segítségével történő mobil robot helymeghatározás

Kísérletet tettünk a fent felvázolt módszer megvalósítására, azonban kénytelenek voltunk megállapítani, hogy egy kiállításon a környezet olyannyira dinamikusan tekinthető, hogy az odometriás helymeghatározási módszer nem, vagy csak nagyon nagy hibával alkalmazható. Gondoljuk csak bele egy gyakori szituációba. A robotot egy tucat látogató veszi körül, így a robot a környező statikus tereptárgyakból semmit sem lát, saját helyzetét tehát a mozgó látogatókhoz viszonyítja. Mivel a viszonyítási pontok nem rögzítettek, a számítás nem lehet pontos.

Az idő szorításában tehát kénytelenek voltunk kiegyezni egy bolyongó mozgást végző robottal, ebben az esetben viszont biztosítani kellett a robot, a kiállítás egy adott területén történő tartását. A bolyongó mozgást úgy definiáltuk, hogy amennyiben a robot maga előtt akadályt észlel, kezdjen elfordulni, amerre pedig szabad utat észlel, induljon el. Működési területként a kiállítás közlekedő részén elhelyezett szőnyeget definiáltuk. A robotnak a reklámozni kívánt pavilon közelében, egy adott működési sugárban kellett üzemeltetni.

A szőnyegen tartást egy színérzékelő szenzor segítségével oldottuk meg, mely érzékelte a padló és a szőnyeg színének eltérését. Az adott sugárban tartást pedig a kommunikációra használt WLAN eszköz jelerősségének figyelésével kívántuk megoldani. A módszer labor körülmények között működni látszott, azonban a kiállításon üzembe helyezve a robotot, felmerültek újabb előre nem látott problémák:

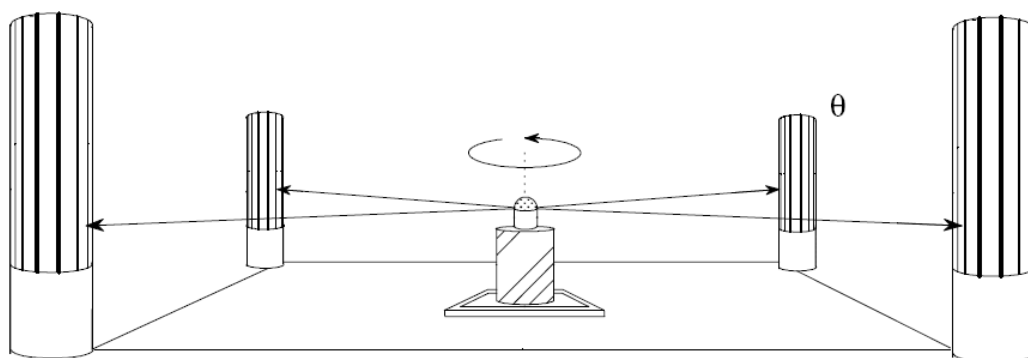
- a szőnyeg és a padló között ~5mm szintkülönbség volt;
- a kiállításon hirdető cégek többsége WLAN eszközöket használt;
- több pavilon néhány centivel kiemelkedett a padló síkjából.

A padló és a szőnyeg szintkülönbsége miatt a robot, ugyan észlelte, hogy elhagyta a szőnyeget, de visszajutnia, csak nagy erőlködések árán sikerült. Ennek oka a viszonylag kisméretű kerekekben keresendő. Erre a hibára a kiállításon derült fény, korrigálása jelenleg

zajlik. A terhelt WLAN spektrumnak köszönhetően a WLAN vételi jelerősség a pavilontól akár 10 méterre gyakran egyik pillanatról a másikra nullára csökkenhetett, így a robot mozgása zavarttá, kiszámíthatatlanná vált. Az alacsony kiemelésű pavilonokat az elhelyezett lézerszkennerek nem tudta észlelni.

A fent felsorolt hibák a funkciók többségének kiiktatásához vezettek. Tapasztaltuk, hogy a lézerszkennert javasolt a földhöz lehető legközelebb elhelyezni, így a viszonylag alacsony tereptárgyak is észlelhetők, azonban így nem vagyunk képesek egy a földdel nem „érintkező” (például asztallap) érzékelésére, ilyen helyeken a robot fennakadhat.

A szerzett tapasztalatokat elemezve egy újabb ötlet született. A szkennerek képesek nem csak a távolság, de a visszaverődési intenzitás (RSSI) mérésére is. Speciális fényvisszaverő prizmák alkalmazásával lehetőségünk nyílna „világítótornyok” elhelyezésére, melyeket a robot észlelve, képes lenne pozíciójának viszonylagos meghatározására (6. ábra).



6. ábra. Speciális fényvisszaverők alkalmazásával megvalósított navigáció

Figyelembe kell venni azonban ebben az esetben is azt, hogy a környezet rendkívül dinamikus (gyakran egyenesen rosszindulatú). Tapasztaltuk, hogy a látogatók kiismerve a robot működését, igyekeznek azt a rossz irányba terelni, bebizonyítva annak „butaságát”. Ilyen környezetben nem biztosítható tehát, hogy a robot látja az elhelyezett jelzőprizmákat. Megoldást ebben az esetben is a rendelkezésre álló információk fűziója jelenti.

A megépített mechanika és vezérlő és szenzorrendszer több évre megfelelő alapot nyújt vezérlő, navigációs és akadályelkerülő algoritmusok fejlesztésére. Fontos hangsúlyoznom azt, hogy, mivel egy valós alkalmazásról van szó, a rendszernek akár egyszerűbb algoritmusokkal, de működnie kell. Látató, hogy hatalmas eltérés van egy laborban tesztelt kutatási célokra tervezett rendszer és egy valós applikáció között. Valódi applikáció esetén olyan körülményeket is figyelembe kell venni, melyek a tervező asztalon talán fel sem merülnének, így egy ilyen fejlesztés rendkívül hasznos és tanúságos.



7. ábra. Néhány kép az elkészült robotról

Irodalom

- [1] Introduction to Autonomous Mobile Robots. Siegwart, R, Nourbahsh I R, The MIT Press Massachusetts institute of Technology Cambridge 2004
- [2] Modeling of the Control Strategies of Wheeled Mobile Robots. Mester Gy, Proceedings of The Kandó Konfernce, pp. 1-4, Budapest, 2006. ISBN 963-7154-42-6
- [3] Microcontrollers, Actuators and Sensors in Mobile Robots. István Matijevics I4th Serbian-Hungarian Joint Symposium on Intelligent Systems September 29-30, 2006 Subotica, Serbia
- [4] LMS100 Laser Measurement System application manual
www.sick.com/home/factory/news/autoident/lms_100/en,
 LMS100_ProductInformation.pdf, (2008.10.10)
- [5] J. Borestein, H.R. Everett, L. Feng „Where Am I? Sensors and Methods for Mobile Robot Positioning” University of Michigan, Michigan 1996

Kun István

kunistvan47@gmail.com

INFORMATIKAI RENDSZEREK MEGBÍZHATÓSÁGÁNAK MATEMATIKAI MODELLEZÉSE

Absztrakt

A cikkben a szoftverek megbízhatóságának problémakörével foglalkozunk, amely lényegesen eltér a megbízhatóságelmélet általános problémakörétől. Ez utóbbi az informatikán belül döntően inkább a hardvermegbízhatóságra érvényes. Foglalkozunk a két problémakör különbségeivel. Ismertetjük az alapvető matematikai modelleket, amelyek két fő csoportra oszlanak: a metrikákra és a prediktív statisztikai modellekre. Kiemelten érdekesek a komplexitási metrikák, amelyek egymástól lényegesen különböző, de egyaránt mély matematikai alapokon nyugszanak. A komplexitási metrikákra épülnek a folyamat-mutatószámok, amelyek a szoftver tervezésének és kódolásának projektjét, a prediktív statisztikai modellek pedig a tesztelés projektjét segítik az időigények reális becslésében.

In this paper we deal with the problem sphere of the software reliability, essentially different from the general problem sphere of reliability. This latter is valid, within information technology, rather on hardware reliability. We deal with the differences of the two problem spheres. We expound the basic mathematical models, which have two main groups: metrics and predictive statistical models. Especially interesting are the complexity metrics, which are laid on two essentially different but equally deep mathematical bases. A realistic assessment of time consumption can help project planning, which is based in software design and coding mainly on complexity metrics, while in software testing mainly on predictive statistical models.

Kulcsszavak: informatika, megbízhatóság, matematika, szoftver ~ information technology, reliability, mathematics, software

1. Kritikus szoftverhibák

Mi az elmélet?

A gondosan tesztelt szoftver soha nem hibásodik meg, mert amíg a számítógép működik, a szoftver nem változik, nem öregedik.

És mi a valóság?

A tényleges helyzetet néhány példa teszi szemléletessé, l. (Pan, 1999):

- Falklandi háború (1982): a Sheffield rombolót azért süllyesztette el egy Exocet rakéta, mert a védelmi radarrendszer szoftvere a rakétát tévesen „barátnak” minősítette.
- Öbölháború (1991): egy Patriot ellenrakéta irányítórendszere 10 másodpercenként 0.000000095 sec-ot tévedett, és az akkumulálódó hibák miatt 100 órás működés után nem találta el a támadó rakétát (28 halott)
- Ariane 5 európai űrrakéta: az Ariane 4 jól működő szoftverében egy apró módosítást végeztek, és az Ariane 5-ben indításkor tűz keletkezett.
- USA, Kalifornia állam: egy helyi telefonközpontban egy kezelőprogramban 3 sort kicseréltek, és a teljes szolgáltatás megbénult.

2. A szoftver-megbízhatóság értelmezése

A hardvereszközök működőképessége egyedileg változik, és akár pillanatonként módosuló véletlen tényezőktől (elhasználódás mértéke, környezeti hatások) függ.

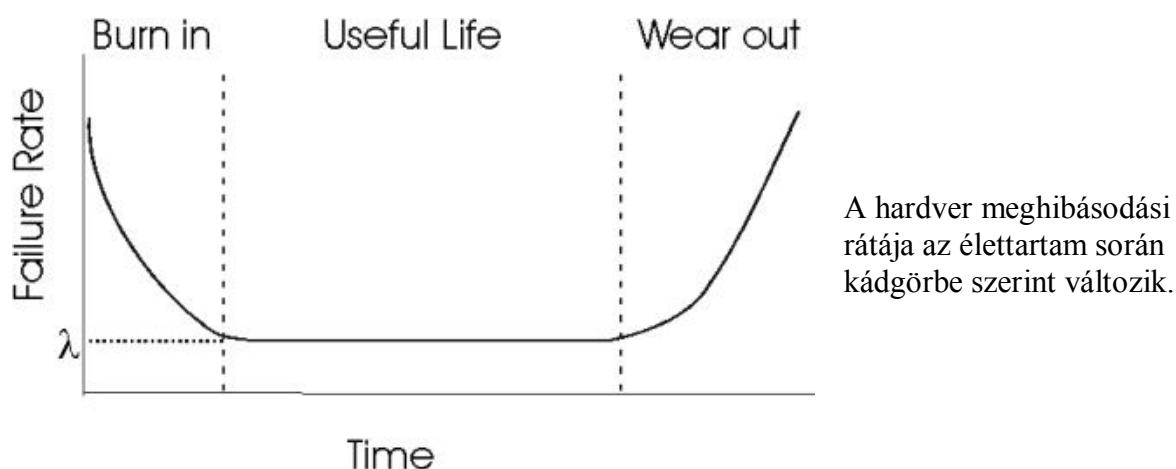
Ezzel ellentétben a szoftverek példányai azonosak, és – az adathordozók hibáitól eltekintve – időben állandóak. A hibátlan programrész mindig hibátlanul működik, a hibás programrész viszont mindig hibásan.

A szoftverek megbízhatóságának statisztikai jellegét tehát nem a szoftver belső tulajdonságai adják, hanem a használat módja: milyen gyakorisággal lépünk be a hibás programrészbe. Még ha a program tele van hibákkal, akkor sem vesszük ezt észre, ha nem használjuk a hibás programágakat. Tipikus példája ennek az a mikroprogram-hiba, amit a Pentium processzor piacra dobásakor egy matematikatanár fedezett fel, mert egy számelméleti algoritmus hibásan működött. A gyári teszteléskor senkinek nem jutott eszébe ilyen algoritmust kipróbálni.

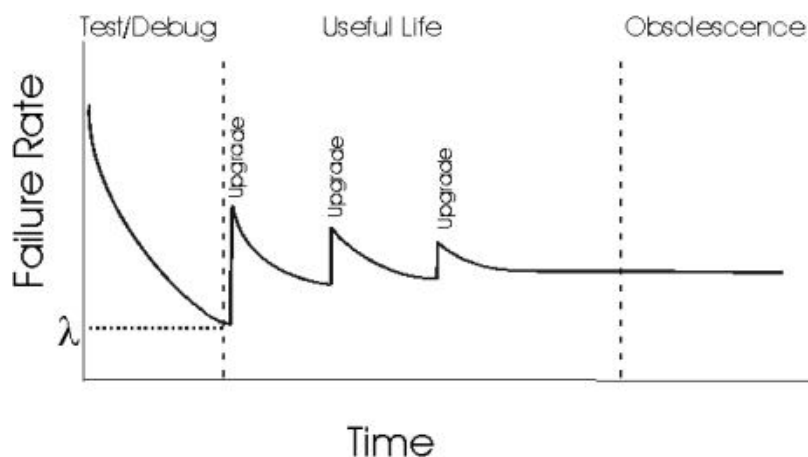
A felhasználót a teljes rendszer hibátlan működése érdekli, gyakran nem is tud különbséget tenni a hardver és a szoftver hibája között. Tipikus szituáció az adathordozó meghibásodása miatt működésképtelenné váló szoftver. Ilyenkor gyakran nehéz elválasztani egymástól a kétféle hibát.

A következő táblázat rendszerezi az említett különbségeket.

HARDVER	SZOFTVER
A hiba oka egyaránt lehet a tervezés, a gyártás, a használat és a karbantartás.	A hiba oka majdnem mindig a tervezés.
A hiba lehet az elhasználódás vagy más, energiával kapcsolatos jelenség következménye. Ennek gyakran vannak korai figyelmeztető jelei.	Nincs elhasználódás. Nincsenek korai figyelmeztető jelek.
Javítással növelhető a megbízhatóság.	Az egyetlen javítási lehetőség az áttervezés (újraprogramozás).
A megbízhatóság függhet bejáratási vagy elhasználódási jelenségektől.	A megbízhatóság nem változik a működési idővel, csakis a hibakeresésbe fektetett munkával.
A meghibásodás valószínűsége függ az eltelt működési (vagy tárolási) időtől.	A meghibásodás nem függ így az időtől. Akkor történik, amikor hibás programrészbe lépünk.
A megbízhatóság környezeti tényezőktől is függ.	A környezeti tényezők nem érintik a megbízhatóságot, legfeljebb az adathordozón keresztül.
A megbízhatóság elméletileg megjósolható a tervezés és a használat alapján.	A megbízhatóság semmilyen fizikai folyamat alapján nem jósolható, mert a tervezés emberi tényezőitől függ.
A megbízhatóság gyakran növelhető tartalékegységek alkalmazásával.	A megbízhatóság nem növelhető tartalékegységek alkalmazásával, ha a párhuzamos programrészek azonosak: amennyiben az egyik hibás, akkor a másik is. A tartalékolás csak akkor segít, ha a párhuzamos ágakban eltérő szerzők által készített eltérő programok vannak.
A rendszer komponenseinek megbízhatósága olyan törvényeket követ, amelyek a komponenseket ért terhelés és más tényezők alapján bizonyos mértékig megjósolhatók.	A hibák általában nem jelezhetők előre az egyes programlépésekre vonatkozó megállapításokból. A programhibák véletlenszerűen szóródva helyezkednek el, és bármelyik utasítás lehet hibás.



1. ábra. A hardver meghibásodási rátájának alakulása



A szoftver meghibásodási rátája farkasfog-szerű: az upgrade ciklus elején megnő, a ciklus végére lecsökken.

2. ábra. A szoftver meghibásodási rátájának alakulása

A szoftver megbízhatósága (és tőle elválaszthatatlanul minősége) tehát némileg kilóg a klasszikus hardver-orientált megbízhatóságelmélet kereteiből. Részletes tárgyalását l. (Kun-Szász-Zsigmond, 2002). A szoftver megbízhatósági rátájának a hardverétől való lényeges eltérését illusztrálja az 1. és 2. ábra.

A matematikai modelleknek két alaptípusa van:

- Metrikák
- Prediktív statisztikai modellek

A metrikákat a NASA szoftverhiba-adatbázisa osztályozza, l. (Long, 2008). További részletes ismertetésüket tárgyalja (Porkoláb-Pataki-Sipos, 2006).

3. A szoftver mutatószáma

A szoftver-mutatószámok alkalmazásának célja elsősorban a minőség mérése, ezen túlmenően pedig a szoftverkészítés folyamatának hatékonyságvizsgálata, továbbá az előállítási folyamat további alakulásának előrebecslése, ide értve a határidőket és költségeket.

A metrika valamilyen számszerű mérési eljárással a szoftverhez rendelt függvényértéket jelent, ahol a független változók a szoftver mért adatai.

Típusai:

- Fizikai méret alapú metrikák
- Hibaszám-metrikák
- Stílus-metrikák (szemantikai elvárásokat – pl. egyértelműség – fogalmaznak meg)
- Komplexitási metrikák

A szoftver tesztelésének, utólagos karbantartásának és módosításának költsége nagyrészt a program strukturális bonyolultságának függvénye. Egy jól használható szoftver-bonyolultsági mérték már a fejlesztési fázisban felfedheti a szoftver kritikus pontjait, elősegítheti az áttekinthetőbb, módosítható és újrafelhasználható kód készítését, és becsléseket adhat a fejlesztési folyamat várható költségeire.

3.1. A méret mutatószámai

A szoftver valamilyen értelemben vett „fizikai” mérete az előállításhoz szükséges munkamennyiség legegyszerűbb jellemzője.

A program sorainak száma

Látszólagos primitívsege ellenére a gyakorlatban jól bevált. Nincs olyan másik metrika, amelyik minden tekintetben jobb lenne. Előnye, hogy általa mindenki könnyen fogalmat alkothat a program bonyolultságáról. Hátránya is éppen egyszerűsége: sokan úgy gondolják, hogy ez az egyetlen, valóságos szoftvermetrika, amely minden fontos dolgot mérni tud.

A programfejlesztési pályázatkírás oldalszáma

A felhasználói dokumentáció oldalszáma

A JACKSON-diagram csúcsainak száma

Funkcióleíró pontok száma a specifikációban

A program hosszának és dokumentációjának aránya

Különösen érdekesek a dokumentációt is figyelembe vevő mérőszámok, mert a dokumentáció készítését sok szoftverfejlesztő másodlagos fontosságúnak tekinti.

3.2. Hibaszám alapú metrikák

Működési zavarok száma

Alkalmassága különböző célokra

A minőség megítélésére: mérsékelten.

A minőség összehasonlítására más programokkal vagy korábbi állapottal: mérsékelten.

Előre meghatározott kritériumoknak való megfelelésre: igen.

A programkészítés közbeni döntések megalapozására: igen.

A jövőbeni célok kitűzésére: mérsékelten.

A fogyasztói megelégedettség mérésére: nem.

Ezer programsorra jutó működési zavarok száma

Alkalmassága különböző célokra:

A minőség megítélésére: mérsékelten.

A minőség összehasonlítására más programokkal vagy korábbi állapottal: igen.

Előre meghatározott kritériumoknak való megfelelésre: igen.

A programkészítés közbeni döntések megalapozására: nem.

A jövőbeni célok kitűzésére: igen.

A fogyasztói megelégedettség mérésére: mérsékelten.

Problémák

Különböző programnyelvek erősen különböző programméretekhez vezetnek.

A forráskódban található megjegyzés-sorok száma eltorzíthatja az eredményt.

Sok forráskód üres sorokat tartalmaz a könnyebb áttekinthetőség érdekében.

Ezer nem-megjegyzés jellegű programsorra jutó működési zavarok száma

Alkalmassága különböző célokra

A minőség megítélésére: igen.

A minőség összehasonlítására más programokkal vagy korábbi állapottal: igen.

Előre meghatározott kritériumoknak való megfelelésre: igen.

A programkészítés közbeni döntések megalapozására: nem.

A jövőbeni célok kitűzésére: igen.
A fogyasztói megelégedettség mérésére: mérsékelten.

Problémák

Külön programok vagy speciális fordítási opciók kellenek a mérőszám meghatározásához.
Csökkenti a megjegyzések beírására való készséget, ezen keresztül pedig a program átláthatóságát és karbantarthatóságát.

Egy felhasználóra jutó működési zavarok száma

Alkalmassága különböző célokra

A minőség megítélésére: nem.
A minőség összehasonlítására más programokkal vagy korábbi állapottal: mérsékelten.
Előre meghatározott kritériumoknak való megfelelésre: mérsékelten.
A programkészítés közbeni döntések megalapozására: nem.
A jövőbeni célok kitűzésére: nem.
A fogyasztói megelégedettség mérésére: igen.

Problémák

Nehéz meghatározni az adott szoftverterméket használók számát; nehéz meghatározni egy adott felhasználónál a használat mértékét.

Ezer tesztelési órára jutó működési zavarok száma

Alkalmassága különböző célokra

A minőség megítélésére: nem.
A minőség összehasonlítására más programokkal vagy korábbi állapottal: mérsékelten.
Előre meghatározott kritériumoknak való megfelelésre: igen.
A programkészítés közbeni döntések megalapozására: nem.
A jövőbeni célok kitűzésére: igen.
A fogyasztói megelégedettség mérésére: igen.

Problémák

Az eredmények erősen függenek a teszt szigorától, kiterjedtségétől és intenzitásától (egyetlen teszt sokszori megismétlése nem adja ugyanazt az eredményt, mint több teszt párhuzamos alkalmazása).

Ha a tesztfutásokat ember indítja, az eredményt befolyásolja a szakképzettség.

A tesztelés során végrehajtott programkód mennyisége függ a tesztelés módszerétől, ezért egyidejűleg olyan más mérőszámot is célszerű alkalmazni, amely megadja, hányszorosan fedi le az adott teszt a programot.

Ezer tesztelési órára jutó működési zavarok száma fedettségi mérőszámmal

Alkalmassága különböző célokra

A minőség megítélésére: igen.
A minőség összehasonlítására más programokkal vagy korábbi állapottal: igen.
Előre meghatározott kritériumoknak való megfelelésre: igen.
A programkészítés közbeni döntések megalapozására: igen.
A jövőbeni célok kitűzésére: igen.

A fogyasztói megelégedettség mérésére: igen.

3.3. Stílus-metrikák

Általános minőségi elvárásokat (pl. stabilitás, áttekinthetőség) mérnek egyszerű forráskód-jellemzőkön keresztül.

Kódsorok átlagos száma metódusonként

Metódusok átlagos száma osztályonként

Osztályok átlagos száma teljes programonként

Absztrakt osztályok aránya az összes osztályok között

A modulból kimenő kapcsolatok átlagos aránya az összes (bemenő+kimenő) kapcsolathoz képest.

3.4. Komplexitási metrikák

A komplexitási metrikák egyaránt lehetnek termékjellemzők (az elkészült szoftver statikus tulajdonságai) és folyamatjellemzők (a szoftverkészítési folyamat által felhasznált idő és munkamennyiség).

Típusai:

- Objektumorientált metrikák
- HALSTEAD-féle komplexitási metrika (információelméleti alapú)
- MCCABE-féle ciklomatikus komplexitási metrika (gráfelméleti alapú)
- HENRY-KAFURA-féle információáramlási metrika (eljárás külső kapcsolatai)

A Unix operációs rendszeren bizonyították, hogy a MCCABE- és a Halstead-komplexitás erősen korrelál egymással és a hibaszámmal is, míg a HENRY-KAFURA komplexitás statisztikailag független tőlük.

3.4.1. Objektumorientált metrikák

Az objektumorientált programtervezés általános elterjedése óta gyakran az ilyen eredetű programjellemzők alapján célszerű bonyolultsági elemzést végezni. Legfontosabb típusait összefoglalja (Porkoláb-Pataki-Sipos, 2006).

Súlyozott metódusok osztályonként

Osztály bonyolultsága: az osztályon definiált metódusok bonyolultságának az összege.

Előnye, hogy a bonyolultság a kódot felhasználó osztályokra és az azokból származtatott további osztályokra tovaterjed.

Öröklődési hierarchia mélysége

Osztály bonyolultsága: hány öröklődési szintnyi „távolságra” van a „gyökérosztálytól”.

Leszármazott osztályok száma

Osztály bonyolultsága: közvetlenül leszármaztatott gyerekosztályok száma.

Előnye, hogy fokozottan figyelembe veszi a kód újrafelhasználását, ami a hibaterjedés egyik fő oka.

Osztályok közötti kapcsolódás

Osztály bonyolultsága: az adott osztályhoz kapcsolódó osztályok száma.

Kapcsolódás: az egyik osztály felhasználja a másik metódusait vagy attribútumait (l. a 3.4.4. pontban a HENRY-KAFURA metrikát).

3.4.2. A HALSTEAD-féle komplexitási metrika

A bonyolultság nem triviális mérőszámai közül legismertebb a M. H. HALSTEAD által kidolgozott komplexitási metrika. Ez a forrásnyelvi kód szövegelemzésén és információelméleti megfontolásokon alapszik.

A következő alapmennyiségekre van szükség:

n_1 — a különböző operátorok (eljárások, függvények, műveletek) száma;

n_2 — a különböző operandusok száma;

N_1 — az operátorok összesített előfordulási száma;

N_2 — az operandusok összesített előfordulási száma.

Az alapmennyiségekből lehet kiszámítani a komplexitási metrikákat:

A program szókincse

Képlete: $n = n_1 + n_2$

Jelentése: a programban található különböző azonosítók száma.

A program hossza

Képlete: $N = N_1 + N_2$

Jelentése: a programban található azonosítók összes előfordulásainak együttes száma.

A program térfogata

Képlete: $V = N \log_2 n = \ln n^N$

Jelentése: a program kódolásához szükséges bitek száma.

A komplexitási mérőszámok nyelvészeti eredetűek. A program szókincse a programban, mint szövegben található különböző szavak száma. A program hossza a programban, mint szövegben található összes szavak száma. Mint látjuk, ez a két fogalom közel áll az elnevezés hétköznapi értelmezéséhez.

A program térfogata kissé bonyolultabb fogalom. Induljunk ki abból, hogy n különböző szó kódolásához elméletileg $\log_2(n)$ bitre van szükség. Ugyanis a szavakat ilyenkor kódolhatjuk a 0, 1, 2, 3, ... $n-1$ számokkal, és a számokat kettes számrendszerben is felírhatjuk. Ha n éppen 2-nek egy pozitív egész kitevőjű hatványa, akkor $n-1$ kettes számrendszerbeli alakja pontosan $\log_2 n$ számú 1 értékű bitet tartalmaz, pl. $15 = 1111_2$. Ha pedig n 2-nek két szomszédos pozitív egész kitevőjű hatványa közé esik, akkor ugyan $\log_2 n$ nem egész szám, de n kettes számrendszerbeli alakjához pontosan ugyanannyi bitre van szükség, mint a nála éppen nagyobb 2-hatványnak, vagyis annyira, mint $\log_2 n$ felfelé egészre kerekített értéke. A kódoláshoz szükséges bitek számát a szókincs információtartalmának tekinthetjük. (A $\log_2 n$ értéket egyébként az n elemszámú halmaz HARTLEY-információjának nevezzük.) Vagyis a program térfogata a programban szereplő azonosítók összes előfordulási száma szorozva az egy azonosító kódolásához szükséges bitek számával, tehát éppen a programnak, mint szövegnek a kódolásához szükséges bitek száma. Ezt a mennyiséget a program bonyolultságának, komplexitásának mérésére használjuk. A fogalom azért célszerű, mert egyaránt függ a program fizikai méretétől és a benne előforduló szókincs összetettségétől.

A HALSTEAD-mérőszámok alkalmazása bizonyos esetekben problémákat vet fel.

- Vannak olyan programozási eszközök, amelyek nem tekinthetők sem operátornak, sem operandusnak. Ilyenek például a címkék vagy a ciklusutasítások.

- Egy azonosító többféle operátort vagy operandust is jelölhet a program különböző pontjain. Így például egy változónév a magas szintű programozási nyelvekben több modulban is előfordulhat, mint a modul lokális változója, továbbá a + jel egyaránt jelenthet aritmetikai vagy logikai összeadást és előjelet, tehát három teljesen különböző dolgot.
- A komplexitási metrika bünteti a programozási nyelvbe eleve beépített látszólagos redundanciát. Például a másodfokú egyenlet megoldóképletének algebrai jelölésmódja a következő alakú: $(-b + \sqrt{b^2 - 4ac}) / (2a)$. Ugyanez a formula a szintén gyakran alkalmazott fordított lengyel jelölésrendszerben: $/+ - b \sqrt{-^2 b^4 ac^2 a}$. Az algebrai jelölésmód a zárójelezés miatt nagyobb programhosszt von maga után. A legtöbb programozási nyelvben mégis ezt használják, mert az emberi gondolkodásmód miatt kevésbé bonyolultnak tűnik.

A HALSTEAD-metrika használata komoly szakmai vitákat váltott ki [BENMEL]. Bírálói is elismerik azonban, hogy a tervezés szakaszában jó előrejelzést adhat a program bonyolultsága miatt várható hibák számáról.

3.4.3. A MCCABE-féle ciklomatikus komplexitási mutatószám

Rajzoljuk fel egy program G vezérlésfolyam-gráfját a következő módon: a gráf csúcsai az utasítás-szekvenciáknak (elágazás nélküli utasítás-sorozatoknak) felelnek meg, élei pedig a program által a szekvenciák között létrehozott lehetséges közvetlen átmeneteknek. Ekkor felírhatjuk az úgynevezett ciklomatikus mutatószámot.

$$\text{Képlete: } v(G) = e - n + 2$$

ahol

v (nú) – a ciklomatikus komplexitás

e – a gráf éleinek száma

n – a gráf csúcsainak száma

MCCABE javasolta a $v(G)$ számot a program komplexitásának mérésére, ily módon iránymutatónak a program fejlesztéséhez és teszteléséhez. A tesztelési munka tervezésére azért alkalmas, mert bizonyítható, hogy $v(G)$ pontosan egyenlő a vezérlésfolyam-gráf független (legalább egy eltérő élt tartalmazó) útjainak maximális számával, vagyis a tesztelendő útvonalak maximális számával (hiszen ennél több tesztelési útvonalat megadva biztosan találunk köztük két azonos útvonalat).

Strukturált programok esetében nincs szükség a program gráfjára sem, hiszen ebben az esetben könnyű meghatározni az elágazási pontok számát.

A ciklomatikus komplexitást a szoftver kockázati szintjének jellemzésére is használják. Az általános ajánlás szerint a 10-nél alacsonyabb mutatószám-értékre kell törekedni.

Ciklomatikus komplexitás	Kockázati szint
1-10	Egyszerű program, kevés kockázat
11-20	Mérsékelt bonyolult program, mérsékelt kockázat
21-50	Bonyolult program, magas kockázat
Több mint 50	Nem tesztelhető program, nagyon magas kockázat

A MCCABE mutatószám problémái:

- Nem kezeli külön az egyszerű (nem többfelé ágaztató) feltételes utasításokat.
- Nem veszi figyelembe a program deklarációs részét.

Vannak a ciklomatikus komplexitási mutatószámoknak olyan módosításai, amelyek kiküszöbölik a fenti problémákat.

3.4.4. A HENRY-KAFURA-féle információáramlási metrika

HENRY és KAFURA a programmodulok közötti információáramlás alapján definiált egy bonyolultsági mértéket. A programmodulba bemenő és az onnan kimenő adatutakat és vezérlésátadásokat számolja össze.

Más néven fan-in - fan-out elemzést tartalmaz.

Fan-in: az adott modult hívó modulok száma.

Fan-out: az adott modul által hívott más modulok száma.

Ezek után a HENRY-KAFURA mérték:

$$\text{Komplexitás} = \text{Programhossz} \times (\text{Fan-in} \times \text{Fan-out})^2$$

Ez egyetlen modulra vonatkozik, összegzéssel állapítható meg a teljes program komplexitása.

Előnye, hogy már a tervezés közben is jól használható.

Hátránya, hogy kizárólag a programmodulok külvilággal folytatott kommunikációját veszi figyelembe, ami a valóságos bonyolultságnak csak egyik tényezője.

4. Folyamat-mutatószámok

4.1. A Walston-Felix folyamat-mutatószámok

C. E. WALSTON és C. P. FELIX, az IBM kutatói 60 nagy szoftverprojekt különböző adatainak statisztikai elemzése alapján alkották matematikai modelljüket a szoftverkészítés folyamatának jellemzésére.

Munkamennyiség

$$\text{Képlete: } E = 5,2 L^{0,91}$$

ahol

E – a program létrehozásához szükséges munkamennyiség, ember-hónapokban;

L – a program forráskódjának hossza 1000 programsor egységben.

Látható, hogy E értéke nem egyenesen arányos a programsorok számával, hanem annál kissé lassabban növekszik.

Termelékenység

$$\text{Képlete: } P = \frac{L}{E} = \frac{L}{5,2 L^{0,91}} = 0,19 L^{0,09}$$

ahol:

P – egy ember által havonta átlagosan létrehozott programkód hossza, ezer sorban kifejezve.

Az előbbi megjegyzést folytatva, itt még világosabban látszik, hogy a program hosszának növekedésével párhuzamosan, bár igen enyhén, de nő a havonta átlagosan előállítható sorok száma. Ez eléggé természetes, hiszen a rutinszerű, méretarányos programkód-írási munkát megelőzi egy kevésbé rutinszerű, tehát a mérettől kevésbé függő tervezési tevékenység.

A formula nem tükrözi az egyes programok közti nehézségi különbségeket, amelyek növelhetik, vagy csökkenthetik a termelékenységet. Ennek a hiányosságnak a kiküszöbölésére a szerzők később bevezettek egy termelékenységi szorzót, amelynek értéke a program jellegétől függ, és ugyancsak korábbi projektek adataiból becsülhető.

4.2. A Halstead-féle folyamat-mutatószámok

A HALSTEAD-féle komplexitás-fogalomra alapozva folyamat-mutatószámokat definiálhatunk.

A program nehézsége

$$\text{Képlete: } D = \frac{n_1}{2} \frac{N_2}{n_2}$$

Látható, hogy a program nehézsége egyenesen arányos a programozó által vagy automatikusan elvégzett operátor-deklarációk számával és egy operandus átlagos előfordulási számával.

Munkamennyiség

$$\text{Képlete: } E = VD$$

ahol

E – a program létrehozásához szükséges munkamennyiség, ember-hónapokban;

V – a HALSTEAD-féle komplexitási mutatószámoknál megismert programtérfogat;

D – a program nehézsége.

A mutató előzetes kiértékelésekor a specifikáció ismeretében jól becsülhető a különböző operátorok és operandusok száma: n_1 és n_2 , a fejlesztők programozási stílusa alapján következtetni lehet az operandusok átlagos előfordulási számára is: N_2/n_2 , de a program hossza ekkor még nem ismert. HALSTEAD rámutatott arra, hogy közelítőleg fennáll:

$$N \approx n_1 \log_2 n_1 + n_2 \log_2 n_2$$

Ennek alapján lehetséges egy viszonylag egyszerűen kiszámítható közelítő formula alkalmazása.

$$\text{Képlete: } E = \frac{n_1 N_2 (n_1 \log_2 n_1 + n_2 \log_2 n_2) \log_2 n}{2n_2}$$

ahol

n_1 — a különböző operátorok (eljárások, függvények, műveletek) száma;

n_2 — a különböző operandusok száma

$$n = n_1 + n_2$$

E értékét itt a programkódolás úgynevezett elemi döntéseiben mérjük. Egy elemi döntés lényegében a programkód adott helyén szükséges szimbólum kiválasztását jelenti. Ennek időigénye is kiszámítható.

Elemi döntés időigénye

$$\text{Képlete: } T = \frac{E}{18}$$

ahol:

T – egy elemi döntés meghozatalához szükséges, másodpercben mért idő.

Amennyiben csak a HALSTEAD-mutatószámoknál szereplő programhossz ismert, itt is lehetséges némileg egyszerűbben kiszámítható közelítő formula alkalmazása.

$$\text{Képlete: } T = \frac{N^2 \log_2 n}{72}$$

ahol:

N – a programban található azonosítók összes előfordulásainak együttes száma;

n – az $N = n \log_2 (n/2)$ egyenlet (csak közelítően kiszámítható) megoldása.

5. Prediktív statisztikai modellek

A legfontosabb alapmodellek már évtizedekkel ezelőtt megszülettek, l. (Mellor-Bendell, 1986).

5.1. Duane modellje

A modell jellemzői:

- futási időre vonatkozik
- determinisztikus
- nem számlálja a hibákat
- csak a meghibásodásokkal foglalkozik, a javítással nem
- a programot fekete doboznak tekinti
- folyamatosan érkező és összesített adatokkal is tud számolni

A modell alapötlete:

- a komplex műszaki rendszerek bizonyos mértékig a szoftverhez hasonlóan kezelhetők
- az előforduló hibákat teljesen ki lehet javítani
- az egyszer már előfordult hibákat a felhasználó azonos formában nem ismétli meg

A modell koncepciója

Úgynevezett „tanulógörbe”, amely a használat során bővülő ismereteket figyelembe veszi az előrejelzésben

Jelölések

- U – összes figyelembe vett programfutási idő
 $c(u)$ – u idő elteltéig jelentkezett hibák száma
 $q(u)$ – u idő elteltéig érvényes meghibásodási ráta
 a, b – skálaparaméterek

Matematikai feltevések

A tapasztalatok szerint az $(u, q(u))$ koordinátájú pontok logaritmikus beosztású papíron egy negatív irányzögű egyenes közelében helyezkednek el, vagyis logaritmusaik kapcsolata lineáris regresszióval jól leírható:

$$\log[q(u)] = (b - 1) \cdot \log(u) + \log(a)$$

ahol $b < 1$; innen

$$q(u) \approx a \cdot u^{b-1}$$

Ugyancsak a tapasztalatok szerint

$$q(u) \approx \frac{c(u)}{u}$$

tehát az előfordult hibák számának növekedésével így alakul a $(0, u)$ időintervallumban bekövetkező meghibásodások számának várható értéke:

$$c(u) \approx a \cdot u^b$$

A modell értékelése

A programfutási idővel és az újonnan előkerülő hibákkal számolva a modell előrejelzési képessége igen jó; rosszul használható abban az esetben, ha a kezdeti adatok erősen eltérnek a feltevésektől, mert ezekre nagyon érzékeny a modell.

5.2. Jelinski és moranda modellje

A modell jellemzői

- naptári idő
- sztochasztikus
- a folyamatosan érkező adatokat is fel tudja dolgozni
- gyakoriságokkal számol
- fekete doboz
- a hibák száma véges
- a hibák csak akkor számítanak, ha megjelennek
- a javítás tökéletes
- a meghibásodási ráta csak a hibák megjelenésével változik

Jelölések

T	– az első programfutástól számított naptári idő
t	– a legutóbbi hibától számított naptári idő
t_i	– az $i-1$ és i sorszámú meghibásodások közti naptári idő
n	– a programban található összes hibák száma
c	– az adott időpontig megtalált és kijavított hibák száma
$q(c)$	– c számú hiba után érvényes meghibásodási ráta
z	– skálaparaméter
Σ	– összegzés 1-től c -ig

Matematikai modell

Feltételezzük, hogy

$$q(c) = z \cdot (n - c)$$

vagyis a következő időegység alatt felbukkanó hibák számának várható értéke a programban maradt hibák számával arányos. Bizonyítható, hogy n optimális becslését kapjuk a következő egyenletből:

$$\sum \frac{1}{n-i} = \frac{c \cdot T}{n \cdot T - \sum i \cdot t_i}$$

és ennek felhasználásával becsülhető z is:

$$z = \frac{c}{n \cdot T - \sum i \cdot t_i}$$

A modell értékelése

Eredeti formájában kevésbé vált be a gyakorlatban. Kiindulópontja több későbbi, sikeres modellnek.

5.3. Musa modellje

A modell jellemzői

- programfutási idő
- sztochasztikus
- a folyamatosan érkező adatokat is fel tudja dolgozni
- gyakoriságokkal számol
- fekete doboz
- a hibák száma véges

- a hibák csak akkor számítanak, ha megjelennek
- a javítás tökéletes
- a meghibásodási ráta csak a hibák megjelenésével változik

Jelölések

- t – a legutóbbi hibától számított programfutási idő
 n – a programban található összes hibák száma
 $c(t)$ – az adott időpontig megtalált és kijavított hibák száma
 $y(t)$ – t futási idő elteltével a következő meghibásodásig hátralevő idő várható értéke (a megbízhatóságelméletben szokásos jelölése: MTTF)
 $m(t)$ – $c(t)$ várható értéke
 C – tesztkompressziós faktor; azt fejezi ki, hogy a tesztelés során hányszor gyorsabban akadunk hibára, mint normál programfutás során

Matematikai modell

A t futási összidőig megtalált hibák számának várható értéke:

$$m(t) = n \cdot \left\{ 1 - \exp\left(-\frac{C}{y(0) \cdot n} \cdot t\right) \right\}$$

ahol $\exp(x) = e^x$, tehát az e alapú exponenciális függvény. Látható, hogy a jobboldalon a kapcsos zárójelen belüli rész t növekedésével 1-hez tart, így $m(t)$ is tart n -hez. A legközelebbi meghibásodásig eltelő idő várható értéke (MTTF):

$$y(t) = y(0) \cdot \exp\left(\frac{C}{y(0) \cdot n} \cdot t\right)$$

A jobboldalon az exponenciális részben t együtthatója pozitív, ezért a jobboldal végtelenhez tart. Tehát sok programfutás után a legközelebbi meghibásodásig eltelő idő minden határon túl nő. A megbízhatósági függvény:

$$R(t) = \exp\left(-\frac{t}{y(t)}\right)$$

Ennek alapján meghatározható, hogy ha a legközelebbi meghibásodásig várhatóan eltelő időt y_1 -ről y_2 -re akarjuk növelni, ehhez hány hibát kell megtalálnunk és kijavítanunk:

$$\Delta_c = (y(0) \cdot n) \cdot \left\{ \frac{1}{y_1} - \frac{1}{y_2} \right\}$$

Ugyancsak meghatározható, hogy ehhez mekkora programfutási időre van szükség:

$$\Delta_t = \frac{y(0) \cdot n}{C} \cdot \ln\left(\frac{y_2}{y_1}\right)$$

A modell értékelése

A programfutási idő alkalmazásával a gyakorlatban is bevált. Figyelembe veszi, hogy különbség van a tesztelési és felhasználási célú programfuttatás között. Lehetőséget ad a továbbfejlesztésre, új paraméterek bevezetésével jobb illeszkedés elérésére. Hátránya, hogy nem tesz különbséget az egyes hibák veszélyessége között.

Példa

Egy nagy program feltételezhetően kb. 300 hibát tartalmaz. A program indításától az első hiba megjelenéséig átlagosan eltelt idő (MTTF) 1.5 óra. A tesztkompressziós faktor becsült értéke 4.

Mennyi ideig kell tesztelni a programot ahhoz, hogy a megmaradó hibák számát 300-ról 10-re csökkenthessük?

Megoldás:

$$\Delta_c = (y(0) \cdot n) \cdot \left\{ \frac{1}{y_1} - \frac{1}{y_2} \right\}$$

Behelyettesítve:

$$300 - 10 = (300 \cdot 1,5) \cdot \left\{ \frac{1}{1,5} - \frac{1}{y_2} \right\}$$

Innen

$$y_2 = 45 \text{ óra}$$

Továbbá

$$\Delta_t = \frac{y(0) \cdot n}{C} \cdot \ln \left(\frac{y_2}{y_1} \right)$$

Behelyettesítve:

$$\Delta_t = \frac{300 \cdot 1,5}{4} \cdot \ln \left(\frac{45}{1,5} \right) = 382,6$$

Innen

$$\Delta_t = 382,6 \text{ óra}$$

Tehát ennyi tesztelési időre van szükség, hogy a programhibák száma 10-re csökkenjen.

Végül

$$R(t) = \exp \left(- \frac{t}{y(t)} \right)$$

Behelyettesítve:

$$R(50) = \exp \left(- \frac{50}{45} \right) = 0,33$$

Vagyis a 382.6 órányi tesztelés elvégzése után legalább 50 óra hibamentes működés valószínűsége 0,33 lesz.

5.4. Goel és Okumoto modellje

A modell jellemzői

- programfutási időt alkalmaz
- sztochasztikus
- gyakoriságokkal számol
- fekete doboz
- a hibák száma véges, de véletlen
- a hibák csak akkor számítanak, ha megjelennek
- a javítás nem feltétlenül tökéletes
- a meghibásodási ráta csak a hibák megjelenésével változik

Jelölések

- t – a legutóbbi hibától számított programfutási idő
 n – a programban található összes hibák számának várható értéke
 $c(t)$ – az adott időpontig megtalált hibák száma
 $m(t) - c(t)$ várható értéke
 z – arányossági tényező a meglevő és megmutatkozó hibák között

Matematikai modell

Az időegység alatt megmutatkozó hibák átlagos száma egyenesen arányos a programban még benn található hibák átlagos számával.

A t futási összidőig megtalált hibák számának várható értéke:

$$m(t) = n \cdot \{1 - \exp(-z \cdot t)\}$$

Látható, hogy a jobboldalon a kapcsos zárójelen belüli rész t növekedésével 1-hez tart, így $m(t)$ is tart n -hez.

Feltételezzük, hogy $c(t)$ Poisson-eloszlást követ, paramétere és várható értéke $m(t)$.

Értékelés

Goel és Okumoto modellje egyaránt közel áll Musa, valamint Jelinski és Moranda modelljéhez. Egyetlen új paraméter bevezetésével modellezhető a nem tökéletes javítás. Legyen p annak a valószínűsége, hogy sikeres a javítás. z helyett pz paramétert használhatunk.

Hivatkozások

Kun, I., Szász, G., Zsigmond, Gy. (2002): *Minőség és megbízhatóság I.-II.*, LSI, Budapest.

Long, J. (ed.) (2008): *Metrics Data Program*, National Aeronautics and Space Administration, <http://mdp.ivv.nasa.gov/index.html>

Mellor, P., Bendell, A. (eds) (1986): *Software Reliability. State of the Art Report*, Pergamon Infotech Ltd, Oxford-New York-Toronto.

Pan, Jiantao (1999): *Software Reliability*, http://www.ece.cmu.edu/~koopman/des_s99/sw_reliability/

Porkoláb, Z., Pataki, N., Sipos, Á. (2006): *Jelenleg használatos szoftvermetrikák összehasonlító elemzése*, Tanulmány, GVOP-3.2.2.-2004-07-0005/3.0, Budapest.

Leitold Ferenc

fleitold@veszprog.hu

VÍRUSVÉDELEM KIVÁLASZTÁSA

Absztrakt

A vírusvédelmi rendszerek kiválasztása nem egy egyszerű feladat. Alapvetően három módszer közül választhatunk:

- 1. Hagyatkozunk a gyártókra, hogy mit állítanak termékeikről.*
- 2. Saját magunk próbálkozunk meg a vírusvédelmek vizsgálatával, tesztelésével.*
- 3. Független tesztelő szervezet elemzéseire bizzuk választásunkat.*

Az első eset nem feltétlenül járható, hiszen minden gyártó a saját termékeit dicséri, hiszen azt szeretné eladni. A másik két lehetőség alapja a gyártótól független vizsgálat. Azonban ennek a kivitelezése sajnos nem kevés erőforrást igényel, így egy korrekt vizsgálatot nem feltétlenül tud egy átlagos felhasználó elvégezni. A CheckVir tesztlaborban automatikus módszerek alkalmazásával arra a feladatra vállalkozunk, hogy rendet tegyünk a vírusvédelmi rendszerek tesztelésének káoszában. Ebben a cikkben a vírusvédelmi rendszerek tesztelésének legfontosabb problémáit tekintjük át és a CheckVir tesztek legfontosabb újdonságait összegezzük.

It is not easy to select an antivirus solution. We can use three ways:

- 1. We select the product using the information provided by vendors.*
- 2. We can examine and test the products.*
- 3. We select the product using the information provided by an independent testing organization.*

The first case is not a good solution because every vendor suggests only his products. The base of the other two cases is the examination which is independent from the vendor. On the other hand the correct examination is a very expensive task and it can not be executed by an average user. In the CheckVir laboratory we would like to execute automatic testing jobs and provide exact information related to the antivirus solutions. In this paper the most important problems are discussed and new methods of the CheckVir project are summarized.

Kulcsszavak: vírusvédelem, tesztelés, vírus, kártevő ~ virus protection, testing, virus, malware

1. Vírusvédelemek tesztelésének problémái

A vírusvédelemek tesztelése, vizsgálata a szoftvertesztelésnek egy teljesen különálló területévé nőtte ki magát, ez az „általános” szoftverteszteléshez képest egy teljesen más terület. Ezen a területen ugyanis számos speciális körülmény nehezíti a tesztelést.

Egyrészt talán a vírusvédelmeken kívül nincs még egy olyan szoftverterület, ahol olyan gyorsan jelennének meg az új verziók. Ennek oka, hogy – mint matematikailag is bizonyított – általános vírusvédelem nem létezhet. A vírusvédelmek gyártói így az ismert kártevőkkel foglalkoznak elsősorban, ellenük próbálnak 100%-os védelmet biztosítani. Természetesen voltak és vannak is próbálkozások, kísérletek arra vonatkozóan, hogy bizonyos módszerekkel ismeretlen kártevőket is azonosítsanak. De mitől lesz egy kártevő ismert? Az „ismertség” itt arra vonatkozik, hogy a vírusvédelem gyártója a konkrét kártevő (vagy esetleg egy csoportjuk) ismeretében készíti el a kártevő ellenszerét (felismerési és eltávolítási algoritmusát). Így viszont az újabb és újabb kártevők megjelenésével újabb és újabb verziójú védelmeket kell kibocsátani. Létezik olyan gyártó, mely átlagosan 5-6 percenként (!) ad ki egy új verziót. Nyilvánvaló, hogy ennek még csak a követése (minden verzió letöltése és archiválása) is komoly feladat.

A gyakorlatilag folyamatosan megjelenő új verziók mellett a vírusvédelmek esetén egyre inkább megjelenik a „cloud technology” fogalom, ami azt jelenti, hogy a védelmek a folyamatos internetes kapcsolat révén a gyártó által felállított központtól segítséget kérve hozzák meg döntéseiket. Ez azt jelenti, hogy a védelem működése különböző időpontokban más és más lehet.

További lényeges különbséget jelent, hogy a kártevők nagy száma miatt rengeteg tesztkörnyezetet feltételezhetnénk. Tegyük fel ugyanis, hogy létezik 10 millió kártevő. Elméletileg (de hangsúlyosan csak elméletileg) egy kártevő vagy jelen van egy tesztelési környezetben vagy nem, azaz így $2^{10 \text{ millió}}$ db tesztelési környezetet képzelhetnénk el. Ez természetesen kezelhetetlen, de még akkor is gondot okoz a mennyiségi probléma, ha csak azokat az eseteket vesszük alapul, ahol csak egyetlen kártevő van jelen (ez nyilván 10 millió a példa szerint).

Nagyon nehéz definiálni, hogy egy vírusvédelmi szoftvernek milyen elvárásoknak kell megfelelnie, mi az a működés, ami a vírusvédelem szempontjából korrekt, megbízható működésnek tekinthető. Az sem egyértelmű – és ebben is vannak különbségek a gyártók között –, hogy mely programokat tekintünk kártevőknek és melyeket nem. Sok védelem ugyanis olyan programokat is kártevőként azonosít, melyek esetén kérdéses a megítélés. Például egyes védelmek valamely szoftverhez licenszkulcsot generáló ún. feltörő (crack) programot is kártevőként azonosítanak. Hasonlóan gondot jelent – mint ahogy az Juraj Malcho (ESET) előadásában a minapi Virus Bulletin konferencián elhangzott, hogy egyre másra jelennek meg az olyan, gyakorlatilag hivatalosnak tűnő alkalmazások, melyek mögött teljesen legális cégek állnak. Ezek a cégek aztán mindent megtesznek azért, hogy a vírusvédelmek gyártóinak adatbázisából kikerüljön a termékük.

Az AMTSO-t (Anti-Malware Testing Standards Organization) 2008-ban alapították elsősorban kártevők elleni védelmi szoftvereket fejlesztők, de a munkában számos tesztelés végző szervezet mellett néhány magánszemély is részt vesz. A szervezetnek jelenleg 38 tagja van, köztük természetesen valamennyi jelentős fejlesztő. A hazai színeket a Virusbuster mellett a Checkvir tesztlabort üzemeltető Veszprog Kft. képviseli. Az elsődleges célkitűzések

között szerepel, hogy a vírus- és kártevővédelmi szoftverek tesztelésére vonatkozóan ajánlásokat, oktatási anyagokat dolgozzon ki, tesztelést segítő eszközöket bocsásson rendelkezésre, illetve az érintett felek között fórumot biztosítson.

2. Tesztelési módszerek

Vírusvédelmi rendszerek esetén a fent vázolt problémák miatt elképzelhetetlen, hogy a szoftver minden ágát teszteljük. Bizonyos szempontokat – melyek megfelelnek az AMTSO ajánlásainak is – azonban célszerű betartani.

A tesztelési eljárásnak célszerűen nyíltnak és átláthatónak kell lennie. Ez vonatkozik egyrészt a tesztelési metódus és a konkrét tesztelési folyamatok átláthatóságára is. A nyílt és átláthatóság követelménye nem feltétlenül jelenti a reprodukálhatóság biztosítását. Ennek legfőbb oka a dinamikus internethasználat, mely mind a védelmek (fenti 2. probléma), mind a kártevők részéről egyaránt jelen van. A nyíltságot és átláthatóságot azonban a dokumentáltság szintjének emelésével javíthatjuk. Ehhez célszerű a tesztelt állapotot (installált rendszert), a naplóállományokat, hálózati forgalmat elmenteni, illetve a problémás szituációkról képet és videót is rögzíteni.

Mint azt a fenti problémák esetén láhattuk, a vírusvédelmek valamennyi folyamatát nem tesztelhetjük. Bizonyos szempontokat vizsgálhatunk “csak”, célszerűen azokat, melyek a legfontosabbak a felhasználó szempontjából:

- a. **Hatékonyság**, azaz a védelem milyen biztonsági szintet tud biztosítani (kártevők korrekt ismerete – felismerés, eltávolítás). Ez a szempont kifejezetten az antivírus képességeire vonatkozik: Milyen kártevők elleni védelemre készítették fel a védelmet? Milyen területeket képes vizsgálni? Ide tartoznak a különböző diszkrétterületek vizsgálati lehetőségei, fájlformátumok, tömörítők és egyéb fájlok tárolására használható formátumok vizsgálati lehetősége. Ebbe a csoportba tartozik természetesen a téves riasztások tesztelése is.
- b. **Megbízhatóság** (stabil, hibamentes működés). Képes-e a védelem úgy működni, hogy folyamatosan ellássa feladatát. A stabilitás vizsgálatánál a tesztelés során hangsúlyozottan kell törekedni a reprodukálhatóságra.
- c. **Teljesítmény** (sebesség, számítógép lassítása, bootolás időigénye). Általában a teljesítménnyel szembeni felhasználói elvárás akkor jelenik meg, ha védelem képes hibamentesen megfelelő biztonsági szintet nyújtani. Nem véletlen, hogy az AMTSO alapelvei között szerepel az, hogy a hatékonyságot és a teljesítményt együtt, kiegyensúlyozottan kell tesztelni. Ennek oka az, hogy ha például egy védelem nem vizsgál meg bizonyos dolgokat, nyilván gyorsabban képes végrehajtani feladatát. De hiába gyorsabb, ha nem véd bizonyos problémákkal szemben.

Vírusvédelmi rendszerek tesztelése esetén – a kártevők ismeretének vizsgálata során – kulcskérdés, hogy milyen és mennyi mintát használunk. A minőségre vonatkozóan az AMTSO május elején fogadott el egy dokumentumot, mely a használt minták validálásával foglalkozik. E szerint a tesztelés során olyan kártevő mintákat kell alkalmazni, melyek egyrészt működőképes kódot tartalmaznak, illetve valóban képesek a kártékony tevékenységet végrehajtani. Ennek biztosítása/bizonyítása nem egyszerű feladat. Mint az a fenti problémák között is szerepelt, nem egyértelmű, hogy mi tekinthető kártevőnek és mi nem. Hasonlóképpen számos védelmi rendszer olyan állományt is kártevőként azonosít,

amelyet semmilyen környezetben nem lehet futóképesé tenni, azaz végrehajtani, például tönkretett futtatható állományok. A tesztelés szempontjából a mennyiség is nagyon fontos kérdés, azonban a használt minták mennyiségét (mint a tesztelési módszer egy lényeges elemét) a tesztelés céljának kell meghatározni. A tesztelés kiterjedhet egyrészt a létező kártevők összességére. Ebben az esetben nyilván milliós nagyságrendű készlettel lehetne statisztikailag helyes következtetésre jutni (itt viszont a korrekt validálás okozna nagy problémát). A szűkítésre két lehetőség kínálkozik: egyrészt vizsgálhatunk bizonyos típusú kártevőket, amivel egy adott területre fókuszálva vonhatunk le következtetéseket a vírusvédelmek tudására vonatkozóan. Másrészt figyelembe vehetjük az elterjedtségi adatokat is. A létező kártevők mennyiségéhez képest az elterjedt kártevők száma több nagyságrenddel kevesebb. Ezen kártevők körében már statisztikailag is helyes következtetést vonhatunk le néhány ezres mintakészlettel. Felmerülhet még továbbá olyan vizsgálatnak a lehetősége is, ahol nem az a cél, hogy a felismerési képesség alapján rangsoroljuk a védelmeket, hanem hogy egy-egy konkrét biztonsági probléma kezelésére következtessünk, azaz például válaszoljunk olyan kérdésekre, amelyek arra terjednek ki, hogy valamely felmerült probléma jelent-e biztonsági kockázatot. Ilyen esetben néhány minta is elegendő lehet a vizsgálathoz.

A védelmi rendszerek számos tevékenységgel azonosíthatnak egy kártevőt. Amennyiben a felhasználó indítja el interaktív módon a vizsgálatot, on-demand eljárásról beszélünk. Az azonosítást a folyamatosan figyelő ún. on-access védelem is megteheti. Ez utóbbi felfedezheti a kártevőket a fájlhoz történő hozzáféréskor, de előfordulhat, hogy bizonyos kártevőket a védelem csak akkor képes azonosítani és persze blokkolni, ha azokat elindítjuk. Ez utóbbi – proaktívnak hívott – működés egyre gyakoribb a vírusvédelmek esetén. A tesztelési folyamat során tehát célszerű proaktív vizsgálatot végezni. A módszer természetéből adódóan ezt viszont csak úgy szabad elvégezni, ha az operációs rendszer bootolását követően minden egyes alkalommal csak egyetlen kártevőpéldánnyal tesztelünk. Az ily módon történő tesztelés ezért rendkívül időigényes. Gondoljunk csak bele: Ha egy számítógépet használunk egy védelmi rendszerhez és egyetlen kártevő tesztelése 5 percet vesz igénybe – amibe beletartozik az eredeti, biztosan vírusmentes operációs rendszer visszaállítása is –, akkor egymillió minta teszteléséhez mintegy 9 és fél évre lenne szükség. Proaktív tesztet mindezek alapján tehát nagy mennyiségű mintán belátható időn belül nem végezhetünk. További nehézséget jelent, hogy egyes kártevők az azonosításukhoz szükséges tevékenységeket esetenként internetes kapcsolat révén biztosítják. Ebben az esetben viszont bonyolult feladat annak biztosítása, hogy a kártevő ne kerülhessen ki a tesztkörnyezetből.

3. Valós idejű tesztelés a CheckVir tesztlaborban

A CheckVir tesztlaborban az NKTH Baross Gábor Programjának (KD_INTEG_07-FB124076), illetve a Gazdaságfejlesztési Operatív Program (GOP-2.1.1-09/A-2009-1298) támogatásával a vírusvédelmi rendszerek folyamatos, valós idejű (real-time) tesztelésére alkalmas rendszert alakítunk ki. A tervezett rendszer alkalmas arra, hogy a vizsgált rendszerek tesztelését naponta néhány alkalommal automatikusan elvégezze. A rendszer tehát naponta (többször is) megpróbálja a védelmi rendszereket (és persze az operációs rendszert is) frissíteni, majd ha ténylegesen történt frissítés, akkor előre definiált tesztek sorát hajtja végre. Az eredmények pedig a tesztelést követően azonnal megjelennek az interneten. Nyilvánvaló, hogy a tesztek végrehajtásához idő kell, néhány percenként megjelenő frissítések esetén a rendszer nem lehet képes valamennyi verzió átfogó tesztjére. A termékenként naponta 1-2 teszt végrehajtása esetén azonban így is sokkal inkább a valós tudáshoz és teljesítményhez közelít a vizsgálatok eredménye.

A CheckVir projekt célja, hogy aktuális információkat biztosítson a vírusvédelmi eljárásokat tartalmazó megoldások hatékonyságára, megbízhatóságára és teljesítményére vonatkozóan. Tekintettel arra, hogy a teszteredmények a vizsgálatot követően azonnal publikálásra kerülnek, így a tesztelés nem a múlt, hanem a jelenre vonatkozik.

3.1. Technikai háttér

A CheckVir tesztlaborban jelenleg mintegy 15 Intel P4-es számítógép végzi a kártevők szaporítását és a teszteléseket. A GOP pályázat támogatásával most olyan cluster rendszer alakulhat ki, amely további 24 db négymagos Intel számítógépet jelent. Ez pedig a jelenlegi számítási kapacitást megsokszorozza.

A tesztfeladatok egy keretrendszerben kerülnek végrehajtásra. A rendszert vezérlő számítógép folyamatosan generálja a végrehajtandó feladatokat, amit aztán a kliens számítógépek elvégeznek, majd egy újabb feladatot keresnek maguknak. A keretrendszer olyan feladatokat képes végrehajtani, amely például egy termék frissítésére, vagy akár egy tesztelési részfeladat végrehajtására vonatkozik. Amennyiben egy termék frissítése sikeresen megtörtént, a teljes környezet archiválásra kerül és automatikusan létrejönnek az új verzióra vonatkozó tesztfeladatok. A rendszer működése során a fentiekben túlmenően az operációs rendszer frissítését végző feladatok is végrehajtásra kerülnek.

A teszteredmények a kiértékelést követően egy helyi adatbázisba kerülnek, ahonnan percenkénti szinkronizálással másolódnak a web kiszolgáló adatbázisába. A webkiszolgáló pedig dinamikusan jeleníti meg az eredményeket.

A valós idejű tesztelés folyamatos működése így természetesen a webszerver és a tesztlabor közötti kapcsolattól is függ. Ennek bizonytalansági kockázatát alternatív internet-szolgáltatókkal próbáljuk csökkenteni.

3.2. Internet-kapcsolat kezelése

A rendszer megvalósítása szempontjából egy lényegesen külön részfeladat a keretrendszerben lévő, a frissítéseket és magukat a tesztfeladatokat is végrehajtó kliens számítógépek internet-kapcsolatának a kezelése. A projekt szempontjából két probléma merült fel, melyek együttesen szükségessé tették egy úgynevezett intelligens proxy szerver kialakítását:

- Mind a kártevők, mind pedig a védelmek esetén megjelent a már említett “in-the-cloud” technológia használata. Kártevők esetén ez azt jelenti, hogy a kártékony kód egy részét az internetről tölti le, a védelmek esetén pedig folyamatos kapcsolatot jelent a gyártó rendszerével.
- A kártevők jelentős részének azonosítása ma már csak proaktív védelemmel oldható meg. Ez azt jelenti, hogy a védelem csak akkor képes azonosítani és blokkolni a kártevőt, ha a felhasználó azt elindítja.

A két problémával külön-külön a projekt során tervezett rendszer képes lenne megbirkózni, azonban a két probléma együttes kezelése már nehézkes, hiszen az alábbiakat kell biztosítani a tesztkörnyezetben:

- A védelmi rendszereknek legyen lehetősége a gyártó rendszeréhez korlátozás nélkül csatlakozni.

- Egyazon kártevő különböző időpontban (különböző védelmi rendszerekkel) történő vizsgálatakor biztosítani kell, hogy az internetről ugyanazt a kódot töltsse le. Ellenkező esetben az eredmények összehasonlítása nem lehet megalapozott. A letöltött kódot persze archiválni is célszerű.
- Biztosítani kell, hogy a kártevők ne legyenek képesek arra, hogy az internetkapcsolaton keresztül más számítógépeket megfertőzzenek.

Mindezek alapján olyan internetkapcsolatra van szükség, ami a védelmi rendszerek gyártói felé engedik a védelmi rendszer forgalmát, a kártevők esetén pedig gyakorlatilag egy virtuális internetet biztosít.

A tesztkörnyezet kialakítása során kézenfekvőnek tűnik az a megoldás, hogy használjunk valamilyen proxy szervert. Egy proxy képes tárolni a „külső” hálózat felől érkező adatokat és azt továbbítani egy „belső” tesztkörnyezetben futó számítógép felé. Egy proxy fontos eleme lehet a tesztkörnyezetnek, azonban önmagában semmiképpen sem tudja a feladatot ellátni. Használata során különböző problémák jelentkezhetnek. Ezek közül a legfontosabbak:

- Nem minden hálózati protokoll támogatja a proxy használatát, bár a leggyakrabban használtak (pl.: http, ftp) igen.
- Egy proxy szerver a cache-ét folyamatosan frissíti, így egy „korábbi állapot” megőrzése nem automatikus.
- Egy http proxy bizonyos fejlécek segítségével utasítható arra, hogy ne tárolja le a cache-ében az adott tartalmat.
- Egy futó alkalmazás képes érzékelni, hogy proxy-n keresztül kapcsolódik a külső hálózat felé, azáltal másképp működhet, mint azt „normális esetben” proxy nélkül tenné.

Az előzőek figyelembe vételével a tesztkörnyezetben tehát nem támaszkodhatunk kizárólag egy proxy szerverre. Fontos feladat a tényleges hálózati forgalom rögzítése, ennek analízisa. A proxy szervert ezen túlmenően fel kell vételezni azzal a képességgel, hogy képes legyen adott szituációhoz igazodni. A megfigyelésnek vannak olyan szakaszai, amikor észlelni és rögzíteni kell a hálózati forgalmat. Amennyiben ez rendelkezésre áll, akkor csakis ezt felhasználva oldható meg az, hogy a proxy szervert „intelligenciával” lássuk el.

A tesztkörnyezettel szemben támasztott legfontosabb működési követelmények:

- Legyen lehetőség előre és dinamikusan is meghatározni, hogy a tesztkörnyezetből mely gépek érhetik el a külső hálózatot, illetve ezen belül mely számítógépeket.
- Biztosítani kell a belső tesztgépek számára a névfeloldást és az IP címek automatikus hozzárendelését (DHCP).
- Naplózni kell a bekövetkező eseményeket.
- A tesztkörnyezetnek a „lehetőségekhez mérten” zártnak kell lennie, tehát biztosítani kell azt, hogy „nem kívánt módon” számítógépek ne fertőződjenek meg.

Az előző kritériumok alapján célszerű olyan operációs rendszert használni a környezet vezérlésére, ahol minimálisra csökkenthető a vírusveszélyből és a támadásokból eredő veszély. Linux operációs rendszerben az előző feladatok megoldhatók, a Linux tűzfala segítségével finoman szabályozható a külső elérés, illetve az átmenő forgalom.

3.3. Tesztfeladatok

A végrehajtandó tesztfeladatok a vírusvédelmi rendszerek három lényeges tulajdonságát mérik: hatékonyság, megbízhatóság, teljesítmény. A hatékonyság és a megbízhatóság a védelmi rendszerek estén bizonyos mértékig összetartozó fogalmak, hiszen egy felhasználó nyilvánvalóan a hatékony védelmi rendszert tekinti megbízhatónak.

A hatékonyság problémakörébe olyan vizsgálatok tartoznak, amelyek a védelmi rendszer azon képességét mérik, amelyek arra vonatkoznak, hogy milyen problémák esetén képesek védelmet nyújtani. A kártevők elleni védelemre szorítva a kérdéskört: mely kártevőket, mely területeken képes megakadályozni tevékenységében. Az viszont itt másodlagos, hogy ezt milyen módszerrel teszi. Továbbá ide tartozik természetesen annak a vizsgálata is, hogy a kártevőktől mentes, tiszta állományok közül melyeket és milyen arányban minősít a védelem kártékónak.

A megbízhatóság ellenőrzése a védelmi rendszer korrekt, hibamentes működésének vizsgálatát jelenti. Ebben a kérdéskörben olyan tesztekét képzelhetünk el, amelyek a védelmi rendszert megpróbálják akár az átlagosnál nagyobb feladat elé állítani, mintegy terheléses vizsgálatot végezve. A korrektséghez hozzátartozik a védelmi rendszer konzekvens viselkedése is például a különböző védelmi módszerek (on-demand, on-access) esetén.

A teljesítmény a felhasználó szempontjából leginkább a különböző védelmi módszerek sebességét jelenti: milyen gyorsan képesek végezni egy adott feladattal, mennyire lassítják a számítógép működését.

A CheckVir projektben az alábbi tesztfeladatokat tervezzük automatikusan végrehajtani:

Kártevők ismeretének a vizsgálata (felismerés): Alapfeltétel, hogy a tesztelt megoldás képes legyen valamilyen naplóállomány készíteni a vizsgálatról. A felhasználó által indított on-demand ellenőrzés során a kártevők találatainak az összesítése történik. A folyamatosan figyelő on-access védelmek esetén a vizsgálat kicsit bonyolultabb. Itt nemcsak a naplóállományokat elemezzük, hanem megvizsgáljuk, hogy a kártevők másolása esetén mi történik a forrással és mi lesz a "célban". Természetesen itt olyan beállításokat kell alkalmaznunk, ami arra utasítja a védelmet, hogy kártevő esetén valamilyen módon gátolja meg a másolást. Tekintettel arra, hogy a védelmi rendszerek jelentős része ma már proaktív védelemmel is rendelkezik, az olyan kártevők esetén, amiket a másolás során nem azonosított a védelem, szükség van a proaktív védelem vizsgálatára. Ehhez a kártevőket el kell indítani a tesztkörnyezetben és vizsgálni a védelmet, hogy meggátolja-e a kártevő működését. Ehhez azonban minden egyes kártevő vizsgálatát megelőzően kártevőmentes környezetre van szükség.

Kártevők ismeretének a vizsgálata (eltávolítás - helyreállítás): A kártevők kódjának eltávolításának, az eredeti kártevőmentes állapot visszaállításának vizsgálata mind az on-demand, mind az on-access, illetve a proaktív esetben is elvégezhető. Mindegyik esetben a vizsgálat arra terjed ki, hogy a védelem működése előtti állapot hogyan változott meg. A változásokat természetesen a védelmi rendszer naplójával is összevetjük.

Téves (false positive) riasztások vizsgálata: Az on-demand ellenőrzések esetén a védelmi rendszerek által generált naplóállományok vizsgálata alapján, on-access esetben pedig a

naplóállományok, illetve a forrás és a célterületek alapján történik azon fertőzésmentes állományok körének a meghatározása, amelyek esetén a védelem – tévesen – kártevőt jelez.

Sebesség ellenőrzése kártevőmentes környezetben: A sebesség ellenőrzését alapvetően kártevőmentes környezetben célszerű elvégezni. Kártevő(k) találata esetén ugyanis már másodlagossá válik a sebesség, a felhasználók számára sokkal fontosabb lesz a biztonságos helyreállítás. Másrészt pedig a sebesség nagyban függ a találat esetén elvégzendő akciótól (törlés, eltávolítás, karanténba helyezés, ...). Kártevőmentes környezetben a sebességet nagyban befolyásolja a hardver és szoftver környezet is. On-demand esetben az indítás és befejezés közti időtartam jelenti az ellenőrzés idejét. On-access esetben ez egy kicsit bonyolultabb. Ekkor ugyanis, ha például másolással történik a vizsgálat, akkor – a korrekt összehasonlíthatóság érdekében –, az indítás és befejezés között eltelt időtartamot csökkentenünk kell a védelem nélküli rendszerben ugyanezen feladat elvégzéséhez szükséges időtartammal. Így kapjuk meg ugyanis tisztán a védelem időszükségletét. A sebességellenőrzések mindegyikét – a hiba mértékének csökkentése érdekében - legalább 20-szor végezzük el. A vizsgálat eredménye ezen időtartamok statisztikai jellemzői (minimum, maximum, átlag, szórás).

“Konténer” teszt: A számítógép használata során átlagos körülmények között is előfordulhat, hogy egy felhasználó olyan állomány(oka)t hoz létre, amely fájl(oka)t tartalmaz. Ez történhet a felhasználó intereaktivitásával, vagy akár – mintegy észrevétlenül – teljesen automatikusan. A felhasználó közreműködése lehet például, ha egy ZIP állományt hoz létre vagy egy dokumentumba beleágyaz egy másik állományt. Az automatikus esetben például a felhasználó egy e-mail üzenetet tölt le és azt az e-mail kliense tárolja el. Az ilyen típusú állományok esetén a védelmi rendszernek ismernie kell ezen állományok felépítését. Az ilyen vizsgálatok elvégzése azért nagyon fontos, mert ha például egy védelem azt az üzenetet adja – miután egy számítógépet teljesen átvizsgált –, hogy az vírusmentes, akkor legyünk tisztában ezen üzenetnek a korlátaival. A vizsgálat során olyan állományt használunk, melyet valamennyi, a tesztelésben résztvevő védelem ismer (például az EICAR tesztfájlt: www.eicar.com) és ezt az állományt csomagoljuk be különböző “konténerekbe”. A vizsgálat során azt teszteljük, hogy képes-e a védelem az adott „konténerben” megtalálni a kártevőt illetve, hogy ezt konténerbe ágyazott konténerek sorában milyen mélységig képes megtenni. Ezen túlmenően speciális körülmények között is vizsgáljuk a védelem képességeit: hosszú fájlnevek használata, jelszóval védett konténerek, ...

3.4. Minták

A kártevők elleni védelmi rendszerek tesztelésének egy sarkalatos kérése mindig a használt kártevőminták körében rejlik. Manapság már több, mint 20 millió kártevő létezik a világon. Ezen kártevők nagyon nagy hányada nem jelent potenciális veszélyt egy átlagos felhasználó számára. Nagyon nehéz azonban meghatározni, hogy melyek azok a kártevők, amelyek valóban veszélyeztetik az átlagos felhasználó számítógépét. És persze az is igaz, hogy ezek – mivel különböző mértékben vannak elterjedve –, különböző arányban számíthatnánk a teszteredményekbe. Az elterjedtségi adatok azonban folyamatosan változnak, így ilyen súlyozás gyakorlatilag kivitelezhetetlen. Nem beszélve arról, hogy az elterjedtségi adatok gyártóról gyártóra változnak.

A CheckVir tesztlaborban a valós idejű tesztekhez a kártevők kétfajta mintakészletét használjuk. Az első csomagban a védelmi rendszerek gyártóitól származó elterjedtségi adatokat dolgozzuk fel a Wildlist (www.wildlist.org) listáival együtt. Ebben a készletben az

elmúlt három hónapban elterjedtként kezelt kártevőket teszteljük. A második csoportba a mindenkori utolsó fél évben a tesztlaborba érkezett minták kerülnek. Mindkét csoportban a kártevőket típus szerint osztályozzuk. Ez azonban nem minden esetben esik egybe néhány gyártó osztályozásával, itt is vannak ugyanis különbségek. A kártevőminták esetén alapvető feladat továbbá a minták validálása. Ez két dolog igazolását jelenti: Egyrészt igazolnunk kell a kártevő kódjának működőképességét, másrészt pedig azt, hogy valóban képes a káros tevékenység végrehajtására. Ehhez olyan automatikus rendszert használunk, amely mind natív, mind pedig virtuális környezetekben képes az említett feladatok elvégzésére.

Összegzés

Mint azt láthattuk, a vírusvédelmi rendszerek tesztelése messze nem triviális feladat. Általában is igaz, mindenfajta tesztelésre, hogy az nem azt igazolja, hogy egy szoftver hibamentes, funkcionálisan megfelelően működik, csupán azt képes bizonyítani (ha hiba adódott), hogy a szoftver nem tökéletes. Ez fokozottan igaz a vírusvédelmekre is, hiszen gyakorlatilag megoldhatatlan, hogy teljes, átfogó tesztet végezzünk egy-egy antivírus verzióval. Mindezek ellenére a vírusvédelmi rendszereket oly módon kell (és lehet is) vizsgálni, amivel kimutathatóak azok a problémák, melyek az átlagos felhasználónál is előfordulhatnak. A CheckVir projekt célja egy folyamatosan működő, valós időben történő, automatikus tesztelés biztosítása, mely lehetőséget ad arra, hogy a felhasználók (a laikustól a rendszergazdáig) megfelelő információkkal rendelkezzenek a vírusvédelem kiválasztásához.

Molnár András

molnar.andras@nik.bmf.hu

ROBOTREPÜLŐGÉPEK FÖLDI ÁLLOMÁSA ÚJ MEGKÖZELÍTÉSBEN

Absztrakt

A legtöbb földi állomás korlátozott, előre meghatározott számú és dedikált funkciójú munkaállomást tartalmaz. A legolcsóbb rendszerek esetében a gyakorlati munka nehézkes mivel egy, esetleg két munkaállomást biztosít a rendszer melyeken keresztül kell a repülőgépet kontrollálni, valamint az általa szolgáltatott felderítési információkat kiértékelni. Léteznek ugyan hálózatba kapcsolt munkaállomások, de azok kisméretű, olcsó robotrepülőgépek számára nem elérhetőek.

A fejlesztés célja, létrehozni egy olyan univerzális földi állomást, amely gyakorlati szempontból korlátlan számú munkaállomással rendelkezik úgy, hogy azok funkcióját a mindenkori felhasználó dönthesse el. Az így kialakított földi állomás rugalmasan telepíthető, hatékonyabb kiértékelést és döntési lehetőségeket biztosít a felhasználók számára.

Most of the ground control stations contains only a limited and predetermined number of workstations with a dedicated function. The work with the cheapest stations is difficult because there are only one or two workstations. The user has to control the plane and evaluate the data via these. There are network connected workstations though but these are inaccessible to low cost UAVs. The aim of the development is to create a universal ground control station which has unlimited number of workstations who's function can be determined by the actual user. This type of ground control station is easy to install and it ensures a more effective way to evaluate the data and make operational decisions for the controlled UAV.

Kulcsszavak: *pilóta nélküli repülőgép, földi állomás ~ unmanned aerial vehicle, ground station*

Bevezetés

A fejlesztést több éves kutatás és elemzés előzte meg. A kutatások kiterjedtek a különféle UAV rendszerek technikai megvalósításaira [1,2,3,4,5,6], képességeinek elemzéseire, valamint a felhasználásuk körülményeire. Megállapítást nyert, hogy minden UAV rendszer földi állomása biztosítja a repülő eszköz, repülés előtti és alatti teljes ellenőrzését. Ez azt jelenti, hogy a földi állomás műszerei képesek a kezelőt ellátni a fedélzeten mért összes, vagy legtöbb létfontosságú információval. Ugyanez a rendszer lehetőséget biztosít az egyes paraméterek módosítására, hangolására. További képességei a földi állomásnak, hogy az UAV hasznos terhet jelentő rendszerek (például felderítő kamera) kezelését is biztosítják. Ez általában a rendszerek paraméterezését, illetve az általuk szolgáltatott információk megjelenítését jelenti.

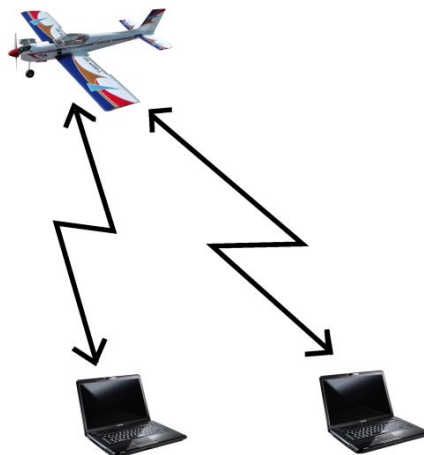
A kutatás során érzékelhetővé vált a jelenlegi rendszerek (elsősorban a kisméretű robotrepülőgépek hordozható, vagy könnyű gépjárműbe integrálható földi állomásainak) szűk keresztmetszete. Általában elmondható, hogy az eszközök a gyártók által megjelölt feladatok végrehajtására alkalmasak, de kezelésük kényelmetlen. Legnagyobb hátrányt a repülőgép kezelését és az általa szolgáltatott adatok megjelenítését biztosító munkaállomások erősen korlátozott száma jelenti. A repülés alatt igen körülményes az adatok elemzésébe bevonni további szakértőket, így a felderítő képességein múlik a repülés eredményessége.

A dedikált munkaállomásokkal kialakított rendszerek általános jellemzői

A hagyományos kialakítású földi munkaállomások jellemzően előre meghatározott feladat ellátására alkalmasak. Ezeket a gyártók igyekeznek úgy kifejleszteni, hogy az adott célnak a lehető legjobban megfeleljenek. A repülőgép ellenőrzését és vezetését biztosító munkaállomás rendszerint mindent tartalmaz, ami az adott repülőgép üzemeltetéséhez kellhet. Hasonló módon vannak kialakítva a felderítő felületek is. Általában ezek a feladatkörök a következők:

- UAV konfigurálása.
- Útvonal tervezése.
- Telemetria megjelenítése.
- Fedélzeti képek videók megjelenítése, feldolgozása.
- Egyéb fedélzeti szenzorok adatainak megjelenítése, feldolgozása.
- A repülés folyamatába történő beavatkozáshoz szükséges eszközök (kapcsolók, üzemmód váltók).
- A hasznos teher kezelését biztosító eszközök (kapcsolók, üzemmód váltók).
- Vészrendszerek.

A mennyiben a fenti funkciókat dedikált rendszerek valósítják meg, úgy a fejlesztés és a gyártás jól kézben tartható. Javítás, hibakeresés szempontjából átlátható. Ennek a struktúrának felel meg az 1. ábrán látható rendszer.



1. ábra. Dedikált munkaállomásokkal kialakított UAV rendszer

Az 1. ábrán látható kommunikációs csatornák nem szükségszerűen különbözőek, bár jellemzően a telemetria és a repülőgép irányítása, valamint a nagy sávszélességet igénylő képi információk két egymástól független csatornán valósulnak meg. Logikailag hasonló rendszerhez jutunk, ha az adatkommunikáció ugyan egy csatornán zajlik, de a földi munkaállomások kialakítása a gyártó által előre meghatározott célt támogatja. Ilyen kialakítás például az, ha az egyik állomás a repülőgép vezetését, míg a másik a fedélzeti kamera képének kiértékelést teszi lehetővé.

A gyártó által előre meghatározott funkciókkal rendelkező munkaállomás merev alkalmazhatóságot biztosít. A felhasználó nem alakíthatja igényei szerint ki a munkahelyeket. Sok esetben szükség lenne további, úgynevezett megfigyelő munkahelyekre, de a dedikált rendszerek esetében ezek kialakítása körülményes. Azok a rendszerek, amelyek lehetővé teszik a további munkahelyek beiktatását, rendszerint a közvetített kép elosztását biztosítják valamilyen videó csatlakozási lehetőséggel. Az így kialakított plusz munkahely csupán megfigyelésre alkalmas. Nincs lehetőség a rendszerbe való beavatkozásra, mint például kamera mozgatása, nagyítás változtatása, stb.

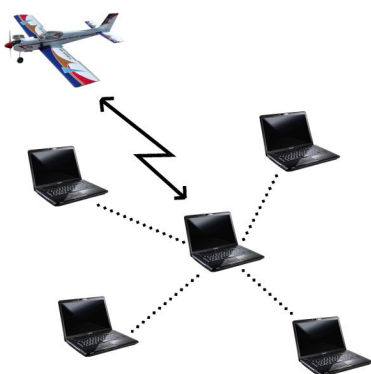
Az elosztott architektúrájú munkaállomásokkal kialakított rendszer általános jellemzői

Az elosztott architektúrájú földi állomás kifejlesztése során szem előtt kellett tartani azokat a funkciókat, amelyekkel a dedikált rendszerek rendelkeznek. Ezek mindegyike szükséges az UAV-k üzemeltetéséhez, így törekedni kellett azok maradéktalan és korlátozásmentes megvalósítására, miközben rugalmassá kellett tenni a munkaállomások felhasználhatóságát. Ennek megfelelően az elosztott architektúrájú rendszer az alábbi módon egészül ki:

- **Dedikált eszközök:**
 - Adatbázis kezelő.
 - Hálózati adatszolgáltató.
- **Önálló kliensek:**
 - UAV konfigurálása.

- Útvonal tervezése.
- Telemetria megjelenítése.
- Fedélzeti képek videók megjelenítése, feldolgozása.
- Egyéb fedélzeti szenzorok adatainak megjelenítése, feldolgozása.
- A repülés folyamatába történő beavatkozáshoz szükséges eszközök (kapcsolók, üzemmód váltók).
- A hasznos teher kezelését biztosító eszközök (kapcsolók, üzemmód váltók).
- Vészrendszerek.

Jól látható, hogy az elosztott rendszer esetében is megjelenik egy dedikált rendszer. Ennek feladata a repülőgéppel történő kapcsolattartás és a kliensek kiszolgálása. A rendszer általános felépítését a 2. ábra szemlélteti.



2. ábra. Elosztott architektúrájú munkaállomásokkal kialakított UAV rendszer

Természetesen a repülőgép és a központi számítógép között kialakított kommunikációs csatorna nem szükségszerűen egy. Logikáját tekintve több csatornán is történhet adatforgalom, de ezek mindegyike a központi számítógépen keresztül valósul meg. A központi gép és a kliensek (munkaállomások) között a hagyományosnak mondható TCP/IP alapú kommunikáció zajlik, bár a hálózatba kapcsolt gépek protokollja ezen az absztrakciós szinten nem releváns. Elméletileg megfelel minden olyan hálózati protokoll, amely a biztosítani tuja a megfelelő sávszélességet és adatsebességet.

A megvalósított rendszer tesztelése során a gépek közti kommunikációra megfelelőnek bizonyult a 100 Mbytes Ethernet, valamint a WiFi kapcsolat.

Az elosztott architektúrájú rendszerek hátránya elsősorban a fejlesztés bonyolultságában jelentkezik. A szerver program esetében körültekintően kell eljárni, mivel előre nem tudható, hogy hány kliens van éppen bekapcsolva, illetve azok mikor küldenek utasításokat a repülőgép felé. Gondos tervezéssel és körültekintő programozással azonban készíthető megfelelően megbízható program.

A központi (szerver) számítógép feladata

A központi gép feladata három fő csoportra bontható:

1. Az adatok fogadása és továbbítása a repülőgép felé. A központi gépnek természetesen nem feladata a közvetlen adatkapcsolat biztosítása, de maradéktalanul le kell kezelnie a rádiófrekvenciás adó-vevő egység kommunikációs csatornájának adatforgalmát.
2. A fogadott adatok archiválása egy olyan adatbázisba, amelyből tetszőleges időpillanatban kinyerhetők a repülés adatai. Az adatbázis kell, hogy tartalmazza azokat a képi információkat is, amelyeket a repülőgép a küldetése során a földi állomás felé továbbított. Az adatbázis felépítése olyan kell, hogy legyen, hogy abból hatékonyan lehessen megkapni olyan adatokat, amelyek valamilyen logikai kapcsolatban vannak egymással. Ilyen például az egy időpillanathoz tartozó telemetriai és képi adat!
3. A kliensekkel történő kapcsolattartás, ami alapvetően a repülési adatok továbbítását, valamint a kliensek felől érkező utasítások archiválását és a repülőgép felé történő továbbítását jelenti.

A rendszer-architektúra tekintetében a szerver program egy dedikált számítógépen kell, hogy üzemeljen. Ennek a gépnek kell csatlakoznia a rádiófrekvenciás adó-vevő egységhez. Az alkalmazott számítógépen teljesítményétől függően lehetséges a szerverprogram futtatása mellett egy vagy több kliens alkalmazás futtatása is, de ebben az esetben az elosztott architektúra előnye elvész.

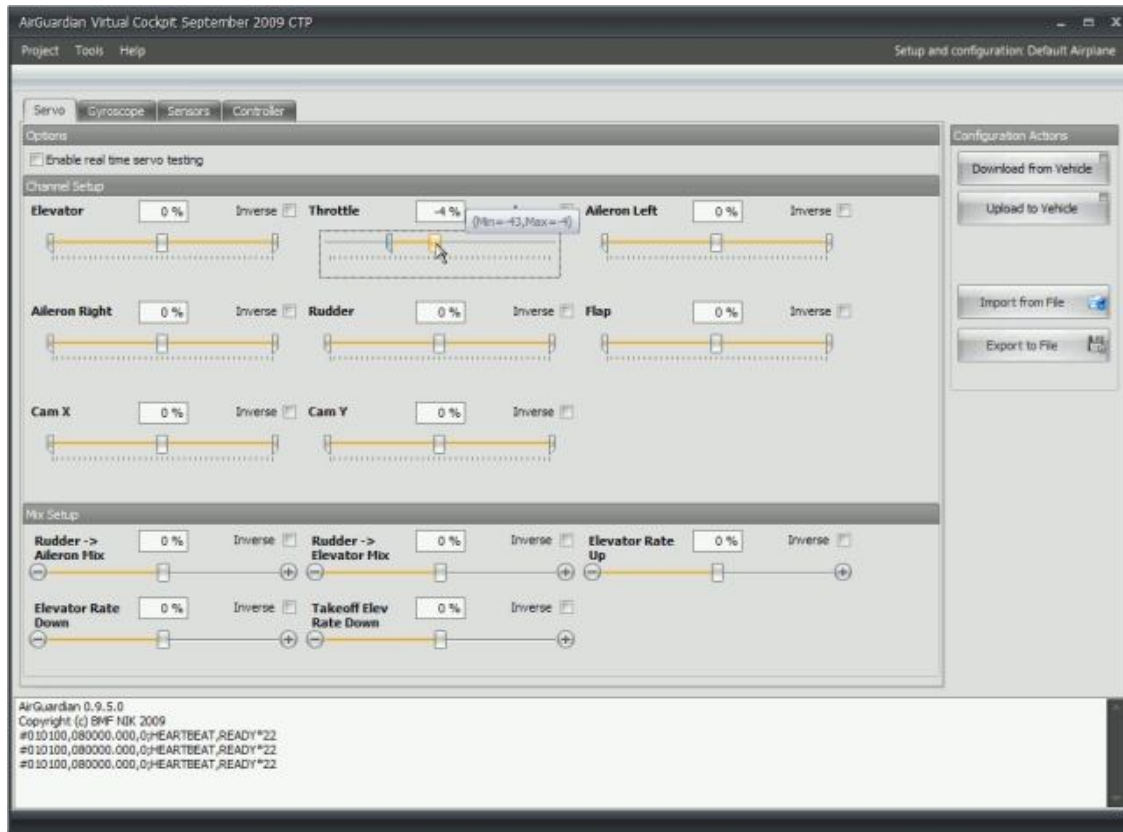
Kliensalkalmazások

A kliens alkalmazások valósítják meg a földi rendszer felhasználói kapcsolatát. Gyakorlatilag ezeken a klienseken keresztül valósulnak meg a már ismertett UAV funkciók. A kliensek egy olyan munkaállomáson működnek, amely összeköttetésben van a szerver géppel. (Amennyiben a szerver és a kliens programok egyazon számítógépen futnak, úgy a csatlakozás csupán logikai. A kapcsolat ebben az esetben is a programok közötti TCP/IP kommunikációval valósul meg.) Tekintettel arra, hogy egy adott feladatkört egy kliens program valósít meg, a munkaállomások a rájuk telepített kliensekkel válnak az adott feladatra alkalmassá. Ennek értelmében például bármely, a szerver géphez kapcsolt munkaállomás alkalmazható, mint virtuális pilótafülke, vagy felderítő esetleg útvonaltervező munkahelyként. Ezen logika azt sem zárja ki, hogy több munkaállomáson is egy időben futtathatók legyenek azonos kliensek. Megvalósítható például több felderítő állomás üzemeltetése úgy, hogy azok ugyanazt az adatot jelenítik meg a felhasználóknak, de azok akár eltérő módon is elemezhetik őket. Például az egyik munkaállomáson megfigyelhető a kamera képe, míg egy másikon ugyanannak a képnek valamilyen digitálisan feldolgozott változata. Ezzel a módszerrel a repülőgéptől érkező felderítési adatok azonos időben többféle feldolgozással is elemezhetők, ami jelentősen növelheti a releváns információk kinyerésének esélyét.

UAV konfigurációs modul

A konfigurációs modulon keresztül nyílik lehetőség a robotrepülőgép belső paramétereinek kezelésére (3. ábra). A modul több logikai felületre lett osztva, így önálló felület biztosítja a kezelőszervek (szervók) közép és végállásainak beállítását, valamint az egyes kormányok egymásra hatásának (mix) beállítását. Egy másik felület biztosítja a fedélzeti szenzorok kalibrációjának és egyéb jellemzőinek beállítását. Ilyen eszközök a magasság és sebességmérők,

valamint a fedélzeti energiaforrások állapotát mérő szenzorok. Külön felületen lehet az IMU-t (Inertial Measurement Unit, azaz inerciális mérő egység) konfigurálni, ami gyakorlatilag az „X, Y, Z” tengelyek erősítését jelenti.



3. ábra. A konfigurációs modul szervó beállító nézete

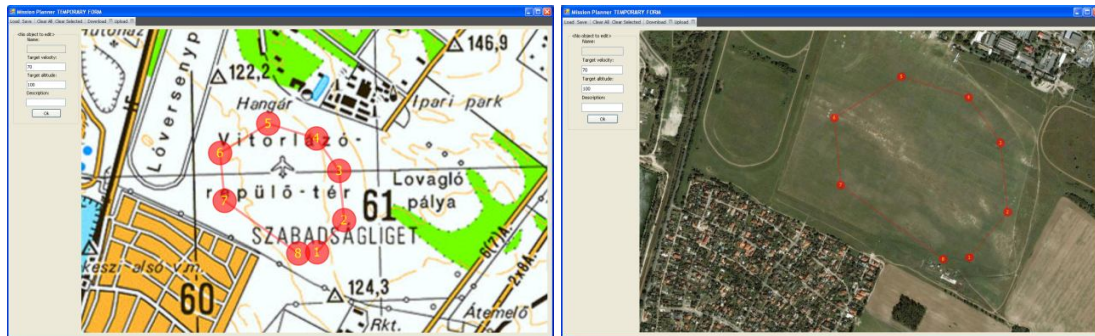
A modul lehetőséget biztosít az UAV fedélzetéről a teljes konfigurációs állomány letöltésére, illetve a földön elvégzett módosítások feltöltésére. Mivel minden UAV saját konfigurációs állománnyal rendelkezik, azok minden esetben az adott repülőgép fedélzeti egységében találhatók. A földi egység konfigurációs állományát a repülőgép közvetlenül nem használja, az csak az állomány kezelését támogatja. A repülőgépen a konfigurációs állomány csak a feltöltést követően válik aktívvá.

A modul használatára egy beállított repülőgép esetén már nincs szükség, így ez a felület a napi felhasználás során általában nem kerül betöltésre.

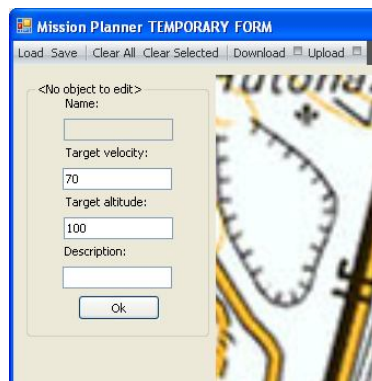
Útvonal tervező

Az útvonaltervező modul segítségével lehet megtervezni az UAV repülési programját. A modulban térképen vagy műholdképen készíthető el a tervezett repülés nyomvonala (4. ábra). A nyomvonal tervezése fordulópontok, vagy útvonalpontok megadásával lehetséges. Minden útvonalponthoz meg lehet adni sebesség és magasság paraméter, valamint egy megjegyzést (5. ábra), ami segíti a kezelőt a későbbi értelmezésben. A megadott sebesség és magasság a

repülőgép számára az adott útvonalpont érintését követően válik követendővé. Ez a módszer ad lehetőséget a különböző magasságok és az adott objektum közelében történő tartózkodási idők beállítására.



4. ábra. Az útvonal tervező modul térképpel (bal oldal) és műholdképpel (jobb oldal)



5. ábra. Egy útvonalponthoz megadható attribútum mező

Az útvonaltervező modul által készített repülési tervek elmenthetők, de az adott feladat végrehajtáshoz a megfelelő útvonalat fel kell tölteni a repülőgép fedélzeti egységébe. Az útvonal egyes elemei repülés közben is módosíthatóak, de azok csak akkor kerülnek végrehajtásra, ha a módosított útvonal feltöltésre került. Amennyiben a módosítás a már végrehajtott útvonalszakaszon történik, a feltöltést követően sem lesz hatása a repülésre. Érdemben módosítani egy adott útvonalterven a még végre nem hajtott útvonalszakaszon lehet.

Virtuális pilótafülke

A Virtuális Pilótafülke modul szolgáltatja a repülőgép kezelője számára az összes repüléssel kapcsolatos információt (6. ábra).



6. ábra. A Virtuális Pilótafülke modul

A képernyő négy logikai blokkra osztható:

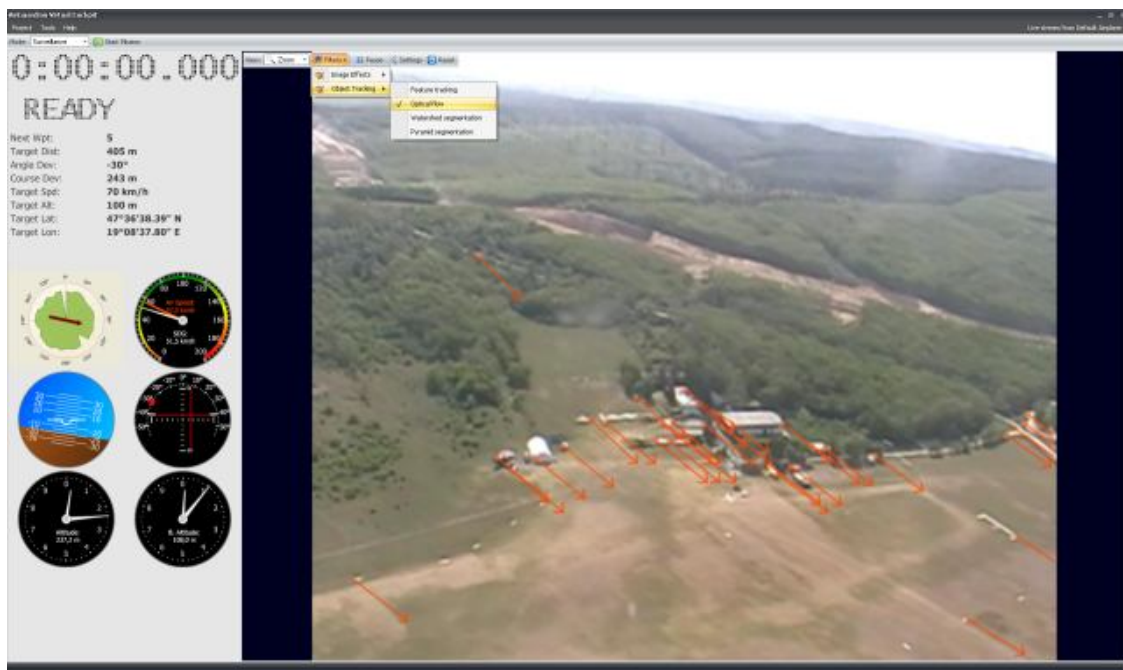
1. A térképen vagy műholdképen (a felhasználó választásától függ) nyomon követhető a repülőgép pillanatnyi pozíciója és az addig megrepült nyomvonala. A program lehetőséget biztosít a térkép nagyítására, illetve kicsinyítésére, így a felhasználó beállításától függően láthatóvá válhat a teljes repülési terület, vagy kinagyítható a repülőgép pillanatnyi pozíciója. A térképen megjelenített repülőgép sziluett a jobb láthatóság érdekében nem arányos a térképpel.
2. A képernyő bal oldalán a gépről továbbított videó folyam élő képe látható. Bár ezen a modulon is lehetőség van a kamerakép valós idejű módosítására (képszűrések, mozgások, objektumok automatikus megjelölése, stb.), ezt a feladatot célszerű a felderítő modulon elvégezni. Amennyiben az itt megjelenített kamera képe a repülőgép hossz tengelyével megegyezően előre néz és rögzített, felhasználható a repülőgép vezetésére, mivel a horizont dőléséből, illetve helyzetéből a repülőgép térbeli helyzete meghatározható.
3. A fedélzeti műszerek valós időben adnak tájékoztatást a gép pillanatnyi állapotáról. A kettős sebességmérő segítségével láthatóvá válik a gép földhöz viszonyított sebessége és a gép körül áramló levegő sebessége. A két érték különbségéből az adott helyen a szél sebességére lehet következtetni. A diagram informálja a kezelőt az elmúlt két perc repülési adatairól, így lehetőség nyílik az állapotváltozások tendenciájának megállapítására is. A navigációs műszer segítségével jól ellenőrizhető a tervezett

útvonaltól való eltérés mértéke mind magasság, irányszög és oldalirányú hiba tekintetében.

4. Az ikonok segítségével magas szintű utasítások adhatók a repülőgépnek. Ilyenek lehetnek a kamera ki- vagy bekapcsolása, felszállás, hazarepülés, leszállás, stb.

Felderítő modul

A felderítő modul feladata, hogy a fedélzeti felderítő kamera képét a lehető legnagyobb részletességgel jelenítse meg a képernyőn, és a megfigyelőt segítse a releváns képi tartalmak felismerésében (7. ábra). Bár ezen a felületen is megjelennek a legfontosabb fedélzeti műszerek, azok szerepe csupán annyi, hogy a megfigyelőnek legyen viszonyítási alapja a képvétel körülményeiről.



7. ábra. a Feltérítő modul

A megfigyelő modul lehetőséget biztosít a videó valós idejű elemzésére. Ennek érdekében különféle szűrők és tartalmi elemző algoritmusok kapcsolhatók be. A 7. ábrán egy optikai folyam elemző algoritmus eredménye látható. A piros nyilak a képen felismert objektumok mozgásvektorát ábrázolják. Ezzel a módszerrel a továbbiakban elkülöníthetővé válnak az átlagos mozgásvektortól eltérő vektorú objektumok, így lehetővé válik egy látszólagosan mozgó háttéren mozgó objektumok (járművek) megjelölése.

Tapasztalatok az elosztott architektúrájú földi vezérlőállomással

Az elkészült programrendszer teszt változata valós körülmények között igen jó eredményt hozott. Rugalmassága révén sikerrel alkalmaztuk egyetlen lappal is, de bemutatókon megbízhatóan üzemelt háromgépes WiFi technológiával összekapcsolt rendszer formájában is.

A tesztek során beigazolódott az a feltevés, hogy az elosztott architektúra kényelmes és megbízható repülőgép üzemeltetést tesz lehetővé. A rendszer teljesítmény igénye nem magas így hatékonyan lehetett alkalmazni egyetlen kétféle 2,16 GHz-es lappal 3 GB rammal, XP operációs rendszeren.

Továbbfejlesztési irányok

Az architektúra funkcionális fejlesztése befejeződött. További fejlesztések a szolgáltatások terén várhatók. Újabb kliensek kialakításával speciális fedélzeti egységek adatainak megjelenítése és elemzése is lehetségessé válhat. Az egyes kliensek indítása során a felhasználó autentikációjára is sor fog kerülni, ami lehetőséget biztosít a kezelők tevékenységeinek naplózására és a repülések teljes körű elemzéseire.

Felhasznált irodalom

1. Ye Hong, Jiancheng Fang, Ye Tao: Groun Control Station Development for Autonomous UAV, in Lecture Notes in Computer Sience, ISSN: 0302-9743
2. www.uavnavigation.com, The Ground control Station Software Interface (2009)
3. Groun Control Station, Virtual Cockpit v2.5, www.procerusuav.com, (2009)
4. ISRAEL at Defexpo 2006, Elbit System Ltd.
5. Major Richard Little, A short history of surveillance and target acquisition artillery, Canadian Army Journal Vol. 11.3 Fall 2008
6. Unmanned Vehicles Handbook 2008, SHEPHARD press publication, ISSN:1365-6546

Munk Sándor

munk.sandor@zmne.hu

A JÖVŐ INTERNETE KUTATÁSOK, EGY VÉDELMI/KATONAI KUTATÁSI PROGRAM KERETEI

Absztrakt

Az Internet az elmúlt 25 évben példa nélküli módon fejlődött, néhány tudós új típusú kommunikációs eszközéből a gazdasági növekedés emberek milliárdjainak életét befolyásoló világméretű hajtóerejévé vált. Az Internet korunk legjelentősebb kritikus információs infrastruktúrájává vált. Néhány, az 1970-es évekből származó tervezési döntés következményei jelentősen korlátozzák továbbfejlesztését. Egyre többen mondják, hogy itt az ideje az Internet újragondolásának. A 2000-es évek elején számos új kutatási program indult, a jövő Internet kutatások jelentős szerepet játszanak az EU 7. Kutatási Keretprogramjában és 2009-ben körvonalazódott a Magyar Jövő Internet Kutatási Program is. Jelen előadás célja a jövő Internet kutatások alapvető eseményeinek, irányainak bemutatása és egy kapcsolódó védelmi/katonai kutatási program kereteinek felvázolása.

The Internet has developed at an unprecedented speed over the last 25 years. From a new way of communication between a numbers of scientists it became a worldwide driver of economic growth for billions of people. Internet became the most important critical information infrastructure of our world. Consequences of some design decisions inherited from the 1970s seriously limit its development, so more and more say, that it is time to rethink the Internet. In the early 2000s a lot of new research programs started, and Future Internet programs play an important role in the EU 7th Framework Program. In 2009 a Hungarian Research Program for the Future Internet has also been outlined. The aim of this presentation is to summarize the main events, and directions of Future Internet researches, and to outline the frameworks of a related defence/military research program.

Kulcsszavak: Jövő Internete, kritikus infrastruktúra védelem, védelmi/katonai feladatok, kutatási programok ~ Future Internet, Critical Infrastructure Protection, defence/military tasks, research programmes

Bevezetés

A kis kutatási hálózathoz meg született Internet napjainkra drámai mértékben megváltoztatta a gazdasági és a társadalmi szféra mindennapjait. Az eddigi fejlemények, eredmények még mindig csak a kezdetet jelentik. Ha a mai Internet az élet jelentős összetevője, akkor a jövő Internete még inkább létfontosságú szerepet fog játszani. Az Internet már ma is egy fantasztikus eszköz az embereknek egy óriási "szociális hálózatba" kapcsolására.

Mára már egyértelműen kimondható, hogy az Internet kritikus információs infrastruktúrává vált mind az egyének, mind a gazdasági társaságok, mind a kormányzatok, sőt egyenesen más kritikus infrastruktúrák számára. Az emberek és szervezetek függősége az Internettől egyre növekvő mértékben növekszik és ezzel egyidőben jelentősen változik az a mód, ahogy az Internet szolgáltatásait felhasználjuk, ily módon az Internet kritikus infrastruktúra jellege nyilvánvalóan csak erősödni fog.

A mai Internet azonban számos olyan, az 1970-es években meghozott döntés következményeit hordozza magával, amelyek korlátozzák biztonságát, rendelkezésre állását, rugalmasságát és menedzselhetőségét. Mindebből egyértelműen következik, hogy a jövő információs infrastruktúrája nem fejlődhet ki fokozatos bővítések, fejlesztések révén. Újszerű megoldásokra lesz (van) szükség a technikai átviteli módszerektől kezdve a különböző protokollokon keresztül az Internet architektúrájáig, sőt alkalmazási módszereiig.

Az előzőekben vázolt megállapításokból következően a 2000-es évek elején jelentős kutatási programok indultak a világ számos országában, amelyek az új generációs hálózatok, a jövő Internete különböző sajátosságait, megoldásait, eszközeit vizsgálják. A jövő Internete kutatások jelentős szerepet játszanak az Európai Unió kutatási keretprogramjában is és múlt év végén Magyarországon is megkezdődött egy nemzeti kutatási program előkészítése.

Jelen publikáció célja a jövő Internet kutatások alapvető eseményeinek, irányainak bemutatása és ezen belül egy védelmi/katonai kutatási program kereteinek felvázolása. Ennek érdekében:

- összegzi az Internet jövőjével kapcsolatos legfontosabb megállapításokat;
- vázolja a főbb nemzetközi jövő Internet kutatások eseményeit, irányait;
- ismerteti az Európai Unió jövő Internetéhez kapcsolódó tevékenységét;
- majd bemutatja a magyar nemzeti jövő Internet program kialakulásának eredményeit;
- végül körvonalazza a védelmi/katonai szféra sajátos feladatait és ehhez kapcsolódó lehetséges kutatási irányait.

A jövő Internete, az Internet jövője

A jövő Internete természetesen pontosan nem látható előre, az informatikai fejlődés sokszor néhány év alatt olyan megoldásokat hoz felszínre, amelyeket még a legalaposabb tudományos előrejelzések sem tartalmaztak. Abban viszont egyetértés van, hogy a jövő Internete nem a jelenlegi mellett, helyett felépülő vadonatúj jelenség lesz, de nem is a jelenlegi Internet bővítése, finomítása. Talán éppen ez teszi olyan aktuálissá, jelentőssé és egyben nehezzé a jövő Internet kutatásokat. Jelen előadásban, néhány – elsősorban európai uniós dokumentumra alapozva – csak nagyon röviden összegezzük a kérdéskör legfontosabb megállapításait.

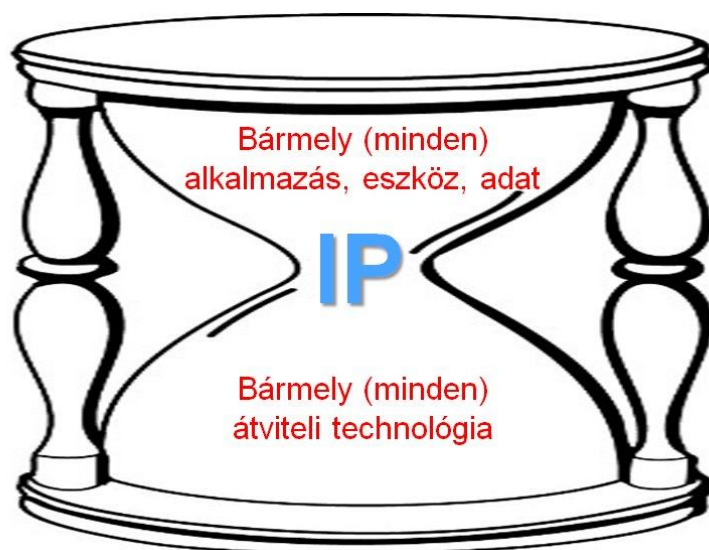
Napjaink Internetének és alkalmazásának *alapvető eredményei, hatásai* számos tanulmányban megfogalmazásra kerültek. Egy Európai Unió dokumentum [1] szerint az Internet:

- egy kísérleti kutatási hálózattól egy a gazdaságot és a társadalmi szolgáltatások nyújtását támogató infrastruktúrává fejlődött;
- mindent áthatóvá és mindenütt jelenlévővé vált, a világ népességének már mintegy negyede számára elérhető és a mobil szélessávú elérés gyors ütemben teszi hozzáférhetővé újabb 2 milliárd felhasználó számára;
- az elektronikus kereskedelem és a szociális hálózatok megjelenése révén kibővítette a felhasználói és fogyasztói lehetőségeket;
- az e-Kormányzat, e-Egészségügy és e-Oktatás megjelenésével elősegítette a közigazgatás, közszolgáltatások modernizációját;
- várhatóan jelentősen hozzájárulhat olyan új problémák megoldásához, mint a klímaváltozás és az energiahatékonyság.

A jövő Internetéhez kapcsolódó **elvárások és célkitűzések** alapját az az igény képezi, hogy az Internet legyen egy védett, hatékony és megbízható környezet, amely nyílt, dinamikus és decentralizált hozzáférést biztosít az információcseréhez és az információkhoz, valamint teljesítménye a felhasználói igényekhez és körülményekhez illeszkedő, méretezhető, rugalmas és adaptív legyen. Mindezekből levezethetők a következő általános célkitűzések [2]:

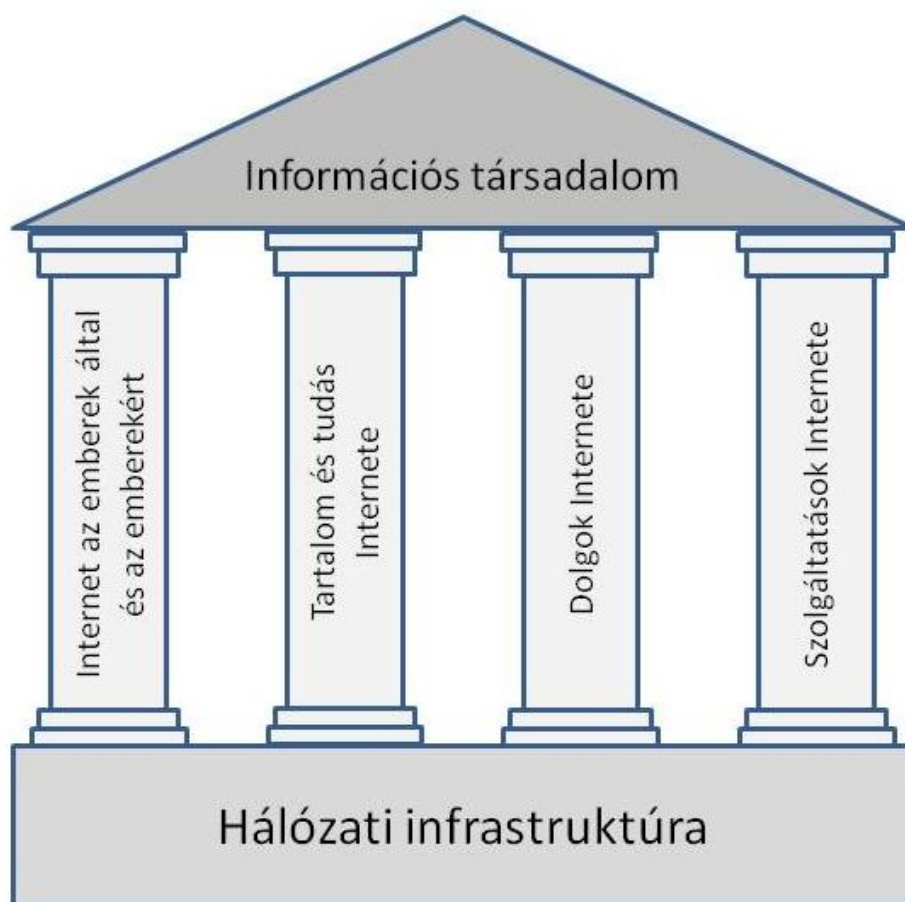
- az előre nem látható felhasználói igények összehangolása a folyamatosan bővülő elérhetőséggel;
- ez emberiség tudáskincsének általános és globális megosztása;
- az Internet-alkalmazás bővülő mennyiségi és fejlődő minőségi követelményeit kielégítő információs és kommunikációs technológiák, képességek és szolgáltatások;
- méretezhetőség a különböző (akár azonos közösségen belüli) régiók és kultúrák közötti kulturális, tudományos és technikai információcsere támogatására;
- mindenütt elérhetőség (fizikai és információs értelemben egyaránt) és nyitottság;
- védettség, elszámoltathatóság, megbízhatóság a személyiségi jogok, méltóság megsértése nélkül;
- mobilitás támogatása, beleértve a társadalom segítségét veszélyhelyzetekben;
- a körülményekhez, tartalomhoz és más tényezőkhöz alkalmazkodóképes teljesítmény;
- innovatív üzleti modellek támogatása, amelyek bővítik a szolgáltatásokat igénybevevők körét és lehetőségeit;
- környezettudatosság és energiaellátás szempontjából fenntarthatóság.

A jövő Internete várhatóan "az" (alapvető, egyedüli?) globális információs infrastruktúra lesz, amelyet a következő, gyakran használt homokóra ábra is hangsúlyoz.



1. ábra: "Minden Interneten, Internet mindenben"

A jövő Internetének **alapvető összetevői** sokszor négy pillér formájában jelennek meg (Internet az emberek által és az emberekért; a tartalom és a tudás Internete; a dolgok Internete; a szolgáltatások Internete), amelyek egy hálózati infrastruktúrára épülnek és az információs társadalmat alapozzák meg.



2. ábra: A jövő Internetének áttekintése

Az "Internet az emberek által és az emberekért" kifejezés által szemléltetett jelenség lényege az egyre bővülő, globálissá váló alkalmazói kör, amikor a tartalom létrehozása és megosztása már nem igényel speciális szaktudást és eszközöket. A tartalomszolgáltatók és tartalom-felhasználók közötti mai határok gyakorlatilag eltűnnek. A tudás könnyen és gyorsan megosztható, a reagálások szinte valós időben történnek, a már ma is létező szociális hálózatokhoz hasonlóan virtuális közösségek jönnek létre.

A "tartalom és tudás Internete" kifejezés a jelenlegi technikai és egyszerű információ-termelői és fogyasztói megközelítés meghaladását jelképezi. A jövő Internetének már egyedi információk helyett tudást és kultúrát kell közvetítenie, olyan magasabb szintű feladatokat kell közvetlenül támogatnia, mint a gondolkodás, tanulás, következtetés, stb., amelyek szükségessé teszik az információk 'intelligens' kezelését és feldolgozását, a jelentés 'megértését', a szemantikus megoldások előtérbe kerülését.

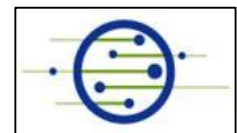
A "dolgok Internete" kifejezés egy olyan világot ír le, amelyben szinte minden dolog egyedileg azonosítható ('címezhető') és képes egymással információt cserélni, ezen információkat együttműködve feldolgozni, vagy felhasználni. Míg a mai Internet gyakorlatilag azonos típusú (de legalábbis nagyon hasonló) eszközök hálózata, a jövő Internete rendkívül heterogén – funkciójukban, technológiájukban és alkalmazási lehetőségeikben eltérő – dolgok között biztosít majd kapcsolatot.

A "szolgáltatások Internete" kifejezés több, egymással kapcsolatban álló jelenség összefoglaló leírása, amelyek az Internet által biztosított szolgáltatások működését és felhasználását jellemzik. Ezek közül az első az Internet-méretű szolgáltatás-orientált megoldások, amelyet ma leggyakrabban felhő-számítástechnikának nevezünk. Ebben a felhasználónak nem kell törődnie azzal, hogy a feladatok hol kerülnek végrehajtásra és az adatok hol kerülnek tárolásra. A második a szolgáltatások körülményekhez igazított, kezdeményező (proaktív), személyre szabott igénybevételek lehetősége. Végül a harmadik jellemző a szolgáltatás-összehangolás (összerendezés), egymásra épülés, összetett szolgáltatások nyújtása más, köztük széles körben alkalmazott alapszolgáltatások felhasználásával.

Jövő Internet kutatások a világban

A jövő Internetének kutatása intenzívebben a 2000-es évek elején indult meg elsősorban az Egyesült Államokban, az Európai Unióban és Japánban. Napjainkra már a fejlett országok többségében folynak ezirányú, nemzeti programokba illeszkedő kutatások.

Az Egyesült Államok jövő Internethez kapcsolódó kutatásai közül mindenképpen meg kell említeni a PlanetLab hálózatot, a GENI hálózatot és a FIND kutatási programot. A **PlanetLab** [3] egy globális kutatói hálózat új típusú hálózati szolgáltatások kifejlesztésének támogatására. A 2002-ben alapított hálózat napjainkra közel mintegy 40 ország, 480 helyszín, több mint 1000 számítógépét foglalja magában. A hálózatba kapcsolódó számítógépeken futó speciális szoftver (MyPLC) biztosítja az elosztott virtualizációt, a PlanetLab erőforrásai egy "szeletének" hozzárendelését egy adott alkalmazáshoz (kutatáshoz). Így lehetséges kutatási feladatokat futtatni a PlanetLab összes (vagy néhány) számítógépén, úgy hogy egyidőben más alkalmazások is futhatnak más "szeleteken".





3. ábra: PlanetLab számítógépek a világban¹

A **GENI** (Global Environment for Network Innovations, Globális Környezet Hálózati Kutatások számára) [4] egy virtuális 'laboratórium' (tesztbed) a jövő Interneté vizsgálatára, amelyet az Egyesült Államok Nemzeti Tudományos Alapítványa (National Science Foundation, NSF) kezdeményezett 2005-ben és amely jelenleg is a kiépítés állapotában van. A hálózat lényegében a PlanetLab hálózat szeletekre épülő virtualizációs megoldását bizonyos részleteiben kibővítő, meghaladó változat.

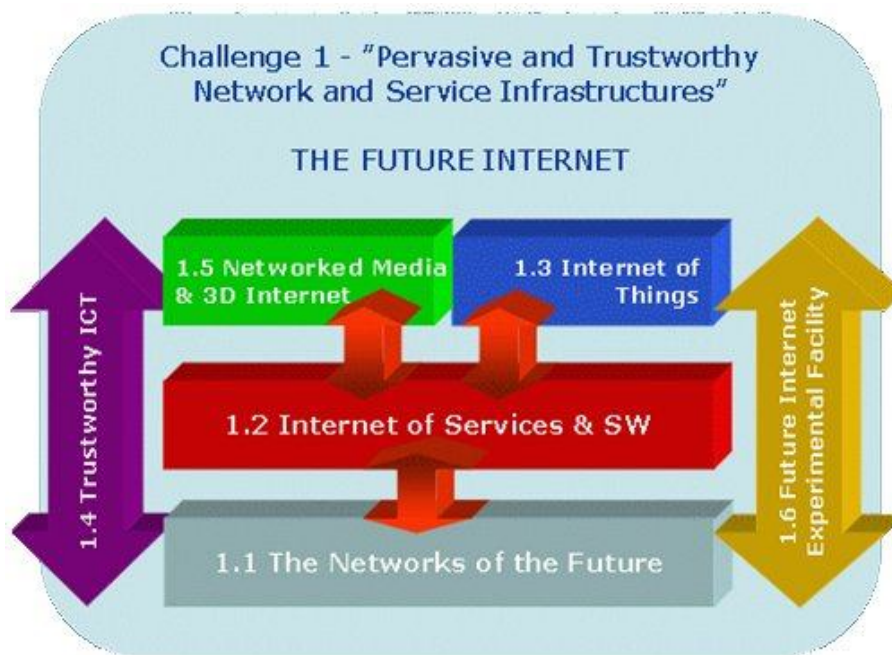


A **FIND** (Future Internet Design, Jövő Internet Tervezés) egy NSF architektúrális kutatási program [5], amely egy 2020 körüli globális hálózat követelményeinek és kiépítési lehetőségeinek vizsgálatára indult, a jelenlegi Internet korlátozásaitól eltekintő feltételezésből kiindulva, vagyis mintha a kezdetektől indulva mindent újra lehetne tervezni. A program olyan kérdések megválaszolását tervezi, mint:

- hogyan tervezhető egy alapjaiban védett és rendelkezésre álló hálózat;
- az információelosztás, a helymeghatározás és az azonosítási kérdések hogyan illeszkedjenek egy új hálózati architektúrába;
- milyen hosszú távú hatással járnak majd a fejlett vezeték nélküli és optikai technológiák;
- a gazdaság és a technika egymásra hatása hogyan alakítja majd a jövő hálózatát;
- hogyan tervezhető egy, a szabad és nyílt társadalmat megőrző hálózat.

Az **Európai Unió jövő Internetéhez kapcsolódó kutatásai** az egymást követő kutatási keretprogramok részeként folynak. Közülük kiemelésre méltó a FIRE és a FEDERICA, amelyek a 2007-2013 közötti időszakra szóló 7. Európai Kutatási Keretprogramba (FP7) illeszkednek. A keretprogram 2009-2010-re szóló infokommunikációs munkaprogramja hét kihívást fogalmazott meg, amelyek közül az első a "Kiterjedt és megbízható hálózati infrastruktúrák" [6].

¹ Forrás: PlanetLab honlap [3]



4. ábra: Az infokommunikációs munkaprogram első kihívásának összetevői²

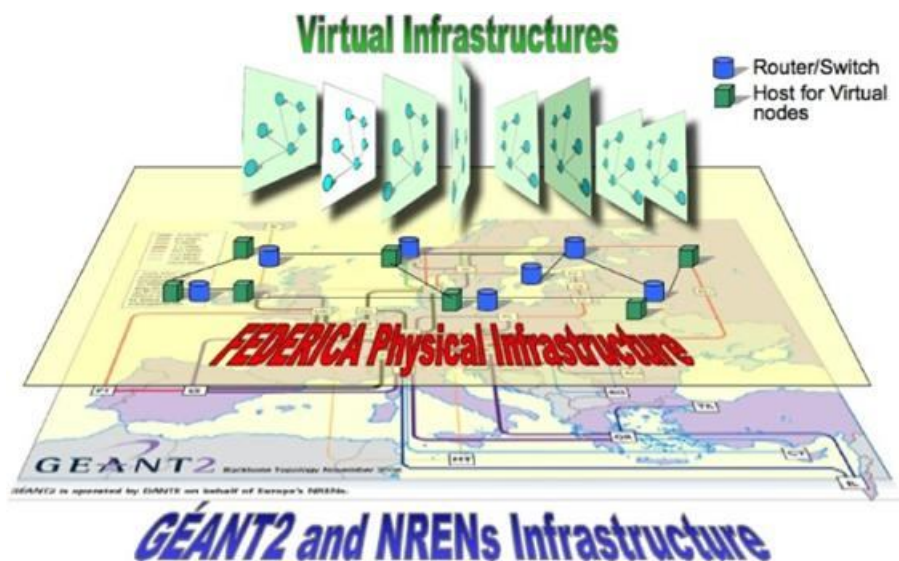
A fentiekben ismertetett kihívás által kitűzött cél megbízható platformok és keretrendszer; szervezeti és országhatárokon átnyúló, skálázható, elosztott, dinamikus fejlődő és együttműködő monitorozási, illetve fenyegetéseket kezelő megoldások, valamint az informatikai (cyber-) jellegű fenyegetések elleni védelem kutatása.

A **FIRE** (Future Internet Research and Experiment, Jövő Internet Kutatás és Kísérlet) [7] egy 2007-ben indult hosszútávú multidiszciplináris kutatási program, amelynek részét képezi egy kísérleti kutatás új koncepciókról, szolgáltatásokról; tesztkörnyezetek, kutatási infrastruktúrák kiterjesztése és a kísérletek számára rendelkezésre bocsátása, végeredményképpen egy európai megközelítés és identitás kialakítása.



A **FEDERICA** (Federated E-Infrastructure Dedicated to European Researchers Innovating in Computing network Architecture, Együttműködő e-infrastruktúra az európai kutatók számára a számítási hálózati architektúrák kutatásához) [8] egy két és fél éves projekt egy új hálózati technológiákat vizsgáló európai kutatási hálózati infrastruktúra kiépítésére, amely nem kapcsolódik egyetlen protokoll-, szolgáltatás-, vagy alkalmazás-típushoz sem. Jellegét tekintve ez a hálózat is a PlanetLab megoldásaira épül. Alapját a NREN és GÉANT2 hálózatok és biztosítja virtuális hálózatok létrehozását.

² Forrás: FP7 ICT munkaprogram első kihívásának honlapja [6]



5. ábra: A FEDERICA hálózat architektúrája³

A jövő Internete és az EU

Az Internet jövőjével kapcsolatos kutatási tevékenység fontosságát felismerve az Európai Unió 2008 márciusában *Bledben* egy rövid, egyoldalas **deklarációt** fogadott el [10], melyben az Internetet Európa gazdasági növekedésnek zálogaként aposztrofálta. Hangsúlyozta a jövő Internetéhez kapcsolódó európai tevékenységek erősítésének és összpontosításának fontosságát Európa versenyképességének megőrzése céljából. Kiemelte egy, az Európai Unió társadalmi és gazdasági ambícióihoz multidiszciplináris megközelítés, valamint a tagállamok és a vállalkozások összefogásának, együttműködésének szükségességét.

Még 2008 májusában az Európai Bizottság Információs Társadalom és Média Főigazgatósága egy több mint 150 oldalas tanulmányban [11] összegezte a **7. Kutatási Keretprogram keretében folyó, a jövő Internetéhez kapcsolódó kutatásokat**. A keretprogram első két évében már mintegy 300 millió euró került allokálásra ezen kutatásokhoz. A tanulmány hat csoportba sorolva ismerteti mintegy nyolcvan kutatási program célkitűzéseit, technikai megközelítésmódját, alapvető kutatási irányait, várható eredményeit és legfontosabb adatait.

Az első csoport *A jövő hálózatai* megnevezése alatt az új hálózati (átviteli) megoldásainak kutatásai találhatók. A *Szolgáltatás architektúrák* csoportba azon kutatások tartoznak, amelyek a hálózat és a szolgáltatási réteg viszonyát; a távközlési, műsorszóró és informatikai szolgáltatások különbözőségeinek feloldási lehetőségeit; a nyílt szolgáltatások, illetve a védettség összehangolását; a személyreszabhatóság és körülményekhez illeszkedés megvalósítását; valamint az üzleti folyamatokra gyakorolt hatásokat vizsgálják. A *Hálózatos médiarendszerek* csoport kutatásai többek között a tartalomszolgáltatás és rendelkezésre bocsátásának a hálózati és szolgáltatási architektúrára gyakorolt hatásait; a 3D média Internet biztonsági kérdéseit; a személyreszabott médiaszolgáltatások lehetőségeit elemzik. A *Dolgok Internete* csoportba tartoznak például a szenzorhálózatok, azonosítócímkék, ad-hoc hálózatok kutatásai. A *Biztonság* csoport programjai a hagyományos kérdések mellett kutatják a dolgok milliárdjai azonosítási kérdéseit; a heterogén biztonsági követelmények, rendszerek összehangolását; a

³ Forrás: EURESCOM honlap [9]

sérülékeny hálózatokra épülő kölcsönösen függő kritikus infrastruktúrák biztonságának kérdéseit; vagy az alaphálózat újszerű kriptográfiai megoldásait. Végül a *Kísérleti tesztkörnyezetek* csoportba a nagyméretű hálózatok tesztelési feltételeinek biztosítására, az összekapcsolódó tesztkörnyezetek kialakítására irányuló kutatások tartoznak.

Az Európai Unió 2009 májusában *Future Internet 2020* címmel már egy 60 oldalas akcióprogramot bocsátott ki [12]. A dokumentum első fejezete bevezetésként az Internet múltját, jelenét és jövőjét összegzi, bemutatja a lehetséges forgatókönyveket és javaslatokat fogalmaz meg a tevékenységi területekre, valamint az Európai Bizottság, az ipar és a tagállamok teendőire. Ezt négy tartalmi fejezet követi, amelyek különböző nézőpontokból vizsgálják a várható jövőt és határolják körül a kulcsfontosságúnak tartott tényezőket. Végül az utolsó fejezet Európa előtt álló kihívásokat, teendőket, javaslatokat tartalmazza.

A *mindennapi élet* szempontjait vizsgáló második fejezet a reggeli felkeléstől egy születésnapi ajándék készítésén, a szórakozáson (tévénézésen), az emberi kapcsolatokon, a munkahelyi feladatokon, majd az otthoni önképzésen (nyelvtanuláson) keresztül az esti lefekvésig vizsgálja a jövő Interneté helyét, szerepét, lehetőségeit, egy olyan környezetet, amelyben a rendszerek és eszközök környezetfüggő módon 'érzéklik', hogy a kért információkat ki, honnan és miért éri el és ennek megfelelően reagálnak.

A *gazdaság, szolgáltatások* kérdéseivel foglalkozó harmadik fejezetben a reggeli újságolvasástól, egy előfizetős Forma 1-es közvetítésen, egy tornateremben edzés közben végzett munkafeladatokon és pizzarendelésen át egy esti virtuális múzeumlátogatásig szemléltet egy olyan környezetet, amelyben a legkülönbözőbb szolgáltatások mindenhol és mindig elérhetőek. Egy másik példa egy szoftver úton, akár egyetlen útra is konfigurálható képességű viselkedésű autót mutat be. A példában szereplő autó egy olyan termék, amely maga is platformként szolgál különböző szolgáltatások számára, így képességei rugalmasan alakíthatóak.

A *dolgok Internetéhez* kapcsolódó negyedik fejezetben többek között egy sítúra követhető végig, amelynek során az autó segít az útvonal megtervezésében; útközből felhívja a figyelmet és bemutatja a nevezetességeket; a szállodai szoba a falak színárnyalatait, mintázatát és a hőmérsékletet igényeikhez igazítja; síelés közben a ruházatuk hőtartása alkalmazkodik a környezet és testük hőmérsékletéhez; végül este a fürdőszobában a tükör zuhanyozás közben híreket mutat. Ebben a környezetben szinte minden eszköz és tárgy "okos", segít és reagál, a felhasználói igények kielégítése érdekében más tárgyakkal, eszközökkel működik együtt.

A jövő Internetének megvalósítása érdekében 2009 októberében az *Európai Bizottság közlemény* [13] bocsátott ki, amelyben a többszereplős együttműködés, a magán-állami partnerség (PPP) kereteit rögzítette. Hangsúlyozta, hogy "Az európai szinten és a tagállamokban zajló számos erőfeszítést kiaknázó, következetes megközelítésre van szükség ahhoz, hogy Európa vezető régióvá váljon a jövőbeni internetes technológiák és alkalmazások terén." [13; 3 o.] A közleményben megfogalmazott alapvető célkitűzések a következők:

- az uniós szinten végrehajtott intézkedések kiaknázása;
- a rövid és középtávú megközelítések összehangolása;
- a tagállamok és az ágazat által támogatott magán-állami partnerség előkészítése.

A közlemény egy olyan jövőt vázol fel, amelyben az Internet egy eszköz egy intelligensebb világ létrehozásához, intelligens infrastruktúrák kialakításához. Összegzi az eddigi uniós és tagállami kutatási kezdeményezéseket, valamint ezek ágazati és innovációs vetületének helyzetét, végül meghatározza a jövő Internetével kapcsolatos cselekvési irányvonalakat:

- a magánberuházásokat is serkentő K+F beruházások erősítését;
- a tagállamok kezdeményezéseinek jobb kihasználását;
- a magán-állami partnerség kiépítését az ágazati érintettekkel.

Összességében megállapítható, hogy az Európai Unió felismerve a jövő Internetének szerepét és a kialakításában történő európai részvétel jelentőségét, kialakította a kutatási kereteket és ehhez jelentős pénzügyi forrásokat is rendelt.

Magyar nemzeti kutatási program

A jövő Interneté kutatás jelentőségét felismerve a Nemzeti Információs Infrastruktúra Program Programtanácsa 2007. novemberi ülésén dr. Bakonyi Péter, a Hungarnet ügyvezető elnöke előterjesztésében jóváhagyta azt a kezdeményezést, hogy kerüljön kidolgozásra az Új generációs Internet kutatási program. Egyben felkérte az előterjesztőket, hogy a NIIF Program keretében kerüljön kidolgozásra egy részletes programjavaslat. A részletes programjavaslatot a NIIF Programtanácsa 2008. március 26-án hagyta jóvá, amely többek között a következők megállapításokat tartalmazta. [14]

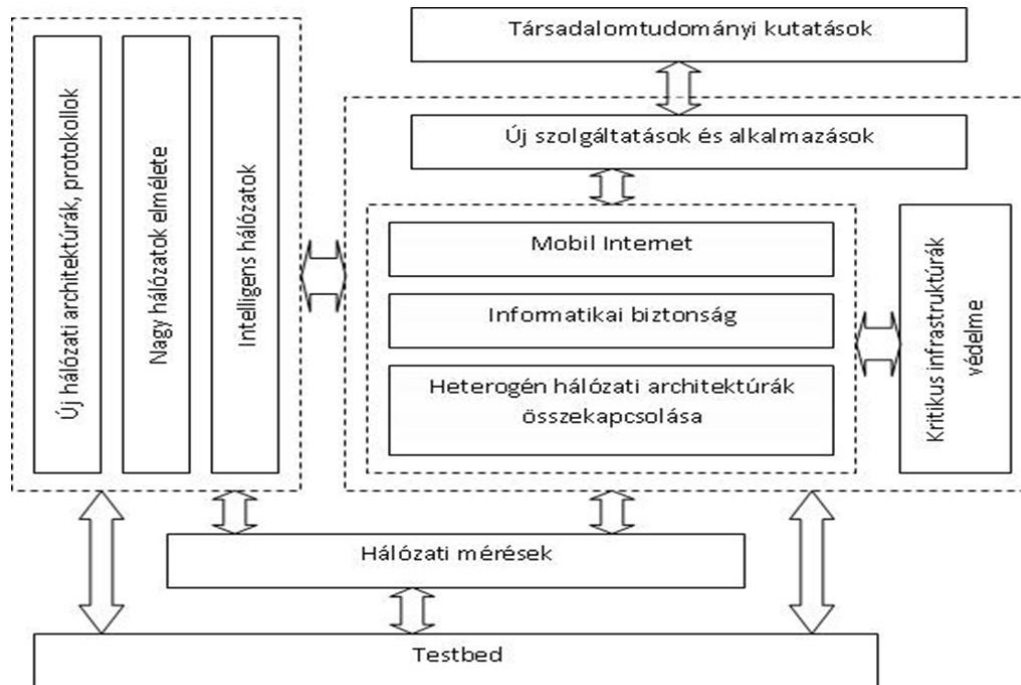
A hazai kutatói hálózat az NIIF Program keretében hosszú évek óta az európai élvonalba tartozó infrastruktúrát biztosít a hazai felsőoktatási, kutatási és közgyűjteményi kör számára. A kutatóhálózati infrastruktúra folyamatos fejlesztése elengedhetetlen ahhoz, hogy a jelenlegi élvonalbeli szerep, és így a hazai kutatás-fejlesztés versenyképessége, illetve az Internet-irányú kutatásokban való nemzetközi részvétel továbbra is megtartható legyen. Ehhez az új generációs Internet kutatásokban való eredményes részvétel alapvetően fontos.

Egy hazai új generációs Internet kutatási program létrehozásának akkor van létalapja, ha megfelelő kutatási háttér és eredmények állnak rendelkezésre. A Magyarországon ma folyó kutatás-fejlesztési tevékenység igen sokrétű: egyrészt az ipari résztvevők, illetve szolgáltatók egy-egy új termék kifejlesztéséhez, technológia bevezetéséhez erős alkalmazott kutatás-fejlesztést végeznek, másrészt a kutatóintézetekben, egyetemeken jelentős alapkutatási tevékenység is folyik. A kutatási eredmények gyakran beépülnek a nagy távközlési cégek termékeibe, melyek közül több is rendelkezik magyarországi kutató-fejlesztő központtal, elsősorban a mobil kommunikáció területén.

Magyarországon a legjelentősebb internetes kutatások a BME-n, az ELTE-n, a SZTAKI-ban, az NIIF-ben és az SZTE-n folynak, vállalati szinten pedig az Ericssonban és a Nokiában. Az egyes intézményekben azonban átlagosan csak néhány ember foglalkozik egy-egy témával, így e kutatási terület nem éri el a kritikus tömeget. Ezért fontos megfelelő koordinációval, a kutatáshoz szükséges források felkutatásával és a nemzetközi együttműködések szervezésével elérni, hogy Magyarország "felkerüljön az Internet-kutatás nemzetközi térképére".

2008 novemberében a program kidolgozásában résztvevő szervezetek – MTA SZTAKI, BME, ELTE, ZMNE – az NIIF szervezésében egy konferencián mutatták be az új generációs Internet kutatási program főbb irányait, az abban való részvétel lehetőségeit, a Európai Unió meghirdetett programjait és az addig ismert nemzeti kutatási programokat. Ezt követően kerekasztal-beszélgetés keretében kerültek megvitatásra az Új generációs Internet kutatási program 2009 évi célkitűzései, a nemzetközi programokban való magyar részvételi lehetőségei. 2009 januárjában a kidolgozás alatt álló program egy mini workshop keretében nagy sikerrel került bemutatásra az Európai Bizottság Információs Társadalom és Média Főigazgatóság szakértői delegációja számára.

A 2009 nyarára kidolgozott kutatási program [14] a nemzetközi áttekintés, a hazai program indításának indoklása, a program szakmai koncepciója, szervezési feladatai, valamint a társadalmi-gazdasági hasznosság bemutatása mellett tartalmazta a tizenegy kiemelt kutatási terület rövid ismertetését, melyek kapcsolatrendszere a következő ábrán látható.



6. ábra: A kutatási program szakmai struktúrája

A védelmi szféra kutatási feladatai

A jövő Internetével kapcsolatban általánosan elfogadott vélemény annak infrastruktúra, mégpedig kritikus infrastruktúra jellege. A korábbiakban megfogalmazottakból is látható, hogy az Internet mindenhol megjelenővé, elérhetővé válik és egyre növekvő szerepet játszik az állampolgárok jólétében, a gazdaság és a társadalom életében, mindez azonban egyre növekvő függőséget is eredményez, amelynek következtében alapvető jelentőségűvé válik a hálózatok védettsége és megbízhatósága, megóvása bármely jellegű hiba, vagy fenyegetés ellen.

A hálózatok egyre növekvő mértékű összekapcsolódása, heterogenitása és komplexitása egyre inkább megnehezíti menedzselésüket, felügyeletüket és védelmüket. A hálózatok összekapcsolódása folyamatosan növeli a kritikus infrastruktúrák közötti kölcsönös függőségek, interdependenciák mértékét és ezzel együtt a hibák, fenyegetések tovaterjedő hatásainak szintjét és lehetőségeit. A jelenlegi Internet nem korunk biztonság-központú szemléletének megfelelően lett kialakítva, így új megoldásokra lesz szükség, amelyek új lehetőségeket teremtenek, de egyben új eszközöket, megoldásokat igényelnek a kritikus infrastruktúra védelem területén is.

A kritikus információs infrastruktúrák és ezen belül a jövő Internetének védelme sajátos, a katonai, illetve a tágabb értelemben vett védelmi szférához kapcsolódó képességeket is igényel, mivel egyes sajátos eszköz- és eljárásrendszerek, valamint az ezek alkalmazására való felkészültség ehhez a szférához kapcsolódik, illetve mert adott tevékenységek végrehajtását,

illetve végrehajtóját jogszabályok írják elő, korlátozzák. Ezen feladatokat részletesebben tárgyalja [15]. A védelmi szféra különböző szervezeteinek hagyományos rendeltetés szerinti feladatmegosztása az információs színtéren azonban nem minden esetben és általában csak kiegészítő értelmezésekkel, megfontolásokkal valósítható meg.

A kritikus infrastruktúra védelemnek a jövő Internetéhez kapcsolódó, sajátos védelmi szférabeli feladataihoz kapcsolódó kutatás számos kérdés vizsgálatára irányulhat. Ezek között kiemelt szerepet a következőkben felsoroltak játszhatnak.

A jövő (és a jelen) Interneté, illetve az ezen keresztül más kritikus infrastruktúrák **biztonságát szándékosan fenyegető szereplőkkel kapcsolatos információk megszerzése** – a potenciális támadók körének naprakész meghatározása, tevékenységük figyelemmel kísérése – a hagyományos hírszerző, felderítő tevékenységhez szorosan kapcsolódik, azonban az informatikai eszközökben megtalálható és az informatikai hálózatokon áramló információk megszerzése, összegyűjtése, elemzése és értékelése újszerű eljárásokat és módszereket igényel.

A jövő (és a jelen) Interneté **biztonságát szándékosan fenyegető szereplők ellen irányuló tevékenység** rendeltetése, hogy csökkentse a fenyegetés megvalósítására irányuló képességeiket, elrettentse őket a támadás végrehajtásától. Ennek újszerű megvalósítási lehetőségei közé olyan különböző megoldások – megelőző támadás, ellentámadás, aktív megfélemlítés – tartoznak, amelyek napjainkban még számos technikai és jogi problémákat vetnek fel.

A jövő (és a jelen) Internetén, vagy annak segítségével végrehajtott – már bekövetkezett – **biztonság-sértések és más jogellenes tevékenységek esetében** alapvető feladat a **sajátos tárgyi bizonyítékok felkutatása és a jogi eljárás számára történő rögzítése** (forensics). Az informatikai bűnügyi eljárások e területen is újszerű módszereket, eszközöket igényelnek.

A védelmi szférához elsősorban saját információs infrastruktúráik védelme szempontjából kapcsolódik a következő két összetevő, amelyek azonban a védelmi szféránál nyilvánvalóan tágabb körben is hasznosíthatóak, vizsgálatuk szélesebb körű együttműködést is igényel.

A jövő Interneté jelentős hatást gyakorol a kritikus információs infrastruktúrákra általában, különös tekintettel a jelentkező **inter- és intra-dependenciákra**. Ezen belül kutatni szükséges: a globális, szövetségi, nemzeti kritikus információs infrastruktúrák Internet-függőségét; a nemzeti (és lokális) kritikus információs infrastruktúrák más kritikus információs infrastruktúráktól való függőségét, illetve a nemzeti (és lokális) kritikus információs infrastruktúrák informatikai eredetű belső veszélyeztettségét.

A jövő Interneté vonatkozásában kritikus jelentősége lesz a **túlélőképességnek**, a szolgáltatások katasztrófhelyzetekben, vagy más okokból kialakuló forgalmi túlterhelés esetén történő fenntartása kérdésének. Ezen keretek között vizsgálhatóak az IP-alapú kommunikáció műszaki-technikai együttműködési kérdései, az átviteli utak biztonsága (tervezés, összekapcsolás, használat).

A kutatási terület általános célkitűzése a fentiekben felsorolt részterületek elméleti alapjainak rendszerezése, továbbfejlesztése; eljárásainak, módszereinek, eszközeinek kutatása: egyes területeken konkrét megoldások megvalósítása, kidolgozása. Mindezek várhatóan a gyakorlatban alkalmazható, de egyben hosszabb távon hasznosítható eredményeket szolgáltatnak.

A kutatási eredmények hasznosításának esélyét jelentős mértékben növelheti a felhasználókban érintett szervezetek (nemzetbiztonsági szolgálatok, MH, Magyar Rendőrség Nemzeti Nyomozó Iroda) szakmai támogatásának megszerzése, szakembereinek bevonása a kutatómunkába.

A jövő Internetje kritikus információs infrastruktúrák védelméhez kapcsolódó sajátos védelmi feladatainak kutatása két területen is támaszkodhat (támaszkodnia kell) egy a kutatást támogató mesterséges környezet (tesztbed) szolgáltatásaira.

Egyrészt az újszerű (sajátos) információszerző, ellentevékenységi, illetve bizonyítékgyűjtő eszközöket, módszereket, vagy legalábbis ezek jó részét és teljes mértékben valós környezetben nem lehet végrehajtani, vizsgálni, ellenőrizni, így ehhez szükség lesz tesztbed igénybevételére. Másrészt a más, kapcsolódó kutatási területeken kidolgozott új megoldásoknak (architektúrák, protokollok, stb.) a saját kutatás szempontjából történő vizsgálata; lehetőségeik és következményei elemzése – ami részét képezi a jelen kutatási elgondolásnak – szintén csak tesztbeden lesz lehetséges.

A kutatás során várható eredmények a tervek szerint alapvetően, de részekben természetesen általánosságban hasznosíthatóak a kritikus infrastruktúra védelemben érintett kormányzati, gazdasági és más szereplők, szervezetek számára is.

Felhasznált irodalom

- [1] The Future of the Internet. Report from the National ICT Research Directors Working Group on Future Internet (FI). – European Commission, Information Society and Media Directorate General, 2008 július-november.
[www.future-internet.eu/fileadmin/documents/reports/FI_Rep_final__281108_.pdf, 2009.12.04.]
- [2] Future Internet. The Cross-ETP Vision Document. Version 1.0 – European Technology Platform on Smart Systems Integration, 2009.
[www.future-internet.eu/fileadmin/documents/reports/Cross-ETPs_FI_Vision_Document_v1_0.pdf, 2009.12.04.]
- [3] PlanetLab, An open platform for developing, deploying, and accessing planetary-scale services. Honlap.
[www.planet-lab.org, 2009.12.04.]
- [4] Geni, Exploring Networks of the Future. Honlap.
[www.geni.net, 2009.12.04.]
- [5] FIND, NSF NeTS FIND Initiative. Honlap.
[www.nets-find.net, 2009.12.04.]
- [6] FP7 , CORDIS, Information & Communication Technologies. ICT Challenge 1: Pervasive and Thrustworthy Network and Service Infrastructures. Honlap.
[cordis.europa.eu/fp7/ict/programme/challenge1_en.html, 2009.12.04.]
- [7] FIRE, Future Internet Research & Experimentation. Honlap.
[cordis.europa.eu/fp7/ict/fire, 2009.12.04.]

- [8] FEDERICA. Honlap.
[www.fp7-federica.eu, 2009.12.04.]
- [9] EURESCOM, European Institute for Research and Strategic Studies in Telecommunications. Honlap.
[www.eurescom.eu, 2009.12.04.]
- [10] The BLED Declaration. Towards a European approach to the Future Internet. – The Future of the Internet konferencia, Bled, 2008.03.31.
[www.future-internet.eu/index.php?id=47, 2009.12.04.]
- [11] The Future of the Internet. A Compendium of European Projects on ICT Research Supported by the EU 7th Framework Programme for RTD. – European Commission, Information Society and Media Directorate-General, Brussels, 2008.05.27.
[[ftp.cordis.europa.eu/pub/fp7/ict/docs/ch1-g848-280-future-internet_en.pdf](ftp://cordis.europa.eu/pub/fp7/ict/docs/ch1-g848-280-future-internet_en.pdf), 2009.12.04.]
- [12] Future Internet 2020. Call for Action by a high level visionary panel. – European Commission, Information Society and Media Directorate-General, Brussels, 2008.05.
[www.future-internet.eu/fileadmin/documents/reports/Future_Internet_2020-Visionary_Panel.pdf, 2009.12.04.]
- [13] COM(2009)479, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. A jövő Internetével foglalkozó magán-állami partnerség. – Európai Bizottság, Brüsszel, 2009.10.28.
[ec.europa.eu/information_society/activities/foi/library/docs/fi-communication_hu.pdf, 2009.12.04.]
- [14] BAKONYI Péter: Új generációs Internet kutatási program, 2007-2013.
[www.jovointernet.hu/index.php?option=com_content&view=category&layout=blog&id=37&Itemid=65, 2009.12.04.]
- [15] MUNK Sándor: Kritikus információs infrastruktúrákhoz kapcsolódó sajátos katonai (védelmi szférabeli) képességeket igénylő feladatok. – Hadmérnök, 2008 (III.)/3., 130-146. o.

Nagy Tibor István

nagy.tibor@nik.bmf.hu

A FELÜGYELET NÉLKÜLI SZENZORHÁLÓZATOK ÉS A PROGRAMOZÁSI NYELVEK KAPCSOLATA

Absztrakt

A felügyelet nélküli szenzorhálózatok a civilszférában és a szárazföldi harcászati felderítésben egyaránt fontos szerepet játszanak. A legtöbb informatikai eszközhöz hasonlóan a szenzorok működéséhez is szükségesek a hardverösszetevőkön túl szoftverkomponensek is, melyeknek elkészítéséhez valamilyen programozási nyelvre van szükség. Ez a publikáció áttekintést ad a felügyelet nélküli rendszereknél használt programozási nyelvekről, és azok jellemzőiről.

The unattended sensor networks play a significant role in both the civil applications and military ground surveillance and reconnaissance. Like most of the IT devices, the sensors also require hardware and software components. Software component are created with programming languages. This paper reviews the programming languages used with unattended systems, and their characteristics.

Kulcsszavak: *szenzor, felügyelet nélküli szenzorhálózat, intelligens szenzorhálózat, programozási nyelvek ~ sensor, unattended sensor network, intelligent sensor network, programming languages*

Bevezető

A felügyelet nélküli, intelligens szenzorhálózatok fontos szerepet játszanak napjaink haditechnikájában, azon belül is a harcászati felderítés legmodernebb és legbiztonságosabb eszközrendszerét biztosítják. A felderítés során az ellenséges erők helyzetét, mozgását, felszereltségük mértékét szükséges beazonosítani annak érdekében, hogy meg lehessen tervezni az offenzív vagy defenzív műveletek részleteit. A felderítés hagyományos módon humán erőforrás felhasználásával történik, amely a legköltségesebb (legfőképp elvesztése esetén). A szenzorhálózat automatizálja a felderítési területen végzendő veszélyes adatgyűjtést és biztosítja az adatok távolról történő feldolgozását, értékelését.

A szenzorhálózatok úgynevezett node-okból, vagy más néven mote-okból állnak, amelyek egy, vagy több – környezeti jellemző mérésére alkalmas – szenzort tartalmaznak. A node-ok képesek egymással rádiós kapcsolatot létesíteni és így egy hálózatot vezeték nélküli hálózatot

létrehozni. Működésükhöz emberi felügyelet nem szükséges, automatikusan képesek elvégezni feladatukat. A bonyolult műveletek miatt nem elég az elektronika, a hardver, szükség van az azt működtető szoftverre is, amely vezérli a hálózat kiépítését, a mért jellemzők begyűjtését, eltárolását, és az adatok továbbítását, azaz a felderítési ciklus két fázisában is jelentős szerephez jutnak: az adatszerzésben és adatfeldolgozásban egyaránt [1]. A szoftver elkészítéséhez pedig szükség van valamilyen programozási nyelvre. Céлом feltárni a programozási nyelvek jellemzőit, elemezni a szenzorhálózatoknál jelenleg használt nyelvek tulajdonságait, illetve csoportosítani ezeket.

Csoportosítási szempontok

A programozási nyelveket sokféle szempont szerint fel lehet osztani. Ezek közül azokat veszem sorra, amelyeket a felügyelet nélküli szenzorrendszerekkel kapcsolatban a legfontosabbnak tartok, azaz a programozási nyelv alapját képező paradigmát, számítási modellt, a nyelv emberközeliségét, illetve a felhasználók körét.

Emberközeliség

Ebből a szempontból két csoportot szoktak megkülönböztetni. Az első az alacsony szintű, vagy más néven hardver közeli nyelvek csoportja. Ezeknek a jellemzője, hogy a programozó a hardver beépített utasításkészletét használhatja fel. Átfogó ismerettel kell rendelkeznie a hardver, illetve annak elemeinek működéséről. Kevés programszerkezeti elem áll rendelkezésre, az összetett feladatok megoldása bonyolult.

A másik csoportba a magas szintű nyelvek tartoznak. Ezek a hardvertől távolabb, a programozóhoz közelebb helyezkednek el. A programozó számára könnyebb a programkészítés, több szerkezeti elem áll rendelkezésre, egy-egy utasítás bonyolultabb feladatok végrehajtására is alkalmas.

Paradigmák

A programozási paradigma – vagy más néven a programozási nyelv számítási modellje – a programozási nyelv által használt szemléletmódot, alapelveket, illetve az ezzel kapcsolatos szabályokat, szabályrendszert jelenti. Erre a szemléletmódra, szabályrendszerre épül a nyelv, annak szerkezete, illetve meghatározza a benne készíthető programok felépítését, és a benne használható szerkezeti elemeket. A paradigma ezen túlmenően behatárolja azon feladatok körét, amelyek a legkönnyebben, legegyszerűbben, vagy éppen a leghatékányabban megoldhatók az adott nyelven. Kialakulásuk és fejlődésük a magas szintű programozási nyelvek megjelenéséhez köthetőek. Egyetértek a fent leírtakkal, de csak azzal a kiegészítéssel, hogy a programozási nyelveknél általában elmondható, hogy nem egy számítási modellt alkalmaznak, hanem több számítási modell ötvözetére, vagy egymás melletti együttélésére alapoznak. Az alábbiakban a fontosabb programozási paradigmák rövid jellemzése olvasható.

Automataelvű paradigma

Az automataelvű paradigmát használó programozási nyelvek végrehajtójának egy automatát tekintünk. Az automata rendelkezik állapotokkal, és az állapotok közti átmenetet leíró függvényekkel. Az állapotok állapotkomponensekből állnak, amelyeket a függvények tudnak megváltoztatni. Az automata rendelkezik egy kiinduló állapottal.

A program és az automata állapotai egymástól elkülönülve tárolódnak. A programban egyszerű vezérlési szerkezetek valósíthatóak meg.

Imperatív (utasításorientált) paradigma

A Neumann elvű számítógépek tulajdonságait kihasználó számítási modell. A Neumann elvű számítógépek legfontosabb jellemzője, hogy címezhető, írható/olvasható memóriával rendelkeznek, amelyben az adatok és a programok utasításai is eltárolásra kerülnek. Az utasítások a számítógép által értelmezhető és végrehajtható „egységnyi” tevékenységek, amelyek egy megadott funkció elvégzésre készítetik a számítógép processzorát. A programban lévő utasítások sorban egymás után, azaz szekvenciálisan hajtódnak végre. A címezhető memória biztosítja a változók használatának lehetőségét, amelyek egy-egy – a program működéséhez szükséges – adat tárolását teszik lehetővé. A program címezhető memóriában tárolásának következménye, hogy a programok végrehajthatóak egy megadott utasítástól kezdve és ezt kihasználva a szekvenciális végrehajtás kiegészíthető ciklusokkal, elágazásokkal is. [2]

A legismertebb képviselői a BASIC, C, Ada, Pascal.

Funkcionális (függvényorientált) paradigma

Egzakt matematikai alapokon nyugvó programozási paradigma. A programszerkezetet függvényekből és a függvények közti matematikai kapcsolatokról – függvénykompozícióból, alternatív függvényekből és rekurzióból – lehet összeállítani. Az adatok tárolásához változók nem állnak rendelkezésre; helyettesítésük függvényparaméterekkel és a függvények visszatérési értékeivel oldhatóak meg. Ebből következik, hogy változó-értékkadás helyett paraméterátadást és rekurziót kell használni. A matematikai alapok miatt az ilyen számítási modellt használó programozási nyelvekben írt programok helyessége egyszerűen, matematikai apparátus felhasználásával bizonyítható, tehát megbízható és biztonságos programok készíthetők velük. Ilyen nyelvet használtak például a párizsi metró irányítórendszerének elkészítéséhez is. [2]

Legismertebb képviselői a Logo, Lisp, ML nyelvek.

Logikai paradigma

Ez a paradigma is a matematika egy részterületének alapelveire támaszkodik. A programot logikai formulákból építi fel. A formulákhoz meghatározhatók következtetési szabályok, amelyek meghatározzák a logikai formula kiértékelését. A formula kitöltött és kitöltetlen – azaz nem meghatározott értékű – is lehet. A kiértékelés eredményei a kitöltetlen paraméterek különböző lehetséges értékei, illetve egy igaz vagy hamis érték lehet. A paradigma legfőbb felhasználási területe a mesterséges intelligencia. Működési alapelvéből adódóan azon feladatok megoldására leghatékosabb, ahol visszalépéses keresést kellene alkalmazni. A visszalépéses keresés egy programozási tétel, amelynek megvalósítása nem logikai paradigmát alkalmazó nyelvek esetén nem könnyű feladat.

Legismertebb képviselője a Prolog programozási nyelv.

Deklaratív paradigma

Szinte minden számítási modell esetén a programban azt kell leírnia a programozónak, hogy az adott feladat megoldásához milyen lépések, utasítások végrehajtásán keresztül lehet eljutni. Ez

alól a deklaratív paradigma talán az egyetlen kivétel. Itt azt kell megfogalmazni, hogy milyen bemenő adatokból milyen eredményt akarunk elérni. Az eredmény elérésének mikéntjét a programozási nyelv elrejtí a programozó elől, illetve automatikusan elvégzi. Az ilyen nyelveket leginkább a relációs adatbázisok kezelésénél használják.

Legismertebb képviselője az SQL lekérdező nyelv.

Objektum-orientált paradigma

Alapelve, hogy a valós világot objektumokra bontja és ezeknek az objektumoknak a számítógépes modelljeit lehet megvalósítani a számítógépes programban. Az objektumok a rájuk jellemző adatokat és az adataikon végzendő műveleteket fogják össze egy egységbe. Ez a paradigma felhasználja az utasításorientált számítási modell elveit is a műveletek elkészítésénél, illetve az adatok tárolásánál. Kialakulásukat a grafikus felhasználói felületű programok iránti felhasználói igény ihlette. Manapság ezt a paradigmát használó programozási nyelvek a legelterjedtebbek.

Legismertebb képviselői: C++, Java, C#.

Programozási nyelv felhasználói köre

A számítógépeknél használatos programozási nyelvek a felhasználók köre szerint két nagy csoportra bonthatók: az amatőr és a professzionális nyelvekre. Az amatőr nyelveket nem informatikus, illetve programozó szakembereknek, hanem „laikusoknak” készítik, az általuk történő felhasználásra optimalizálják őket, emiatt jellemzőjük az egyszerűség: egyszerű programszerkezettel rendelkeznek, emellett nagy utasításkészlettel, melynek segítségével kivesszik a programozó kezéből a nehezen megoldható, de gyakran használt feladatok elkészítését. A professzionális nyelvek kisebb utasításkészlettel rendelkeznek, de nagyobb szabadságot adnak a programozónak, bonyolultabb programszerkezet felépítését teszik lehetővé, biztosítják a programkód újrafelhasználhatóságát modulok, komponensek, vagy más építőelemek felhasználásával. [2]

A fenti helyett a szenzorhálózatok katonai alkalmazásainál a programozási nyelvek felhasználóit négy csoportra bontanám, figyelembe véve, hogy a felügyelet nélküli rendszerek tervezésénél, karbantartásánál és használatánál milyen ismeretekre van szükség:

- Laikusok: olyan szakemberek, akik valamely tudományterületnek (pl.: a hadtudományoknak) szakértői, viszont informatikai tudással nem, vagy csak alapszinten rendelkeznek, programozási tudás pedig szinte egyáltalán nincs birtokukban
- Elektronikai szakemberek: az elektronika, híradástechnika, rádiózás témakörében jártasak, és az ehhez szükséges programozási ismeretekkel is rendelkeznek, ami általában a mikrokontrollerek programozásához szükséges assembly, vagy a nagyintegráltágú áramkörök programozásához használható VHDL hardverleíró nyelv.
- Informatikai szakemberek: az informatikai rendszerek, hálózatok kiépítésében, karbantartásában jártas szakemberek, akik egy programozási nyelvet alap, vagy legfeljebb középszinten ismernek. A számítógépek és elektronikai eszközök összekapcsolásához szükséges alapszintű elektronikai ismeretekkel rendelkeznek.

- Programozók: több programozási nyelvben való magas szintű jártasság és a hozzájuk kapcsolódó egyéb ismeretek birtokában lévő szakemberek, akik az informatikai rendszerek, hálózatok tekintetében csak alapszintű ismeretekkel rendelkeznek, elektronikai ismereteknek pedig nincsenek birtokában.

Szenzorhálózatok programozási nyelvei

Nagyon sok programozási nyelv készült a felügyelet nélküli szenzorhálózatok különböző feladatainak vezérlésére. Az alábbiakban a teljesség igénye nélkül néhánynak a leírása olvasható.

Basic

A BASIC programozási nyelv az utasításorientált nyelvek közé tartozik. Könnyű megtanulni a használatát, a kezdő programozónak nem kell olyan adminisztrációs jellegű utasításokat megtanulnia, amelyeket más programozási nyelvek megkövetelnek (ilyen például a változódeklaráció). Egyszerűsége miatt a programírásban kevésbé, vagy egyáltalán nem járatos személyek számára is rövid idő alatt elsajátítható. Interpreter típusú nyelv, ami azt jelenti, hogy az elkészített program fordítása – BASIC nyelvről a node által végrehajtható utasításokra – a program futtatása közben, utasításonként történik. Ez a tulajdonság a programfutas sebességét csökkenti, azaz a feladatok elvégzéséhez szükséges időt növeli. A Northwestern egyetem Electrical Engineering and Computer Science tanszék kutatói készítettek egy BASIC implementációt, illetve integrált fejlesztőkörnyezetet kimondottan vezeték nélküli szenzorhálózatokhoz. A nyelvbe beépítettek néhány utasítást, amelyek a kommunikációt, energiatakarékos üzemmód vezérlését, az érzékelők által mért információk beolvasását teszik lehetővé. A kutatók egy felméréssel próbálták bizonyítani az általuk kidolgozott nyelv könnyű elsajátíthatóságát. A felmérésben 40 végzett, vagy végzős egyetemistát teszteltek, mindegyikük kevés, vagy egyáltalán semmilyen programozási tudással nem rendelkezett. Eredményként azt kapták, hogy a résztvevők 45-50%-a meg tudott oldani egyszerűbb – előre meghatározott – feladatokat. Vizsgálták ezen túlmenően az elkészített programok és a node-ok fogyasztásának kapcsolatát is. Eredményük szerint a BASIC-ben írt program által okozott fogyasztás – nem számításigényes programok esetén – mindössze 1,5%-kal nagyobb a natív C-ben megírtnál. Feltételezésük szerint nagyobb számítási kapacitást igénylő feladatok nem is igen fordulnak elő a szenzorhálózatoknál [3]. Én ezzel a megállapítással vitatkoznék, mivel az egyes node-ok pontos helyének ismerete hiányában közöttük hálózatot kiépíteni valamilyen szakértőrendszer-elmélet, gráfelmélet felhasználásával lehetséges, amelynek megvalósítása utasításorientált nyelvben meglehetősen számításigényes feladat. A felügyelet nélküli szenzorok harcászati felderítésben történő alkalmazásánál pedig pont ilyen ad- hoc hálózatok kiépítésére lehet szükség.

NESC

Komponens alapú programozási nyelv, a C nyelv egy speciális változata, amelyet kifejezetten a vezeték nélküli szenzorhálózatok korlátozott memóriakapacitásának figyelembe vételével fejlesztettek ki. A benne írt programok előre elkészített komponensekből tevődnek össze, melyek egymással interfészeiken keresztül kommunikálnak. Kész komponensek léteznek a legfőbb hardverfunkciók megvalósítására, mint a csomagkapcsolt kommunikáció, útvonalválasztás, érzékelők adatainak begyűjtése és tárolása.

JAVA

A Sun Microsystems SPOT projektje az intelligens vezeték nélküli hálózatoknak egy implementációja. A Sun SPOT device-ok kisméretű, különböző szenzorokat tartalmazó node-ok, amelyekből egy kis hatótávolságú vezeték nélküli hálózat építhető ki.

Ehhez a technológiához készítettek a Squawk elnevezésű project keretein belül egy olyan Java virtuális gépet, amelynek a lehető legnagyobb részét magát is Java nyelven írták meg. A cél kis memóriakapacitással rendelkező eszközökhöz optimális futtatókörnyezet készítése volt.

Erre a virtuális gépre a Java MicroEdition egy speciális változata használható. Előnye, hogy magas szintű, objektum-orientált nyelven, kisebb költséggel, kényelmesebben, könnyebben tesztelhetően lehet programokat készíteni beágyazott rendszerekhez, mint az assembly, vagy C nyelvek használatával. Rendelkezésre állnak különböző fejlesztőeszközök is a programok elkészítéséhez, teszteléséhez, nyomkövetéséhez, mint például a teljesen ingyenes és a Java-s programozók körében elterjedt és népszerű NetBeans.

TINYSQL

Egy egyszerű, Java programozási nyelven írt relációs adatbázis-kezelő rendszer, amely dBase formátumban tárolja az adatbázisokat [4]. A szenzorhálózatokban történő alkalmazásánál egy táblában kerül eltárolásra a hálózat aktuális időpillanatbeli állapota. A tábla meghatározott időközönként frissül. A sorok az egyes node-okat, az oszlopok pedig a mért jellemzőket, illetve a node-ok bizonyos tulajdonságait jelentik. Az aktuális állapot lekérdezése a szokásos SQL szintaktikával lehetséges, míg a korábbi állapotok úgynevezett mentési pontok létrehozásával tárolhatók.

SWISSQM¹

A SwissQM egy verem alapon működő virtuális gép vezeték nélküli szenzorhálózatokhoz kifejlesztve. Platform független, mivel a nyelvben megírt programból bájtkód készül. Biztosítja az eseménykezelés lehetőségét, függvények definiálását, állapotgépek, Turing-automata elvű programozást, illetve többféle magas szintű programozási nyelv használatát. [5]

WASP

A Northwestern és a Michigani egyetem kutatói által kifejlesztett nyelv, amelynek középpontjában az az elgondolás áll, hogy a szenzorhálózatokat nagy többségében nem programozók, illetve informatikusok használják, hanem valamilyen más tudományterület művelői, akiknek munkájukhoz és kutatásukhoz van szükségük ezekre a felügyelet nélküli eszközökre.

Az egyetem kutatói több alkalmazást és programozási nyelvet is megvizsgáltak. Arra a következtetésre jutottak, hogy a létező nyelvek többsége általános nyelv, laikusok számára nehezen megtanulható, ezért egy új nyelv kifejlesztését tűzték ki célul, amely könnyen elsajátítható és egy adott feladattípushoz használható fel. Ehhez beazonosították azokat az alkalmazás-jellemzőket, amelyek alapján feladatosztályokba lehet sorolni az alkalmazásokat. A jellemzők a következők:

¹ SwissQM - Scalable Wireless Sensor Query Machine

- **Mobilitás:** vannak olyan node-ok, amelyek működésük közben változtatják helyzetüket, és olyanok is, amelyeknek a pozíciója állandó.
- **Mintavételezés kezdeményezése:** meghatározza, hogy a mintavételezés milyen feltétel bekövetkezésekor indul. Lehet periodikus, eseményvezérelt, vagy a kettő ötvözte.
- **Adatátvitel kezdeményezése:** meghatározza, hogy a node-ok milyen feltétel teljesülése esetén kezdeményezhetnek adatforgalmat a hálózaton. Az előző jellemzőhöz hasonlóan ez is lehet periodikus, eseményvezérelt, vagy a kettő ötvözte.
- **Vezérlés:** meghatározza, hogy a szenzorhálózat létrehoz-e olyan jeleket, amelyekkel más hardvereszközök vezérelhetők.
- **Interakció:** meghatározza, hogy a szenzorhálózatnak kell-e tudnia reagálni, választ adni bizonyos parancsokra. Interakcióra tipikusan a telepítésnél, átprogramozásnál, karbantartásnál, illetve a működési paraméterek megváltoztatásánál lehet szükség.
- **Adatok értelmezése:** meghatározza, hogy szükség van-e az érzékelő adatok átalakítására, szűrésére a szenzorhálózaton belül.
- **Adatok egyesítése:** meghatározza, hogy szükség van-e több node-tól érkező adatok egyesítésére
- **Homogenitás:** meghatározza, hogy a hálózat node-jai mind ugyanazt a funkciót látják-e el.

Ezen jellemzők alapján a lehetséges feladatokat hét feladatosztályra bontották fel. Minden feladatosztályhoz egy-egy külön nyelv létrehozását tervezik, amelyből eddig kettőt készítettek el. Az első feladatosztályba a periodikus mintavételezésű, nyers adatokkal, adatok szűrésével és egyesítésével működő, nem mobil, homogén alkalmazások tartoznak. A programozási nyelv külön részben írja le az egyes node-ok, illetve külön másik részben a teljes hálózat működését. A nyelv fordítóprogramja NesC kódot állít elő, amelyből újabb fordítás után generálható a futtatható program. [6]

Szenzorhálózatok rogramozási nyelveinek jellemzői

Az alábbi táblázatban az előző fejezetben leírt nyelvek programozási paradigmák szerinti besorolása látható.

1. táblázat A programozási nyelvek paradigmák szerint

	Automataelvű	Utasításorientált	Funkcionális	Logikai	Deklaratív	Objektum-orientált
BASIC		+				
NesC		+				
Java		+				+
TinySQL					+	
SwissQM	+				+	
WASP		+			+	

A vizsgált nyelvek közül a legtöbb – nem meglepő módon – az utasításorientált paradigmát használják. Hosszú ideig a PC-knél is ezek a nyelvek voltak a legnépszerűbbek, és a nagyintegráltságú áramkörök esetén még most is szinte ez az egyetlen használható számítási modell. Kicsit meglepőbb és érdekes megoldási mód a deklaratív számítási modell használata. A logikai paradigma használata a hálózatképzéskor indokolná a logikai paradigma alkalmazását, azonban a fenti nyelvek közül egyik sem tartozik ebbe a körbe. Az objektumorientált paradigmát pedig csak a Sqawk használja, ami a végrehajtási sebesség és a felhasznált tárkapacitás szempontjából érthető is.

Összefoglaló

A felügyelet nélküli szenzorhálózatok fontos szerepet játszanak a harcászati felderítésben a humán erőforrás kiváltására, illetve a felderítő személyzet életének és biztonságának megvédésében. Mint minden számítástechnikai eszközénél, a node-ok esetében is lényeges elem a hardverösszetevőkön túl az azokat működtető szoftver is. A szoftverek elkészítéséhez valamilyen programozási nyelvre van szükség, melyeknek tulajdonságai meghatározzák a bennük készíthető szoftverek jellegét, megbízhatóságát, biztonságosságát, illetve a velük megoldható feladatok körét. Manapság a kutatások iránya olyan programozási nyelvek kifejlesztése, amelyeket nemcsak informatikai szakemberek, illetve programozók tudnak használni, hanem a felhasználási tudományterület képviselői is könnyen megtanulhatnak. Véleményem szerint a fejlődés iránya és a programozási nyelvek, illetve azok alkalmazási területei ezt a jövőt festik fel.

Irodalomjegyzék

- [1] Kovács L.: *Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben*. PhD értekezés, ZMNE, Budapest, 2003.
- [2] Temesvári T., Szlávi P., Zsakó L.: *Mikrológia 22, Programozási nyelvek: Alapfogalmak*. NJSZT, 2004.
- [3] J. S. Miller, P. A. Dinda, R. P. Dick: *GOTO Considered Helpful: A BASIC Approach to Sensor Network Node Programming*. Technical Report NWU-EECS-09-01, Northwestern University, 2009.01.31.
- [4] <http://www.jepstone.net> (2009.11.21.)
- [5] <http://www.swissqm.inf.ethz.ch> (2009.11.21.)

- [6] L. S. Bai, R. P. Dick, P. A. Dinda: *Archetype-Based Design: Sensor Network Programming for Application Experts, Not Just Programming Experts*. IPSN'09, 2009.04.13-16.

Regula Gergely

regula@iit.bme.hu

Lantos Béla

lantos@iit.bme.hu

BELTÉRI AUTONÓM NÉGYROTOROS HELIKOPTER SZABÁLYOZÓ RENDSZERÉNEK KIFEJLESZTÉSE ÉS HARDWARE-IN-THE-LOOP TESZTELÉSE

Absztrakt

A cikk egy négyrotoros helikopter kinematikai modellezésétől a szabályozó algoritmusának kifejlesztéséig felmerülő elméleti és gyakorlati problémákat tárgyalja. Részletesen bemutat egy új alacsony szintű szabályozási algoritmust. Ezen kívül bemutatja a szabályozás kiegészítő komponenseit, az állapotbecslést és egy pályakövető algoritmust. A helikopterről felállított modell figyelembe veszi a légellenállást, a rotorok giroszkopikus hatását, valamint a helikopter rotorjait meghajtó BLDC motorok dinamikáját. A szabályozó algoritmus a visszalépéses technikán (backstepping) alapul, és képes a helikoptert stabilizálni realisztikus zavarhatások esetén. A kiterjesztett Kalman-szűrőkre alapozott állapotbecslő egy külső kamera-alapú látórendszer és egy fedélzeti inerciális mérőegység (IMU) mérési eredményei alapján becsüli a nem mért mennyiségeket és csökkenti a mérési hibák hatását. A cikk ezen kívül bemutatja a szabályozó rendszer fejlesztésének környezetét, a valós időben elvégzett tesztek eredményeit, valamint kitér a fejlesztés során szerzett tapasztalatokra.

The objects of the article are the kinematic modeling and control design methods of a quadrotor helicopter. The article focuses on both theoretic and practical aspects. A new low-level control algorithm is introduced. In addition, the supplementary components of the control system are described in detail as well. The helicopter's dynamic model takes into account the aerodynamic friction, the gyroscopic effect of the rotors and also the BLDC motor dynamics. The control algorithm is based on the back stepping approach and is capable of stabilising the model even in case of realistic noises. The state estimator consists of extended Kalman filters and estimates nonmeasured signals and also suppresses measurement noises that are provided by an external camera based vision system and an onboard inertial measurement unit (IMU). Software environment and test methods are presented with attention to the common errors. The results of the first flight tests are also included in the article.

Kulcsszavak: UAV, beltéri négyrotoros helikopter, állapotbecslés, kiterjesztett Kalman-szűrő, hardware-in-the-loop tesztelés ~ UAV, quadrotor helicopter, state estimation, extended Kalman filtering, implementation, hardware-in-the-loop test

Bevezetés

Az utóbbi években a pilótánélküli légi járművek (UAV-k) iránt egyre inkább növekszik az érdeklődés mind a kutatók, mind pedig a járműveket alkalmazni készülőkhöz részéről. Mivel az UAV-knek nem csak katonai, hanem számos civil alkalmazási lehetősége is kínálkozik, egyre jelentősebb fejlesztések folynak ezen a területen. A fejlesztés rövid távú célja, hogy egy olyan kisméretű négyrotoros helikoptert fejlesszünk ki, amely képes önállóan végrehajtani egy komplex missziót, amely egy fel- és leszállási fázisból, valamint egy célterületen tartott megfigyelési, ill. mérésvégzési feladatból áll.

A fejlesztés 2006 tavaszán kezdődött a BME Irányítástechnika és Informatika Tanszék és az MTA SZTAKI Rendszer- és Irányításelméleti Kutatólaboratórium együttműködésében. Jelenleg egy olyan beltéri négyrotoros helikopter építésén dolgozunk, amely a későbbiekben alkalmas lesz különböző fejlett irányítási, pályatervezési, ill. képfeldolgozási algoritmusok tesztelésére, valamint pályatervezési, pozicionálási és szenzorfüziós módszerek kipróbálására.

A fejlesztés a következő irányokban indult: irányítási algoritmusok fejlesztése, rendszerterv készítése, elektronikai, mechanikai és aerodinamikai tervezés. A helikopter első prototípusa [1] és [2]-ben jelent meg. 2008-ban sikeres hardware-in-the-loop szimulációkat hajtottunk végre, amelyek igazolták, hogy a fedélzetre szánt MPC555 típusú processzor, amely magas szinten MATLAB Simulinkben programozható, valóban képes lesz a backstepping alapú szabályozást és a kiterjesztett Kalman-szűrőkre épülő állapotbecslést valós időben végrehajtani [3].

A cikk a helikopteren folyó szabályozástechnikai problémákra fókuszál, bemutatja a saját fejlesztésű visszalépéses technikán (backstepping) alapuló szabályozási algoritmust, valamint a fedélzeti irányítás további komponenseit. Ezek között szerepel egy állapotbecslő, amely két kiterjesztett Kalman-szűrőt tartalmaz, valamint egy pályakövető algoritmus is. A rendszer bemutatását követően (1. fejezet) a helikopter és a rotorok modellezése következik (2. fejezet). A 3., 4. és 5. fejezetben a szabályozási rendszer komponensei következnek. A 6. fejezet bemutatja a szimulációs eredményeket, míg a 7. fejezet az algoritmusok megvalósítási kérdéseit tárgyalja. A befejező szakasz röviden összefoglalja az elért eredményeket és a fejlesztés aktuális állapotát.

1. A rendszer felépítése

A helikopter szabályozása pontos pozíció- és orientációmérést igényel. A mérési adatok elsődleges forrása a fedélzetre szerelt Crossbow MNAV100CA inerciális mérőegység (IMU), amely többek között háromdimenziós gyorsulást és szögsebességet mér. A szenzor felépítéséből következően a mérések zajjal és biasszal terheltek. Emiatt integrálás során pontatlanná válnak a pozíció és orientáció becsült értékei. A mérési hibák hatásának csökkentése érdekében kiterjesztett Kalman-szűrőket alkalmazunk az integrálás helyett. Azonban elengedhetetlen, hogy abszolút méréseket is végezzünk. Kültéri járművek esetén megoldás lehet a GPS, ill. A differenciális GPS alkalmazása. Beltéri járművek esetén pedig elterjedt módszer a látórendszerek használata.

A fentiek figyelembevételével a rendszer felépítése az alábbi. A helikopteren egy fedélzeti számítógép van elhelyezve, amely feldolgozza a mérési eredményeket, ill. beavatkozó jeleket számít. A propellerek kefe nélküli egyenáramú (BLDC) motorokra vannak felszerelve. A motorszabályozók és az IMU a központi processzorhoz CAN-buszon keresztül kapcsolódik. Ezen kívül egy szórt spektrumú CDM rádiós csatorna teremt kapcsolatot a helikopter központi egysége és a földi állomás között. A földi állomás küldi a parancsokat és a referenciapályát a helikopternek, valamint ezen a csatornán keresztül érkeznek a pozíció- és orientációmérési eredmények a fedélzeti számítógéphez. A földi állomás felé státuszinformációkat küld a helikopter. A földi állomás hálózaton keresztül csatlakozik a képfeldolgozást végző számítógéphez. A képérzékelő egy kereskedelmi, nagyfelbontású webkamera. További részletek a szenzorrendszerről [4]-ben találhatók.

2. A négyrotoros helikopter dinamikájának modellezése

2.1. A helikopter mozgásegyenletei

A mozgásegyenletek levezetése során feltételezzük, hogy a Földhöz rögzített K_E koordináta-rendszer inerciarendszernek tekinthető. A helikopter tömegközéppontjához rögzített K_H koordináta-rendszert K_E -hez képest a $\xi = (x \ y \ z)^T$ pozíciója és RPY szögekben megadott $\eta = (\Phi \ \Theta \ \Psi)^T$ orientációja jellemzi. Az orientációt az R_t mátrix írja le az alábbi módon:

$$R_t = \begin{bmatrix} C_\Psi C_\Theta & C_\Psi S_\Theta S_\Phi - S_\Psi C_\Phi & C_\Psi S_\Theta C_\Phi + S_\Psi S_\Phi \\ S_\Psi C_\Theta & S_\Psi S_\Theta S_\Phi + C_\Psi C_\Phi & S_\Psi S_\Theta C_\Phi - C_\Psi S_\Phi \\ -S_\Theta & C_\Theta S_\Phi & C_\Theta C_\Phi \end{bmatrix}$$

ahol S_x és C_y a $\sin(x)$ és $\cos(y)$ robotikában szokásos jelölése.

A kapcsolat $\dot{\xi}$, $\dot{\eta}$, ill. a sebesség (v) és szögsebesség (ω) között

$$\dot{\xi} = R_t v$$

$$\omega = R_r \dot{\eta}$$

ahol R_r , ill. az inverzének alakja a következő:

$$R_r = \begin{bmatrix} 1 & 0 & -S_\Theta \\ 0 & C_\Phi & C_\Theta S_\Phi \\ 0 & -S_\Phi & C_\Theta C_\Phi \end{bmatrix} \quad \text{és} \quad R_r^{-1} = \begin{bmatrix} 1 & S_\Phi T_\Theta & C_\Phi T_\Theta \\ 0 & C_\Phi & -S_\Phi \\ 0 & S_\Phi / C_\Theta & C_\Phi / C_\Theta \end{bmatrix}$$

ω idő szerint deriváltja

$$\varepsilon = \dot{\omega} = R_r \ddot{\eta} + \dot{R}_r \dot{\eta}$$

Newton törvényeit alkalmazva a rendszerre, a helikopter translációs és rotációs mozgását leíró egyenletek a K_H koordináta-rendszerben az alábbiak:

$$\sum F_{ext} = m\dot{v} + \omega \times (mv)$$

$$\sum T_{ext} = I\dot{\omega} + \omega \times (I\omega)$$

ahol I a helikopter inerciáját jelöli, és feltételezzük, hogy diagonális, azaz $I = \text{diag}(I_x \ I_y \ I_z)$. A két egyenlet bal oldala a helikopterre ható összes külső erőt és forgatónyomatékot jelöli. Ezek a hatások részben a rotorok forgásából adódnak (F és T), részben pedig a gravitáció (F_g) a giroszkopikus hatás (T_g) és a légellenállás (F_a és T_a) eredményeképpen jönnek létre. Összefoglalva

$$\begin{aligned}\sum F_{ext} &= F + F_g + F_a \\ \sum T_{ext} &= T + T_g + T_a\end{aligned}$$

A helikopteren négy beavatkozó szerv található (négy BLDC motor), amely mindegyike felfelé ható erő kifejtésére képes. Ezek a rotorok szögsebességével négyzetesen arányosak ($f_i = b\Omega_i^2$). A BLDC motorok mindegyikéhez külön szabályozó tartozik, amelyek a kívánt szögsebességre pörgetik a rotorokat. A keletkezett nyomatékok és a felhajtóerő az alábbi módon számítható:

$$T = \begin{pmatrix} lb(\Omega_4^2 - \Omega_2^2) \\ lb(\Omega_3^2 - \Omega_1^2) \\ d(\Omega_2^2 + \Omega_4^2 - \Omega_1^2 - \Omega_3^2) \end{pmatrix}$$

$$f = b(\Omega_1^2 + \Omega_2^2 + \Omega_3^2 + \Omega_4^2)$$

ahol l , b és d a helikopterre, ill. a rotorokra jellemző konstans. A felhajtóerő vektoros formában felírható $F = (0 \ 0 \ f)^T$ módon. A gravitációs erő negatív z -irányban hat, azaz $F_g = -mR_t^T (0 \ 0 \ g)^T = -mR_t^T G$. A giroszkopikus hatás modellezhető a következőképp:

$$T_g = -(\omega \times k)I_r(\Omega_2 + \Omega_4 - \Omega_1 - \Omega_3) = -\omega \times (I_r\Omega_r)$$

ahol I_r a rotor inerciája, k pedig a harmadik standard egységvektor.

Alacsony sebességeken a légellenállás lineáris formulával közelíthető, vagyis $F_a = -K_t v$ és $T_a = -K_r \omega$.

A fenti egyenletekből megkaphatjuk a helikopter mozgásegyenleteit:

$$\begin{aligned}F &= mR_t^T \ddot{\xi} + K_t R_t^T \dot{\xi} + mR_t^T G \\ T &= I_r \ddot{\eta} + I \left(\frac{\partial R_r}{\partial \Phi} \dot{\Phi} + \frac{\partial R_r}{\partial \Theta} \dot{\Theta} \right) \dot{\eta} + K_r R_r \dot{\eta} + (R_r \dot{\eta}) \times (I R_r \dot{\eta} + I_r \Omega_r)\end{aligned}$$

2.2. Egyszerűsített mozgásegyenletek

Bizonyos ésszerű egyszerűsítésekkel, ill. elhanyagolásokkal jelentősen egyszerűsödnek a mozgásegyenletek. Így a szabályozási algoritmus komplexitása is csökkenthető anélkül, hogy látványosan romlana a minősége.

Mivel a helikopter várhatóan viszonylag lassú mozgásokat végez, nem okoz nagy hibát, ha a légellenállás hatását elhanyagoljuk, mivel K_t és K_r elemei nullaközeliek. A következő elhanyagolás is az alacsony sebességgel áll kapcsolatban. Alacsony laterális sebességek esetén ugyanis R_r egységmátrixszal közelíthető. Ugyanez a megfontolás az R_t mátrixra nem igaz. A mozgásegyenletek így az alábbi módon közelíthetők:

$$\begin{aligned}F &= mR_t^T \ddot{\xi} + mR_t^T G \\ T &= I \ddot{\eta} + \dot{\eta} \times (I \dot{\eta} + I_r \Omega_r)\end{aligned}$$

Ezek az egyenletek a [3]-ban és [5]-ben található egyenletekre vezetnek.

2.3. Rotordinamika

A négy motor dinamikája az alábbi jól ismert egyenletekkel írható le ($k = 1, \dots, 4$):

$$L\dot{i}_k = u_{m,k} - Ri_k - k_e\Omega_k$$

$$I_r\dot{\Omega}_k = k_m i_k - k_r\Omega_k^2 - k_s$$

ahol k_e , k_m és k_s jelöli a motorok back EMF, motornyomaték és súrlódási állandóját. Ha a motorok induktivitása elhanyagolható, akkor a két egyenlet összevonható:

$$\dot{\Omega}_k = -k_{\Omega,0} - k_{\Omega,1}\Omega_k - k_{\Omega,2}\Omega_k^2 + k_u u_{m,k}$$

3. A helikopter irányítási algoritmus

3.1. Kapcsolódó kutatómunkák

Számos módszer létezik négyrotoros helikopter irányítására. Ezek között találhatunk lineáris [6], nemlineáris és soft computing technikára épült is [7]. A nemlineáris módszerek közül a leggyakrabban tárgyalt a backstepping alapú, bár létezik csúszó szabályozás, ill. feedback linearizáción alapú technika is [8].

A fent említett munkák nem csak a szabályozási algoritmusban különböznek egymástól, hanem a helikopter dinamikai modelljei is eltérnek egymástól. Többen elhanyagolják a rotordinamikát arra hivatkozva, hogy a tranziensek jóval gyorsabbak, mint a helikopteré. Megint mások a légellenállás hatását hanyagolják el az előbbieken említett okok miatt.

A mostani munka legszorosabban [3]-hoz és [9]-hez kapcsolódik szorosan, hiszen a helikopter modellje azonos a [9]-ben leírttal, azonban törekszünk a jobb hibatűrő képességre.

3.2. Backstepping algoritmus négyrotoros helikopterhez

Az algoritmus részben az [5]-ben lártak, részben pedig a saját kutatásunk [3] eredménye. Az itt bemutatott algoritmus ötvözni igyekszik a két módszer előnyeit, azaz hogy a komplex helikoptermodellt képes legyen irányítani, miközben a realisztikus zavarhatásokat is megfelelően kezeli, ahogyan azt a [3] alapján készült korábbi algoritmusunk is tette. Ehhez először a mozgásegyenletet át kell írni a következő alakra:

$$\ddot{\xi} = f_\xi + g_\xi u_\xi$$

$$\ddot{\eta} = f_\eta + g_\eta u_\eta$$

$$\dot{\Omega}_k = f_{m_k} + g_{m_k} u_{m_k}$$

ahol f_ξ , g_ξ és u_ξ jelentése

$$f_\xi = -G - \frac{1}{m} R_t^T K_t R_t^T \dot{\xi}$$

$$g_\xi = \frac{1}{m} \text{diag}(r_{t,3})$$

$$u_\xi = (f \quad f \quad f)^T$$

Itt $r_{t,3}$ az R_t mátrix harmadik oszlopa, és ezekből építünk fel egy diagonális mátrixot. Ezt azért tehetjük meg, mert az F vektor egyetlen nemnulla elemet tartalmaz. A következő egyenletben f_η , g_η és u_η azonos az alábbiakkal:

$$f_\eta = -(IR_r)^{-1} \left[I \left(\frac{\partial R_r}{\partial \Phi} \dot{\Phi} + \frac{\partial R_r}{\partial \Theta} \dot{\Theta} \right) \dot{\eta} + K_r R_r \dot{\eta} + (R_r \dot{\eta}) \times (IR_r \dot{\eta} + I_r \Omega_r) \right]$$

$$g_\eta = (IR_r)^{-1}$$

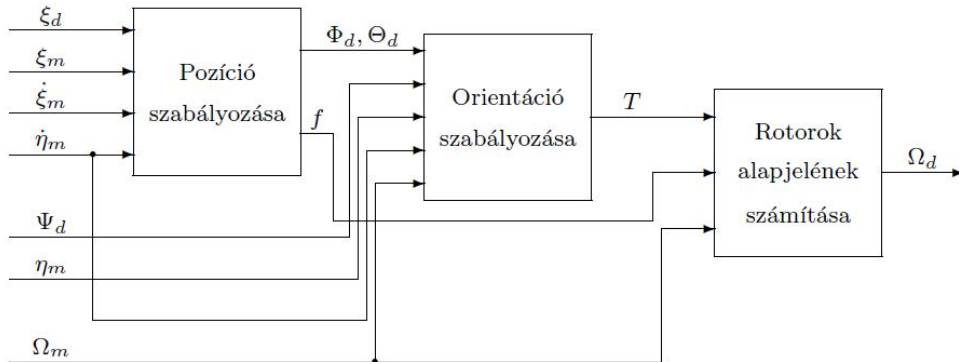
$$u_\eta = T$$

Végül pedig f_{m_k} és g_{m_k} jelöli a következőket:

$$f_{m_k} = -k_{\Omega,0} - k_{\Omega,1}\Omega_k - k_{\Omega,2}\Omega_k^2$$

$$g_{m_k} = k_u$$

Mivel a négyrotoros helikopter alulaktuált rendszer, azaz nagyobb a rendszer szabadságfokainak száma, mint a beavatkozó jelek száma, ezért a szabályozás koncepciója az, hogy a helikoptert egy adott térbeli pontból egy következő pontba juttassa, előírt z-tengelyhez képesti szögben. A referenciajelek tehát az $(x_d \ y_d \ z_d \ \Psi_d)$ négyesből állnak. A szabályozás a helikoptert mindig vízszintes helyzetben stabilizálja. A szabályozás szempontjából a rendszer három alegységre bontható, ahogyan azt az előbbiekben láthattuk. Először a translációs mozgást szabályozzuk, amely megadja a helikopter két hiányzó referenciajelét az orientációt szabályozó alrendszernek. A harmadik alegység felel a motorvezérlők referenciajelenek előállításáért. A szabályozó felépítése az 1. ábrán látható. A d és m indexek a kívánt és a mért mennyiségeket jelölik.



1. ábra. A szabályozó felépítése

3.2.1. A pozíció szabályozása

A backstepping algoritmust részletesen itt mutatjuk be. Definiáljuk először a követési hibát: $q_{\xi_1} = \xi_d - \xi$. Ljapunov direkt módszerét alkalmazva definiáljunk egy olyan pozitív definit függvényt, amelynek az idő szerinti deriváltja negatív definit:

$$V(q_{\xi_1}) = \frac{1}{2} q_{\xi_1}^T q_{\xi_1}$$

$$\dot{V}(q_{\xi_1}) = q_{\xi_1}^T \dot{q}_{\xi_1} = q_{\xi_1}^T (\dot{\xi}_d - \dot{\xi})$$

Ha szabadon megválaszthatnák $\dot{\xi}$ -t úgy, hogy $\dot{\xi} = \dot{\xi}_d + A_{\xi_1} q_{\xi_1}$ legyen, akkor

$$\dot{V}(q_{\xi_1}) = -q_{\xi_1}^T A_{\xi_1} q_{\xi_1} < 0$$

negatív definit lenne, ha A_{ξ_1} -et pozitív definitnek választanánk. Ha azonban definiálunk egy virtuális hibát, q_{ξ_2} -t és egy módosított Ljapunov-függvényt a következő módon:

$$q_{\xi_2} = \dot{\xi} - \dot{\xi}_d - A_{\xi_1} q_{\xi_1} = -\dot{q}_{\xi_1} - A_{\xi_1} q_{\xi_1}$$

$$V(q_{\xi_1}, q_{\xi_2}) = \frac{1}{2} (q_{\xi_1}^T q_{\xi_1} + q_{\xi_2}^T q_{\xi_2})$$

akkor ezek segítségével meghatározhatjuk a szükséges felhajtóerőt a módosított Ljapunov-függvény idő szerinti deriváltjából.

$$\begin{aligned} \dot{V}(q_{\xi_1}, q_{\xi_2}) &= q_{\xi_1}^T \dot{q}_{\xi_1} + q_{\xi_2}^T \dot{q}_{\xi_2} = q_{\xi_1}^T (-q_{\xi_2} - A_{\xi_1} q_{\xi_1}) + q_{\xi_2}^T [\ddot{\xi} - \dot{\xi}_d - A_{\xi_1} (-q_{\xi_2} - A_{\xi_1} q_{\xi_1})] = \\ &= -q_{\xi_1}^T A_{\xi_1} q_{\xi_1} - q_{\xi_2}^T q_{\xi_1} + q_{\xi_2}^T (f_{\xi} + g_{\xi} u_{\xi}) - q_{\xi_2}^T [\ddot{\xi}_d - A_{\xi_1} (q_{\xi_2} + A_{\xi_1} q_{\xi_1})] \end{aligned}$$

Innen u_{ξ} kifejezhető:

$$\begin{aligned} u_{\xi} &= g_{\xi}^{-1} [q_{\xi_1} - f_{\xi} + \ddot{\xi}_d - A_{\xi_1} (q_{\xi_2} + A_{\xi_1} q_{\xi_1}) - A_{\xi_2} q_{\xi_2}] = \\ &= g_{\xi}^{-1} [\ddot{\xi}_d - f_{\xi} + (I_3 + A_{\xi_2} A_{\xi_1}) q_{\xi_1} + (A_{\xi_2} + A_{\xi_1}) \dot{q}_{\xi_1}] \end{aligned}$$

ahol I_3 egy 3×3 -as egységmátrix. Hasonlóan [5]-höz $\ddot{\xi}_d$ -t elhanyagolhatnánk, azonban a szabályozás célja egy térbeli pálya követése lesz folyamatos mozgással, így ennek a tagnak fontos szerepe lesz a későbbiekben. Ha A_{ξ_2} -t is pozitív definitnek választjuk, akkor a Ljapunov-függvény deriváltja valóban negatív definit lesz:

$$\dot{V}(q_{\xi_1}, q_{\xi_2}) = -q_{\xi_1}^T A_{\xi_1} q_{\xi_1} - q_{\xi_2}^T A_{\xi_2} q_{\xi_2} < 0$$

A fenti szabályozójelet alkalmazva a helikopter pozíciójának szabályozására a következő összefüggéshez vezet:

$$\ddot{\xi} = \ddot{\xi}_d + (I_3 + A_{\xi_2} A_{\xi_1}) q_{\xi_1} + (A_{\xi_2} + A_{\xi_1}) \dot{q}_{\xi_1}$$

ami ekvivalens a

$$0 = (I_3 + A_{\xi_2} A_{\xi_1}) q_{\xi_1} + (A_{\xi_2} + A_{\xi_1}) \dot{q}_{\xi_1} + \ddot{q}_{\xi_1}$$

kifejezéssel. Ha A_{ξ_2} -t és A_{ξ_1} -et diagonálisnak vesszük fel, akkor a karakterisztikus egyenletek

$$s^2 + (a_{\xi_2} a_{\xi_1} + 1)s + (a_{\xi_2} + a_{\xi_1}) = 0$$

alakúak lesznek, ami garantálja a stabilitást. Ez azt jelenti, hogy ha a számított f_{ξ} és g_{ξ} értékek közel vannak a valódihoz, a hibák exponenciálisan 0-hoz tartanak.

Ahhoz, hogy a szükséges felhajtóerőn kívül az orientációs alrendszer két hiányzó referenciajelét meghatározzuk, a $g_{\xi} u_{\xi}$ szorzatban a tagok közül bizonyosakat fel kell cserélni úgy, hogy $g_{\xi} u_{\xi} = \tilde{g}_{\xi} \tilde{u}_{\xi}$ legyen, és $\tilde{g}_{\xi}$ invertálható legyen. Ha tehát $\tilde{g}_{\xi}$ -t és $\tilde{u}_{\xi}$ -t így definiáljuk:

$$\begin{aligned} \tilde{g}_{\xi} &= \frac{1}{m} \begin{bmatrix} f & 0 & 0 \\ 0 & f & 0 \\ 0 & 0 & C_{\Phi} C_{\Theta} \end{bmatrix} \\ \tilde{u}_{\xi} &= \begin{pmatrix} C_{\Psi} S_{\Theta} C_{\Phi} + S_{\Psi} S_{\Phi} \\ S_{\Psi} S_{\Theta} C_{\Phi} - C_{\Psi} S_{\Phi} \\ f \end{pmatrix} = \begin{pmatrix} u_{\xi_x} \\ u_{\xi_y} \\ f \end{pmatrix} \end{aligned}$$

akkor a módosított $\tilde{u}_{\xi}$ vektor elemeiből a hiányzó referenciajelek számíthatók

$$\begin{aligned} S_{\Phi_d} &= S_{\Psi} u_{\xi_x} - C_{\Psi} u_{\xi_y} \\ S_{\Theta_d} &= \frac{C_{\Psi} u_{\xi_x} + S_{\Psi} u_{\xi_y}}{C_{\Phi}} \end{aligned}$$

segítségével. Azért tekinthetők ezek referenciajeleknek, mert ha a helikopter a kívánt pozíció felé halad, ezek a mennyiségek 0-hoz tartanak. Megfordítva, ha a helikopter követi a megfelelő irányt, és az adott felhajtóerő hat rá, a célpozícióba fog jutni.

3.2.2. Orientáció szabályozása

A tervezés menete hasonló az előbbi pontban leírtakhoz, így itt csak a főbb lépések szerepelnek. Az orientáció hibáját az előbbihez hasonlóan definiáljuk:

$$q_{\eta_1} = \eta_d - \eta$$

A virtuális követési hiba pedig

$$q_{\eta_2} = \dot{\eta} - \dot{\eta}_d - A_{\eta_1} q_{\eta_1} = -\dot{q}_{\eta_1} - A_{\eta_1} q_{\eta_1}$$

Az előbbi lépéseket követve a végeredmény $T = u_{\eta}$, ahol

$$u_{\eta} = g_{\eta}^{-1} [\ddot{\eta}_d - f_{\eta} + (I_3 + A_{\eta_2} A_{\eta_1}) \dot{q}_{\eta_1} + (A_{\eta_2} + A_{\eta_1}) \dot{q}_{\eta_1}]$$

3.2.3. A pozíció és orientáció egyszerűsített szabályozása

A 2.2-ben alkalmazott megfontolásokkal élve f_{ξ} -ben, f_{η} -ban és g_{η} -ban egyszerűbb szabályozó algoritmusra jutunk. Az egyszerűsítések a következők:

$$f_{\xi} = -G$$

$$f_{\eta} = -I^{-1} [\dot{\eta} \times (I \dot{\eta} + I_r \Omega_r)]$$

$$g_{\eta} = I^{-1}$$

További lehetőség, hogy a referenciajelek második deriváltját 0-val közelítjük, amely következtében az algoritmus tovább egyszerűsödik.

3.2.4. Rotorszabályozás

Kisebbs eltérés az előbbiekhöz képest, hogy a rotor dinamikáját leíró differenciálegyenletben nem második, hanem első idő szerinti derivált szerepel. Ez azt jelenti, hogy nincs szükség q_{m_2}

bevezetésére, és a Ljapunov-függvény $V(q_{m_1}) = \frac{1}{2} q_{m_1}^T q_{m_1}$ -re egyszerűsödik. A hibadinamika

szempontjából azonban mégis érdemes q_{m_1} idő szerinti deriváltját is beiktatni. A referenciajel számítása így a következőre módosul:

$$u_m = g_m^{-1} [\dot{\Omega}_d - f_m + (I_4 + A_{m_2} A_{m_1}) \dot{q}_{m_1} + (A_{m_2} + A_{m_1}) \dot{q}_{m_1}]$$

A motorok számának megfelelően az u_m vektor négy elemből áll.

Érdemes megemlíteni, hogy mivel a felhajtóerő és a nyomatékok a rotorok szögsebességnégyzetének lineáris kombinációi, a referenciajelek az alábbi vektor elemeinek négyzetgyökeiként állnak elő:

$$\begin{pmatrix} \Omega_{1_d}^2 \\ \Omega_{2_d}^2 \\ \Omega_{3_d}^2 \\ \Omega_{4_d}^2 \end{pmatrix} = \begin{bmatrix} 0 & -(2lb)^{-1} & -(4d)^{-1} & (4d)^{-1} \\ -(2lb)^{-1} & 0 & (4d)^{-1} & (4d)^{-1} \\ 0 & (2lb)^{-1} & -(4d)^{-1} & (4d)^{-1} \\ (2lb)^{-1} & 0 & (4d)^{-1} & (4d)^{-1} \end{bmatrix} \begin{pmatrix} T_{3 \times 1} \\ f \end{pmatrix}$$

A Ljapunov-függvény deriváltja pedig

$$\dot{V}(q_{m_1}) = q_{m_1}^T \dot{q}_{m_1} = q_{m_1}^T [(I + A_{m_2} A_{m_1}) \dot{q}_{m_1} + (A_{m_2} + A_{m_1}) \dot{q}_{m_1}] = -q_{m_1}^T (I + A_{m_2} + A_{m_1})^{-1} (I + A_{m_2} A_{m_1}) \dot{q}_{m_1} < 0$$

negatív definit, amennyiben A_{m_2} és A_{m_1} mátrixot pozitív definitnek választjuk.

3.2.5. A szabályozó paramétereinek hangolása

A szabályozó paramétereit alacsony fókuszú karakterisztikus egyenletek, ill. pozitív definit diagonális mátrixok elemeivel állnak kapcsolatban, így megválasztásuk egyszerű. Ráadásul közvetlen a kapcsolatuk a szabályozás gyorsaságával. Figyelembe kell azonban venni, hogy a nagy beavatkozójelek telítést okozhatnak az aktuátorokban.

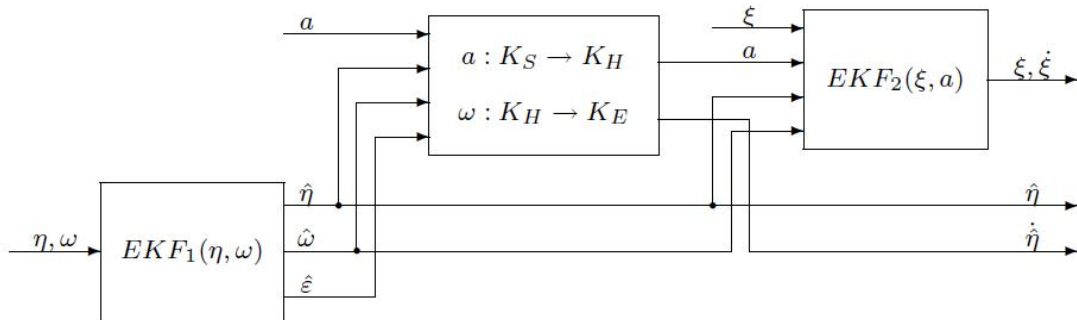
4. Állapotbecslés

Az előbbi fejezetben bemutatott algoritmus az 1. táblázatban látható mennyiségek rendelkezésre állását igényli. A táblázatban *-gal jelölt mennyiségek közvetlenül mérhetők, azonban a pozíció és orientáció mérési gyakorisága nem elegendő. Ráadásul a hosszabb időtartamú mérések azt mutatják, hogy a szenzorok hibái, különösen a bias értéke időben változik. Az említettek miatt tehát szükséges állapotbecslőt alkalmazni a rendszerben.

Mennyiség	Jelentés
ξ	Pozíció*
$\dot{\xi}$	Sebesség
η	Orientáció*
$\dot{\eta}$	Szögsebesség*
Ω	Rotorok szögsebessége*

1. táblázat. A szabályozáshoz szükséges mérendő jelek

Az állapotbecslő két kiterjesztett Kalman-szűrőt tartalmaz, amelyek egymással hierarchikus összeköttetésben állnak. Külön szűrő felelős a pozícióval és az orientációval kapcsolatos jelek becsléséért (EKF_1 és EKF_2). Az állapotbecslő felépítése a 2. ábrán látható. A közepen elhelyezkedő blokk transzformálja a gyorsulás értékét a szenzor koordináta-rendszeréből a helikopterébe.



2. ábra. Az állapotbecslő felépítése

Az állapotbecslés részletes bemutatása előtt érdemes meggondolni, hogy a helikopterre szerelt szenzorokhoz rögzített koordináta-rendszer nem azonos a helikopter koordináta-rendszerével. A két koordináta-rendszer egymáshoz képesti elhelyezkedését az A_s ortonormált mátrix és a p_s vektor írja le.

4.1. A helikopter orientációjának és szögsebességének becslése

A fent említetteknek megfelelően az IMU kimenete három komponensből áll: a valódi értékből és a hozzáadódó véletlen zajból és biasból. A szenzor koordináta-rendszerében kifejezve ez

$$\omega_m = \omega_s = \omega_{s,0} + \omega_{s,b} + \omega_{s,n}$$

alakú, ahonnan a szögsebesség a helikopter koordináta-rendszerében felírva

$$\omega = A_s \omega_{s,0} = A_s (\omega_s - \omega_{s,b} - \omega_{s,n})$$

A Földhöz rögzített inerciarendszerben felírt szögsebesség pedig a

$$\dot{\eta} = R_r^{-1} \omega = R_r^{-1} A_s (\omega_s - \omega_{s,b} - \omega_{s,n})$$

kifejezéssel egyenlő. Mivel a feltételezések szerint a bias lassan változik, az idő szerinti deriváltja 0-hoz közeli. A változást egy képzeletbeli zavarással lehet modellezni (lásd még [10]-ben):

$$\dot{\omega}_{s,b} = \omega_{s,b,n}$$

További feltételezés, hogy az orientáció mérése biast nem tartalmaz, vagyis

$$\eta_m = \eta + \eta_n$$

Ha a mintavételi időt T_s -sel jelöljük, akkor az Euler-féle diszkrétidejű áttérést alkalmazva a következő differenciaegyenletre jutunk:

$$x_{1,k+1} = x_{1,k} + T_s R_{r,k} A_s (-x_{2,k} + u_k + w_{1,k})$$

$$x_{2,k+1} = x_{2,k} + T_s w_{2,k}$$

$$y_k = x_{1,k} + z_k$$

ahol a jelölések a következők:

$$\begin{array}{lll} x_1 = \eta & x_2 = \omega_{s,b} & x = (x_1 \quad x_2)^T \\ w_1 = -\omega_{s,n} & w_2 = \omega_{s,b,n} & w = (w_1 \quad w_2)^T \\ u = \omega_m & y = \eta_m & z = \eta_n \end{array}$$

A fenti egyenletek a következő általános alakra hozhatók:

$$x_{k+1} = f(x_k, u_k, w_k)$$

$$y_k = g(x_k, z_k)$$

ahonnan a kiterjesztett Kalman-szűrő algoritmus a következő jelölésekkel meghatározható:

$$\begin{array}{ll} R_{w,k-1} = E[w_{k-1} w_{k-1}^T] & R_{z,k} = E[z_k z_k^T] \\ A_{k-1} = \frac{\partial f(\hat{x}_{k-1}, u_{k-1}, 0)}{\partial x} & B_{w,k-1} = \frac{\partial f(\hat{x}_{k-1}, u_{k-1}, 0)}{\partial w} \\ C_k = \frac{\partial g(\bar{x}_k, 0)}{\partial x} & C_{z,k} = \frac{\partial g(\bar{x}_k, 0)}{\partial z} \end{array}$$

Itt $\hat{x}_k$ a k-adik becsült értéke az állapotváltozóknak, $\bar{x}_k$ az előzetes becslés. A kiterjesztett Kalman-szűrő algoritmus pedig a következő:

1. predikció

$$\bar{x}_k = f(\bar{x}_{k-1}, u_{k-1}, 0)$$

$$M_k = A_{k-1} \Sigma_{k-1} A_{k-1}^T + B_{v,k-1} R_{v,k-1} B_{v,k-1}^T$$

2. mérési adatok frissítése

$$\begin{aligned} S_k &= C_k M_k C_k^T + C_{z,k} R_{z,k} C_{z,k}^T \\ G_k &= M_k C_k^T S_k^{-1} \\ \bar{x}_k^+ &= \bar{x}_k + G_k (y_k - g(\bar{x}_k, 0)) \\ \Sigma_k &= M_k - G_k S_k G_k^T \end{aligned}$$

4.2. A helikopter Pozíciójának és sebességének becslése

A módszer hasonló az előbbihez. Első lépésként a szenzor által mért jel összetevőit kell megállapítani. Az előbbihez képest újdonság egy tag, a gravitáció hatása:

$$a_s = a_{s,0} + a_{s,b} + a_{s,n} - A_s^T R_t^T G$$

Mivel a helikopterhez rögzített koordináta-rendszer nem inerciarendszer, K_H és K_S között a kapcsolatot

$$a_{s,0} = A_s^T (a + \varepsilon \times p_s + \omega \times (\omega \times p_s))$$

írja le. Innen a K_H -beli gyorsulás kifejezhető:

$$a = A_s a_s - \varepsilon \times p_s - \omega \times (\omega \times p_s) + R_t^T G - A_s a_{s,b} - A_s a_{s,n}$$

A fenti kifejezés első része felfogható a gyorsulásmérő kimenetének transzformáltjaként:

$$a_t = A_s a_s - \varepsilon \times p_s - \omega \times (\omega \times p_s) + R_t^T G$$

Ezt a műveletet végzi el a 2. ábrán a középső blokk, és magyarázatot ad a két kiterjesztett Kalman-szűrő hierarchikus elrendezésére.

A mozgó koordináta-rendszerben történő differenciálási szabály ($\ddot{\xi} = \dot{v} + \eta \times v$) alkalmazásával, és az előbbi pontban alkalmazott módszerek segítségével juthatunk az állapotbecslő differenciálegyenletéhez:

$$\begin{aligned} \dot{v} &= -\omega \times v - A_s a_{s,b} + a_t + A_s a_{s,n} \\ \dot{a}_{s,b} &= a_{s,b,n} \\ \dot{\xi} &= R_t v + v_{\xi,n} \\ \dot{\xi}_m &= \xi + \xi_n \end{aligned}$$

A diszkrétidejű áttérés és a kiterjesztett Kalman-szűrő algoritmus a innen azonos az előbbi pontban leírtakkal.

5. Pályakövetés

5.1. A pályakövetési algoritmus

A tervezés egyik alapvető célja, hogy a helikopter egy térbeli pályán a lehető legkisebb hibával végig tudjon haladni. Ez azt jelenti, hogy egy adott térbeli pontot bizonyos pontossággal meg kell közelíteni mind pozícióban, mind pedig a függőleges tengely körüli előírt orientációban. A követési hibán kívül azonban lényeges szempont, hogy a helikopter mozgása folyamatos legyen. Másképp megfogalmazva a helikopter lehetőség szerint ne lassuljon le látványosan, miközben a célpozíciót megközelíti, hanem haladjon tovább a következő sarokpont felé.

A fent megfogalmazott célok teljesítése érdekében feltételeket fogalmazhatunk meg, amelyek közül akár ha egy is teljesül, a helikopter továbbléphet a következő sarokpont felé.

A pozícióra két feltételt írunk elő:

$$\sum_{j=1}^3 \left(\xi_{d_j}^{(i+1)} - \xi_j \right)^2 < (\Delta \xi_0)^2$$

$$\sum_{j=1}^3 \left(\xi_{d_j}^{(i+1)} - \xi_j \right)^2 < \lambda \sum_{j=1}^3 \left(\xi_{d_j}^{(i+1)} - \xi_{d_j}^{(i)} \right)^2$$

Itt ξ a pillanatnyi pozícióvektor, $\Delta \xi_0$ egy előre definiált konstans térbeli távolság, $\xi_{d_j}^{(i)}$ és $\xi_{d_j}^{(i+1)}$ a követendő pálya két egymást követő sarokpontja. Az első feltétel biztosítja, hogy a helikopter valóban a definiált pálya közelében mozog, míg a második a helikopter folyamatos mozgásban tartásáért felel. A tapasztalat szerint a $\lambda = (3/4)^2$ megfelelő kompromisszum, ha a sarokpontok közel helyezkednek el egymáshoz. Érdeemes megjegyezni, hogy akadályok elkerülésére a módszer korlátozottan alkalmas, azonban az algoritmus nem ezt tűzte ki célul.

Az orientáció követése valamelyest eltér az előbbtől, hiszen bizonyos esetekben fontos lehet, hogy a helikopter milyen orientációban követi a pályát. Emiatt a helikopter orientációjának abszolút hibáját egy korlát ($\Delta \Psi_0$) alá kell szorítani:

$$|\Psi_d^{(i+1)} - \Psi| < \Delta \Psi_0$$

További lehetséges finomítás, hogy az elfordulás iránya is figyelembe vehető, ha $\Psi_d^{(i+1)}$ -et megfelelően választjuk meg. Egy lehetséges megoldás, ha Ψ értékét nem korlátozzuk a $[0; 2\pi)$ intervallumra.

5.2. A pálya simaságának biztosítása

Ha egymástól távol helyezkedik el két sarokpont, akkor a továbblépéskor keletkező hirtelen megnövekedett hibajelek telítésbe vihetik a motorokat, ill. a szabályozási algoritmusban futásidejő hibák keletkezhetnek, így veszélybe kerülhet a jármű és a környezetének biztonsága.

A referenciajelet emiatt érdemes szűrni. A szűrési algoritmust a következő átviteli függvény mintavételezett megvalósítása adja:

$$W(s) = \frac{\gamma |p_s|^{n+1}}{(s + \gamma \cdot p_s)(s + p_s)^n}$$

Érdeemes a paramétereket úgy beállítani, hogy p_s negatív valós, γ pozitív legyen. Ha $n = 5$ és $\gamma = 1/3$, akkor a szabályozójelek simák maradnak, és a szűrő tranzienseit leginkább $\gamma \cdot p_s$ határozza meg.

6. Szimulációs eredmények

Mivel a repülő járművek komplex rendszerek, és hibás működés esetén könnyen kárt tehetnek önmagukban és a környezetükben, a leendő irányítórendszert érdemes alaposan letesztelni. Másrészt ellenőrizni kell, hogy a célhardver képes-e megfelelően ellátni feladatát valós időben. Az említettek miatt hardware-in-the-loop szimulációban tetteltük az irányítórendszert.

A helikopter és a BLDC motorok paramétereit a tervezett méretek alapján határoztuk meg. Az értékeket a 2. táblázat foglalja össze.

Paraméter	Érték
l	0,23 m
b	$1,759 \cdot 10^{-5}$ kg m
d	$1,759 \cdot 10^{-6}$ kg m ²
I_x, I_y	$1,32 \cdot 10^{-2}$ kg m ²
I_z	$2,33 \cdot 10^{-2}$ kg m ²
I_r	$5,626 \cdot 10^{-5}$ kg m ²
m	1,4 kg
K_t	diag([0.1 0.1 0.15]) Ns/m
K_r	diag([0.1 0.1 0.15]) Nm s
$k_{\Omega,0}$	94,37 1/s ²
$k_{\Omega,1}$	3,02 1/s
$k_{\Omega,2}$	0,005
k_u	139,44 V/s ²

2. táblázat. A helikopterre jellemző fizikai paraméterek

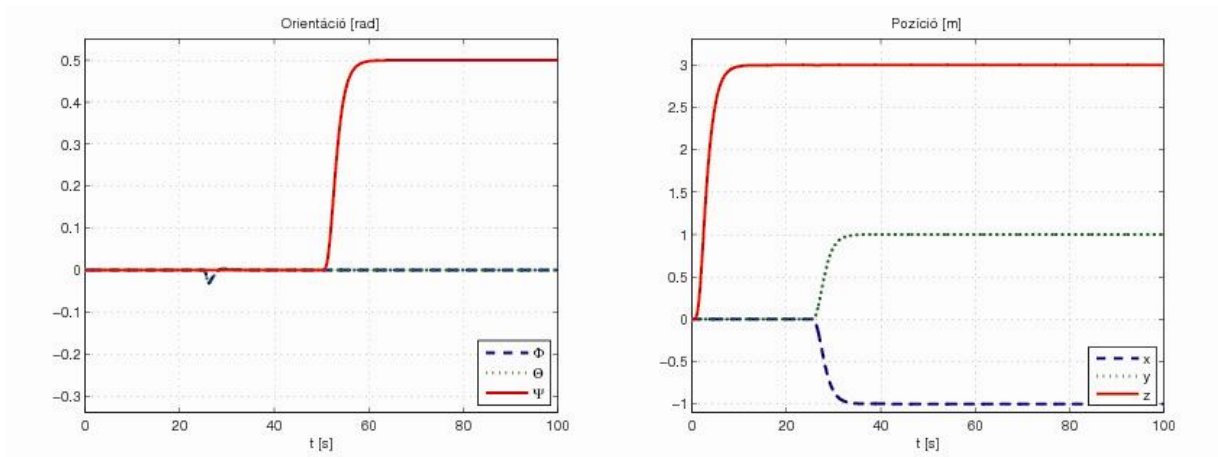
6.1. Simulinkben végrehajtott tesztek

A szabályozás komponenseit fokozatosan beillesztve a rendszerbe Simulinkben teszteltük az algoritmust. A legegyszerűbb esetben mindössze a helikopter modelljét és a szabályozót tartalmazta az összeállítás. A méréseket zajmentesnek tekintettük, és a feladat egyetlen térbeli pont elérése volt megadott orientációban. A referenciajelek az 5. fejezetben leírtaknak megfelelően voltak simítva. A tesztelés mellett a szabályozó paramétereinek behangolása volt az elsődleges cél ekkor (3. táblázat). A mintavételi időt $T_s = 10ms$ értékre állítottuk az IMU legnagyobb működési sebességével összhangban.

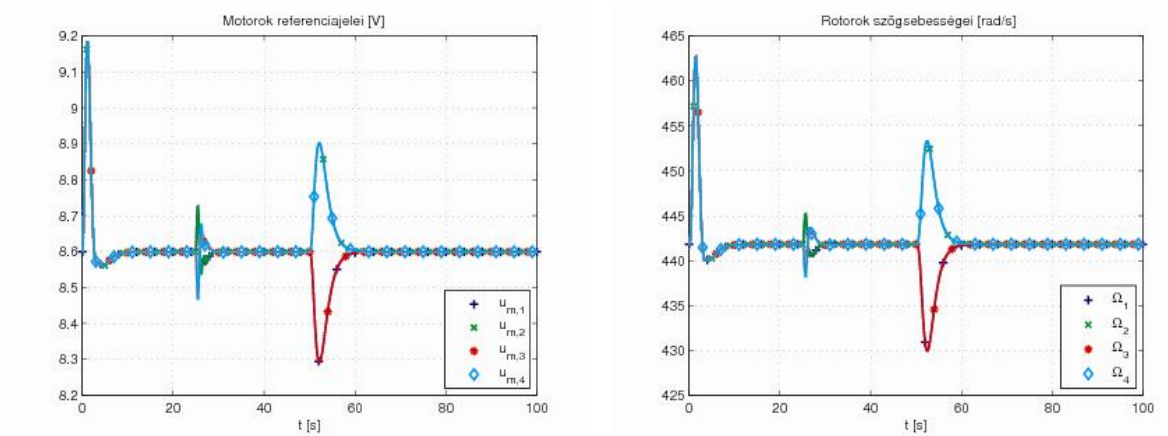
Paraméter	Érték
A_{ξ_1}	diag(2 1.6 1.6)
A_{ξ_2}	diag(1.2 1.2 1.2)
A_{η_1}	diag(12 12 12)
A_{η_2}	diag(8 8 8)
A_{m_1}	diag(0.04 0.04 0.04 0.04)
A_{m_2}	diag(0.016 0.016 0.016 0.016)

3. táblázat. A szabályozáshoz szükséges mérendő jelek

A 3. és 4. ábrán egy egyszerű szimuláció eredményei láthatók, sorrendben a helikopter pozíciója és orientációja, valamint a motorok referenciajelei és a rotorok szögsebességei.

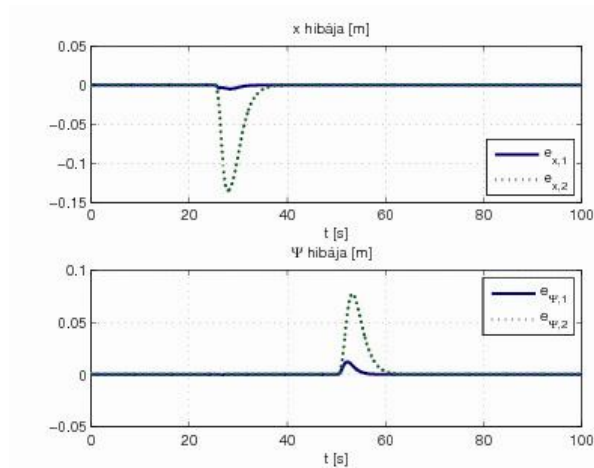


3. ábra. A helikopter pozíciója és orientációja repülés közben



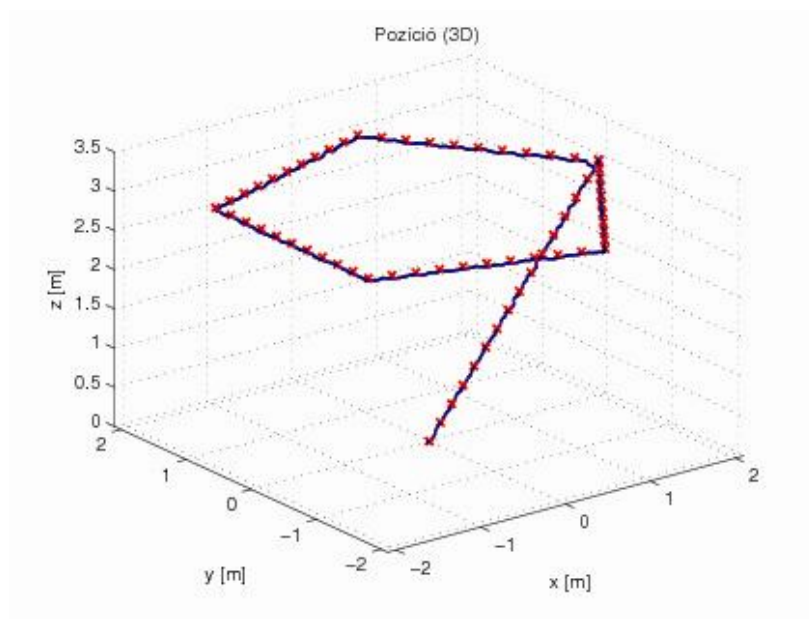
4. ábra. A motorok referenciajelei és szögsebességei

Az eredményeket összehasonlítottuk az egyszerűsített algoritmussal kapott eredményekkel, és a tapasztalat szerint az egyszerűbb változat csupán kevéssel teljesített rosszabbul. Ez igazolja, hogy a helikopter a repülés során a feltételezéseknek megfelelően viselkedett (alacsony sebesség, kis szögelfordulások). Összehasonlításként az 5. ábrán a pozíció x-tengely irányú komponensének hibatranziense látható, ahol a pontozott vonal az egyszerűsített algoritmushoz tartozik.

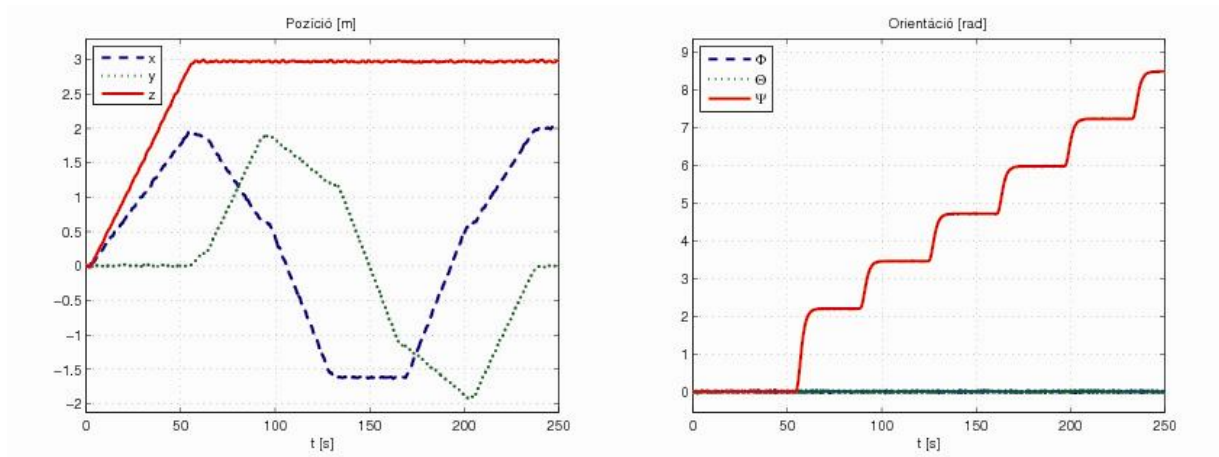


5. ábra. A hibatranziensek a komplex és az egyszerűsített szabályozó esetén (folytonos vonal – komplex, szaggatott vonal - egyszerűsített)

Végül az összes komponens rendszerbe integrálásával a szabályozás egy komplex pálya követésére is alkalmassá válik. A 6. és 7. ábrán egy ilyen feladat végrehajtása látható. A kiterjesztett Kalman-szűrők kezdeti beállításait a 4. táblázat tartalmazza. A beállításokat a valós szenzorok tanulmányozása alapján állítottuk be (bővebb irodalom erről [11]-ben található).



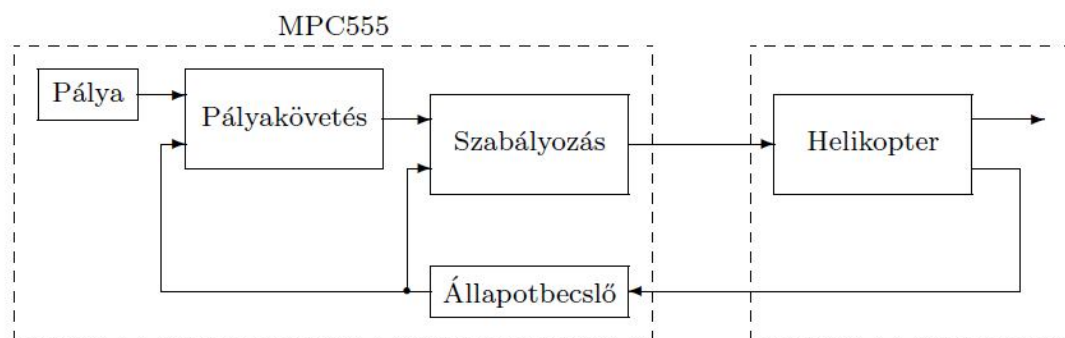
6. ábra. Komplex pályakövetési feladat



7. ábra. A helikopter pozíciója és orientációja komplex pályakövetés esetén

6.2. Valós idejű tesztek

A valós idejű tesztek egy dSPACE DS1103 egység segítségével hajtottuk végre hardware-in-the-loop technikával. A helikopter és a szenzorrendszer működését ezen az egységen emuláltuk, míg a szabályozási feladatokat az MPC555 mikrokontroller látta el, amely a végső összeállításban a fedélzeti elektronika központi egysége. A kommunikáció a két egység között CAN-buszon történik ugyanúgy, ahogy a valódi helikopteren is. A 8. ábrán látható a valós idejű tesztek megvalósításának sematikus vázlata.



8. ábra. A hardware-in-the-loop tesztek sematikus vázlata

6.3. A valódi helikopteren végzett kísérletek

A teljes rendszer megvalósítása során egyszerűbb repülési módokban tesztrepüléseket végzünk. A térbeli pozíció- és orientációmérés működésbe lépése előtt korlátozott ideig a helikopterre szerelt szenzorok segítségével tudjuk becsülni a jármű orientációját. A gondos kalibrációnak köszönhetően két perc alatt mindössze 5-10°-os hibát okoz az IMU jeleinek integrálása.

Ezt alapul véve tesztekét végeztünk az orientáció stabilizálhatóságára. A szabályozás alapja LQ állapot-visszacsatolás, amelyet munkapont környezetében linearizált rendszeren valósítottunk meg. A linearizálás a helikopter vízszintes helyzetben lebegése körül történt. Az állapotegyenlet alakja:

$$A = \frac{\partial f(x,u)}{\partial x} \Big|_{x_0} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

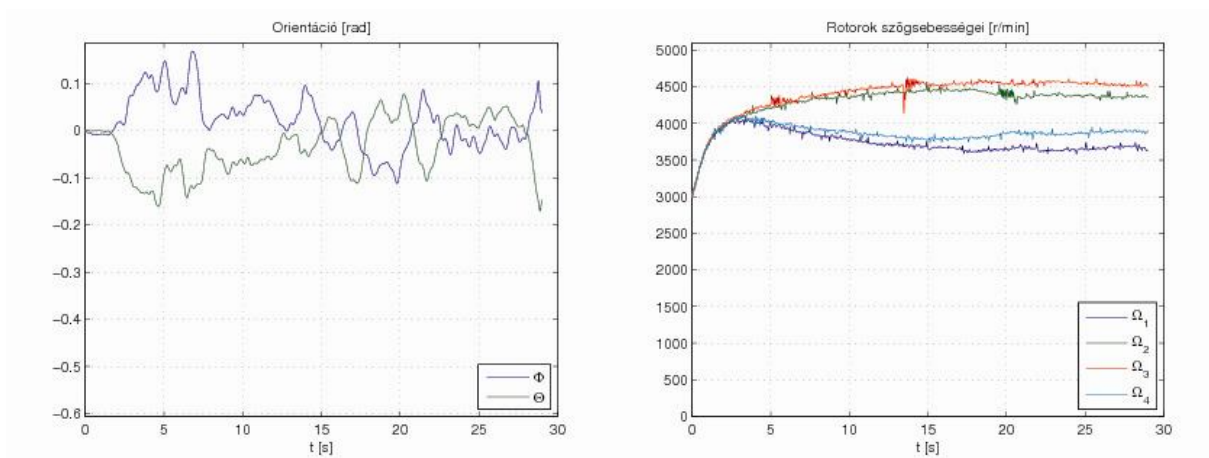
$$B = \frac{\partial f(x,u)}{\partial u} = \begin{bmatrix} 0 & -lb/I_x & 0 & lb/I_x \\ 0 & 0 & 0 & 0 \\ -lb/I_y & 0 & lb/I_y & 0 \\ 0 & 0 & 0 & 0 \\ -d/K_z & d/K_z & -d/K_z & d/K_z \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$C = \frac{\partial g(x,u)}{\partial x} \Big|_{x_0} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$D = \frac{\partial g(x,u)}{\partial u} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

A súlyozómátrix $Q = \text{diag}(1 \ 100 \ 1 \ 100 \ 1 \ 100)$ értékre lett beállítva, a visszacsatolást pedig a fenti rendszer diszkrét idejű állapotegyenletéhez terveztük.

A motorok közti eltérések kiküszöbölésére az LQ visszacsatolást kiegészítettük egy integráló szabályozással, amely a helikopter stabilitására pozitív hatással volt. A következő ábrán egy tesztrepülés eredményei láthatók, ahol a szabályozás a helikoptert vízszintesen stabilizálta. Biztonsági okokból a tesztelés során a teljes felhajtóerő a helikoptert nem volt képes a levegőben tartani, azonban csekély külső beavatkozásra volt csupán szükség.



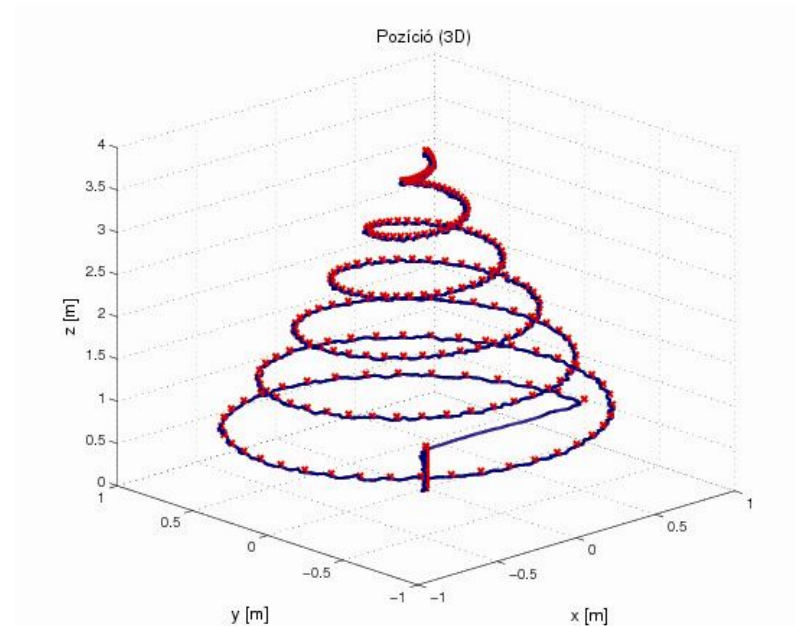
9. ábra. A helikopter orientációja és a rotorok fordulatszáma a tesztrepülés közben

7. A szabályozási algoritmus megvalósítása a célprocesszoron

7.1. Szoftverkörnyezet

Az irányítási algoritmus egy Freescale MPC555 típusú processzoron fut, amely egy Phytec által gyártott alaplapon van elhelyezve. A processzor egy 40Mhz órajelű PowerPC architektúrájú mikrokontroller, amely egy 64 bites lebegőpontos FPU-t is tartalmaz. A szabályozási algoritmust MATLAB/Simulink segítségével terveztük. A hardver támogatottságának köszönhetően automatikusan lehet futtatható kódot tölteni a processzorra. A fordítási és letöltési procedúra a Real-Time Workshop, a Real-Time Workshop Embedded Coder, Embedded Target for Motorola MPC555, valamint a MetroWerks CodeWarrior segítségével történik.

A hardware-in-the-loop szimulációkat a már említett dSPACE DS1103 egység segíti. Az egységet leginkább az autóiparban alkalmazzák gyors prototípustervezésre. Ehhez is tartozik Simulink blokk-könyvtár, azaz a futtatható kódot ugyancsak MATLAB/Simulink segítségével állítjuk elő. A szimulációk során az adatok monitorozását és mentését egy grafikus program segítségével, a ControlDeskkal végezhetjük. A gyűjtött adatokat később MATLAB segítségével tudjuk feldolgozni. A 10. ábrán egy ilyen valós idejű teszt eredményeit láthatjuk.



10. ábra. Komplex pályakövetési feladat szimulációja valós időben

7.2. Kommunikáció

A fejlesztés kezdeti szakaszában bizonyos egységekkel, mint az IMU-val, soros vonalon terveztük a kommunikációt. A tapasztalat azonban azt mutatta, hogy a Simulinkből fordított kód nem volt megfelelő, hiszen jelentős (20ms – 30ms) késleltetést vitt a rendszerbe. Ezért amellet döntöttünk, hogy az MPC555 processzorral minden egyéb egység CAN-buszon kommunikál, és kiegészítő egységek végzik el a konverziót. Gyakorlati okokból azonban ennek következményeként bizonyos jeleket csonkítani kell.

További lényeges szempont, hogy a CAN-buszon az MPC555-nek címzett csomagokat a lehető leghamarabb érdemes feldolgozni, hogy a motorok referenciajeleit a lehető leghamarabb számolni lehessen. Emiatt a kommunikáció mintavételi ideje lényegesen kisebb a szabályozás mintavételi idejénél.

7.3. A fejlesztés során felmerülő szoftverrel kapcsolatos problémák

Több kisebb-nagyobb jelentőségű probléma nehezítette a fejlesztést. A legfontosabb ezek közül a mintavételi idővel volt kapcsolatos. A célprocesszor ugyanis nem képes a teljes szabályozási algoritmust az eredetileg tervezett 10ms-os mintavételi idővel végrehajtani a hardverkorlátok miatt. A mintavételi időt így 30ms értékre állítottuk, azonban ez várhatóan nem okoz stabilitási problémákat.

A könnyen kiküszöbölhető hibák közé tartozik, hogy ha a fordítandó blokk-séma ún. beágyazott S-függvényeket tartalmaz C nyelven megírva, akkor ha ezek tartalmaznak globális változókat, akkor azok fájlanként eltérő nevéeknek kell lenniük, ellenkező

esetben a program futása megjósolhatatlan, mivel a fordítás során az egyik felülírja a másikat.

Egy következő problémával akkor szembesülhet a fejlesztő, ha bizonyos blokkok egymástól eltérő mintavételi idővel működnek. Diszkrét deriválást végző blokkok alkalmazása esetén kritikus hibák fordulhatnak elő, ugyanis ezeknek nem adható meg külön, milyen mintavételi idővel működjenek, vagyis a használatuk kerülendő.

8. Az eredmények összefoglalása

A cikkben egy autonóm működésű négyrotoros helikopter dinamikai modellezését és fedélzeti irányítási algoritmusának kifejlesztését mutattuk be. Részletesen bemutattuk a szabályozás komponenseit, amely egy saját fejlesztésű backstepping elvű szabályozásra épül. Kiegészítő komponensként kiterjesztett Kalman-szűrőkből álló állapotbecslőt tartalmaz, amely a helikopterre szerelt inerciális mérőegység és a BME IIT Tanszéken kifejlesztett külső kameraalapú pozíciónálórrendszer méréseit dolgozza fel.

A szabályozási algoritmus Freescale MPC555 alapú rendszeren valósítottuk meg, és dSPACE DS1103 segítségével hardware-in-the-loop szimulációkat hajtottunk végre. A helikoptert és a szenzorrendszert ez utóbbi egységen emuláltuk.

A szabályozási rendszer komponensei között CAN-busz, ill. rádiófrekvenciás kapcsolat biztosítja az összeköttetést.

A pályakövetés sikeres végrehajtása mutatja a szabályozási algoritmus hatékonyságát.

Köszönetnyilvánítás

A cikkben bemutatott munka hátterét az Országos Tudományos Kutatási Alapprogramok OTKA K 71762 jelű támogatása biztosítja.

Irodalomjegyzék

- [1] A. Soumelidis, P. Gáspár, P. Bauer, B. Lantos, and Z. Prohászka: Design of an Embedded Microcomputer Based Mini Quadrotor UAV, Proceeding of the European Control Conference ECC'07, pp. 2236–2241, 2007.
- [2] A. Soumelidis, P. Gáspár, G. Regula, and B. Lantos, Control of an Experimental Mini Quad-Rotor UAV, Proceeding of the 16th Mediterranean Conference on Control and Automation, pp. 1252–1257, 2008.
- [3] L. Kis, G. Regula, and B. Lantos, Design and Hardware-in-the-Loop Test of the Embedded Control System of an Indoor Quadrotor Helicopter, Proceeding of the

- 6th Workshop on Intelligent Solutions in Embedded Systems WISES'08, pp. 35–44, 2008.
- [4] L. Kis and B. Lantos, Szenzorfüzió alkalmazása beltéri autonóm négyrotoros helikopteren, Hadmérnök, 2009. december.
 - [5] S. Bouabdallah and R. Siegwart, Backstepping and Sliding-mode Techniques Applied to an Indoor Micro Quadrotor, Proceeding of the IEEE International Conference on Robotics and Automation, pp. 2247–2252, 2005.
 - [6] S. Bouabdallah, A. Noth, and R. Siegwart, PID vs LQ control techniques applied to an indoor micro quadrotor, Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems IROS'04, vol. 3, 2004.
 - [7] C. Coza and C. Macnab, A New Robust Adaptive-Fuzzy Control Method Applied to Quadrotor Helicopter Stabilization, Proceeding of the Annual meeting of the North American Fuzzy Information Processing Society NAFIPS'06, pp. 454–458, 2006.
 - [8] A. Das, K. Subbarao, and F. Lewis, Dynamic Inversion of Quadrotor with Zero-Dynamics Stabilization, Proceeding of the 17th IEEE Conference on Control Applications, pp. 1189–1194, 2008.
 - [9] T. Madani and A. Benallegue, Control of a Quadrotor Mini-Helicopter via Full State Backstepping Technique, Proceedings of the 45th IEEE Conference on Decision and Control, pp. 1515–1520, 2006.
 - [10] B. Lantos, State Estimation Based on Image Processing and Inertial Sensors for Indoor Autonomous Systems, BME IIT, Research Report (in Hungarian), 2007.
 - [11] L. Kis, Z. Prohászka, and G. Regula, Implementation and Theoretical Improvement of the Control System of an Autonomous Indoor Quadrotor Helicopter, Proceeding of the 17th International Workshop on Robotics in Alpe-Adria-Danube Region RAAD'08, 2008.

Sipos Marianna

sipos.marianna@zmne.hu

A WINDOWS ÚJ BIZTONSÁGI LEHETŐSÉGEI

Absztrakt

Az asztali gépes alkalmazások tömeges felhasználását felváltotta a szolgáltatás alapú architektúra, ahol az egyes szolgáltatások eléréséhez egyre gyakrabban használjuk az Internetet. A kívülről jövő támadások lehetősége és mennyisége ezzel megsokszorozódott. A Windows a .NET Framework szolgáltatásaival támogatja a védekezést a nem várt kártékony behatolások ellen.

A .NET Framework két biztonsági szolgáltatást kínál: A szerepalapú biztonság és a kóderedet-alapú biztonság lehetőségét. A szerepalapú biztonság a felhasználó jogosultságait ellenőrzi a .NET Framework Futtatókörnyezet által biztosított UAC segítségével, míg a kóderedet-alapú biztonság az assembly tanúsítványa segítségével olyan hozzáféréseket is korlátozhat amit az UAC nem tud.

Jóllehet a szolgáltatások használata a lehetőségek megismerését és némi kényelmetlenséget jelent, de biztonságunk érdekében a mindennapi életben is vállaljuk mindezt.

At first the masses used desktop applications, but the structure of applications is service oriented in these days. We use often the services through the Internet. The attacks coming from outside multiplied. The services of .NET Framework give the potentiality protection against malicious attacks.

.NET Framework has two kinds of security services: Role-based security and code access security. The role-based security controls the users permissions with the User Account Control service. The code access security controls the assemblies permissions used the assemblies certificate. CAS gives us the chance to protect our computer from malwares.

The use of security services is comfortless, and needs some preparedness, but the situation is the same in casual.

Kulcsszavak: szoftver, biztonság, Windows ~ software, security, Windows

Előzmények

A PC-k tömeges elterjedése növelte az igényt, hogy a számítógépeket ne csak egyedi programok írására, hanem a mindennapi élet feladatainak megkönnyítésére szolgáló

alkalmazások futtatására is használjuk. A Windows létrehozásakor a Microsoft célja az volt, hogy asztali gépekre készülő alkalmazások futtatását tegyék lehetővé mindenkinek, elérhető áron. A kényelmesen kezelhető grafikus felület (1. ábra) egyszerűvé tette a monitoron a tájékozódást, az egér használatával gyorsan és egyszerűen lehetett a programokat indítani, kezelni.



1. ábra A Windows 1.0 grafikus felülete [1]

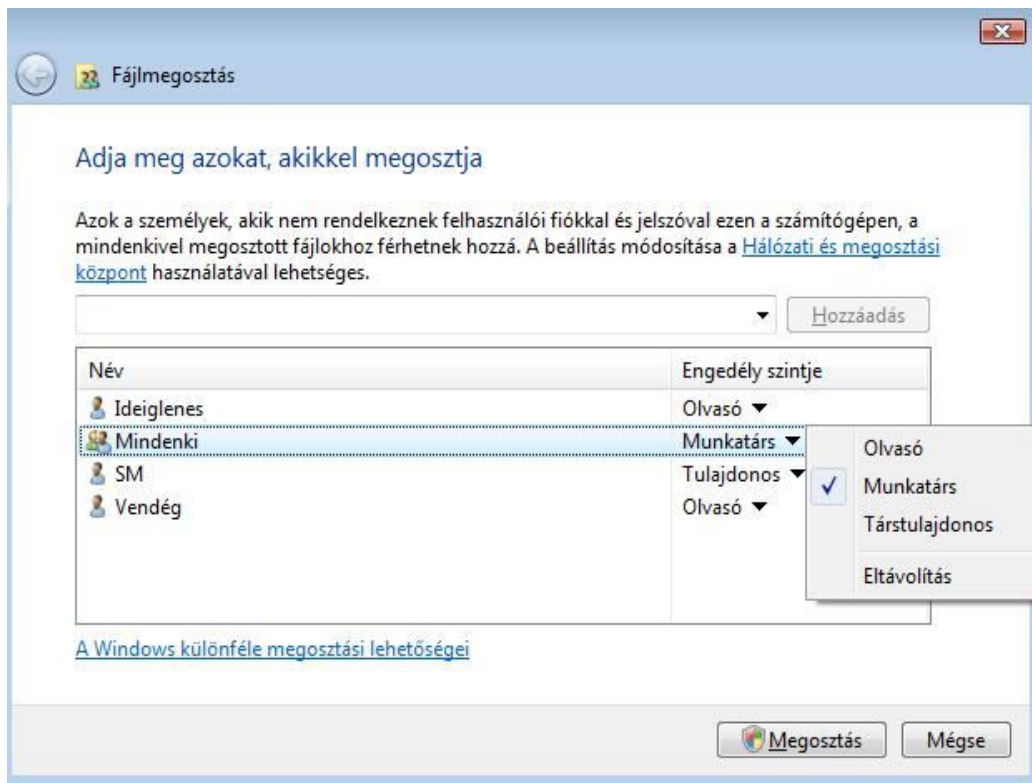
Megbízhatóságát üzleti alapon épp annyira biztosították, hogy a tömeges felhasználás során az átlagos felhasználó ne ütközzön problémákba. A cég üzleti sikerei annak köszönhetőek, hogy piackutatással meghatározták az igényeket és pontosan azokhoz illesztették a szoftver képességeit. Sem többet, sem kevesebbet nem adott az elvárásoknál. Ha nem felel meg a felhasználói igényeknek, nem terjed el a piacon, másrészt viszont a vártnál minél többet nyújt, annál jobban csökken az üzleti haszon.

Akkoriban főként egyedi gépeken futó alkalmazások felhasználására volt igény. Egy gépet többnyire egy személy használt, vagy egy család, esetleg egy kis munkahelyi közösség. Mivel nem volt internethozzáférés, nem kerültek a gépekre a szülők elől titkolt magánbeszélgetések, vagy munkaidőben végzett magánügyek adatai, és persze mások sem férhettek hozzá a család vagy a munka adataihoz, amivel aztán visszaélhettek volna. Ami a gépen volt, azt a felhasználók mindannyian tudták. Az asztali gépeknél ma is ritkán van szükség a közös használatból eredő mappahozzáférés védelmére. Hálózati kapcsolatok nélkül az idegen felhasználó legfeljebb az egyedül hagyott gép elé ülve juthatott adatokhoz. Ennek védelmét egy egyszerű jelszó bekérésével megoldhattuk. A legtöbb felhasználó ezzel az eszközzel sem élt.

Hálózat és internet használat

A hálózatok használatának és az internet elérésének elterjedése megváltoztatta a számítógépek használatát. Ma már az a ritka, ha offline használjuk gépeinket. Általában a bekapcsolás során bejelentkezünk a hálózatra. A szoftvereket is jó ideje úgy fejlesztik, hogy működésükhöz szerverekkel kell kommunikálniuk.

Az első megoldás adataink védelmére, vagy megosztására nézőpont kérdése, a nyilvános mappa és a mappák megosztásának lehetősége volt. Itt még speciális beállítások is rendelkezésünkre álltak, megadhattuk, hogy az adott könyvtárat mely felhasználói csoport és milyen engedéllyel érheti el. (2. ábra)



2. ábra A mappák megosztását beállító ablak

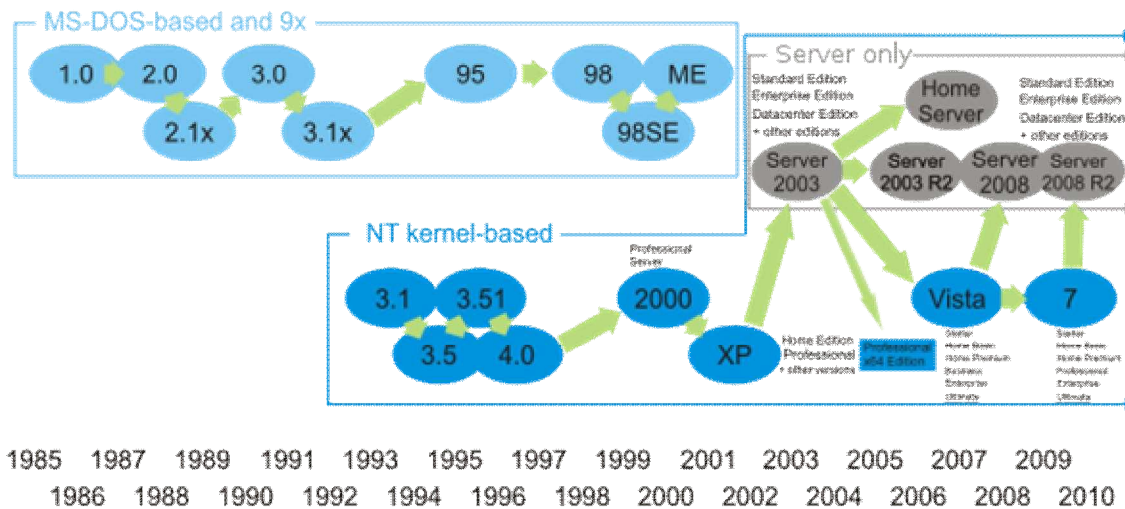
Lehetőség volt a felhasználói jogok korlátozására. Ezzel a rendszergazdák többnyire a rendszer működőképességének megőrzése érdekében éltek oly módon, hogy bizonyos mappák módosítását megtiltották. Nagyon ritkán használták az egyénre szabás lehetőségét. Általában megelégedtek az alapértelmezésben létező rendszergazda és általános felhasználó csoportok használatával. Beállították az általános felhasználók jogosultságait és akinek több hozzáférésre volt szüksége, az átkerült a rendszergazda csoportba. Tehát a szűk lehetőségeket szűkösén használták.

A hálózatok használatának egyre sokoldalúbbá válása és a kívülről érkező egyre kifinomultabb támadások további védekezési lehetőségeket igényeltek. A .NET Framework, mely Windows XP esetén még egy opcionálisan telepíthető réteg az operációs rendszer felett, a Vista megjelenésével beépült az operációs rendszerbe.

Ha megnézzük a Windows fejlődését bemutató ábrát (3. ábra), két nagy változást láthatunk benne. Az első, amikor a grafikus felület az operációs rendszer részévé vált egybe esett a 16 bitről 32 bitre történő váltással. A második a .NET framework beépülése az operációs rendszerbe egyben a 32 bitről 64 bitre váltás megvalósítása. Ha már az első esetben kiemeltük a grafikát megjegyezném ezen a területen is jelentős a változás. Míg a korábbi Windows-ok a bitképes ábrákat támogatták a WPF (.NET 2.0) megjelenésével áttér a vektorgrafikus képábrázolásra.

Microsoft Windows

family tree



3. ábra A Windows fejlődése [2]

Természetesen sok további változást is hozott a .NET bevezetése, ezek közül ebben a cikkben a biztonsági szolgáltatásaival foglalkozunk.

.Net hozzáférés-szabályozás

Hozzáférés-szabályozás alatt a hálózaton vagy a számítógépen található objektumok elérésének engedélyezését értjük felhasználók, csoportok vagy számítógépek részére. A szabályozás elemei:

- Engedélyek
- Objektumok tulajdonjoga
- Engedélyek öröklődése
- Felhasználói jogok
- Objektumok naplózása

A szabályozható objektumok a következők:

- Fájlok, mappák
- Active Directory objektumok
- Beállításjegyzék objektumok (registry)
- Rendszerobjektumok (pl. folyamatok, feladatütemező, nyomtatásvezérlés, naplózás)

Az objektumok típusa határozza meg, milyen engedély adható. Pl. az NTFS-engedélyek és hozzáférési korlátozásaik a következő táblázatban olvashatók:

Speciális engedélyek	Teljes hozzáfér	Módosít	Olvas és végrehajt	Mappa tartalomlista	Olvasás	Írás
Mappa bejárása, fájl végrehajtása	x	x	x	x		
Mappa lista, adat olvasása	x	x	x	x	x	
Attribútum olvasása	x	x	x	x	x	
Kiterj. Attribútum olvasása	x	x	x	x	x	
Fájl létrehozás, írás	x	x				x
Mappa létrehozás, adat hozzáfűz	x	x				x
Attribútum írása	x	x				x
Kiterj. Attribútum. írása	x	x				x
Almappák és fájlok törlése	x					
Törlés	x	x				
Engedély olvasása	x	x	x	x	x	x
Engedély módosítása	x					
Saját tulajdonba vétel	x					
Szinkronizálás	x	x	x	x	x	x

Felhasználói fiókok felügyelete

A felügyeletet az UAC (User Account Control) végzi. Feladata, hogy segít megelőzni a számítógépen végzett nem engedélyezett változtatásokat. A változtatások előtt az UAC előbb engedélyt kér. Ha van az adott felhasználónak jogosultsága, az engedélyt megkapja. Ha nincs jogosultsága, rendszergazdai jelszót kér. Ez a megoldás teszi lehetővé, hogy ha egy rendszergazdai jogokkal rendelkező felhasználó nem rendszergazdaként lép be, akkor is el tudja végezni a munkája során adódó rendszergazdai jogosultságot igénylő feladatokat, és az aktuális user nevében nem lehet a gépre a háttérben rosszindulatú szoftvereket (malware) kémprogramokat telepíteni.

Az UAC üzenetei:

- **A Windows a beleegyezését kéri a folytatáshoz**
Amikor olyan Windows programot futtatunk, mely hatással van más felhasználók adataira.
- **Egy programnak engedélyre van szüksége a továbblépéshez**
Ha a futtatni kívánt program rendelkezik digitális aláírással, mely tartalmazza a nevét és a kiadó nevét. Eldönthetjük megbízunk-e benne.

- **Egy azonosítatlan program kér hozzáférést a számítógéphez**
Ha a futtatni kívánt program nem rendelkezik digitális aláírással, nem azonosítható. Döntsük el, hogy megbízunk-e benne.
- **Ez a program le van tiltva**
A rendszergazda által letiltott program. Ha szüksége van rá, kérjen engedélyt a futtatáshoz.

Kóderedet-alapú biztonság

A CAS (Code Access Security) [3] az alkalmazás jogosultságát nézi, nem a felhasználóét. Ehhez eszközként a tanúsítvány ellenőrzést használja. A CAS segítségével a szerepalapú biztonsággal nem korlátozható hozzáférések is ellenőrizhetők. pl.

- Az adott alkalmazás tud vagy nem tud Web kérést küldeni az internetre.
- Egy alkalmazás kérhet vagy nem DNS-t

Amint azt a 4. ábrán is láthatjuk 7 alapértelmezett engedélyhalmaz áll rendelkezésünkre:

- FullTrust: Nem ellenőrzi a CAS
- SkipVerification: Elkerülheti az ellenőrzést. Javítja a teljesítményt, feláldozza a biztonságot.
- Execution: Csak futhat.
- Nothing: Még csak nem is futhat.
- LocalIntranet
- Internet
- Everything: Összes standard, beépített engedély. Abban különbözik a FullTrust-tól, hogy a CAS ellenőrzés végrehajtódik rajta.

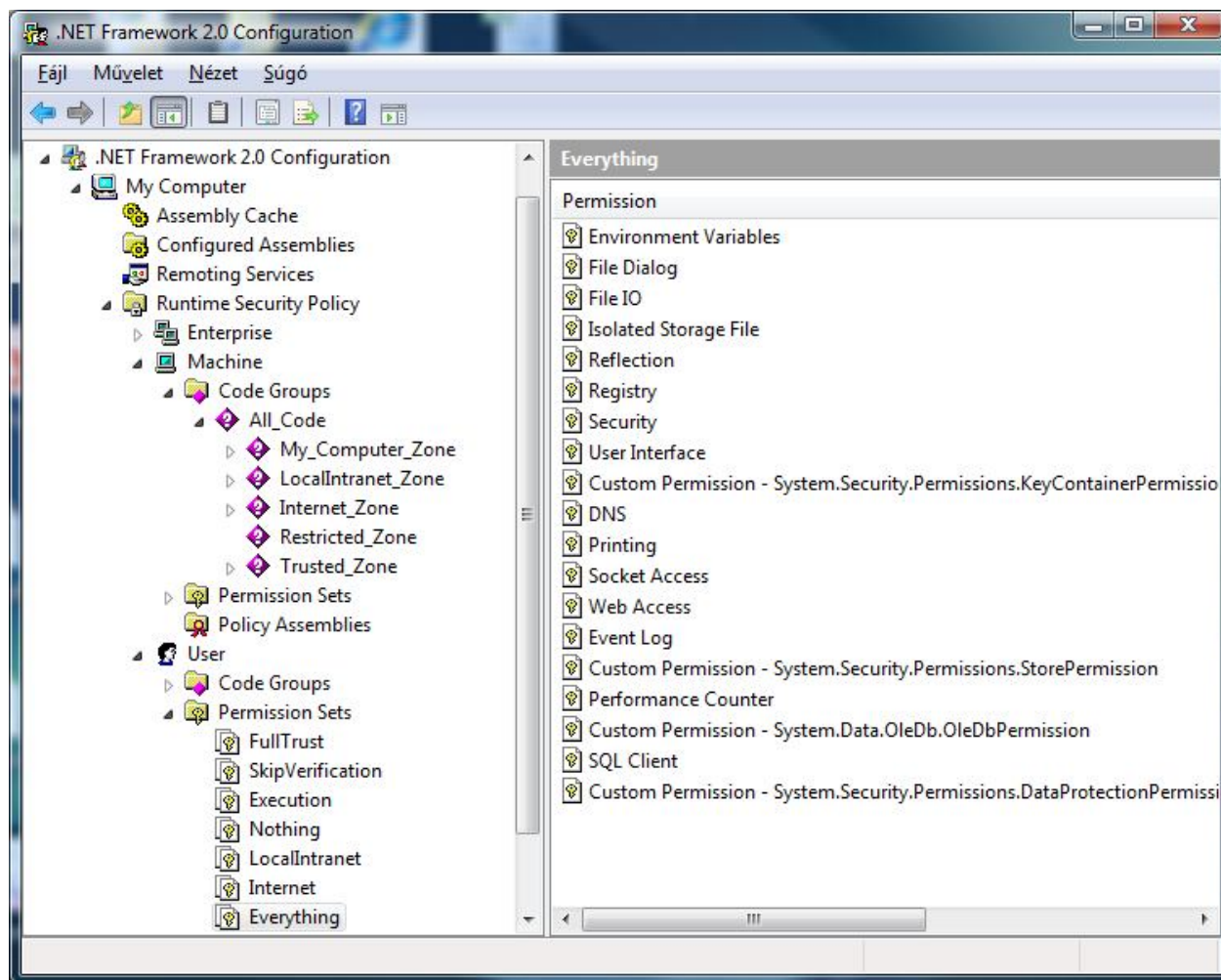
A .NET Framework Configuration (4. ábra) eszköz segítségével [4] mi magunk is létrehozhatunk engedélyhalmazokat, és meghatározhatjuk a hozzájuk tartozó engedélyeket.

A biztonsági házirend három házirend szintet bocsát rendelkezésünkre. Ezek:

- Enterprise
- Machine
- User

A házirendek mindegyikéhez tartoznak kódcsoporthok. Az assemblyket kódcsoporthokba sorolhatjuk. Az egyes kódcsoporthokhoz kiválaszthatjuk az engedélyhalmazt, melynek engedélyeivel rendelkezik. Alapértelmezésben az adott gép (machine) házirendje tartalmaz az All_Code csoporton belül kódcsoporthokat. Ezek mindegyike zóna. Vagyis egy kód attól függően tartozik a csoportba, hogy honnét futtatjuk. A következő zónák állnak rendelkezésünkre (4. ábra):

- My_Computer_Zone
- LocalIntranet_Zone
- Internet_Zone
- Restricted_Zone
- Trusted_Zone



4. ábra Kódcsoportok és engedélyhalmazok

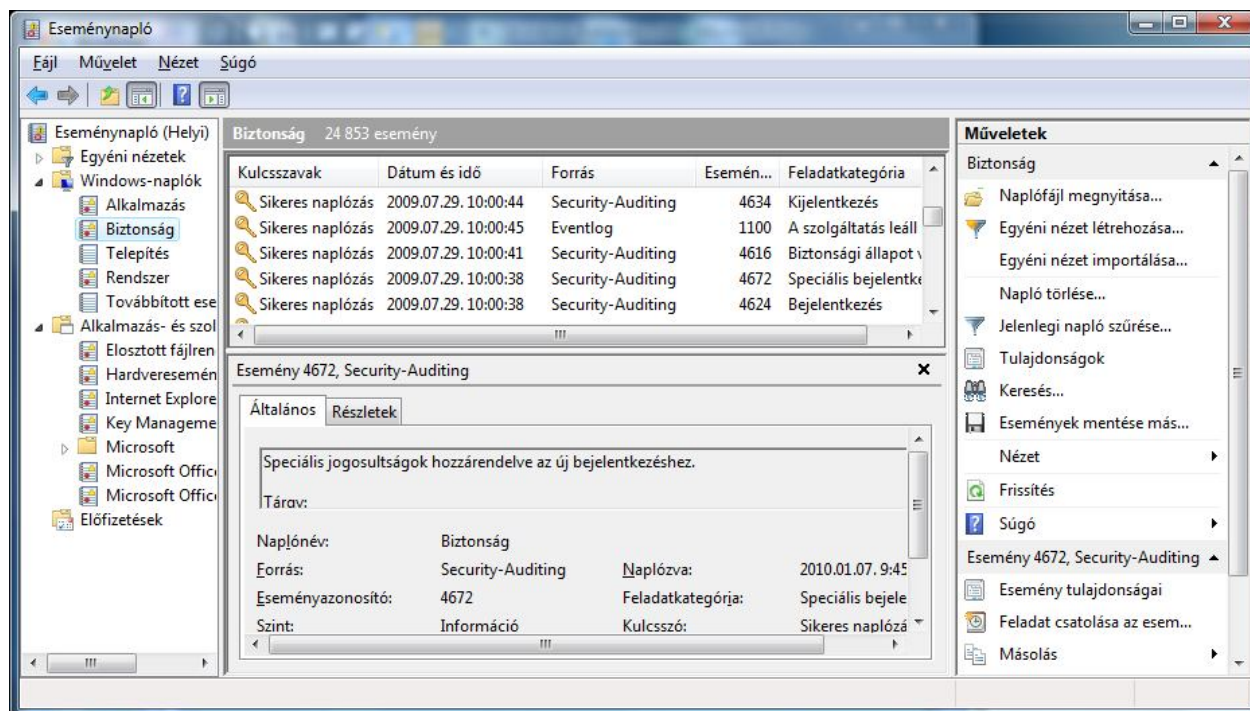
További kódcsoportokat mi magunk hozhatunk létre.

A futtatott kódnál a házirend kiértékeli mindhárom házirend szintet. Besorolja a kódot az ott megadott kódcsoportok valamelyikébe, majd meghatározza az engedélyhalmazt, és az abban megadott engedélyeket. A három házirend által meghatározott minimális engedély áll rendelkezésre a kód futásához.

Ha már meghatároztuk az egyes kódok lehetőségeit, a hibás esetek elemzéséhez még a naplózást kell beállítanunk.

Naplózás

A naplózás beállítására a vezérlőpult, felügyeleti eszközök, eseménynapló (5. ábra) szolgáltatás ad lehetőséget.



5. ábra A Vista Eseménynaplója

Összegzés

A szinte mindent megengedő Windows egy alapos, de bonyolult biztonsági rendszert dolgozott ki a .NET Framework szolgáltatásaként. Két lehetőség volt a bevezetésnél. Vagy alapértelmezésben nem szorítja rá a felhasználót a biztonsági szolgáltatásokra, és akkor a felhasználó nem is vesz azokról tudomást. Vagy a gépen futtatott kódok engedélyt kérnek a biztonságot veszélyeztető helyek hozzáférésehez.

A .NET futtatókörnyezet szolgáltatásai „sokkolták” a felhasználók nagy részét. A számos bírálat ellenére, talán túl gyorsan érkezett? Vagy a felhasználói tömegek nem igénylik? Vagy amit soha be nem vallanánk, az ablakok olyan figyelmeztetéseket küldenek, melyeket nem értünk, így fölöslegesnek ítélnék?

Gondoljunk arra, ha egy biztonságos környéken élve nem zárjuk a lakásokat, mert fölösleges gond kulccsal a zsebünkbe közlekedni. Aztán egyre több turista jön a nagyvilágból és viszik hírét ennek a nyugalmas környéknek, ahol még az ajtót sem kell bezárni. Meghallják ezt a besurranó tolvajok is. S a könnyű rablás reményében megszállják a környéket. Rögtön megváltoznak a szokásaink és elkezdjük zárni az ajtókat, garázsokat, kertkapukat, majd megerősítjük ablakainkat, riasztót szerelünk a lakásra. Természetesen a munkahelyünk ugyanezt teszi. Pedig milyen kényelmetlen sok kulcsot cipelni a zsebünkbe, azonosító kártyákra figyelni, riasztó kódokat, jelszavakat megjegyezni!

Hivatkozások:

- [1] A kép forrása: Wikipedia, <http://en.wikipedia.org/> History of Microsoft Windows
<http://upload.wikimedia.org/wikipedia/en/4/4e/Windows1.0.png>
- [2] A kép forrása: Wikipedia, <http://en.wikipedia.org/> Timeline of Microsoft Windows
http://en.wikipedia.org/wiki/Timeline_of_Microsoft_Windows
- [3] Albert I., Balássy Gy., Charaf H., Erdélyi T., Horváth Á., Levendovszky T., Péteri Sz., Rajacsics T.: A .net framework és programozása, szak kiadó, 2004.
- [4] .NET Framework 2.0 Configuration tool súgója.

Szabolcsi Róbert

szabolcsi.robert@zmne.hu

MODELLING OF DYNAMICAL SYSTEMS

Absztrakt/Abstract

A szerző célja, hogy komplex módszereket mutasson be a dinamikai rendszerek modellezésére. Jelen írás az elektromos, mechanikai és elektro-mechanikus rendszerekre, vagyis a mechatronikai rendszerekre fókuszál. A matematikai modellezés a legfontosabb fázis az automatikus rendszerek elemzésében és azok előzetes tervezésében. Szerző a számítógépes elemzés és tervezés területeire koncentrál, amely során számos példát mutat be a modellezési és irányítási problémák köréből.

Purpose of the author to give a complex set of methods applied for modeling of the dynamical systems. The more attention is paid for electrical, mechanical, and electro-mechanical systems, i.e. for mechatronical systems. Mathematical modeling is the most important phase in automatic systems' analysis, and preliminary design. Author of the paper devotes attention to computer aided analysis and design. Examples for this are taken from the wide branch of modeling and control problems.

Kulcsszavak/Keywords: *dinamikus rendszerek, irányítás, modellezés ~ dynamical systems, control, modeling*

I. INTRODUCTION

Modeling of the dynamical systems is in the focus of attention of scientists since many decades. Today there is a main motivation to have necessary information for automated control of the dynamical systems. Dynamical systems can be technical (e.g. electrical systems, mechanical systems etc.), biological (e.g. blood pressure control, insulin control etc.) ones, and also they can represent many other branches of economics, society, sciences etc. Dynamical modeling is necessary for computer aided preliminary design, too. There are many powerful tools to design a control system for the first possible scheme.

The designed system must be tested for design criteria, and in case of necessity must be re-designed. Purpose of the author is to present a typical set of possible dynamical systems applied in Mechatronics, and, in Robotics, too. There are many famous classical examples of

Mechanics, theory of electricity, Electrotechnics being involved in this paper to show how to get a complex set of dynamical characteristics of them. Solution of the analysis task is supported by MATLAB[®], by SIMULINK[®] software, and by theirs toolboxes.

II. BRIEF HISTORY & LITERATURE OVERVIEW

Mathematical backgrounds for modeling of deterministic dynamical systems are given detailed in [2, 3], and stochastic systems are discussed in [1]. The theory of the control systems both for SISO and MIMO applications are outlined in [4, 5, 7, 8, 9]. In general, systems and signals are investigated by Pokorádi, L. [12]. Mathematical models of the turbulent air are discussed in [6, 10, 11, 14]. Computer aided simulation is supported by MATLAB [13].

III. MODELLING DYNAMICAL SYSTEMS

3.1. MODELLING OF THE “MASS-SPRING-DAMPER” MECHANICAL SYSTEM.

The dynamical model of the “mass-spring-damper” mechanical system can be seen in Figure 3.1. [2, 5, 7].

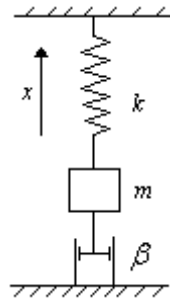


Figure 3.1. The sketch of the “mass-spring-damper” mechanical system.

Equation of motion of the free vibration system can be derived as [2, 5]:

$$\frac{d(mv)}{dt} = \Sigma F_i. \quad (3.1)$$

From Figure 3.1. it is easily can be seen that the resulting damping force is as follows [2, 3, 5]:

$$\Sigma F_i = kx + \beta \frac{dx}{dt}. \quad (3.2)$$

In Eq (3.2): kx is the spring force opposing to translational motion of the constant mass, m ; $\beta \frac{dx}{dt}$ is the viscous damper wall friction force. Resulting equation of motion of the mechanical system as given below:

$$m \frac{d^2x}{dt^2} + \beta \frac{dx}{dt} + kx = 0. \quad (3.3)$$

The solution of the second order differential equation (3.3) with constant parameters is given in [2, 3] to be as follows:

$$x(t) = Ae^{\lambda_1 t} + Be^{\lambda_2 t}, \quad (3.4)$$

where A and B are constants derived by the initial conditions, λ_1 , and λ_2 are solutions of the characteristic polynomial of

$$m\lambda^2 + \beta\lambda + k = 0. \quad (3.5)$$

Solving eq (3.5) yields to the following roots [2]:

$$\lambda_1 = -\frac{\beta}{2m} + \sqrt{\left(\frac{\beta}{2m}\right)^2 - \frac{k}{m}}; \quad \lambda_2 = -\frac{\beta}{2m} - \sqrt{\left(\frac{\beta}{2m}\right)^2 - \frac{k}{m}}. \quad (3.6)$$

Let us suppose that $\beta \neq 0$. For further discussion we suppose that

A) $\beta^2 > 4 \cdot k \cdot m$. In this particular case solutions of the eq (3.5) are real and negative ones, i.e.

$$\lambda_1 < 0, \lambda_2 < 0, |\lambda_2| > |\lambda_1|. \quad (3.7)$$

Let us suppose system parameters to be as follows:

$$\text{Case a)} \quad A = 1; B = -2; \lambda_1 = -1; \lambda_2 = -2. \quad (3.8)$$

$$\text{Case b)} \quad A = -1; B = 2; \lambda_1 = -1; \lambda_2 = -2. \quad (3.9)$$

$$\text{Case c)} \quad A = 1; B = 2; \lambda_1 = -1; \lambda_2 = -2. \quad (3.10)$$

For systems defined by equations (3.8)-(3.10) computer aided simulation was done, and the results can be seen in Figure 3.2, Figure 3.3, and finally, Figure 3.4.

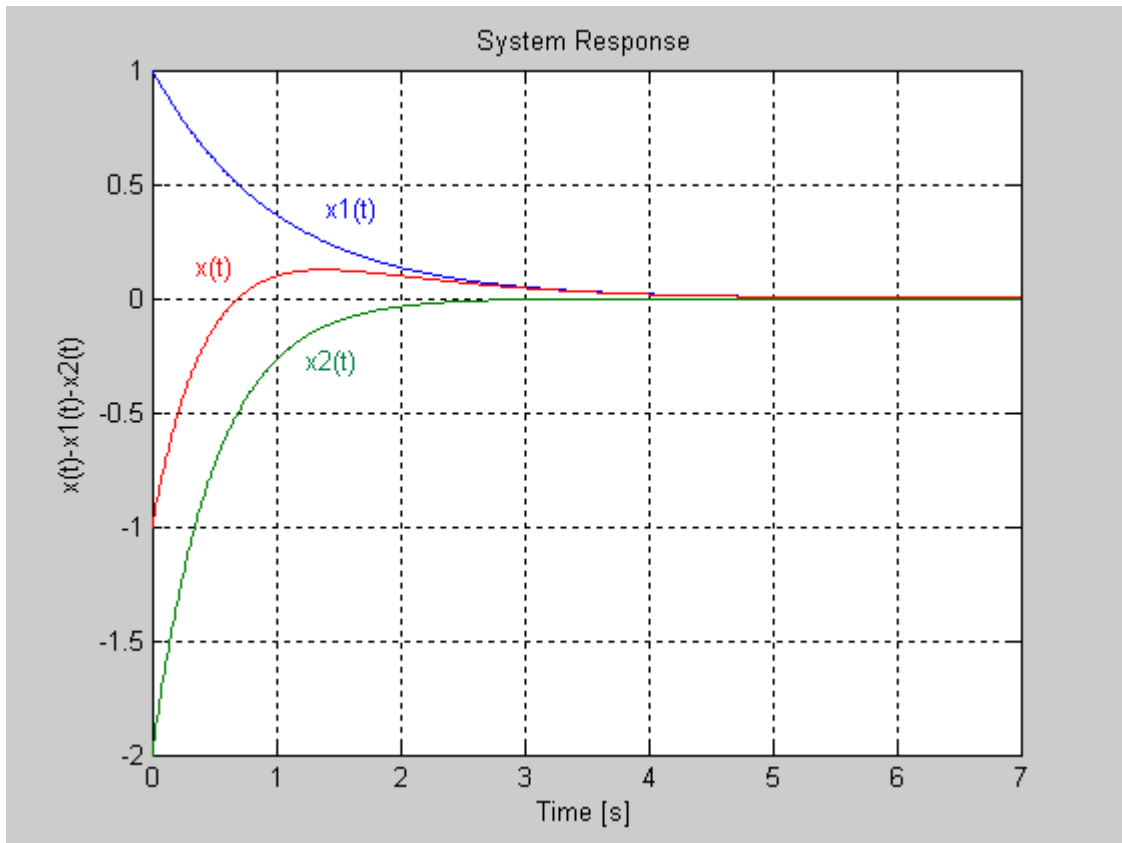


Figure 3.2. Case a) $A = 1$; $B = -2$; $\lambda_1 = -1$; $\lambda_2 = -2$

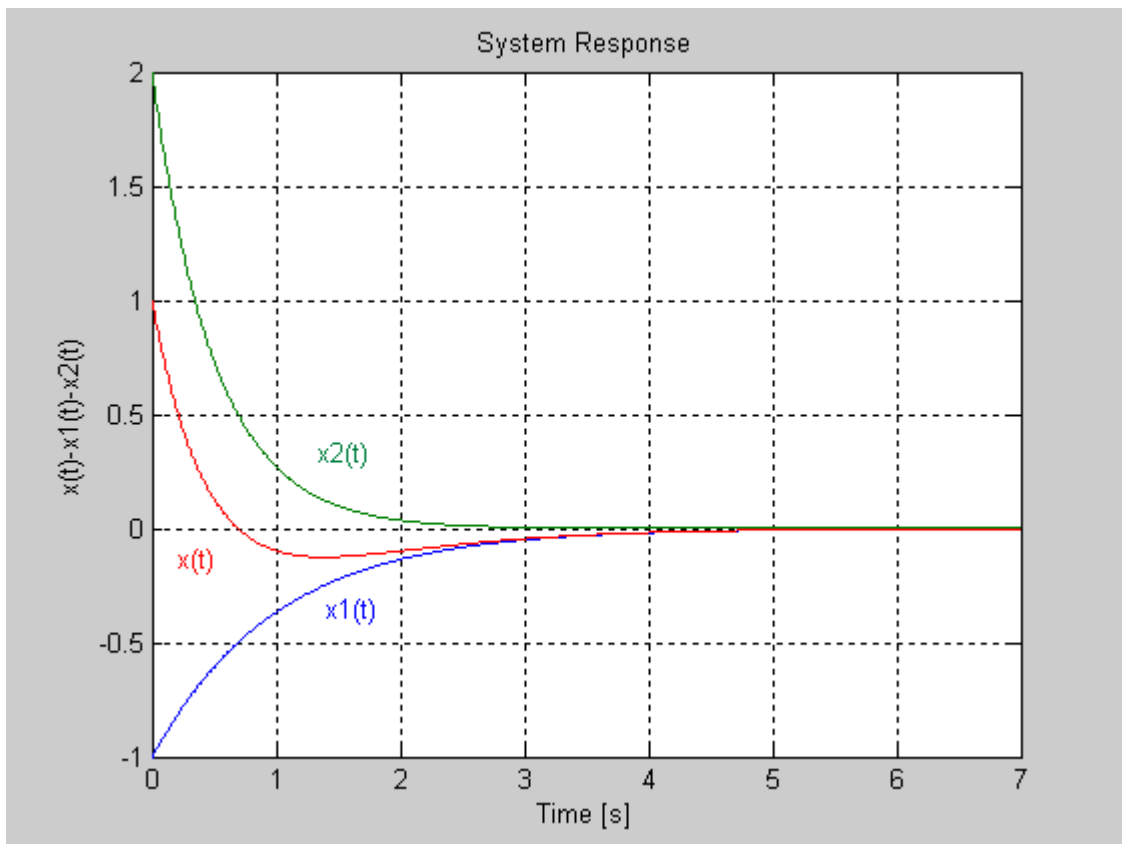


Figure 3.3. Case b) $A = -1$; $B = 2$; $\lambda_1 = -1$; $\lambda_2 = -2$

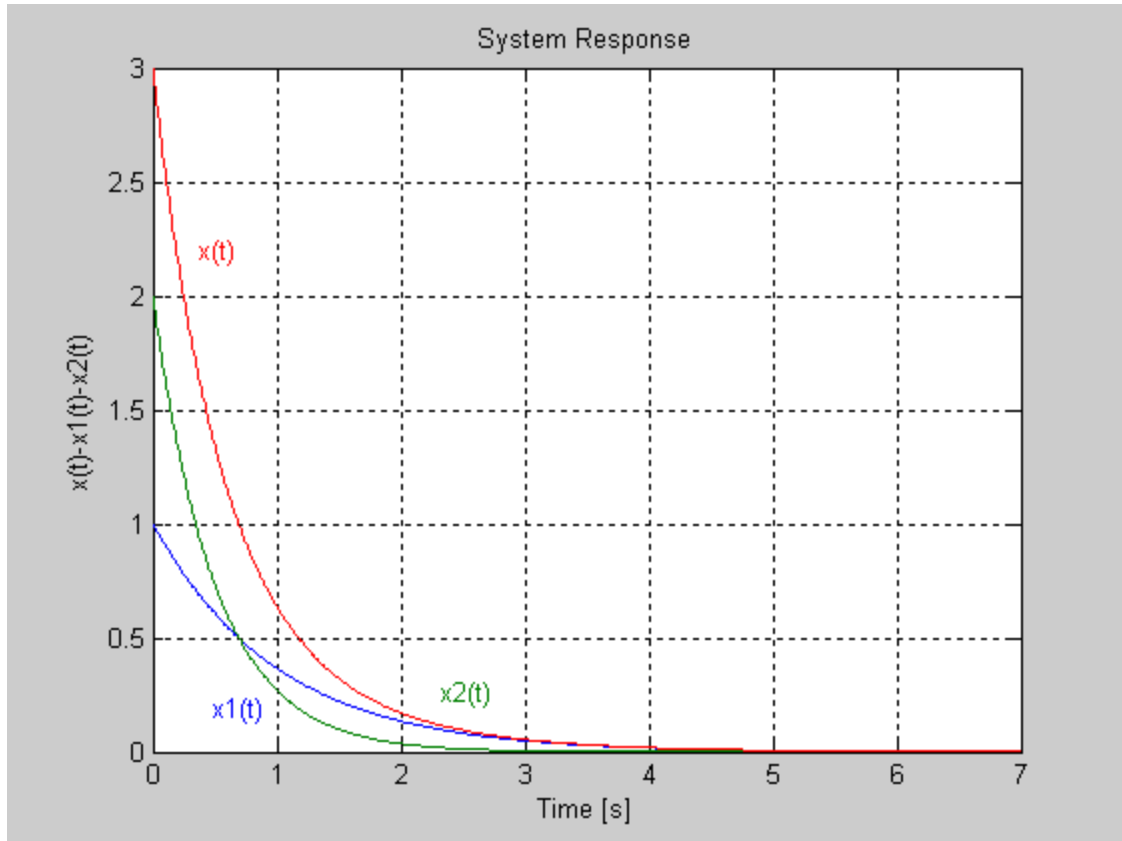


Figure 3.4. Case c) $A = 1$; $B = 2$; $\lambda_1 = -1$; $\lambda_2 = -2$

From Figures 3.2.-3.4. it is easily can be derived that the mechanical system behaves aperiodically having exponential responses.

B) $\beta^2 < 4 \cdot k \cdot m$. In this particular case solutions of the characteristic polynomial (3.5) are complex conjugates ones having negative real parts. It is well-known that solution of eq (3.4) can be derived as [2, 5]:

$$x(t) = C e^{-\frac{\beta}{2m}t} \cos\left(\sqrt{\frac{k}{m} - \left(\frac{\beta}{2m}\right)^2} t\right) + D e^{-\frac{\beta}{2m}t} \sin\left(\sqrt{\frac{k}{m} - \left(\frac{\beta}{2m}\right)^2} t\right). \quad (3.11)$$

In eq (3.11) C and D are unity constant parameters depending on initial conditions. Let the mechanical system has parameter as given below:

$$\frac{\beta}{m} = 1; \quad \frac{k}{m} = 2, \quad m = 1 \text{ kg} \quad (3.12)$$

Substituting equation (3.12) into equation (3.11) yields to the next formula:

$$x(t) = e^{-0,5 t} \cos(1,75 t) + e^{-0,5 t} \sin(1,75 t) \quad (3.13)$$

Results of the computer simulation of equation (3.13) can be seen in Figure 3.5.

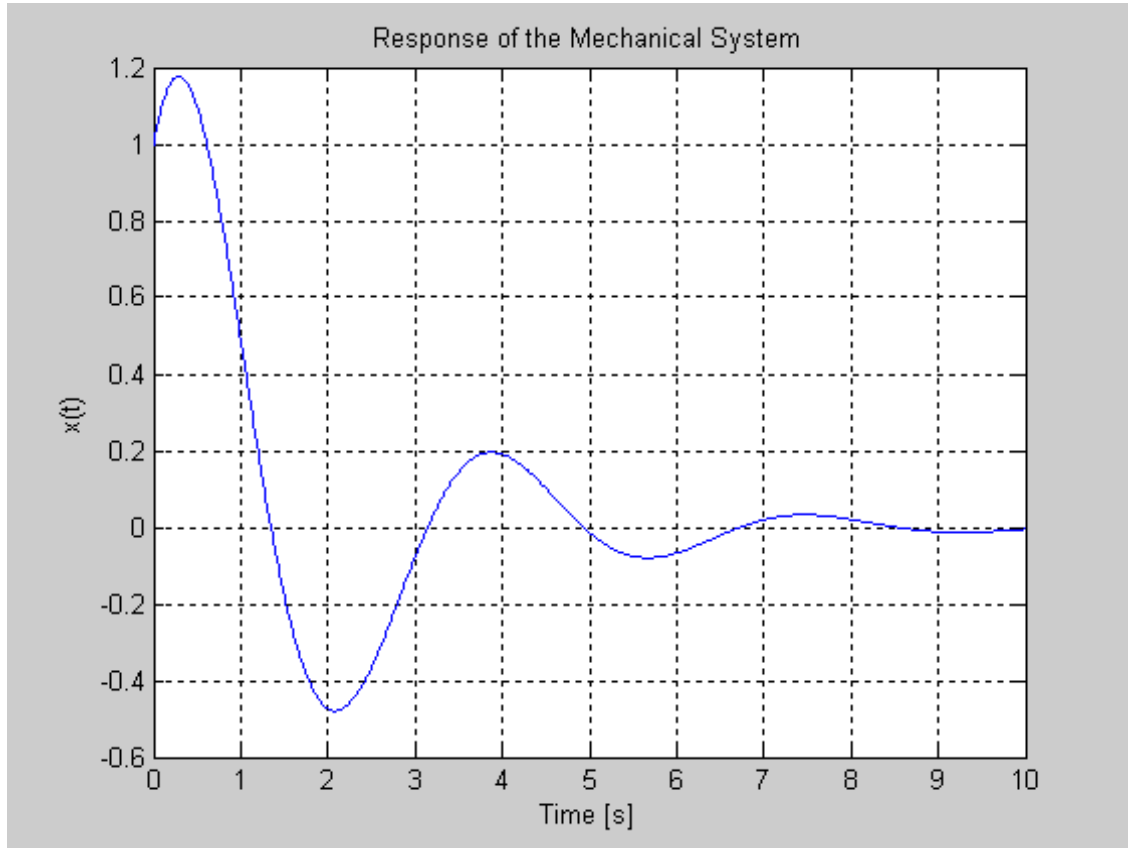


Figure 3.5. Dynamical System Response ($C=1$, $D=1$)

3.2. MODELLING OF THE “MASS-SPRING” MECHANICAL SYSTEM CONSTRAINED TO SINUSOIDAL INPUT SIGNAL

The ‘mass-spring’ mechanical system can be seen in Figure 3.6, where l is the spring length in the steady-state position; x is the increase of the spring length, m is the mass of body. For undamped mechanical system equation of motion can be derived as follows [2, 5]:

$$m \frac{d^2 x}{dt^2} + kx = a_o \sin \omega t \quad (3.14)$$

From Figure 3.6. coordinate of the mass measured from its basic level easily can be determined as:

$$a_o \sin \omega t + l + x \quad (3.15)$$

Using Newton’s Second Law dynamic equation (3.14) can be rewritten as:

$$m \frac{d^2}{dt^2} (a_o \sin \omega t + l + x) + kx = 0, \quad (3.16)$$

or in other manner:

$$m \frac{d^2 x}{dt^2} + kx = ma_o \omega^2 \sin \omega t = F_o \sin \omega t \quad (3.17)$$

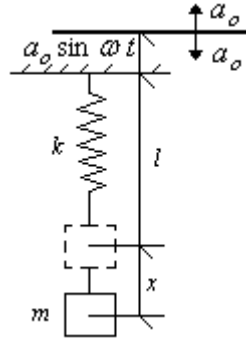


Figure 3.6. The “mass-spring” system.

Solution of the dynamical equation (3.14) can be derived as sum of the solution of the homogeneous equation of the linear system (3.14), and a particular solution of the inhomogeneous linear equation (3.14). Let find particular solution in the form of the next formula:

$$x = C \sin \omega t. \quad (3.18)$$

Substituting equation (3.18) into equation (3.17) results in

$$-mC\omega^2 + kC = F_o. \quad (3.19)$$

From equation (3.19) we have

$$C = \frac{F_o}{k - m\omega^2}. \quad (3.20)$$

Let $\omega_o = \sqrt{\frac{k}{m}}$ denote the resonance peak frequency of the mechanical system being investigated.

Thus, particular solution (3.18) can be rewritten as:

$$x = \frac{F_o}{m} \frac{\sin \omega t}{\omega_o^2 - \omega^2} = \frac{F_o}{k} \frac{\sin \omega t}{1 - \frac{\omega^2}{\omega_o^2}} \quad (3.21)$$

Solution of the dynamical equation can be found as

$$x = A \cos \omega_o t + B \sin \omega_o t + \frac{F_o}{m} \frac{\sin \omega t}{\omega_o^2 - \omega^2}, \quad (3.22)$$

where constants A , and B can be found using initial conditions. Let for $t = 0$ initial conditions are as follows:

$$x(0) = 0; \quad \left. \frac{dx}{dt} \right|_{t=0} = v_o = 1. \quad (3.23)$$

Finally, resulting equation of (3.22) can be derived as [2, 5]:

$$x = v_o \frac{\sin \omega_o t}{\omega_o} + \frac{F_o}{m} \frac{\sin \omega t}{(\omega_o^2 - \omega^2)\omega_o} (\omega_o \sin \omega t - \omega \sin \omega_o t) \quad (3.24)$$

Dynamical system defined by equation (3.24) was constrained to computer simulation. Results can be seen in Figure 3.7.

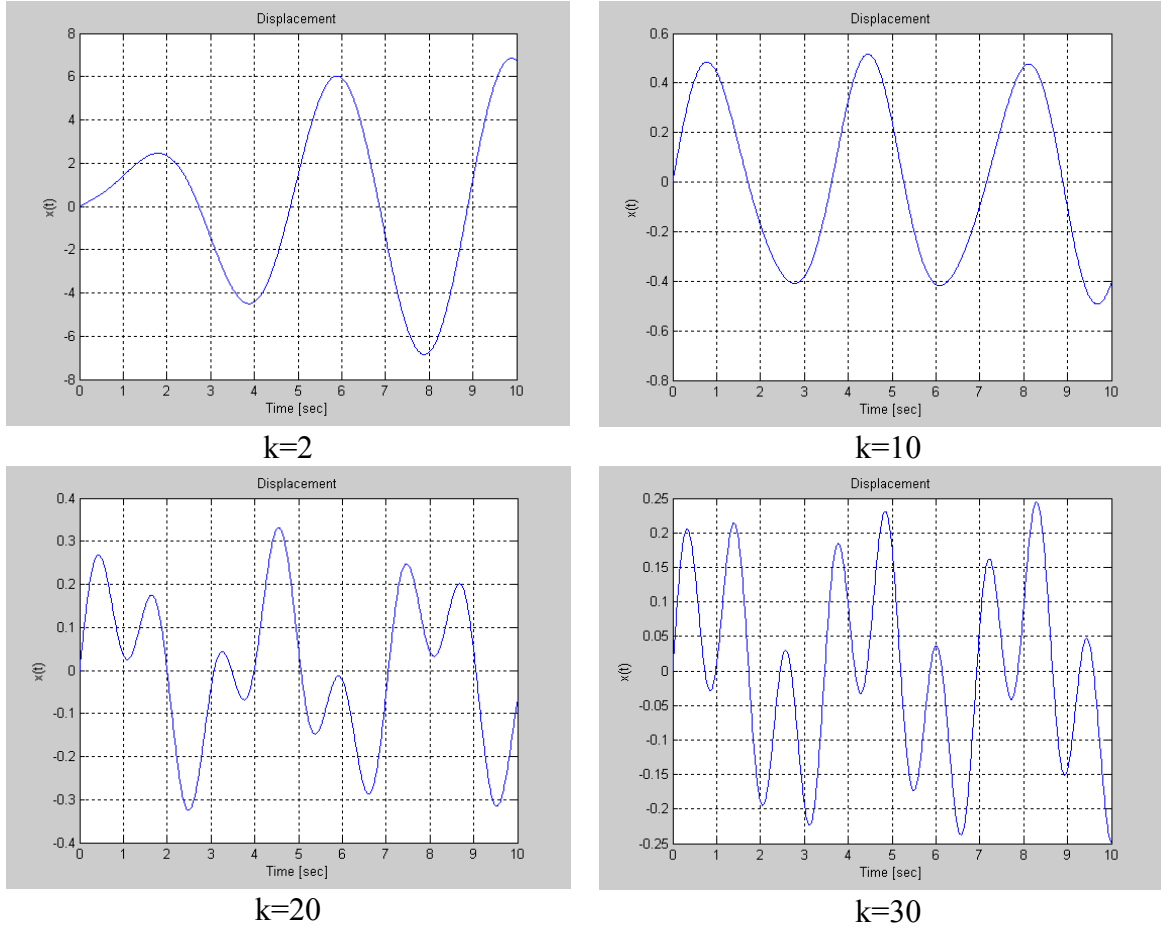


Figure 3.7. Mass-spring system displacement

For particular case of $\omega = \omega_o$ particular solution of (3.21) does not exist, and instead of we try to find this solution in the next form:

$$x = C t \cos \omega t \quad (3.25)$$

Substituting eq (3.25) into equation (3.14) constant C can be derived as

$$-2Cm\omega_o \sin \omega_o t - Cmt \omega_o^2 \cos \omega_o t + kCt \cos \omega_o t = F_o \sin \omega_o t \quad (3.26)$$

Suppose that $m\omega_o^2 = k$, equation (3.26) can be simplified to that of

$$C = -\frac{F_o}{2m\omega_o} \quad (3.27)$$

Thus, final form of the solution of equation (3.14) can be derived as:

$$x = A \cos \omega_o t + B \sin \omega_o t - \frac{F_o}{2m\omega_o} t \cos \omega_o t \quad (3.28)$$

The ‘spring-mass’ system is often supplemented with viscous damper, i.e. equation of motion (3.14) can be re-written as follows:

$$m \frac{d^2 x}{dt^2} + \beta \frac{dx}{dt} + kx = F_o \sin \omega t. \quad (3.19)$$

Let find particular solution of the inhomogeneous equation of (3.19) in the following manner:

$$x = a \sin \omega t + b \cos \omega t . \quad (3.20)$$

Constants a and b can be found with substitution of eq (3.20) into (3.19), and it yields:

$$(k - m\omega^2)a - \beta\omega b = F_0 , \quad (3.21)$$

$$(k - m\omega^2)b - \beta\omega a = 0 . \quad (3.22)$$

Solving system of equations (3.21), and (3.22) for coefficients a and b , and substituting them into equation (3.20) gives the following formula:

$$x = F_0 \frac{(k - m\omega^2)}{(k - m\omega^2)^2 + \beta^2\omega^2} \sin \omega t - F_0 \frac{\beta}{(k - m\omega^2)^2 + \beta^2\omega^2} \omega \cos \omega t . \quad (3.23)$$

It is well-known that final solution of equation (3.1) can be derived as sum of equations (3.23), and (3.4). From (3.4) it evident that (3.4) part is goes to zero while time goes to infinity, i.e. behavior of the dynamical system determined by eq (3.23).

IV. MATHEMATICAL MODELS OF THE STOCHASTIC CONTINUOUS ATMOSPHERIC DISTURBANCES

There are two powerful mathematical models of the continuous gust representations. The first is, the so-called von Kármán spectrum, which is better fit registrations of the turbulent air records. The von Kármán power spectral density (PSD) function is given below as follows [1, 6, 10, 11]:

$$\Phi_{\text{Kármán}}(\Omega) = \frac{\sigma^2 L}{\pi} \frac{1 + \frac{8}{3}(1,339L\Omega)^2}{(1 + 1,339L^2\Omega^2)^{11/6}} , \quad (4.1)$$

where L [m] is the gust wavelength, $\Omega = \omega U_0^{-1}$ [rad/m] is spatial frequency, ω [rad/s] is the observed angular frequency, and finally, σ [m/s] *r.m.s.* gust velocity.

The second one, the more favored PSD function is the Dryden PSD function, which can be programmed more easily then the von Kármán-model. If there is no structural analysis is performed the use of Dryden PSD function is permissible. The Dryden PSD function can be defined as given below [1, 6, 10, 11, 14]:

$$\Phi_{\text{Dryden}}(\Omega) = \frac{\sigma^2 L}{\pi} \frac{1 + 3L^2\Omega^2}{(1 + L^2\Omega^2)^2} . \quad (4.2)$$

Having goal to analyze hypothetical aircraft mathematical models with no interest in investigation of the structural behavior and supposing aircraft to be rigid one, the simplest mathematical form of the PSD function defined by equation of (4.2) we will use in this article. Regarding basic references of [6, 10, 11, 14] one can define PSD functions of the component speed of the turbulent air along body axis system of the aircraft, i.e.:

$$\Phi_{u_g}(\Omega) = \frac{2\sigma_u^2 L_u}{\pi} \frac{1}{1 + (L_u\Omega)^2} \quad (4.3)$$

$$\Phi_{v_g}(\Omega) = \frac{\sigma_v^2 L_v}{\pi} \frac{(1 + 3(L_v\Omega)^2)}{[1 + (L_v\Omega)^2]^2} \quad (4.4)$$

$$\Phi_{w_g}(\Omega) = \frac{\sigma_w^2 L_w}{\pi} \frac{(1 + 3(L_w \Omega)^2)}{[1 + (L_w \Omega)^2]^2} \quad (4.5)$$

where $\sigma_i^2 = \int_0^\infty \Phi_i(\Omega) d\Omega_i \big|_{i=u,v, \text{ or } w}$. Since $\omega = U_o \Omega$ formulas of (4.3)–(4.5) may be rewritten as follows:

$$\Phi_{u_g}(\omega) = \frac{2\sigma_u^2 L_u}{U_o \pi} \frac{1}{\{1 + (L_u / U_o)^2 \omega^2\}}, \quad (4.6)$$

$$\Phi_{v_g}(\omega) = \frac{\sigma_v^2 L_v}{U_o \pi} \frac{(1 + 3(L_v / U_o)^2 \omega^2)}{\{1 + (L_v / U_o)^2 \omega^2\}^2}, \quad (4.7)$$

$$\Phi_{w_g}(\omega) = \frac{\sigma_w^2 L_w}{U_o \pi} \frac{(1 + 3(L_w / U_o)^2 \omega^2)}{\{1 + (L_w / U_o)^2 \omega^2\}^2}. \quad (4.8)$$

For generating random signals with the required intensity, scale length, and PSD functions for given speed and height of the flight, a hypothetical wide-band noise generator with PSD function of $\Phi_N(\omega)$ must be used to provide signal with the linear filter, chosen such that it has an appropriate frequency response so that the output signal from the linear filter will have a PSD function of $\Phi_i(\omega)$ (see Figure 4.1.) [6]:

$$\Phi_i(\omega) = \left| G_i(s) \right|_{s=j\omega}^2 \Phi_N(\omega) = G_i(s) G_i(-s) \big|_{s=j\omega} \Phi_N(\omega). \quad (4.9)$$

If the white noise source is chosen so that its power spectrum is similar to that of called ‘white’ noise one can write that

$$\Phi_N(\omega) = 1. \quad (4.10)$$

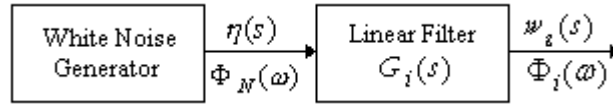


Figure 4.1. Block Diagram for Generating Stochastic Signals.

Substituting equation (4.10) into equation of (4.9) result the following formula

$$\Phi_i(\omega) = \left| G_i(s) \right|_{s=j\omega}^2 \Phi_N(\omega) = G_i(s) G_i(-s) \big|_{s=j\omega}. \quad (4.11)$$

The linear filter transfer functions of $G_i(s)$ are given in [6] to be:

$$G_{u_g}(s) = \frac{\sqrt{K_u}}{s + \lambda_u}, \quad G_{v_g}(s) = \sqrt{K_v} \frac{s + \beta_v}{(s + \lambda_v)^2}, \quad G_{w_g}(s) = \sqrt{K_w} \frac{s + \beta_w}{(s + \lambda_w)^2}, \quad (4.12)$$

where:

$$K_u = \frac{2U_o \sigma_u^2}{L_u \pi}, \quad K_v = \frac{3U_o \sigma_v^2}{L_v \pi}, \quad K_w = \frac{3U_o \sigma_w^2}{L_w \pi}, \quad (4.13)$$

$$\beta_v = \frac{U_o}{\sqrt{3}L_v}, \quad \beta_w = \frac{U_o}{\sqrt{3}L_w}, \quad (4.14)$$

$$\lambda_u = \frac{U_o}{L_u}, \quad \lambda_v = \frac{U_o}{L_v}, \quad \lambda_w = \frac{U_o}{L_w}. \quad (4.15)$$

It is easily can be derived that substitution equations (4.12)–(4.15) into equation (4.9) results in the PSD functions of the Dryden-models's PSD-functions of (4.6)–(4.8). If the air

turbulence model is used for analysis of its effects on flight of the small UAV aircraft let the initial parameters be as they are given below:

$$H = 100 \text{ m} \cong 328,084 \text{ feet}; \quad U_0 = 25 \text{ m/s} = 90 \text{ km/h}^2. \quad (4.16)$$

From equations (4.13)–(4.15) it is evident that for derivation of transfer functions of the linear filters defined by equation (4.12) it is necessary to know turbulence scale of L_i , and turbulence intensity of σ_i , measured along appropriate axis of the given coordinate system. Let us consider NASA-parameters taken from [6, 10] to be as follows:

$$\text{■ along longitudinal (OX) axis: } 3,4 \text{ m/s} \leq \sigma_u \leq 0,85 \text{ m/s} \quad (4.17)$$

$$\text{■ along lateral (OY) axis: } 2,8 \text{ m/s} \leq \sigma_v \leq 0,7 \text{ m/s}, \quad (4.18)$$

$$\text{■ along vertical (OZ) axis: } 1,8 \text{ m/s} \leq \sigma_w \leq 0,45 \text{ m/s}. \quad (4.19)$$

For extreme weather conditions (thunderstorm) MCLEAN [6] suggests turbulence intensities as they given below:

$$\sigma_u = \sigma_v = \sigma_w = 7 \text{ m/s}. \quad (4.20)$$

Turbulence integral scale lengths L_i of the low altitude turbulence models for $10 \text{ feet} \leq h \leq 1000 \text{ feet}$ can be derived using following formulas [6, 10]:

$$L_u = 2L_v = \frac{b}{(0,177 + 0,000823 \cdot h)^{1,2}}, \quad L_w = 0,5 b. \quad (4.21)$$

Regarding MCLEAN, for extreme weather conditions (thunderstorm) one can apply following integral scale lengths given in [6]:

$$L_u = L_v = L_w = 580 \text{ m}. \quad (4.22)$$

Constant speed components of the turbulent air are given in military standards of [4, 7] as function of theirs exceedance. For the low altitude random turbulence models intensity of the turbulence, σ_w can be measured as [6, 11, 14]:

$$\sigma_w = 0,1 u_{20}, \quad (4.23)$$

where u_{20} is constant longitudinal component speed of the turbulent air measured at the altitude of $h = 20 \text{ feet}$. Using equations of (4.21)–(4.22) integral scale lengths of the air turbulence were found and they are summarized in Table 1.

Table 1. Integral scale lengths at altitude of $H = 100 \text{ m} \cong 328,084 \text{ feet}$.

Scale length, [m]	Nominal (Nom)	Extreme (Thunderstorm)
L_u	862,185497 feet $\cong$ 262,7941311 m	580
$L_v = 0,5 L_u$	431,0927485 feet $\cong$ 131,3970655 m	580
L_w	50	580

Using equations of (4.17)–(4.20) turbulence intensities were found and they are summarized in Table 2.

² 1 foot $\cong$ 0,3048 m — 1 m $\cong$ 3,28084 feet

Table 2. Turbulence intensities.

Turbulence intensities	NASA-Min (Min)	NASA-Max (Max)	Extreme (Thunderstorm)
σ_u , [m/s]	0,85	3,4	7
σ_v , [m/s]	0,7	2,7	7
σ_w , [m/s]	0,45	1,8	7

Constant longitudinal component speed of the turbulent air, called u_{20} , were found using military standard of [10], and using equations of (4.21)–(4.22). Constant speed of u_{20} are summarized in Table 3.

Table 3. Constant speed of u_{20} .

Turbulent Air Characteristics	NASA-Min (Min)	NASA-Max (Max)	Extreme (Thunderstorm)
$\sigma_w = 0,1 u_{20}$, [m/s]	0,45	1,8	7
u_{20} , [m/s] – [km/h]	4,5 – 16,2	18 – 64,8	70 – 252

Linear transfer functions defined by equations (4.12) having parameters given by equations of (4.13)–(4.15), and satisfying conditions derived by equations (4.16)–(4.24), and considering weather conditions given by Table 1., and Table 2, can be determined, and they can be found in the following tables given below [11, 14]:

Table 3. Parameters of the linear filters providing longitudinal speed component of the air turbulence, $u_g(t)$.

Filter Parameters		
Weather Conditions	$K_u = \frac{2\sigma_u^2 U_o}{L_u \pi} \left[\frac{m^2}{s^3} \right]$	$\lambda_u = \frac{U_o}{L_u} \left[s^{-1} \right]$
NASA-Min	0,043756496	0,095131547
NASA-Max	0,700103937	0,095131547
Extreme (Thunderstorm)	1,344584864	0,043103448

Table 4. Parameters of the linear filters providing lateral speed component of the air turbulence, $v_g(t)$.

Filter Parameters			
Weather Conditions	$K_v = \frac{3\sigma_v^2 U_o}{L_v \pi} \left[\frac{m^2}{s^3} \right]$	$\beta_v = \frac{U_o}{\sqrt{3}L_v} \left[s^{-1} \right]$	$\lambda_v = \frac{U_o}{L_v} \left[s^{-1} \right]$
NASA-Min	0,089027057	0,109848449	0,190263095
NASA-Max	1,324504595	0,109848449	0,190263095
Extreme (Thunderstorm)	8,902705783	0,024885787	0,043103448

Table 5. Parameters of the linear filters providing vertical speed component of the air turbulence, $w_g(t)$.

Filter Parameters			
Weather Conditions	$K_w = \frac{3\sigma_w^2 U_o}{L_w \pi} \left[\frac{m^2}{s^3} \right]$	$\beta_w = \frac{U_o}{\sqrt{3}L_w} \left[s^{-1} \right]$	$\lambda_w = \frac{U_o}{L_w} \left[s^{-1} \right]$
NASA-Min	0,096686627	0,288675134	0,5
NASA-Max	1,546986047	0,288675134	0,5
Extreme (Thunderstorm)	2,016877296	0,024885787	0,043103448

Using parameters of Table 3, Table 4, Table 5, transfer functions of the linear filters defined by equation (4.12) can be derived as follows [11, 14]:

$$G_{u_g}^{Min}(s) = \frac{0,20918}{s + 0,09513}, \quad (4.24-1)$$

$$G_{u_g}^{Max}(s) = \frac{0,83672}{s + 0,09513}, \quad (4.24-2)$$

$$G_{u_g}^{Extr}(s) = \frac{1,15956}{s + 0,04310}, \quad (4.24-3)$$

$$G_{v_g}^{Min}(s) = 0,29837 \frac{s + 0,10984}{s^2 + 0,38052s + 0,03620} \quad (4.25-1)$$

$$G_{v_g}^{Max}(s) = 1,15087 \frac{s + 0,10984}{s^2 + 0,38052s + 0,03620}, \quad (4.25-2)$$

$$G_{v_g}^{Extr}(s) = 2,98374 \frac{s + 0,02488}{s^2 + 0,08620s + 0,00186} \quad (4.25-3)$$

$$G_{w_g}^{Min}(s) = 0,31094 \frac{s + 0,28867}{s^2 + s + 0,25}, \quad (4.26-1)$$

$$G_{w_g}^{Max}(s) = 1,24377 \frac{s + 0,28867}{s^2 + s + 0,25} \quad (4.26-2)$$

$$G_{w_g}^{Extr}(s) = 1,42016 \frac{s + 0,02488}{s^2 + 0,08620s + 0,00185} \quad (4.26-3)$$

Using linear transfer function models of equations (4.24)–(4.26) it is easy to generate random time series with given statistical parameters, which can be applied both for identification, modeling, analysis and design purposes [6, 10, 11, 14].

4.1. RESULTS OF THE COMPUTER SIMULATION

Using principle derived by Figure 1., and using transfer functions of the linear filters defined for several weather conditions one can generate computer code for solution of this problem. In our preliminary study we have used MATLAB® R2009 [13]. Regarding mathematical models of the random air outlined in Chapter 4 all components of the speeds of the turbulent air measured along axes of the aircraft body-axis system, and they will be presented in the next sections.

4.1.1. RANDOM LONGITUDINAL SPEED COMPONENT OF THE TURBULENT AIR

The longitudinal speed component is very important from the point of view of the basic flight conditions, i.e. aircraft flight is limited with its minimum longitudinal speed of, say, $u_{\min}$. From Chapter 3 it is known that equilibrium speed of the hypothetical UAV aircraft is $u_o = 25 \text{ m/s}$. Result of the computer simulation can be seen in Figure 4.2.

From Figure 4.2, it is easily can be determined that in time domain of (50÷100) seconds, in other words, in the root of the turbulent zone, the mean value of the longitudinal speed is approximately, $u_{mean} \cong 4,2 \text{ m/s}$, which is 16,8 % of that of the equilibrium one. There is a question arising from analysis of the characteristics of the longitudinal speed component direction, i.e. it can be coinciding one to that of the mean direction of the flight, or it can oppose aircraft flight

In other words, longitudinal speed component of the turbulent air can be called for head-wind, or, tail wind. Going that way, longitudinal speed of the aircraft flying through atmospheric turbulence can be derived as follows:

$$\text{for "head-wind": } u_{head} = u_o - u_{mean} = 25 - 4,2 = 20,8 \text{ m/s} , \quad (4.27)$$

$$\text{for "tail wind": } u_{tail} = u_o + u_{mean} = 25 + 4,2 = 29,2 \text{ m/s} . \quad (4.28)$$

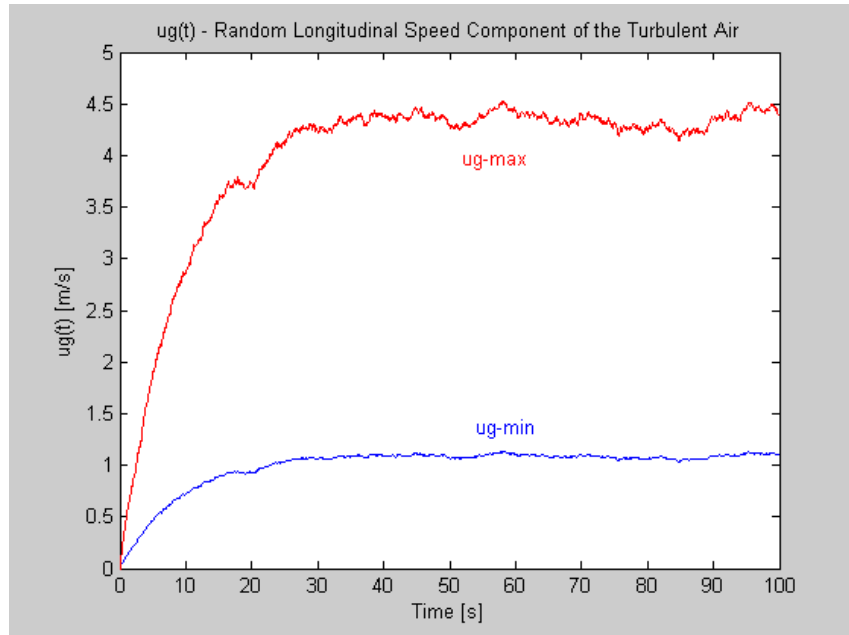


Figure 4.2. Longitudinal Speed Component of the Stochastic Air.

4.1.2. RANDOM LATERAL SPEED COMPONENT OF THE TURBULENT AIR.

Using the same manner as it was shown in previous section, computer code for random lateral speed component of the turbulent air was generated, and results of the computer simulation can be seen in Figure 4.3. From Figure 4.3. it is easily can be seen that in the time domain of about (50÷100) seconds, the mean values of the lateral speed are:

$$v_{\max} \cong 1,7 \text{ m/s}, v_{\min} \cong 0,5 \text{ m/s} . \quad (4.3)$$

If to suppose weather conditions having statistical parameters between weather conditions of NASA-Min, and NASA-Max, it can be supposed that mean value of the lateral speed is, approximately, of 1 m/s.

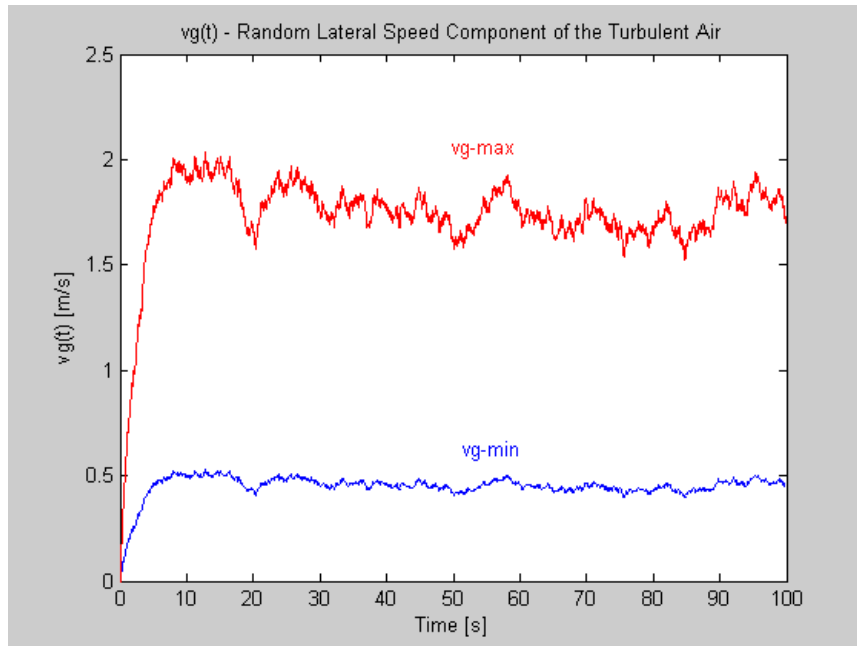


Figure 4.3. Lateral Speed Component of the Stochastic Air.

It means that during flight aircraft changes its lateral coordinate for about $\cong 4$ m in one second.

If to take into consideration the free-flight of the aircraft, or even if in normal flight aircraft “pilot” does not corrects the lateral coordinate, in 50 seconds time period, being investigated above, aircraft maintains distance of 1250 m, changing its lateral coordinate for 200 m. It is obvious, that there is a strong need to compensate lateral deviation measured from the flight direction.

4.1.3. RANDOM VERTICAL SPEED COMPONENT OF THE TURBULENT AIR.

Random vertical speed of the turbulent air is very important from many aspects of the altitude control of the aircraft, from the point of view of the modeling of the aeroelastic structural motion of the fuselage, and wings. There are many other reasons highlighting importance of the knowledge of the stochastic vertical speed of the atmospheric turbulences. Results of the computer simulation including NASA-Min, and NASA-Max weather conditions can be seen in Figure 4.4. From Figure 4.4. it is easily can be seen that in the time domain of about (50÷100) seconds, the mean values of the vertical speed are as follows:

$$w_{\max} \cong 0,7 \text{ m/s} , w_{\min} \cong 0,2 \text{ m/s} . \quad (4.4)$$

It to take mean value of the vertical random speed of the wind to be of 0,5 m/s, during flight aircraft changes its altitude for 1,8 m per second. For the free-flight of the aircraft, or even if in normal flight aircraft “pilot” does not corrects the height of the flight, in 50 seconds time period, being investigated above, aircraft maintains distance of 1250 m, changing its height of the flight for 90 m, to that of the initial of $H_o \cong 100 \text{ m}$. It means that having no control on aircraft altitude, in turbulent air aircraft nearly duplicates its height of the flight. It is obvious, that height of the flight must be controlled, and altitude must be kept at its constant value.

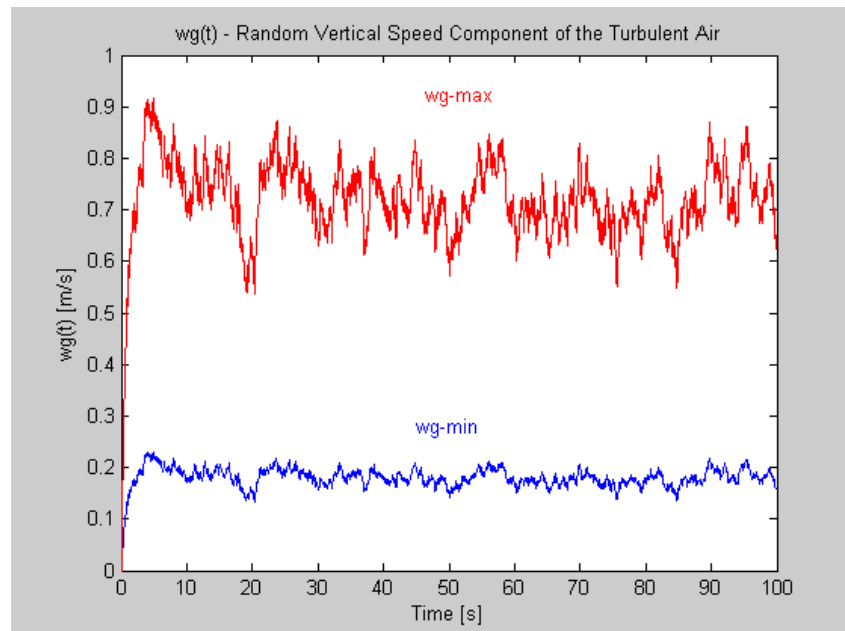


Figure 4.4. Vertical Speed Component of the Stochastic Air.

4.1.4. RESULTS OF THE COMPUTER SIMULATION OF THE ATMOSPHERIC TURBULENCES FOR THE "NASA-MIN" WEATHER CONDITIONS

Using results of the previous computer simulation, for "NASA-Min" weather conditions all appropriate time series of the longitudinal, lateral, and vertical components of the random air were plot in one, common coordinate system, and they can be seen in Figure 4.5.

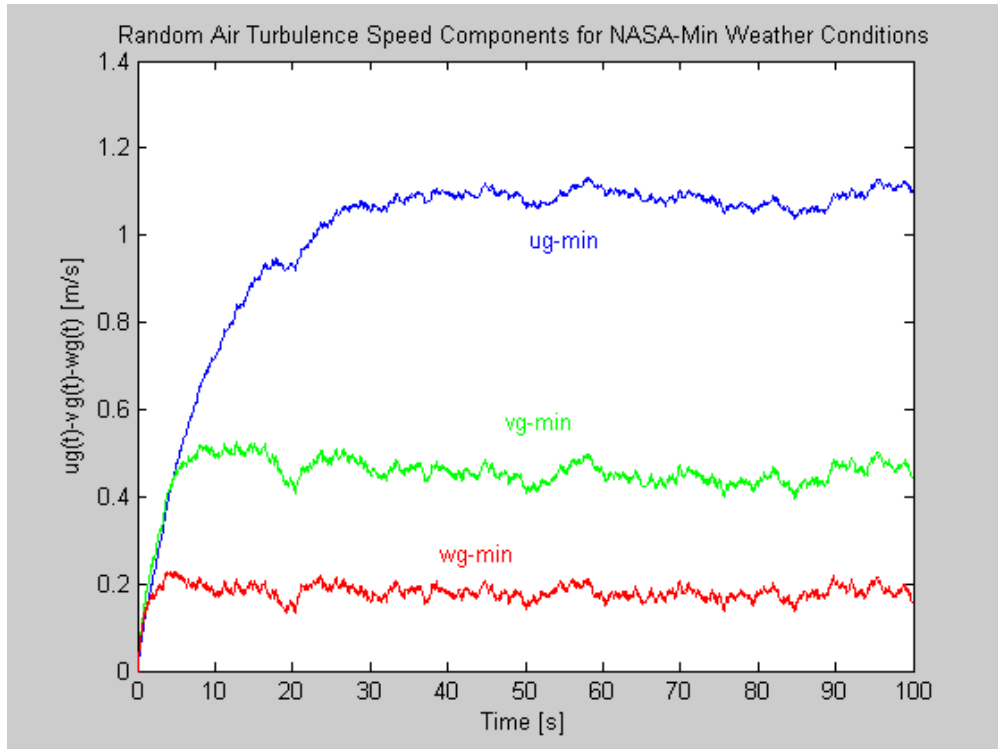


Figure 4.5. Results of the Computer Simulation for "NASA-Min" Weather Conditions.

4.1.5. RESULTS OF THE COMPUTER SIMULATION OF THE ATMOSPHERIC TURBULENCES FOR THE "NASA-MAX" WEATHER CONDITIONS

Using results of the computer simulation made before, for "NASA-Max" weather conditions all appropriate time series of the longitudinal, lateral, and vertical components of the random air were plot in one, common coordinate system, and they can be seen in Figure 4.6.

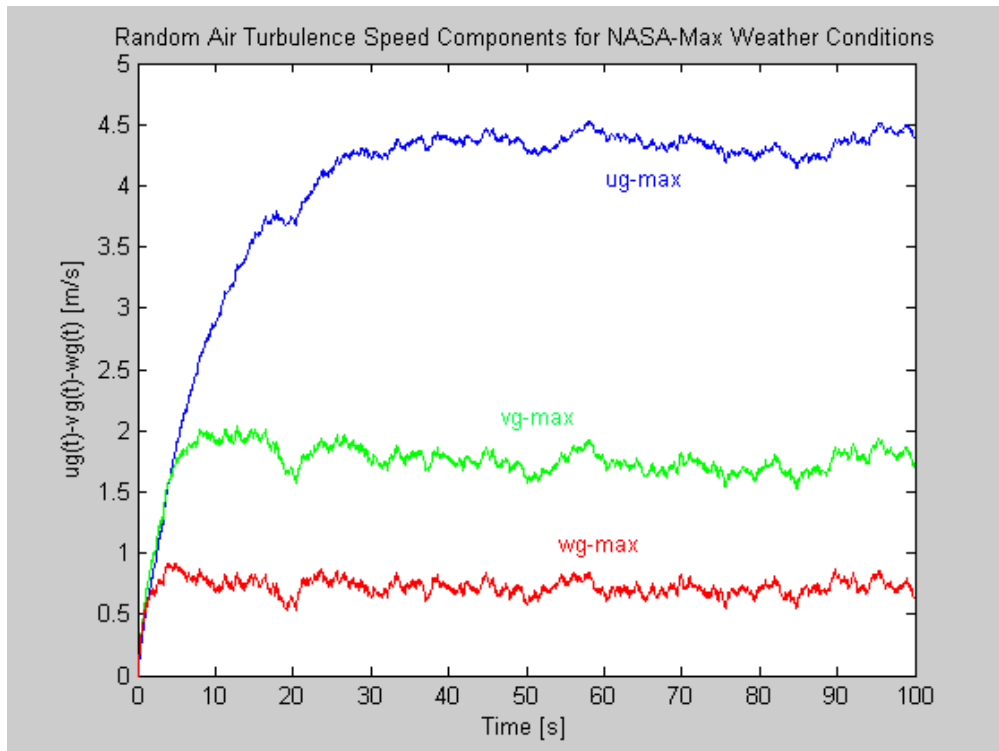


Figure 4.6. Results of the Computer Simulation for “NASA-Max” Weather Conditions.

From Figure 4.6. it is easily can be derived that longitudinal speed component, $u_g(t)$, of the atmospheric turbulence has largest mean value. It is evident that for head-wind weather conditions, there is exists a maximum value of the longitudinal random speed, $u_{g_{\max}}(t)$, which is allowed to avoid stalling of the aircraft.

4.1.6. RESULTS OF THE COMPUTER SIMULATION OF THE ATMOSPHERIC TURBULENCES FOR THE "EXTREME – THUNDERSTORM" WEATHER CONDITIONS

Result of these computer simulations are mainly hypothetical, however, it is necessary to know how extreme air masses are moving. These results are very important although from the point of view of the flight achieved beyond visual range for large distances, when there are big differences between weather conditions at arrival and departure airfields. Result of the computer simulation can be seen in Figure 4.6.

The most important result is that atmospheric turbulence has largest value in the mean of lateral component of the turbulent air. The other important statement coming form this analysis, that if to consider maximum value of the longitudinal head-wind to be of $u_{g\_head}(t) = 5 \text{ m/s}$, this maximum value is reached at about 5 seconds of the computer-aided simulation. It means that to avoid stalling of the aircraft it is necessary to compensate decrease of the longitudinal speed of the aircraft increasing throttle, or it is necessary to maintain maneuver to keep given flight parameters in the defined flight envelope of the given type of the aircraft.

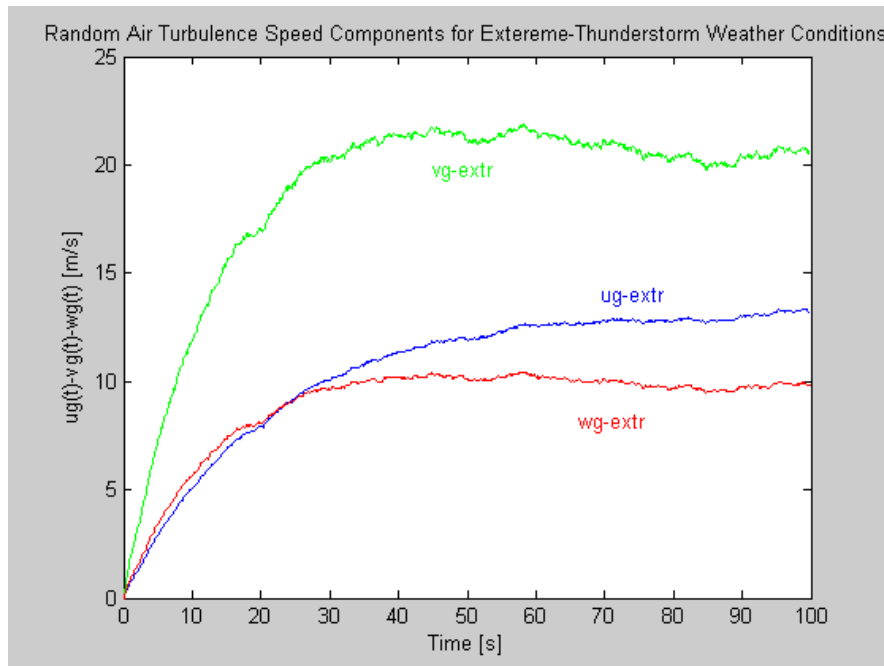


Figure 4.6. Results of the Computer Simulation for “Extreme” Weather Conditions.

The most important result is that atmospheric turbulence has largest value in the mean of lateral component of the turbulent air. The other important statement coming from this analysis, that if to consider maximum value of the longitudinal head-wind to be of $u_{g\_head}(t) = 5 \text{ m/s}$, this maximum value is reached at about 5 seconds of the computer-aided simulation. It means that to avoid stalling of the aircraft it is necessary to compensate decrease of the longitudinal speed of the aircraft increasing throttle, or it is necessary to maintain maneuver to keep given flight parameters in the defined flight envelope of the given type of the aircraft.

V. SUMMARY

Mathematical models are widely used during preliminary analysis, identification, and design of the automatic control systems. They can be both deterministic and random ones, regarding their time domain behavior. They support system description whether it is continuous, or discrete. Modeling of dynamical systems is supported by many computer packages e.g. MATLAB[®], SIMULINK[®], and their toolboxes.

OPUS CITATUM

- [1] Korn, G. A. *Random-Process Simulation and Measurements*, McGraw-Hill Book Company, New York – Toronto – London – Sydney, 1966.
- [2] Kármán, T. – Biot, A. M. *Matematikai módszerek műszaki feladatok megoldására*, Műszaki Könyvkiadó, Budapest, 1967.
- [3] Korn, G. A. – Korn, T. M. *Matematikai módszerek műszakiaknak*, Műszaki Könyvkiadó, Budapest, 1975.

- [4] Kuo, B. C. *Automatic Control Systems*, Prentice-Hall, Englewood Cliffs, New Jersey, 1982.
- [5] Ogata, K. *Modern Control Engineering*, Prentice-Hall International Inc., Englewood Cliffs, New Jersey, 1990.
- [6] McLean, D. *Automatic Flight Control Systems*, Prentice-Hall, Int., New York – London – Toronto – Sydney – Tokyo – Singapore, 1990.
- [7] Dorf, R. C. – Bishop, R. H. *Modern Control Systems*, Prentice Hall International, Upper Saddle River, New Jersey, 2001.
- [8] Stefani, R. T. – Shahian, B. – Savant Jr., C. J. – Hostetter, G. H. *Design of Feedback Control Systems*, Oxford University Press, New York-Oxford, 2002.
- [9] Nise, N. S. *Control Systems Engineering*, John Wiley & Sons, Inc., 2004.
- [10] MIL-STD-1797A, Notice 3, *Flying Qualities of Piloted Aircraft*, Department of Defense, Interface Standard, 2004.
- [11] Szabolcsi, R. *Mathematical Models for Gust Modeling Applied in Automatic Flight Control Systems' Design*, CD-ROM Proceedings of the “5th International Conference in the Field of Military Sciences 2007”, 13-14 November 2007, Budapest, Hungary.
- [12] Pokorádi, L. *Jelek és rendszerek modellezése*, Campus Kiadó, Debrecen, 2008.
- [13] MATLAB[®] 7 *Getting Started Guide*, The MathWorks[™], Inc., 2009.
- [14] Szabolcsi, R. *Stochastic Noises Affecting Dynamic Performances of the Automatic Flight Control Systems*, Review of the Air Force Academy, No1/2009, pp(23-30), ISSN 1842-9238, Brasov, Romania.

Szénási Sándor

szenasi.sandor@nik.bmf.hu

GPGPU – ÚJ ESZKÖZÖK AZ INFORMÁCIÓBIZTONSÁG TERÜLETÉN

Absztrakt

A processzor architektúrák elmúlt években bekövetkező fejlődésének legfőbb iránya a feldolgozóegységek számának növelése, ez a többmagos processzorok megjelenésén túlmenően egészen újszerű architektúrák kialakulását is jelenti, mint például az általános célú számításokra használható grafikus kártyák. Ezek az eszközök kiemelkedő ár/teljesítmény aránnyal rendelkeznek, az általuk kínált elméleti csúcsteljesítmény azonban csak megfelelően tervezett és implementált algoritmusok használata esetén aknázható ki hatékonyan. A gyakorlatban felmerülő problémák esetében ez a teljesítmény így gyakran nem, vagy csak részben használható ki, ennek vizsgálatát mutatja be ez a tanulmány.

In the last few years, the general trend in processor development has been to increase the number of processing units. This means not only to introduce multi-core processors, but also to develop patent architectures like GPGPUs (General Purpose computation on Graphics Processing Units). The cost/benefit ratio of these devices is outstanding, but their peak performance can be achieved by only properly designed and implemented algorithms. So in practice this performance usually not (or not fully) achievable, this is the main topic of this article.

Kulcsszavak: GPGPU, CUDA, párhuzamos algoritmusok, teljesítmény mérések ~ GPGPU, CUDA, parallel algorithms, performance benchmarks

PÁRHUZAMOSÍTÁS KIKÉNYYSZERÍTÉSE

Az informatikában megszokottá vált, hogy a különböző hardver eszközök, köztük a processzorok teljesítménye évről-évre folyamatosan növekszik, miként ezt a közkezdvelt Moore-törvény is kimondja. Ez a nagyon egyszerű jóslat hosszú éveken keresztül jónak bizonyult, napjainkban azonban egy érdekes változásnak lehetünk tanúi. A processzorgyártók néhány évvel ezelőtt kénytelenek voltak szembesülni azzal, hogy nem tudják az órajel-frekvenciákat az eredetileg elképzelt ütem szerint növelni, ami miatt új utakat kellett keresni a további fejlesztések számára. Ezek közül az utóbbi években a legszembetűnőbb a többmagos processzorok megjelenése, amelyek az évenkénti teljesítménynövekedést egy meglehetősen

kézenfekvő ötlettel biztosítják: egy processzoron belül bizonyos egységeket egyszerűen megdupláznak, amelynek segítségével az eszköz elméleti számítási kapacitása is duplázódik.

Ezzel a piac által elvárt szükséges növekedés tehát igazolható, és természetesen nincs szó csalásról, ez a teljesítménynövekedés valóban elérhető és kézzelfogható. Azonban a gyakorlati felhasználás tekintetében már fontos megszorításokkal kell szembenéznünk, ha hozzá akarunk férni a megnövekedett számítási kapacitáshoz. Hagyományosan, ha csak a legnagyobb értékesítési területet, a személyi számítógépek piacát tekintjük (ahol a fejlesztők számára elengedhetetlen, hogy minden újonnan megjelenő eszköz kompatibilis legyen elődeivel), a processzorok teljesítményének növelése azonnali, közvetlen gyorsulást jelentett az alkalmazások futtatása során. Egy kétszer nagyobb teljesítményű processzor telepítése, az alkalmazások bármiféle módosítása nélkül is körülbelül kétszer rövidebb futási időt eredményezett. A jelenlegi trend esetén azonban ez már nem ennyire magától értetődő, egy manapság elérhető nagyteljesítményű kettő vagy négymagos processzoron futtatva a hagyományos alkalmazásokat valószínűleg nem érhető már el azonnali kétszeres vagy négyszeres gyorsulás. Sőt, annak is meglehetősen nagy az esélye, hogy a processzor magok számának növelésével a program futási ideje szinte egyáltalán nem változik (leszámítva némi közvetett gyorsulást, amely annak köszönhető, hogy az egyszerre több feladatot végrehajtó operációs rendszer ilyenkor egy teljes processzormagot szentelhet az említett feladatnak).

A processzorgyártók tehát ezzel a lépéssel a szoftverfejlesztőkre hárítottak meglehetősen sok megoldandó problémát, amennyiben a nagyobb számítási kapacitást ki akarják használni. Egyrészt a programozók hagyományosan nem párhuzamos algoritmusokat fejlesztettek/fejlesztnek. Mivel éveken keresztül általánosnak tekinthető volt az egy darab vezérlő egység használata (természetesen régen is léteztek többprocesszoros rendszerek, de ezek szerepe jóval kevésbé volt hangsúlyos, mint napjainkban), ezért a programozók is erre optimalizálták algoritmusait. Ezzel az alkalmazásfejlesztés egyszerűbb, gyorsabb, áttekinthetőbb lett. Napjainkra azonban látható, hogy a processzorok gyorsítása már főleg a párhuzamosítás irányában képzelhető csak el, így ennek megfelelően a programokat is adaptálni kell ehhez az új környezethez, ehhez egyelőre még hiányzik a szakértelem és tapasztalat.

Ennél nagyobb problémát jelent az, hogy vannak feladatok, amelyek jellegükből adódóan nem párhuzamosíthatók. Egy hosszabb számítási sorozat, amelynek minden művelete függ az előző műveletek (rész)eredményeitől, csak egymást követő lépések sorozataként számítható ki, ami mindösszesen egy végrehajtóegységet igényel. Hiába van több, az ezek adta lehetőség nem használható ki. Emiatt az egyszerű programozási technikák megújításán túl szükség van egy sokkal nagyobb paradigmaváltásra is, az eddig ismert és gyakorlatban jól alkalmazott szekvenciális algoritmusok módosítására, illetve új, párhuzamosíthatóbb eljárások keresésére.

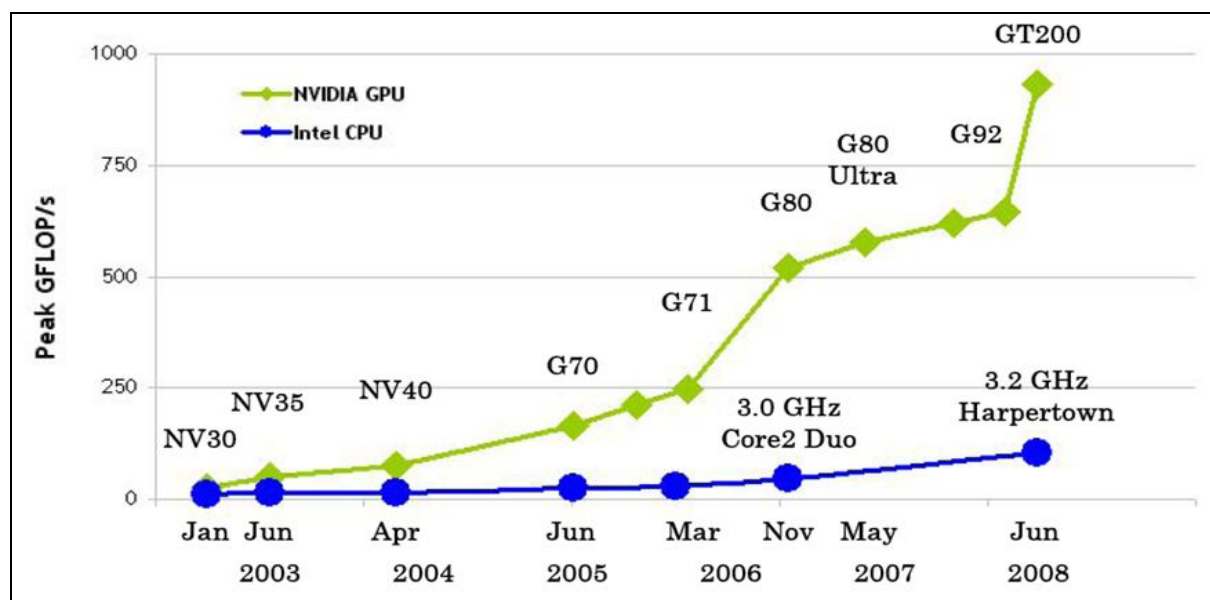
ÁLTALÁNOS CÉLÚ GRAFIKAI FELDOLGOZÓ EGYSÉGEK

Számítási kapacitás tekintetében általában a számítógép központi végrehajtóegységének teljesítményét vizsgáljuk, az utóbbi években azonban egy újszerű lehetőséggel is számolnunk kell, ezek pedig a személyi számítógépekben található grafikus kártyák.

Ezek az eszközök hagyományosan a monitoron látható kép megjelenítéséért felelősek. A múltban ez meglehetősen egyszerű feladatként jelent meg: a memória egy bizonyos területén lévő tartalomnak átalakítása analóg/digitális kimenetűvé, a 90-es években azonban itt is lezajlott egy nagyszabású változás. A számítógépes játékipar (és részben a tervezői

rendszerek) igényeit kielégítve megjelentek az úgynevezett grafikai gyorsító kártyák. A videojátékok megvalósításukat tekintve mind egymástól független alkalmazások, azonban a háromdimenziós megjelenítés tekintetében nagyjából hasonló algoritmusokat alkalmaznak. Mivel egy játékprogram erőforrásigényét tekintve ez igen tekintélyes részt jelent, megjelentek úgynevezett kiegészítő kártyák, amelyek célirányosan ezt a 3D számítást segítették, ezzel jelentősen csökkentve a központi egység terhelését.

Ezek a kiegészítő kártyák először fizikailag külön kártyaként jelentek meg, a videokártyához kapcsolódóan, de hamarosan a két eszközt integrálták, ennek következtében a grafikus kártyák az egyszerű jelátalakításon túl hamarosan meglehetősen nagy számítási kapacitással rendelkező kiegészítő eszközökké váltak. Kezdetben ezek céljuknak megfelelően különböző, a 3D számításokhoz szükséges számításokat elvégző részegységeket tartalmaztak, a későbbiekben azonban folyamatosan növekedett ezen egységek száma, illetve az utóbbi években ezen egységek felépítése is egyre hasonlóbba vált, mígnem a közelmúltban megjelentek az első, azonos felépítésű feldolgozóegységeket tartalmazó eszközök.



1. ábra: CPU – GPU csúcsteljesítmények változása [1]

Ez a lépés pedig egy egészen újszerű helyzetet teremtett az alkalmazás fejlesztők számára. Az így létrejövő eszközök ugyanis már általános célú feldolgozó egységeket tartalmaznak, így bár a grafikus kártyák fő feladata továbbra is a kép megjelenítése maradt, megjelent a lehetőség, hogy ezeket az eszközöket egyéb, általános célú programok futtatására használjuk. Hamarosan a grafikus vezérlőkártya gyártók is meglátták az ebben rejlő lehetőségeket, és eszközeiket átalakították olyan formában, hogy egyszerű módon támogassák az általános célú alkalmazások futtatását. Az új technológia hangzatos nevet is kapott: GPGPU – General-Purpose computation on Graphics Processing Units.

Ki kell hangsúlyoznunk, hogy az új lehetőség nem csak technikai érdekességgént van jelen, a napjainkban kapható videokártyák ugyanis már akár több száz végrehajtó egységet is tartalmazhatnak, ezeket használva az alkalmazások futásideje akár két nagyságrenddel is kisebb lehet. Az 1. ábrán látható az évek tükrében a CPU-k (központi feldolgozó egység) és GPU-k (grafikus vezérlő) sebességének növekedése. Jól látható, hogy az évek folyamán a GPU-k nagyságrendekkel nagyobb teljesítményre tettek szert, mint korunk legmodernebb CPU-i.

ELÉRHETŐ ELMÉLETI TELJESÍTMÉNY

Azonban a gyakorlati megvalósítás tekintetében már fontos megszorításokkal kell szembenéznünk: ha hozzá akarunk férni a megnövekedett számítási kapacitáshoz, ez csak a nagyszámú végrehajtó egység kihasználásával, tehát megfelelően párhuzamosítható algoritmusok tervezésével, és ezek megfelelő implementálásával érhető el, amelyek a már előzőleg is említett akadályok miatt egyelőre nehézkesnek tűnnek.

Mindez a jelenlegi videokártya piacra pedig hatványozottan érvényes. A grafikus vezérlőkártyákban a hagyományos CPU-khoz képest meglehetősen egyszerű végrehajtó egységekkel találkozhatunk (utasításkészlet, sebesség, optimalizálási lehetőségek tekintetében). Ezek ereje tehát csak nagy számuknak köszönhető, ez azonban igényli azt, hogy egy feladat esetén ezek az egységek mind kihasználhatóak legyenek, tehát nagyon sok szálon párhuzamosan futtatható programokra van szükség. Érdekes tehát néhány gyakorlati vizsgálatot elvégezni, hogy ezek az eszközök a való világ feladataiban mennyire tudják megközelíteni az elméletben ígért teljesítményüket.

Az egyes GPGPU-k elméleti teljesítménye meglehetősen egyszerűen kiszámolható. Tekinthetjük példaként az nVidia cég egyik nagyteljesítményű eszközét, a GTX280-as videokártyát. Ennek alapvető adatait tartalmazza az 1. táblázat:

Mag típusa:	GT200
Megjelenés ideje:	2008 jún.
Feldolgozó egységek száma	240
Shader órajel-frekvencia	1,296 Ghz
FP32 utasítás/órajel	3
Memória órajel-frekvencia	2214 Mhz
Memória interfész	512 bit

1. táblázat [2]

Ez alapján egyszerűen kiszámítható az elméleti számítási kapacitás. A magok órajel-frekvenciája 1,296 Ghz, illetve ideális esetben egy órajel-ciklus alatt 3 darab lebegőpontos művelet végrehajtására képesek. Mivel az említett videokártya 240 darab egymástól független végrehajtó egységet tartalmaz, így a tényleges maximális teljesítmény ezek szorzata, tehát 933,12 GFLOPS. Ez messze meghaladja a jelenleg kereskedelmi forgalomban kapható átlagos eszközök által elérhető teljesítményt.

Mivel az általános programozási feladatok az egyszerű számítások mellett nagymennyiségű memória műveletet is szoktak tartalmazni, célszerű megvizsgálni a kártya ezen tulajdonságait is. A szóban forgó GTX280-as kártya esetén a memóriavezérlők 2214 Mhz órajel-frekvencián működnek, sávszélességük pedig 64bit. 8 darab ilyen memóriavezérlő található az eszközön, így ebben az esetben is egyszerűen számítható az elérhető maximális átvitel: 1133,57Gb/s. Tehát ideális körülmények között másodpercenként 141,7 GB adat átvitelére alkalmas.

Fontos azonban megjegyezni, hogy mindezek a rendkívül impozáns adatok pusztán elméleti határokat jelentenek (a gyártók által megadott adatokra alapozva), ezt a tényleges teljesítményt a gyakorlati alkalmazások valószínűleg soha nem fogják elérni, csak külön erre a célra írt tesztprogramokkal lehet megközelíteni (ahol az utasítások jellege és sorrendje éppen a kártya számára legoptimálisabb).

Emiatt fontos különböző gyakorlati teszteket végezni valós problémákkal, amelyek segítenek meghatározni a kártya való világban kihasználható teljesítményét, amelyek alapján sokkal egyszerűbb döntéseket hozni a gyakorlati használhatóság területén.

MÁTRIX-SZORZÁS VIZSGÁLATA

Az előzőekből kiderült, hogy az új eszközök használata nem ad automatikus sebességnövekedést, egy hagyományos program futtatása körülbelül hasonló eredményt adna, mint az előző generációs processzorok esetén. Valódi előny kimutatásához célszerű valamilyen jól párhuzamosítható algoritmust vizsgálni, ilyeneket a matematikai feladatok között meglehetősen gyakran találunk, tekintsük példaként az egyszerű mátrix szorzás algoritmusát, ahol az egyes részeredmények kiszámítása egymástól teljesen független.

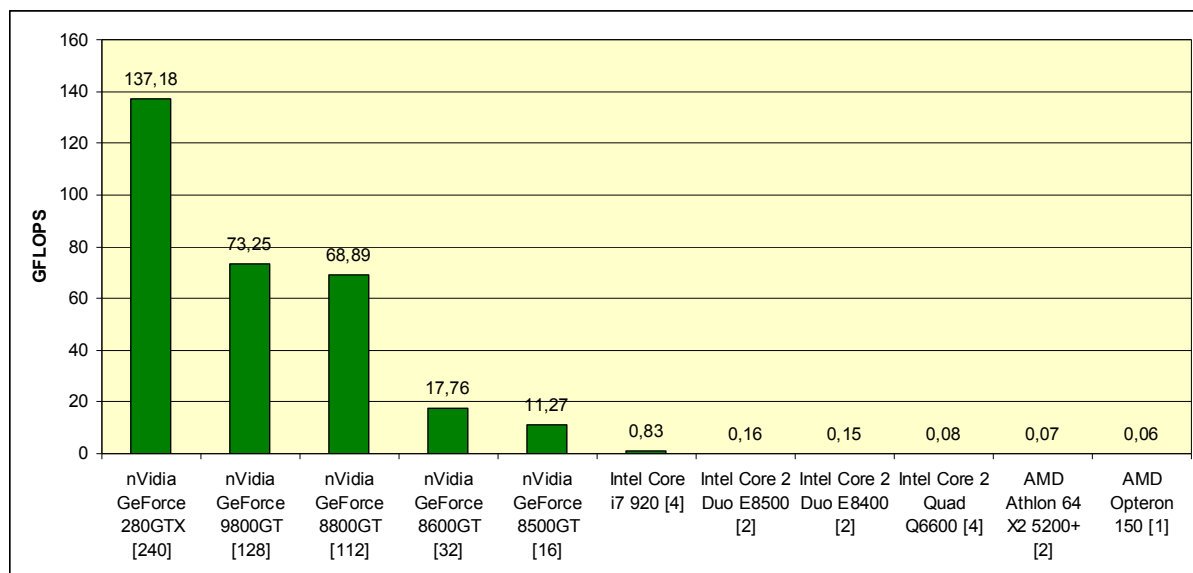
Egyprocesszoros rendszer esetén a megoldás két egymásba ágyazott ciklust igényelne, amelyek segítségével kiszámítható egymás után minden sor és ezen belül minden oszlop értéke (minden elem számítás egy harmadik ciklust igényel, amely összeszorozza, majd összeadja a bemeneti mátrixok elemeit).

A párhuzamosítás itt meglehetősen egyszerűen megoldható, platformtól függően különféle megoldásokat célszerű alkalmazni. Többmagos CPU-k esetében a magok száma nagy valószínűséggel alacsonyabb, mint a feldolgozandó mátrix elemeinek a száma, emiatt valamilyen formában ki kell osztani az egyes egységek között a feldolgozandó mátrix elemeket. Az egyik lehetőség, hogy a feldolgozó szoftver a magok számával megegyező számú szálat indít el, majd ezek számára kijelöli a mátrix megfelelő szegmenseit. Az egyes szálak által végrehajtott algoritmus itt tulajdonképpen megegyezik az egyprocesszoros rendszernél megismerttel (három egymásba ágyazott ciklus), csak minden szál a teljes mátrixnak csak egy részén dolgozik. Másik lehetőség, hogy a mátrix elemeinek számával megegyező számú szálat indít a program, minden szál csak egy elem kiszámításával foglalkozik. Ebben az esetben az egymással párhuzamosan futó szálak fizikai végrehajtóegységekre való felosztását az operációs rendszer fogja végezni valamilyen ütemezési stratégia szerint. Mivel a szálak ütemezése meglehetősen időigényes folyamat, valószínűleg az előző megoldás vezet jobb eredményre.

A GPGPU-k programozása esetén azonban más megközelítéssel célszerű megoldani a feladatot. A feldolgozó egységek meglehetősen nagy száma, illetve a keretrendszer sajátosságai miatt (adatpárhuzamos végrehajtás esetén tudnak csak hatékonyan együttműködni a feldolgozóegységek) a második változat használható jól.

A gyakorlati megvalósítás során használt CUDA keretrendszer esetén nincs is lehetőség az egyes szálak közvetlen felparaméterezésére, a program indítása tulajdonképpen kimerül a feldolgozandó, illetve az eredmény mátrixot tartalmazó memóriaterületek azonosításában, az elindítandó szálak programkódjának (kernel), illetve indítási paramétereinek meghatározásában.

A szálak létrehozását, azok adatalemekhez való rendelését ebben az esetben már nem a programozó irányítja, hanem ez a keretrendszer feladata. Amennyiben a feldolgozandó mátrix mérete meghaladná a fizikai végrehajtóegységek számát, akkor a keretrendszer automatikusan több lépésben végzi el a feldolgozást, ilyenkor egymást követően többször fog lefutni a megadott kernel a mátrix különböző részein. Ennek pontos módját szintén a keretrendszer határozza meg, nincs szükség külön programozói munkára (teljes mátrix felbontása kisebb részekre, egyes részekhez szálak rendelése, kernel többszöri elindítása stb.), sőt ennek befolyásolására lehetőség sincs.



2. ábra: Mátrix szorzás mérési eredmények [3]

A technikai háttér részletezése nélkül a 2. ábra mutatja a mérési eredményeket. A feladat jelen esetben két 2048 x 2048 méretű mátrix összeszorozása, amelyek egyszeres pontosságú lebegőpontos számokat tartalmaznak. A mérés során a különböző architektúrákon le lett futtatva ugyanaz a programkód, ezzel meg lett határozva a futásidő. Ez, illetve a végrehajtott lépések darabszáma alapján már egyszerűen kiszámítható a másodpercenként végrehajtott lebegőpontos műveletek száma.

Érdeemes megjegyezni, hogy az időmérés során figyelembe lett véve a videokártyák esetén felmerülő adatátviteli idő is. A jelenleg elérhető eszközök ugyanis rendelkeznek a fontos megszorítással, hogy a feldolgozó egységek csak a videokártya saját memóriájához férnek hozzá közvetlenül. A mátrix szorzás tehát valójában ezekből a részlépésekből áll: (1) a két bemeneti és egy kimeneti mátrix számára memória lefoglalása, majd az első kettő adatainak átmásolása a videokártya memóriájába (2) a két bemenő mátrix összeszorozása, az eredmények eltárolása a videokártya memóriában (3) az eredmény mátrix átmásolása a videokártya memóriából a számítógép központi memóriájába. A CPU-k esetében ez a másolás szükségtelen, hiszen a hagyományos CPU már eleve a központi memóriában dolgozik (a memória lefoglalás itt is megjelenik, de ennek időszükséglete elhanyagolható). Ha szigorúan csak a szorzásra koncentrálunk a mérések során, akkor természetesen jogos lehet eltekinteni ettől a késlekedéstől, de ha a gyakorlat szempontjából reálisan szeretnénk összehasonlítani a különböző eszközöket, akkor mindenképpen érdemes figyelembe venni ezt, a csak a GPGPU-k esetén jelentkező hátrányt (tulajdonképpen ezzel egy elemi lépésnek tekintjük az adatok elérését, a számítás végrehajtását, majd az eredmények elérhetővé tételét).

Az első 5 oszlop GPGPU-k teljesítményét mutatja a bemutatott mátrix szorzási művelet során, a következő 6 oszlop pedig néhány jelenleg is elérhető CPU teljesítményét. Jól látható a különbség a két architektúra között, a tesztben szereplő leggyorsabb grafikus kártya teljesítménye 137,18 GFLOPS, míg a hagyományos processzorok között a leggyorsabb is csak 0,83 GFLOPS teljesítményt mutatott.

A táblázat tartalmazza az eszközökben található végrehajtó egységek számát (CPU-k esetében a magok száma, GPU-k esetében pedig az ezeknél jóval egyszerűbb feldolgozóegységek száma). Jól látható, hogy a magok számának növekedésével az elérhető teljesítmény is egyenesen arányosan növekszik. Ennél a feladatnál (és a hozzá tartozó párhuzamosított megoldásnál) tehát tényleg jól kihasználható a végrehajtó egységek nagy száma, a mérési eredmények azt sejtetik, hogy az egységek számának további növelésével nem csak a papíron számítható csúcskapacitás növekszik majd, hanem a gyakorlatban kihasználható teljesítmény is. Ez egyben azt is jelenti, hogy ezek az algoritmusok lineárisan gyorsíthatók további eszközök felhasználásával, ami a gyakorlatban egy meglehetősen jó alternatívát biztosít az információbiztonság gyakorlati feladatai esetén (pl. egy hasonlóan jól párhuzamosítható algoritmussal egy egyébként 1 évig tartó kódtörés 20 videokártyával már csak két hetet vesz igénybe).

N-TEST SZIMULÁCIÓ VIZSGÁLATA

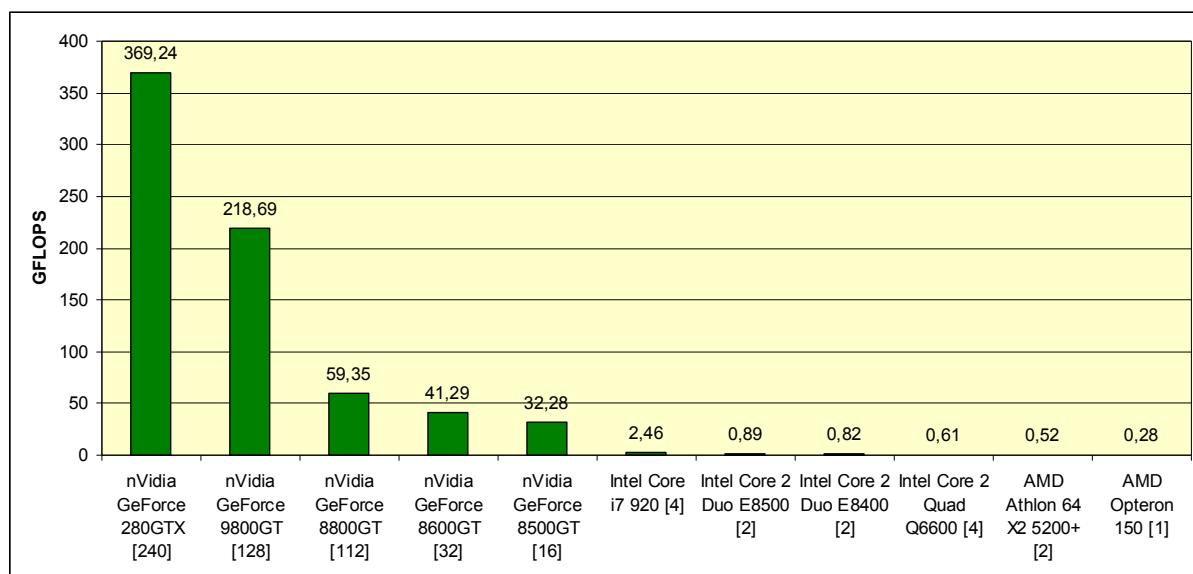
A mátrix szorzás esetében jól látható a párhuzamosítás adta előny, azonban az elért teljesítmény messze nem érte el az elvi maximumot. Ennek legfőbb oka az, hogy figyelembe vettük a mátrixok adatainak mozgatását is, ami jelentősen lerontotta a GPU által nyújtott eredményeket.

Célszerű lehet emiatt egy olyan vizsgálat elvégzése, amely szintén jól párhuzamosítható feladatot jelent, azonban meglehetősen kicsi az adatszükséglete (mind a bemeneti, mind pedig a kimeneti oldalon). Erre egy jó választás lehet az N-test szimuláció: eltároljuk N darab test adatait (pozíció, sebesség, tömeg), majd minden egyes iterációs lépésben kiszámoljuk a testek által egymásra ható gravitációs erőket, és ennek megfelelően változtatjuk az egyes testek sebességét/pozícióját.

A testek számának növelésével gyorsan növekszik a szükséges lebegőpontos műveletek száma, mivel minden test esetén ki kell számolni az összes többi test által rá ható erőket, tehát a számításigény $O(N^2)$ nagyságrendű. A memóriában azonban nincs szükség sok adatra, pusztán az egyes testek paramétereit kell eltárolni, ennek szükséglete értelemszerűen N konstansszorososa.

A feladat szintén jól párhuzamosítható, hiszen a számítás legnagyobb része az egyes testek egymásra ható erőinek (majd ezek eredőjének) kiszámítására vonatkozik, ezek pedig egymástól függetlenül elvégezhetők. Joggal várhatjuk tehát, hogy a mérési eredmények a mátrix szorzáshoz viszonyítva még jobban kidomborítják majd a GPGPU-k előnyeit, hiszen itt is nagy párhuzamos számítási kapacitásra van szükség, az adatmozgatás pedig ehhez viszonyítva meglehetősen kevés (a testek kezdőállapota a bemenet, majd pedig a szükséges iterációs ciklusok végén a testek végső állapota a kimenet).

A mérési eredményeket a 3. ábrán látható táblázat foglalja össze:



3. ábra: Mátrix szorzás mérési eredmények [3]

Láthatóan sikerült még jobban megközelíteni az elvi maximális teljesítményt. Szintén jól látható, hogy a végrehajtó egységek számának növelésével szinte egyenes arányban növekszik az elérhető teljesítmény, tehát ez a probléma (illetve a rá kidolgozott megoldás) szintén jól kihasználja a párhuzamos architektúra adta lehetőségeket.

KIEGYENSÚLYOZOTT BINÁRIS-FA FELDOLGOZÁS VIZSÁLATA

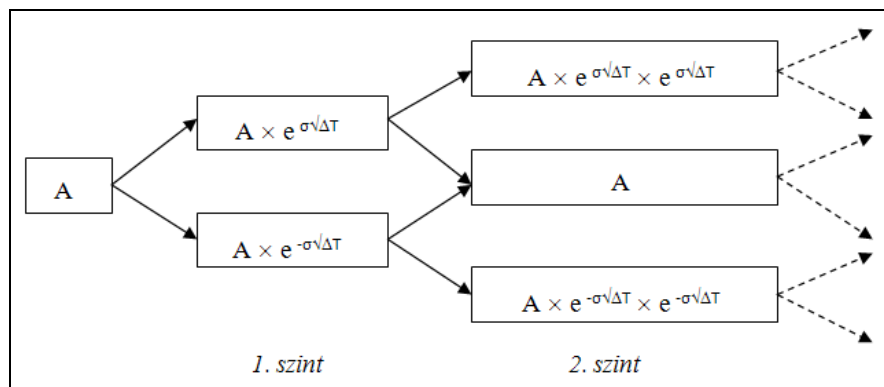
Gyakorlati feladatok során azonban meglehetősen ritka, hogy a teljes probléma megoldása során egymástól független úton lehet számítani az egyes részeredményeket. Általában az egyes részeredmények kiszámítása egymással valamilyen kapcsolatban álló számításokat igényel, vagy esetleg szükség van néhány további részeredmény már előzőleg meghatározott értékére.

Az ilyen számítások egy jelentős része jól modellezhető egy fa adatszerkezet segítségével. Az adatszerkezet levél elemei (a 4. ábrán a legjobboldalibb elemek) tartalmazzák a kiinduló adatokat, amelyekkel azonnal meg lehet kezdeni a szükséges számításokat. A fa felsőbb szintjein lévő elemek kiszámításához azonban már szükség van az alattuk lévő szintek teljes feldolgozására.

Értelemszerűen a teljes párhuzamosítás itt nem valósítható meg, hiszen nem lehet egy időben számolni a fa összes csomópontjához tartozó értéket, pl. a fa gyökérelemének feldolgozása csak az összes többi elemé után következhet. Ez felvett számos kérdést, amelyeket csak jóval összetettebb algoritmusokkal lehet megvalósítani, ezek közül általában a legnagyobb problémát a különféle szinkronizációs lehetőségek beépítése jelenti.

Bár nem lehet minden elemet egy ütemben kiszámítani, egyes részfeladatok még lehetnek meglehetősen jól párhuzamosíthatók. Jelen esetben az adott pillanatban kiszámítható csomópontok jól körülhatárolhatók, ezek mindig a fa levélelemei. Szintén könnyen belátható, hogy (lásd 4. ábra) jelen esetben ezek tulajdonképpen egymástól függetlenül kiértékelhetők.

Egy végrehajtó egység esetén ez egy ciklust jelent, amely végigszalad az összes levélelemen, egyesével kiszámítva a hozzájuk tartozó értékeket. GPGPU-k használata esetén itt is célszerű kihasználni a meglehetősen nagy számú mag által nyújtott lehetőségeket, emiatt minden lépésben érdemes az aktuális levélelemek számának megfelelő mennyiségű szálát indítani, amelyek mind kiszámítják egy-egy levélelem értékét. Miután ez megtörtént, az eddig egyel magasabb szinten lévő csomópontok lesznek az új levél elemek, így már ezekre is végre lehet hajtani ugyanezt a lépést. Értelmszerűen egyre kevesebb levéllel találkozunk, míg végül feldolgozásra kerül a fa gyökére is, ami megadja a végső eredményt.



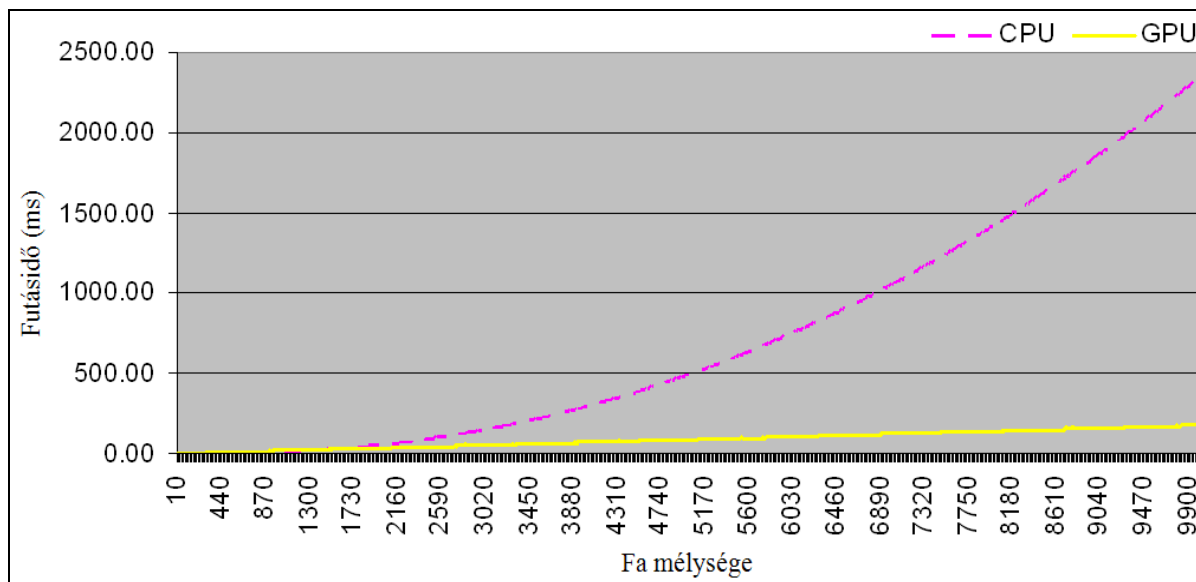
4. ábra: Az implementált bináris fa felépítése

Az implementált program egy egyszerű európai opcióárazást hajt végre, amely esetben a fa gyökérpontja jelenti az aktuális (ismert) árfolyamot, az ebből kiinduló fa egyes ágai jelentik az árfolyamok lehetséges mozgását különféle valószínűségi változóknak megfelelően, a fa csomópontjai az árfolyamok lehetséges értékeit az egyes jövőbeni időpillanatokban, a fa levelei pedig a lehetséges árfolyam értékeket az opció lejáratának időpontjában. A felépítéséhez szükséges az aktuális árfolyam (A), a teljes vizsgált időtartam (T), az iterációk száma (N), az egy iteráció által lefedett időtartam ($\Delta T = T / N$), illetve a volatilitás (σ). A felépített fa levélelemeiben az így kiszámított lehetséges árfolyamértékek alapján már egyszerűen kiszámítható az opció jövőbeni értéke, ez alapján pedig jelenértékszámításokkal (figyelembe véve, hogy a fa egyes ágaira milyen valószínűséggel juthattunk el) egyszerűen kiszámítható az előző szintek csomópontjaiban az opció értéke. Ezt folyamatosan megismételve, a gyökérpontig jutva megkapjuk az opció jelenlegi értékét.

A jelenértékszámításhoz használt GPU kernel kódja:

```
optionpricing.cu  
  
for(int i = N; i > 0; i--)  
{  
    for(int j = 0; j < i; j++)  
    {  
        BASE_TYPE upv = stock_tree[j];  
        BASE_TYPE downv = stock_tree[j + 1];  
        BASE_TYPE prev_value = upv / Mu;  
        BASE_TYPE Pu = (prev_value * exprft - downv) /  
            (upv - downv);  
        BASE_TYPE option = (Pu * option_tree[j] + (1 - Pu) *  
            option_tree[j + 1]) / exprft;  
        option_tree[j] = option;  
        stock_tree[j] = prev_value;  
    }  
}
```

A feladat ideális a GPU-n való végrehajtásra, mivel az adatmozgatások száma minimális, nem szükséges a teljes fa másolására a videokártya memóriája és a központi memória között, elég a fa felépítéséhez szükséges paraméterek átadása (milyen valószínűséggel kell mozogni felfele/lefele, milyen mértékű változások várhatóak, illetve milyen mélységű legyen a teljes fa). A feladat az előzőekben megismert módon, szintenként párhuzamosítva végrehajtható, majd a gyökérelém feldolgozását követően a végeredmény előáll. Ezt természetesen vissza kell juttatni a központi memóriába, de mivel nincs szükség a számítási részeredményekre, ez is csak egyetlen szám másolását jelenti.



5. ábra: A kiegyensúlyozott bináris fa feldolgozásának futásideje

A nagyfokú párhuzamosság és a minimális memóriaátvitel miatt jelentősen kisebb végrehajtási időre számíthatunk a GPGPU használatával, mint a CPU esetében, emiatt jelen esetben nem is a különböző eszközök összehasonlítása az érdekes, sokkal inkább az, hogy a különböző mélységű fák feldolgozása során hogyan viszonyul egymáshoz a két különböző architektúra által nyújtott teljesítmény. Ennek megfelelően az 5. ábra a végrehajtási időt mutatja a fa méretének függvényében (a konkrét mérések során GPU: nVidia GeForce

280GTX, 240 végrehajtó egység; CPU: Intel Core2 Quad Q6600 2,4Ghz, 4 mag; a rendszer 32 bites lebegőpontos számokkal számolt mindkét esetben).

Az eredményeket célszerű a fa mélységének (és így a végrehajtott iterációk számának) függvényében vizsgálni:

- Kis számú iteráció esetében ($N < \sim 1500$): bár a GPU jóval több maggal rendelkezik, mint a CPU, így magát a tényleges számítást már itt is gyorsabban el tudja végezni, mint a hagyományos eszközök, azonban ez az előny nem használható ki jól, mivel a program futtatása során meglehetősen sok járulékos költség keletkezik (kernel indítása, kernel leállítása, szinkronizáció, bemenő adatok átvitele, eredmények kiolvasása a videokártya memóriából).
- Nagy számú iteráció esetében ($N > \sim 1500$): az előbb említett járulékos költségek természetesen továbbra is fennállnak, azonban a GPU nagy számítási kapacitásával már tudja ezeket ellensúlyozni. A tesztelt eszköz 240 végrehajtó egységgel rendelkezik, felépítéséből adódóan ezeket is csak akkor tudja megfelelően hatékonyan kihasználni, ha az általa futtatandó szálak száma jóval meghaladja ezt a számot. Emiatt amikor már nagy számú levelet kell feldolgozni, akkor a GPU teljes kihasználtsággal működhet, ez pedig jelentős előnyt jelent számára a CPU hagyományos 4 magjával szemben.

Tehát megadott iterációs szám alatt a GPU használata felesleges, egy megadott (gyakran csak a gyakorlati tesztek során jól meghatározható) határ felett azonban kimondottan jól teljesítenek ezek az eszközök. Érdemes azonban megjegyezni, hogy a feladat többi tulajdonsága is hozzájárult ehhez az eredményhez: kevés memóriaátvitelre volt szükség, nagy mennyiségű lebegőpontos számítást kellett végrehajtani, ezek a számítások pedig jelentős részt egymástól függetlenek voltak.

EREDMÉNYEK ÉRTÉKELÉSE

A mérési eredményeket figyelembe véve tehát egyértelműen kimondható, hogy a GPGPU technológia által nyújtott teljesítmény nem csak elméleti lehetőségeket rejt, hanem jelentős részt a gyakorlatban is jól kihasználható. Mindig az adott alkalmazás dönti el, hogy érdemes-e az új technológiát felhasználni, ez ugyanis csak akkor vezet jó eredményre, ha meglehetősen nagy számú párhuzamos műveletet kell elvégezni, enélkül a hagyományos CPU kevés, ámde jóval fejlettebb magjai egyszerűbb és hatékonyabb megoldást kínálnak. Nehéz lenne pontosan definiálni, hogy melyek ezek a feladatok, néhány egyszerű tapasztalati alapelvet azonban célszerű figyelembe venni:

- *Memória átvitel minimalizálása:* a GPGPU architektúrák egyik legnagyobb hátránya jelenleg, hogy ezek az eszközök csak a saját memóriájukban képesek műveletvégzésre, tehát minden bemenő adatot ide kell másolni, illetve a további feldolgozás részére az eredményeket innen vissza kell másolni a központi memóriába. Ez meglehetősen nagy idővesztést jelent (a mátrix szorzás példájában közel 90%-át az eltel időnek), emiatt a nagy memóriaigénnyel rendelkező alkalmazások esetén érdemes figyelembe venni ezt a veszteséget. Amennyiben ez lehetséges, célszerű a kimenet/bemenet mennyiségét csökkenteni, pl. ha a bemenet kevesebb paraméter alapján egyszerűen generálható, célszerű azt a videokártyán belül elvégezni.

- *Adatpárhuzamos végrehajtás:* az eszközök felépítéséből adódóan a nagy számú végrehajtó egység csak ugyanazon programkód futtatására alkalmas, az egyes különálló aritmetikai egységek ugyanis nem feltétlenül rendelkeznek saját vezérléssel. Emiatt bár az elágazások és ciklusok lefordíthatók és futtathatók ezeken az architektúrákon is, azok indokolatlan használata jelentősen csökkenti a teljesítményt. Ezen esetekben célszerű a programkódot átstrukturálni, amennyiben ez nem lehetséges, felülvizsgálni, hogy érdemes-e GPGPU segítségével megvalósítani a feladatot.
- *Nagy mennyiségű szál futtatása:* szintén a vizsgált eszközök felépítéséből adódik, hogy igazán csak akkor használhatók hatékonyan, amennyiben meglehetősen nagy mennyiségű szálát kell párhuzamosan futtatniuk. Ez az alsó határ nem feltétlenül csak a végrehajtó egységek számát jelenti (ha ennél kevesebb szálát kell indítani, akkor teljesen nyilvánvaló, hogy nem használjuk ki az eszköz adta lehetőségeket), hanem annak többszöröse is lehet, mivel a vizsgált kártya működése során alkalmas arra, hogy ha egy szál várakozó állapotba kerül (pl. memóriából adatra vár) akkor az ezt futtató végrehajtó egységet ez idő alatt egy másik szál futtatására használja fel. Mindez az átütemezés hardveresen, többlet veszteség nélkül történik.
- *Optimalizálás szükségessége:* természetesen a hagyományos CPU alapú programozás során is jelentős az optimalizálás szerepe, azonban az új technológia esetén ez még lényegesebb lehet. Egyrészt a fordítóprogramok még nem kellőképpen kiforrottak, így az optimalizálás jelentős részt a programfejlesztő feladata, másrészt az egyes eszközök egymástól jelentősen különböznek, így a konkrét futtatást végző hardverre testreszabott kód (memóriaméretetek, memóriakialakítás stb.) nagyságrendekkel jobb eredményeket nyújthat.

A felmerülő hátrányoktól eltekintve azonban jól látható, hogy az információbiztonság területén lényeges aritmetikai számításokat (mind a kódolás/dekódolás, mind pedig az esetleges kódolt szövegek feltörése esetén) a hagyományos CPU-khoz képest nagyon nagy teljesítménnyel hajtják végre ezek a piacon napjainkban is elérhető eszközök.

Felhasznált irodalom

- [1] Nvidia CUDA Compute Unified Device Architecture Programming Guide, Version 2.0, Nvidia, June 2008
- [2] GeForce 280GTX spec.: http://www.nvidia.com/object/product_geforce_gtx_280_us.html (Letöltés ideje: 2009.07.01)
- [3] Cs. Csillingh, Cs. Iványi, S. Szénási: Multiplatform Performance Analysis of Parallel Workloads on Graphics Hardware, Morgan Stanley-BME Financial Innovation Centre Kick-off & Workshop, Budapest, 2009
- [4] Nvidia CUDA Compute Unified Device Architecture Programming Guide, Version 1.1, Nvidia, Nov. 2007

Vámosy Zoltán

vamosy.zoltan@nik.bmf.hu

MOBIL ROBOTOK GÉPI LÁTÁS ALAPÚ NAVIGÁCIÓJA

Absztrakt

A szerző által a robotépítő tevékenység területén elért eredményeit és megoldásait prezentálja az értekezés. A kutatási célkitűzések és módszerek bemutatása után, az eredményeket három csoportra osztva mutatja be: beltéri környezetben végzett navigáció és akadályelkerülés; kültéri környezetben lokalizáció pontosítása és térképkészítés; szakmaspecifikus alkotásként elkészített olyan rendszerek, mint lépegető robotok járási stratégiájának megvalósítása és körbelátó szenzorok képének minőségi javítása.

The paper presents the summary of the research goals on robots and the applied methods the achieved results and solutions on the area divided on three parts: navigation and obstacle avoidance in indoor environment; localization and map building in outdoor environment; such specific system as a software that makes it possible to easily develop stepping strategies, or a method to significantly improve the quality of the image of the PAL optics and the omnidirectional sensors.

Kulcsszavak: mobil robot, navigáció, PAL optika ~ mobile robot, navigation, PAL optics

BEVEZETÉS ÉS A KUTATÁSOK ELŐZMÉNYEI

Különböző szenzorokat, illetve ezekből felépített szenzorrendszereket gyakran alkalmaznak a robotikában annak érdekében, hogy a robot a folyamatosan változó környezetét (az akadályokat, valamint a környezetét jellemző objektumokat) valamilyen szinten megismerhesse és szükség szerint reagáljon ezek jelenlétére. A gépilátás-alapú rendszereknek kitüntetett szerepe van ezen eszközöknél, mert segítségükkel nagy mennyiségű információ nyerhető. A kilencvenes évek közepe óta fejleszték képfeldolgozás és más szenzorok használatán alapuló robotrendszereket. Az első eredményeim a képi információ alapján tanulásra képes, robotosított osztályozó rendszer, valamint neurális hálózatot használó vizuális alapú pályatervezés témakörben értem el [4], [22], [23], [24].

A későbbiekben számos mobil robot készült a vezetésemmel, melyek majd mindegyike – más szenzorok mellett – hagyományos és körbelátó kamerákat is használt. A dolgozat az e területen elért eredményekre koncentrál, tehát hosszabb fejlődési folyamat eredményeit foglalja össze. Ezen időszak alatt új technológiák és eszközök jelentek meg a területen, váltak általánosan elterjedtté, biztosítanak teljesen más szintű megközelítési lehetőségeket, mint korábban. E folyamatot példával is szemléltetni lehet. Egyrészt a kilencvenes években az élő kamera képek bevitelét még drága digitalizáló kártyák segítségével lehetett csak megoldani, most pedig filléres eszköz és USB csatolón keresztül egyszerűen kapcsolható kitűnő minőségű webkamera. Másrészt a GPS-es eszközök és a hozzá kapcsolódó szoftverrendszerek széleskörű elterjedése is teljesen más szintű lehetőségeket biztosít, mint az ezredfordulón, amikor még mesterségesen torzították a rendszer pontosságát, és az OEM GPS vevők csak a legszükségesebb adatokat biztosították, ráépülő programok nélkül. A folyamatos változás, számos új feladatot és lehetőséget kínált.

A látás a legnagyobb teljesítményű érzékelés. A környezet érzékelése lehetővé tesz számos olyan mozgást, amelyet adott világunk szabályoz. Az ember általában anélkül végzi mozgását igen nagy hatékonysággal, hogy pontosan értené, miként működik ez a folyamat. Nagy számú kutató, pszichológustól mérnökgig dolgozik a vizuális érzékelés komplex problémáján. Közös célunk olyan mesterséges látórendszer építése, amellyel vizsgálható, hogy egy robot miként használhatja hozzá illő nagy teljesítménnyel, „robustus” módon a háromdimenziós térben történő tevékenységekhez azt a képi információt, amely valójában csak kétdimenziós. A kifejlesztett érzékelési rendszer lehetővé teheti, hogy a robot olyan mindennapi feladatot oldjon meg, mint „menj a folyosón a végéig, majd fordulj jobbra”.

Minden érzékelő rendszerben, legyen az akár emberi vagy mesterséges, a kritikus komponens az érzékelés módja, amelyet a környezeti információ begyűjtésére használunk. A biológia területén lényeges megfigyelés, hogy mennyire többféle a szemlencsék geometriája. A rovarok többsége és az emberszabásúak széles látótérből szereznek adatokat és a szemük képes térfüggő felbontásra, fókuszálásra. Ezek érzékelési kapacitása a szemük speciálisan adaptálódó geometriai változásával magyarázható. Ehhez hasonlóan, ebben a munkában az olyan nagy látómezejű megoldás előnyeit vizsgálom, amelyet körbelátást biztosító kamera eredményez, vagyis a vízszintes látómező 360 fokok [25, 26].

Mindannyiszor, ha képet kapunk egy körbelátó kamerától, felvetődik a kérdés, mit tegyünk vele, miként dolgozzuk fel? Szükséges-e, hogy a környezet belső modelljét, reprezentációját formáljuk meg a segítségükkel? Biztosíthatnak-e időről időre úgy információt a világról, hogy nem készül belső részletes reprezentáció [27]? Ez az alapkérdés régóta foglalkoztatja a számítógépes látással foglalkozó szakembereket, és az egyik központi kérdése a vizuális érzékelés megértésének.

A huszadik század közepén Gibson [28] újszerű megközelítést vezetett be a látás területén. Az optikai tömbre helyezte a hangsúlyt, miszerint annak invariáns tulajdonságai határoznak meg minden információt (struktúrákat és eseményeket) a környezetről. Elmélete szerint az információ csak úgy „felkapható” a megfigyelő számára, amint az a környezetben mozog. Ezért Gibson azt állította, hogy az érzékelés direkt: az érzékelés és a beavatkozás szorosan összefügg, belső reprezentáció szükségessége nélkül. Adott a környezet komplexitása, ahol nem lehet mindent egyszerre feldolgozni, így ez az elmélet azt hangsúlyozza, hogy az érzékelés szelektív figyelmi mechanizmuson alapszik.

1982-ben Marr [29] munkája a látás számítógépes megközelítését indította el, amely a modern gépi látás alapját jelentette. Ebben a munkában a vizuális érzékelés szekvenciális, moduláris felépítését vezette be, ahol a belső reprezentáció, modell volt a kiindulópont. Ez az indirekt megközelítés tehát gyökeresen eltér Gibsonétól. Számítógépes módszere szerint egy előzetes vázlattal kezd, amely információt tartalmaz a kép régióiról és a határokról. Ebből a reprezentációból folytatólagosan egy 2 1/2D-s vázlatot épít, amelyet meghatároz a megfigyelő

nézőpontja és a tárgyak helyzete (távolsága) és orientációja. Végül a környezet érzékelésének nézőpont-független 3D modelljét készíti el.

A vizuális érzékelésben megközelítem az indirekt technikát követve konstruálja meg a környezet modelljét. Ebben az értelemben Marr módszerét követem, de attól eltérően nem építek minden állapothoz sorozatos és részletes belső modellt. Ehelyett arra koncentrálok, hogy olyan reprezentációt készítsék, amely alkalmas a feladat megoldására. Például ha egy város főutcáján haladunk, elegendő, hogy helyzetünket egy épülettömbnyi pontossággal ismerjük. Ha viszont be akarunk lépni egy épület ajtaján, lényegesen nagyobb pontosságra van szükségünk.

A környezet belső reprezentációját minden egyes navigációs feladathoz testre kell szabni és ennek megfelelően kell a szükséges információ mennyiségét is begyűjteni. Az állatok számos esetben felváltva használják a „mérőldköveken”, jelző elemeken alapuló navigációt és a megközelítő úthoz tartozó integrációs módszereket [30].

Amikor a robotnak nagyobb távolságot kell megtennie, akkor a világ érzékelésére megjelenés alapú környezeti reprezentációt alkalmazunk. Az olyan precizitást igénylő feladatoknál, mint a dokkoló helyzet megközelítése, vagy az ajtónyílásokon történő áthaladás, az érzékelés a megjelenés alapú módszerről olyan technikára vált át, ahol a képjellemzők kerülnek hangsúlyozottabban a figyelem középpontjába. A működés e két módját két különböző modellel jellemezhetjük és topológiai navigációnak, illetve vizuális útkövetésnek nevezzük.

A hosszabb távú (alacsonyabb precizitású) és a rövidebb távú (magas precizitású) érzékelő modulok fontos szerepet játszanak a robotnavigációs problémának hatékony és robusztus megoldásában. Ez a megközelítés azért lényeges, mert gyakran nem az fontos, hogy milyen hatékonysággal lehet használni e modelleket, hanem a világmodell elkészítésére kerül a hangsúly.

CÉLKITŰZÉSEK

A cikkben azokat a részfeladat megoldásokat vizsgálom az általunk készített mobil robotok segítségével, amelyeket a navigáció során különböző (mikro, illetve makro) munkakörnyezeti feltételekből kiindulva kell megoldani. A dolgozat célja a mobil robotok navigálási feladataihoz kapcsolódó részproblémák (akadály-elkerülés, környezet feltérképezés, pályatervezés, valamint navigáció) ismertetése és a vizsgált lehetséges megoldások bemutatása.

Előbb a mobil robotok különböző szenzorok, illetve PAL-optika használatával történő beltéri navigációját, az akadály-elkerülés lehetséges megoldásait vizsgálom. Megoldásokat keresek az akadály-elkerüléshez, pályatervezéshez, foglaltsági hálós reprezentációhoz, illetve vektoros térképkészítéshez. Megvizsgálom a pályatervezési algoritmusokat abból a szempontból, hogy melyik alkalmazható egyszerű szenzorcsoporthoz jeleik felhasználásával, relatíve kis számítási igényt – mikrokontroller lehetőségeit – feltételezve. Összehasonlítom ezeket a foglaltsági hálós térképreprezentáció esetében. A megoldást négy lábú lépegető robot tárgyreflexiós szenzorcsoporthoz jeleik feldolgozásával történő navigációhoz kívánom felhasználni. Kidolgozok olyan képfeldolgozó eljárásorozatot PAL-optika használatával, amely képes négy lábú lépegető mobil robot lábkörnyezetének valósidejű vizsgálatára és ennek felhasználásával akadály-elkerülésre. Megoldást keresek robotnavigáció során alkalmazható olyan akadálydetektálásra és térképkészítésre, ahol az adatok nagy tömörséggel reprezentálhatók. Vizsgálom a strukturális megvilágítást alkalmazó képfeldolgozás használatát saját fejlesztésű lézerszenzorral, illetve az adatok fúzióját más elvű érzékelők esetében is. Olyan általános megoldásra törekszem, ahova egyszerűen beilleszthetők a különböző érzékelőktől származó adatok.

A kültéri környezet lokalizációs feladataira fejleszték ki módszereket, vizsgálom OEM GPS használatának lehetőségét, a lokalizációs adatok pontosítási módszerét ismert környezetben, illetve a körbelátó optikával készített képsorozatokból a térképkészítés menetét. Megoldást keresek mobil robot kültéri durva lokalizációjára GPS használatával. Különböző GPS szenzorok esetén tanulmányozom, hogy mennyire pontosan lehet meghatározni a robot helyzetét. Megvizsgálom, hogy a GPS érzékelő által meghatározott helyzetet milyen módon tudom körbelátó képek használatával ismert környezetben pontosítani. Számítógépes program formájában megvalósítok olyan eljárást, amelynek a segítségével mobil robotok navigálásához topológiai térkép építhető felülnézeti körbelátó képek központi részének transzformálásával. Az elkészített térkép segítségével pályát határoznak meg, az eredményeket kültéren tesztelem saját készítésű guruló mobil robot segítségével.

Végül olyan szakmaspecifikus problémákra tervezek választ adni, mint a lépegető robotok esetén alkalmazandó járási stratégia kialakításának módszere, a mobil robotnavigációs és akadály-elkerülési problémájának gyakorlati megvalósítása, illetve az alkalmazott körbelátó kép minőségének és felbontásának érdemi javítása, hogy minél több részletet figyelembe lehessen venni az előző feladatoknál. Kifejleszték saját készítésű négy lábú robothoz statikusan stabil járási stratégiát, majd vizsgálom, hogy a robot gyorsabb előrehaladása érdekében milyen dinamikus stabilitást adó lépésszekvencia készíthető. Kidolgozok olyan mozgásszerkesztő szoftvereszközt, amelynek segítségével hatékonyan lehet a saját megvalósítású hatlábú robothoz járási algoritmusokat kialakítani. Bemutatom saját fejlesztésű és készítésű guruló és lépegető robotok esetében az előző célok fizikai megvalósítását, rámutatok a navigációra és térképezésre kifejlesztett algoritmusok és módszerek kihasználásának lehetőségeire. Hagyományos kameraképen optikai folyam számíttással vizsgálom az akadályok detektálásának lehetőségét. Megmutatom szakmaspecifikus alkotásként a PAL-optika és a körbelátó szenzorok képe minőségének javítását és így összetett navigálási feladatokban való alkalmazhatóságuk hatékonyabb lehetőségét.

ALKALMAZOTT MÓDSZEREK

Optikai folyam technikák

Az optikai folyamon [31] azt értjük, ahogy a képintenzitások mozgása megjelenik egymás utáni képeken. Különböző típusú képbemenetekhez az egyes optikai folyam algoritmusok más-más eredményt adhatnak [32], ezért célszerű a bemeneti adatok milyenségének figyelembevételével választani a lehetséges algoritmusok közül, hogy a kapott vektormező minél jobban közelítse a képeken látható objektumok valós fizikai mozgását. Inputként a videó egymáshoz közeli képkockáit szokás megadni.

Az optikai folyam algoritmusok az összetartozó képpontok megtalálásához feltételezik, hogy ezek intenzitása közel megegyezik. Szinte az összes módszer alapját ez a feltételezés adja, amit optikai folyam korlátozásként ismerünk [32]

Jelölje $I(x, y, t)$ egy adott t pillanatban a képintenzitást, amely egy időben változó képsorozatból származik. Két feltételezéssel élünk:

- az $I(x, y, t)$ intenzitás a kép nagy részén alig függ az x, y koordinátáktól;
- a mozgó vagy álló objektumok pontjainak intenzitása (lényegében) nem változik az idő múlásával.

Legyen néhány objektum a képen, vagy csak néhány objektumpont, ami dt idő alatt (a gyakorlatban egymás utáni képvétel alatt) elmozdul egy (dx, dy) távolságra. Az $I(x, y, t)$ intenzitásértékek Taylor-sorba fejtésével és a 2. feltétel felhasználásával kapjuk:

$$-\frac{\partial I}{\partial t} = \frac{\partial I}{\partial x} \frac{dx}{dt} + \frac{\partial I}{\partial y} \frac{dy}{dt}. \quad (1)$$

Ezt a kifejezést rendszerint az optikai folyam feltételi egyenletének (vagy csak optikai folyam korlátozásnak) nevezik, ahol $dx/dt=u$ és $dy/dt=v$ az optikai folyammező x és y koordináta irányú összetevői.

Az egyenlet két ismeretlent (u , v) tartalmaz. A megoldásra a következő technikák a legelterjedtebbek [32]:

- A differenciális módszerek: régebbi technológiák, de megbízhatóak. Az újabbaknak nem sikerült jelentős minőségjavulást hozniuk. Mozgási modell szempontjából a paraméter nélküli algoritmusokhoz sorolhatók;
- Horn–Schunck-féle módszer [31];
- Lucas–Kanade-módszer és ennek piramisos változata [33]
- Korrelációs technikák (block matching) [34].

Neurális hálózatok

A neurális hálózat egy többprocesszoros, párhuzamos adatfeldolgozású számítógép [35]. Az egyes processzorokat neuronoknak (vagy sejtprocesszoroknak) nevezzük, melyek feladata a teljes rendszer feldolgozó képességéhez viszonyítva egy nagyon egyszerű átviteli függvény megvalósítása. Ezek a neuronok különféle módon kapcsolódhatnak egymáshoz, és ezek a kapcsolatok határozzák meg a topológiát.

A hálózatnak három fő jellemzője van: a processzorok, a topológia és a tanítási módszer.

A processzorok a bemenetükre érkező jeleket súlyozottan összegzik (W_{ij} az i -t j -vel összekötő kapcsolatból adódó súly) és egy átviteli függvény segítségével képezik kimenetüket. Átviteli függvényeként leggyakrabban ugrás, korlátozott lineáris, vagy szigmoid függvényt alkalmaznak.

A topológia a processzorelemek egymással alkotott kapcsolatának rendszerét jelenti, ami a legegyszerűbb esetben lehet úgynevezett előrecsatolt, vagy visszacsatolt, illetve a kettő kombinációja. Az előrecsatolt hálózat jellemzője, hogy benne a jelek a bemenet felől mindig a kimenet felé haladnak, míg a visszacsatolt hálózatok esetében több-kevesebb esetben a jel haladhat visszafelé is.

A tanítási módszer főbb típusai a felügyeletes tanítás és a felügyelet nélküli tanítás. A tanítási szabályként leggyakrabban az úgynevezett Hebb-szabályt, vagy a Delta-szabályt alkalmazzák.

EREDMÉNYEK

Beltéri, lokális környezetre vonatkozó megoldások

Beltéri környezetben a mobil robotok különböző szenzorok, illetve PAL-optika használatával történő navigációja, akadály-elkerülése terület megoldásainak részletezése:

1. Az akadály-elkerüléshez, pályatervezéshez, foglaltsági hálós reprezentációhoz, illetve vektoros térképkészítéshez kapcsolódó eredményeim:

Pályatervezési algoritmusokat valósítottam meg és hasonlítottam össze foglaltsági hálós térkép-reprezentáció esetében. Képfeldolgozás alapú eljárást fejlesztettem ki négy lábú lépegető mobil robot lábkörnyezetének valós idejű vizsgálatára és az akadály-elkerülésre PAL használatával.

A kifejlesztett EXPLORADORES II. robotrendszerben [19], [21] tárgyreflexiós szenzorcsoporttal alkotott térképek esetén foglaltsági hálós reprezentáció alkalmazásával összehasonlítottam szabályrendszer alapú, neurális hálózattal támogatott, tanulásra képes, potenciálmezővel kalkuláló és gráfbejáráson alapuló pályatervezési módszereket. Rámutattam az egyes technikák használhatóságára, előnyös, valamint részben a reprezentációból és a nagy

memóriaigényű megvalósításból adódó hátrányos oldalaira (1. táblázat). A hullám-továbbterjesztéses módszernek olyan továbbfejlesztését adtam, amely előre nem ismert környezetben is megoldást szolgáltat [20].

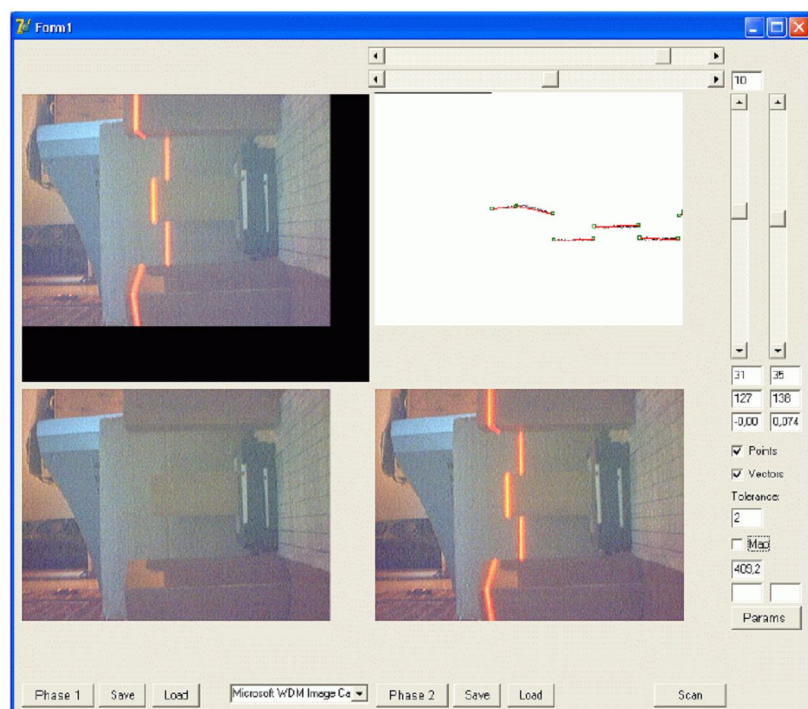
Lépegető robotok esetében felmerülő feladatra adok választ PAL-optikával készített kép feldolgozásával. Olyan képfeldolgozó eljárásgyűjteményt készítettem, amelyből felépített rendszer [16], [17] négy lábú robot hasára szerelt körbelátó kamera képének vizsgálatából valós időben detektálta a lábak lokális környezetét és így lehetővé teszi az ütközésmentes, biztonságos mozgást.

<i>Módszer (algoritmus)</i>	<i>Környezeti feltétel</i>	<i>Előny (e) / hátrány (h)</i>	<i>Fejlesztő javaslat, megjegyzés</i>
szabályalapú	ismeretlen	e: mikrovezérlőben megvalósítható => autonómia, h: minden esetre fel kell készülni; nem mindig talál utat; kis hatékonyság	utolsó lépés tárolásával javítható
neurális hálós	ismeretlen	e: nem kell minden esetet számba venni, h: tanítás eredményét tesztelni kell; nem mindig talál utat	utolsó lépés tárolásával javítható
tapasztalatgyűjtő	ismeretlen	e: megismert környezetben hatékony lehet, h: nem mindig talál megoldást	saját módszer
hullám- továbbterjesztéses	ismert	e: ha van megoldás, megtalálja a legrövidebb utat, h: nagy memóriaigény	továbbfejlesztés: számítási szempontból növelt hatékonyság nyolcas szomszédság esetén
módosított hullám- továbbterjesztéses	ismeretlen	e: megtalálja a megoldást, h: nem globálisan optimális	saját eredmény
gráfbejáráson alapuló	ismert	h: jelentős számítási igény	
képfeldolgozás alapú	ismeretlen	e: valós idejű működés, h: fényviszonyokra érzékeny; lokális technika	saját eredmény

1. táblázat A vizsgált pályatervező algoritmusok összefoglalása

Módszert adtam robotnavigációnál alkalmazható akadálydetektálásra strukturális megvilágítást alkalmazó képfeldolgozás használatával. Szenzoradatok térképbe illesztésének más megközelítését is vizsgáltam. Ezen belül megadtam akadályok detektálásának és tárolásának egy tömörebb, vektoros reprezentációját, amely általános célú megvalósítást [12], akár több szenzor adatainak fúzióját is képes kezelni. Saját fejlesztésű, strukturális megvilágítást alkalmazó lézerszenzorral, ultrahangos érzékelővel [10] eredményesen teszteltem a rendszert (1. ábra).

A lézerszenzor működési elve a következő: a vetítő által kibocsátott lézersugár a megfigyelt testre vetül, majd arról az érzékelő egységbe érkezik. A strukturált megvilágítás módszere szerint a minta torzulásából következtetünk a tárgy távolságára és alakjára. Kalibrálás után egy adott célpontról visszaverődő csíkdarab helyzetéből a tárgy pont távolsága egyértelműen meghatározható.



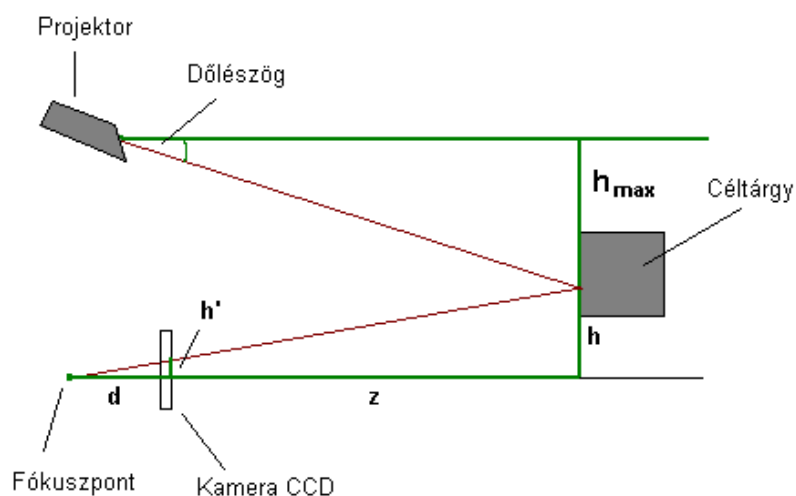
1. ábra. A rendszer felhasználói felülete. (lent) Inputkép lézermintával és nélküle lent; (fent) simított kép és a vektorizálás eredménye (elforgatva)

A mérési módszert szemlélteti a 2. ábra. Az ábrán d jelöli a fókusz távolságot (a CCD és a fókuszpont távolsága), z a tárgy fókuszponttól mért távolságát, h a lézercsík tényleges magasságát, h' a kameraképen érzékelhető magasságot és $h_{\max}$ a maximális magasságot. Hasonló háromszögekből:

$$d / h' = z / h, \quad (2)$$

amiből a kamera dőlésszögét (α) figyelembe véve kapjuk

$$z = \frac{d h_{\max}}{h' + d \tan \alpha}. \quad (3)$$



2. ábra. Strukturált megvilágításos mérés

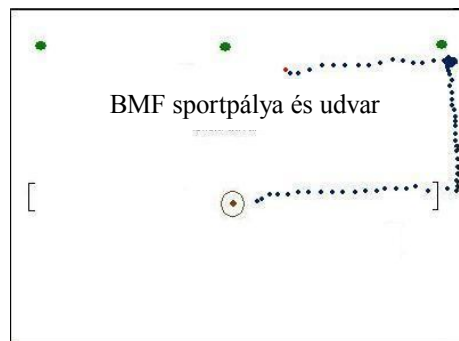
Kültéri navigációs eredmények

Kültéri környezetben a lokalizációs feladatra kifejlesztett megközelítéseket (GPS használatának lehetőségét, ismert környezetben az így kapott helyzetadatok pontosítási módszerét) és a térképkészítés, valamint lokalizáció körbelátás-alapú megoldását mutattam be. Eredményeim kültéri navigációval és körbelátás alapú térképkészítéssel kapcsolatban:

Megoldást adtam mobil robot kültéri durva lokalizációjára GPS használatával. Eljárást dolgoztam ki és valósítottam meg mobil robot kültéri lokalizációjának pontosítására ismert környezetben, körbelátó képek használatával.

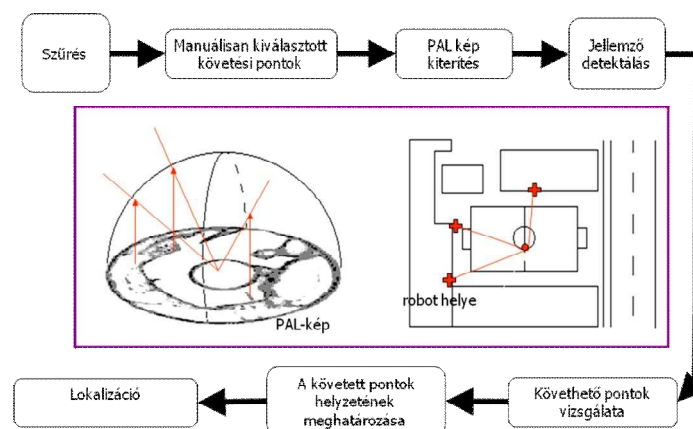
A látásalapú technikákat kültéri környezetben célszerű más szenzorok használatával kombinálni. Ezt alkalmazva GPS segítségével történő durva lokalizáció lehetőségét vizsgáltam a kifejlesztett rendszerben (3. ábra) [11], [13], [14].

Bemutattam, hogy ismert környezetet feltételezve, CCEXplorer robotunk [14] körbelátó kamerás kiegészítésével miként javítható a lokalizáció. A gyűrűs képen megjelenő jellemző pontok vizsgálatával és térgeometriai számítással a mobil robot helyzetét tovább pontosítottam a GPS segítségével mérhető értékek mintegy felére. A helyzetinformáció mellett a robot orientációját is származtattam a képből [9].



3. ábra. Navigációs rendszer tesztelése robottal [14] (Jelek: kézilabdakapuk: [, pálya közepe: karika, világítóoszlopok: 3 nagy pont a felső részen, útpontok: kisebb pontok)

A jellemző pontokat Harris-féle módszerrel, a jellemzők követését Lucas–Kanade-féle technikával oldottam meg (4. ábra). A lokalizáció a GPS-es értékeknek kevesebb, mint felére volt javítható annak függvényében, hogy a robot éppen milyen relatív helyzetet foglalt el az ismert pontokhoz képest.



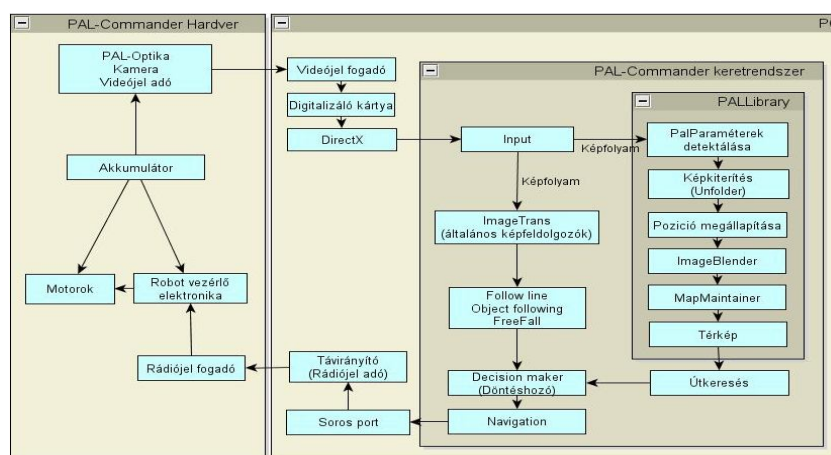
4. ábra. A lokalizáció főbb lépései és a tesztkörnyezet (a BMF korábbi telephelyének sportpályája) vázlata [9]

Mobil robotok navigálásának céljából eljárást dolgoztam ki és valósítottam meg topológiai és felülnézeti térképek létrehozására. Egy olyan PAL-optikával felszerelt mobil robot (5. ábra) megtervezését és kivitelezését mutattam be, amely autonóm navigációra képes [8]. Autonómián itt olyan feladatok önálló elvégzésére való képességet értek, mint vonalkövetés, akadálykerülés, és főként önálló helyzet-meghatározás, térképezés, illetve térkép alapján pálya bejárása.



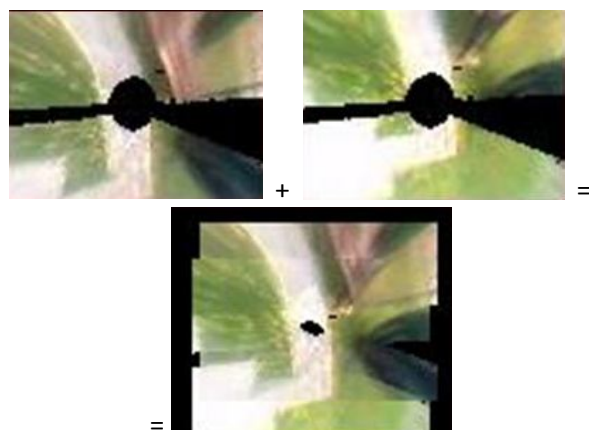
5. ábra. Modellautóból átalakított robot PAL-optikával: PALCOM

Az elkészített rendszer (6. ábra) főbb jellegzetessége, hogy az alapvető vonalkövetési, sávkövetési és objektumkövetési feladatokon túl, egy hibrid módszerrel, genetikus algoritmussal és hiba-visszaterjesztéses neurális háló segítségével képes feltérképezni a számára ismeretlen környezetet [2], [6], [7]. Ennek felhasználásával a robot képes a felhasználó által megadott célpozícióba ütközésmentesen eljutni.



6. ábra. A PALCOM-rendszer moduljai és kapcsolataik

A térképkészítés olyan virtuális felülnézeti képpé transzformálással kezdődik, amikor a gyűrűs kép központi részét úgy módosítom, hogy az eredetileg egyenes vonalakról készített kép egyenesnek is látszódjék. Az így kapott képrészeket un. blinding szűrő felhasználásával és az említett, betanított neurális háló segítségével ragasztom össze nagyobb rendszerré (7. ábra). Az útkeresés során a kapott térképen adaptív binarizálással határozom meg a szabad területeket és hullám-továbbterjesztéses algoritmussal határozom meg a célbajutáshoz szükséges pályát.



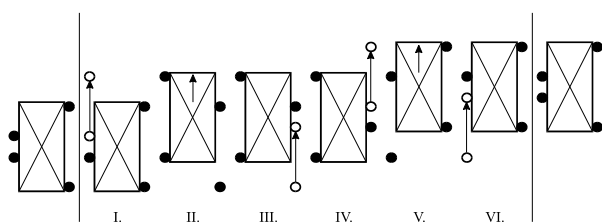
7. ábra. Virtuális felülnézeti képpé transzformált PAL-képek összeragasztása [2], [6]

Szakmaspecifikus eredmények

Ezután olyan szakmaspecifikus problémákra adtam választ, mint a lépegető robotok esetén alkalmazandó járási stratégia kialakításának metódusa, a mobil robotnavigációs és akadály-elkerülési problémájának gyakorlati megvalósítása, illetve az alkalmazott körbelátó kép minőségének és felbontásának érdemi javítása, hogy minél több részletet figyelembe lehessen venni az előző feladatoknál. Szakmaspecifikus alkotásként megvalósított mobil robotok és navigációjuk terén elért eredmények:

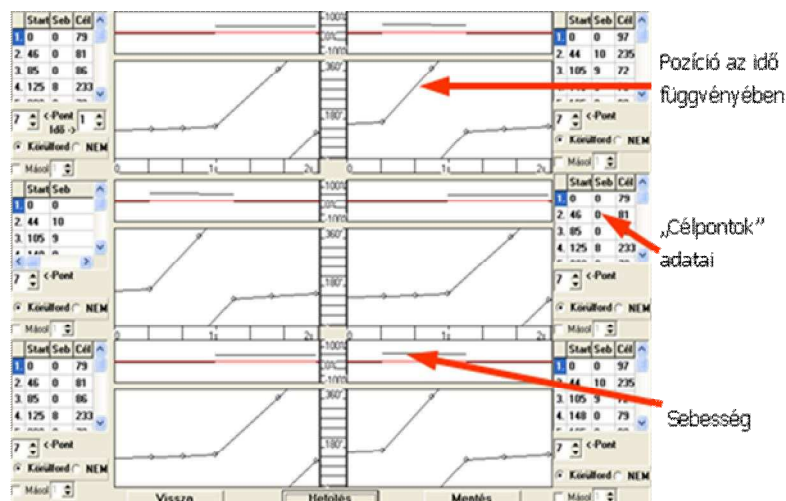
Saját készítésű négy lábú és hat lábú robotokon járási stratégiákat vizsgáltam és mozgásszerkesztő szoftvereszközt készítettem járási algoritmusok kialakításához. Lépegető robotok esetén az egyik alapvető feladat, a megfelelően összehangolt, stabil járási stratégia kialakításának vizsgálata. Négy lábú mobil robot esetén statikus stabilitást nyújtó mozgássorozatot készítettem előre- és hátrafele haladáshoz, forduláshoz, valamint oldalra lépéshez, majd gyorsabb mozgás érdekében olyan változatot is kifejlesztettem, amikor maga a haladás dinamikusan stabilizál [3], [19], [21].

A példa (8. ábra) az előrelépés fázisait szemlélteti. A kitöltött körök (●) azokat a lábakat jelképezik, amelyek éppen érintkeznek a talajjal, tehát alátámasztási pontok, az üres körök (○) pedig a felemelt lábakat ábrázolják. A nyilak a lábak, illetve a test mozgását jelölik.

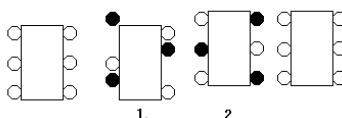


8. ábra. Előrelépés stratégiája [21]

A FOBOT hat lábú robot lábai forgómozgást végeznek és azokat kellett megfelelően szinkronizálni a haladás érdekében. A hatékony ütemezés céljából mozgásszerkesztő programot fejlesztettem ki (9. ábra), amely sikeres szimulációs ellenőrzés után a robotnak elküldi a megfelelően beállított és időzített utasításszekvenciát. A lábak mozgatása tesztelhető egyenként, vagy összehangoltan. Ez utóbbi esetben lehetőség van járási stratégiák kialakítására – tripod (10. ábra), quadropod, „hernyó” mozgások készültek el –, továbbá a pozíciók változásának számszerű és grafikusán ábrázolt megjelenítésére és figyelemmel kísérésére [14].

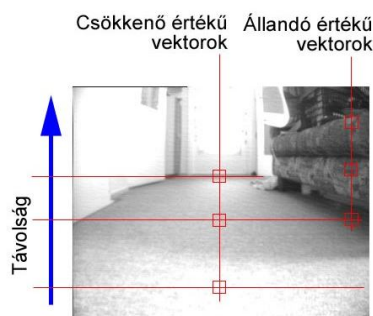


9. ábra. Járásszerkesztő



10. ábra. Tripod lépés

Az elkészített guruló mobil robotok és kifejlesztett navigációs rendszereik közül a CCExplorer modellautó alapú rendszert ismertettem részletesebben [15]. A robot optikai folyamatok vizsgálatával detektálta az előtte lévő munkakörnyezetet (11. ábra), GPS használatával lokalizálta pozícióját és később körbelátó optikás kép segítségével pontosította azt ismert környezetben [9].



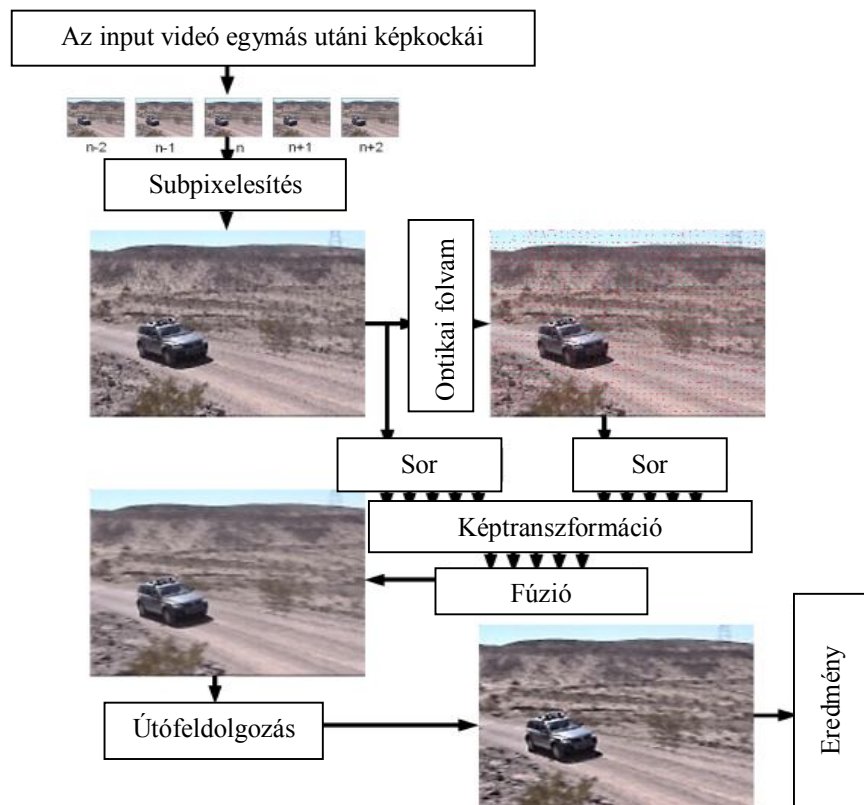
11. ábra. Mélységadatok számításának elve kétdimenziós kép alapján

Saját megvalósítású roboton keresztül megmutattam a PAL-optika és a körbelátó szenzorok képének minőségi javítását és így összetett navigálási feladatokban történő alkalmazhatóság hatékonyabb lehetőségét. Azt vizsgáltam, hogy miként lehet a PAL-optikás képsorozatok minőségét, részletgazdagságát javítani a super-resolution technikával. Kihasználva ezt a lehetőséget, tovább pontosíthatjuk az egyébként egyszerűen kinyerhető helyzet- és irányadatokat, ezáltal mobil robotikában még precízebb térképeket, vagy akadályhelyzeteket határozhatunk meg. Különböző optikai folyamat technikákat implementáltam és hasonlítottam össze a minőségjavítás szempontjából [5]. A kifejlesztett super-resolution rendszer tetszőleges videószekvenciát képes feldolgozni és PAL-képek esetén részletgazdag körbelátó képsorozatokot készít [1].

ÖSSZEGZÉS, KONKLÚZIÓ

A kilencvenes évek közepétől több mobil robotot készítettem – a kutatásokba bevont hallgatók segítségével –, melyek majd mindegyike más szenzorok mellett, hagyományos és körbelátó kamerákat is használt. A robotépítő tevékenység e területen elért megoldásait prezentálja a cikk három csoportra osztva: beltéri környezetben végzett navigáció és akadályelkerülés; kültéri környezetben lokalizáció pontosítása és térképkészítés; szakmaspecifikus alkotásként elkészített olyan rendszerek, mint lépegető robotok járási stratégiájának megvalósítása és körbelátó szenzorok képének minőségi javítása.

Beltéri környezetben a mobil robotok különböző szenzorok, illetve PAL-optika használatával történő navigációjához, akadály-elkerüléséhez pályatervezési algoritmusokat valósítottam meg és hasonlítottam össze foglaltsági hálós térkép-reprezentáció esetében. Rámutattam az egyes technikák (szabályrendszer alapú, neurális hálózattal támogatott, tanulásra képes, potenciálmezővel kalkuláló és gráfbejáráson alapuló pályatervezési módszerek) használhatóságára, előnyös, valamint részben a reprezentációból és a nagy memóriaigényű megvalósításból adódó hátrányos oldalaira. Az akadály-elkerülési feladat kiegészítéseként, képfeldolgozás alapú eljárást fejlesztettem ki négy lábú lépegető mobil robot lábkörnyezetének valós idejű vizsgálatára PAL optika használatával.



12. ábra. Az implementált rendszer működésének sematikus ábrája [5]

Szenzoradatok térképbe illesztésének más megközelítését is vizsgáltam. Ezen belül megadtam akadályok detektálásának és tárolásának egy tömörebb, vektoros reprezentációját, amely általános célú megvalósítást, akár több szenzor adatainak fúzióját is képes kezelni. Saját fejlesztésű, strukturális megvilágítást alkalmazó lézerszenzorral, ultrahangos érzékelővel teszteltem a rendszert.

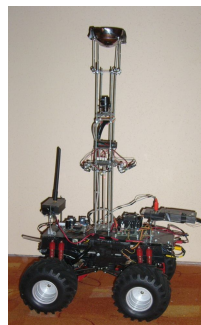
Kültéri környezetben a lokalizációs feladatra kifejlesztett megközelítéseket (GPS használatának lehetőségét, ismert környezetben az így kapott helyzetadatok pontosítási módszerét) és a térképkészítés, valamint lokalizáció körbelátás-alapú megoldását mutattam

be. A gyűrűs képen megjelenő jellemző pontok vizsgálatával és térgeometriai számítással a mobil robot helyzetét tovább pontosítottam a GPS segítségével mérhető értékek mintegy felére. A helyzetinformáció mellett a robot orientációját is származtattam a képből. Mobil robotok navigálásának céljából eljárást dolgoztam ki és valósítottam meg topológiai és felülnézeti térképek létrehozására. Egy olyan PAL-optikával felszerelt mobil robot megtervezését és kivitelezését mutattam be, amely autonóm navigációra képes. Az elkészített rendszer főbb jellegzetessége, hogy hibrid módszerrel, genetikus algoritmussal és hiba-visszaterjesztéses neurális háló segítségével képes feltérképezni a számára ismeretlen környezetet.

A térképkészítés olyan virtuális felülnézeti képpé transzformálással történik, amikor a gyűrűs kép központi részét úgy módosítom, hogy az eredetileg egyenes vonalakról készített kép egyenesnek is látszódjék. Az így kapott képrészeket ún. blending szűrő felhasználásával és az említett, betanított neurális háló segítségével ragasztom össze nagyobb rendszerre. E térkép felhasználásával a robot képes a felhasználó által megadott célpozícióba ütközésmentesen eljutni.

Ezután olyan szakmaspecifikus problémákra adtam választ, mint a lépegető robotok esetén alkalmazandó járási stratégia kialakításának módszere, a mobil robot navigációs és akadály-elkerülési problémájának gyakorlati megvalósítása, illetve az alkalmazott körbelátó kép minőségének és felbontásának érdemi javítása, hogy minél több részletet figyelembe lehessen venni az előző feladatoknál. Saját készítésű négy lábú és hat lábú robotokon járási stratégiákat vizsgáltam és mozgásszerkesztő szoftvereszközt készítettem járási algoritmusok kialakításához.

Saját megvalósítású roboton keresztül megmutattam a PAL-optika és a körbelátó szenzorok képének minőségi javítását és így összetett navigálási feladatokban történő alkalmazhatóság hatékonyabb lehetőségét. Azt vizsgáltam, hogy miként lehet a PAL-optikás képsorozatok minőségét, részletgazdagságát javítani a super-resolution technikával. Különböző optikai folyam technikákat implementáltam és hasonlítottam össze a minőségjavítás szempontjából. A kifejlesztett super-resolution rendszer tetszőleges videószekvenciát képes feldolgozni és PAL-képek esetén részletgazdag körbelátó képsorozatokot készít.



13. ábra. CCEXplorer első verziója előrenéző kamerával és a körbelátó rendszerrel

Az elért eredmények nemcsak a bemutatott kutatási feladatokban hasznosíthatók, hanem némelyik általánosabb megoldást is eredményezett. A lépegető robot hasára szerelt PAL-optikához készített képfeldolgozási rendszer olyan eljárásgyűjtemény, amely minimális továbbfejlesztéssel akár biztonsági szoftverként is funkcionálhat. A kamera mennyezetre helyezésével nagyobb környezet változása is egyszerűen vizsgálható. A kifejlesztett GPS-es rendszert járművekkel is sikerült tesztelni és az eredmény helyesen jelent meg a térképen. A super-resolution technikát megvalósító rendszer általános megoldást prezentál, így

kisfelbontású képsorozatot (pl. TV esetén) képes a mostani elvárásoknak eleget tévő nagyobb felbontásúra (HD minőségűre) alakítani.

Ezúttal is szeretném kifejezni kiemelt hálámát és tiszteletemet Greguss Pál professzor úrnak, aki körbelátó optikájával, és főként értékes meglátásaival, ötleteivel segítette kutatásaimat.

Felhasznált irodalom

- [1] Nagy, A., Vámosy, Z., „Super-resolution for Traditional and Omnidirectional Image Sequences”, Acta Polytechnica Hungarica, Vol. 6/1, Budapest Tech, 2009. pp. 117–130, ISSN 1785 8860
- [2] Vámosy, Z., „Map Building and Localization of a Robot Using Omnidirectional Image Sequences”, Acta Polytechnica Hungarica, Vol. 4/3, Budapest Tech, 2007. pp. 103–112, ISSN 1785 8860
- [3] Vámosy, Z., Molnár, A., „Exploratores, négy lábú lépegető robot készítése”, Híradástechnika (50th years of the Telecommunications Sci. Soc.), Vol. L. no. 9, 1999/9, pp. 50–76. ISSN 0018–2028
- [4] Vámosy, Z., Csink, L., Schröder, J., Okulan, N., Katzer, I., Molnár, F., Szabó, E., „Recognition Based Object Classifying System in Robot Environment”, Annales Univ. Sci. Budapest., Sect. Comp. Vol. 17, 1998. pp. 405–416., ISSN 0138–9491
- [5] Nagy, A., Vámosy, Z., „OpenCV C# Wrapper Based Video Enhancement Using Different Optical Flow Methods in the Super-Resolution” In: Proc. of 6th International Symposium on Intelligent Systems and Informatics, Subotica, Serbia, September 26–27, 2008, ISBN 978-1-4244-2407-8
- [6] Vámosy, Z., „Topological Map Building from PAL Images with Navigation Purpose”, in Proc. 6th International Symposium on Applied Machine Intelligence and Informatics, Herl'any, Slovakia 2008, pp. 217–220., ISBN 978-1-4244-2106-0, IEEE C. N.: CFP0808E-CDR
- [7] Vámosy, Z., „Map Building and Localization of a Robot Using Omnidirectional Image Sequences”, in. Proc. 4th International Symposium on Applied Computational Intelligence and Informatics, SACI 2007, Timisoara, Romania, 2007, pp. 191–194., ISBN: 1-4244-1234-X, IEEE C. N. 07EX1788
- [8] Mornailla, L., Pekár, T. G., Solymosi, Cs. G., Vámosy, Z., „Mobile Robot Navigation Using Omnidirectional Vision”, in Proc. 15th International Workshop on Robotics in Alpe-Adria-Danube Region, June 15–17, 2006, Balatonfüred, Hungary, CD, ISBN 963 7154 48 5
- [9] Vámosy, Z., Tóth, Á., Hirschberg, P., „PAL Based Localization Using Pyramidal Lucas-Kanade Feature Tracker,” in. Proc. 2nd Serbian-Hungarian Joint Symposium on Intelligent Systems, Subotica, Serbia and Montenegro, 2004, pp. 223–231.
- [10] Vámosy, Z., Fekete, B., Nyitrai, L., Molnár, A., „Ultrasonic Based Device for Blind and Visually Impaired People”, in. Proc. 13th International Workshop on Robotics in Alpe-Adria-Danube Region, Brno, Slovakia, 2004, pp. 405–407. ISBN 80-7204-341-2

- [11] Molnár, A., Vámosy, Z., „Navigation of a GPS Based Robot Vehicle”, in. Proc.13th International Workshop on Robotics in Alpe-Adria-Danube Region, Brno, Slovakia, 2004, pp. 408–413. ISBN 80-7204-341-2
- [12] Vámosy, Z., Kladek, D., Fazekas, L., „Environment Mapping with Laser-based and Other Sensors”, in. Proc. IEEE International Workshop on Robot Sensing, ROSE 2004, Graz, 2004, pp. 74–78. ISBN: 0-7803-8297-8
- [13] Vámosy, Z., „Navigation with a Six-legged Mobile Robot”, in Proc. of the 3rd International Mechatronics Symposium, in Memoriam Pál Greguss, Budapest, Hungary, 2003, (CD issue) ISBN 963-7154-22-1
- [14] Vámosy, Z., Molnár, A., Balázs, A., Pécskai, B., Supola, B., „FOBOT, the Hexapod Walking Robot”, in. Proc. 35th International Symposium on Robotics (IFR), Paris-Nord Villepinte, 23–26. March 2004, abstract: pp. 15–16, (CD issue)
- [15] Vámosy, Z., Molnár, A., Hirschberg, P., Tóth, Á., Máthé, B., „Mobile Robot Navigation Projects at BMF NIK”, in. Proc. International Conference in Memoriam John von Neumann, Budapest, December 12, 2003, pp. 209–219.
- [16] Molnár, A., Vámosy, Z., „Navigation of Mobile Robot Using PAL Optic”, in Proc. 10th International Conference on Advanced Robotics ICAR 2001, Workshop on Omnidirectional Vision, Budapest, 22–25 Aug. 2001, pp. 89–92.
- [17] Vámosy, Z., Molnár, A., „Obstacle Avoidance for a CLAWAR Machine”, in Proc. of 2nd International Symposium on Climbing and Walking Robots – CLAWAR’99, Portsmouth, Professional Engineering Publishing Limited, London, 1999, pp. 597–603.
- [18] Vámosy, Z., Novák, A., Horváth, M., „I. Henrik Wheeled Mobile Robot - Optimal Path Planning and Tracking Based on Visual Information”, in. Proc. 8th International Workshop on Robotics – RAAD’99, Munich, Germany, 1999, pp. 171–176.
- [19] Vámosy, Z., Molnár, A., Brünner, R., Varga, L., „EXPLORADORES II., the Four-Legged Mobile Robot”, in. Proc. International Symposium on Climbing and Walking Robots – CLAWAR’98, Brussel, Belgium, 1998, BSMEE. pp. 41–45.
- [20] Vámosy, Z., Molnár, A., Brünner, R., Varga, L., „Path Planning Methods for a Quadruped Mobile Robot”, in. Proc. DAAAM’98, Cluj-Napoca, Romania, DAAAM International, Wien, Austria, 1998, pp. 483–484.
- [21] Brünner, R., Molnár, A., Varga, L., Vámosy, Z., „Exploradores, Quadruped Robot”, in. Proc. 7th International Workshop on Robotics in Alpe-Adria-Danube Region - RAAD’98, Bratislava, Slovakia, 1998, Slovak Academy of Sciences, pp. 215–220.
- [22] Vámosy, Z., „Recognition of Moving Objects with Varying Methods”, in. Proc. Fifth International Workshop on Robotics in Alpe-Adria-Danube Region – RAAD’96, HRA, Budapest, 1996, pp. 361–366.
- [23] Vámosy, Z., Vargha, Zs., Hangyási, T., „Vision Based Path Planning with Neural Networks”, in. Proc. Fifth International Workshop on Robotics in Alpe-Adria-Danube Region – RAAD’96, HRA, Budapest, pp. 535–538.
- [24] Vámosy, Z., Csink, L., Schröder, J., Okulan, N., Katzer, I., Molnár, F., Szabó, E., „Recognition Based Object Classifying System in Robot Environment”, in. Proc. Fourth Symposium on Programming Languages and Software Tools, Visegrád, 1995, pp. 418–426.

- [25] C. Mei, P. Rives, "Single view point omnidirectional camera calibration from planar grids". In Proc. ICRA, 2007 pp. 3945–3950.
- [26] Greguss, P., "Panoramic imaging block for 3D space", US patent 4,566,763, January 1986, Hungarian Patent granted in 1983.
- [27] R. A. Brooks, "Intelligence Without Representation", Artificial Intelligence Vol. 47 1991 pp.139–159.
- [28] J. J. Gibson, "Ecological Optics", Vision Research, 1961, I., pp. 253–62.
- [29] D. Marr, Vision. Freeman Publishers, San Francisco, 1982.
- [30] R. Wehner and S. Wehner, "Insect navigation: use of maps or Ariadne's thread?", Ethology, Ecology, Evolution 2, 1990) pp. 27–48.
- [31] B. Horn, B. Schunck, "Determining optical flow", In Artificial Intelligence, vol. 17, 1981/2, pp. 185–204.
- [32] G. Bradsky, A. Kaebler, Learning OpenCV, O'Reilly, 2008, Intel, Open Source Computer Vision Library, <http://www.intel.com/technology/computing/opencv>, látogatva: 2008-08-12
- [33] B. Lucas, T. Kanade, „An Iterative Image Registration Technique with an Application to Stereo Vision”, in Proc. 7th International Joint Conference on Artificial Intelligence (IJCAI), 1981, pp. 674–679.
- [34] Y. M. Chi, T. D. Tran, R. Etienne-Cummings, „Optical Flow Approximation of Sub-Pixel Accurate Block Matching for Video Coding”, In. Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2007), vol. 1, April 2007 pp. 1017–1020.
- [35] Vörös, G., Bevezetés a Neurális számítástechnikába, LSI Oktatóközpont, Budapest, 1997.

Varga Péter

varga.peter@kvk.bmf.hu

Illési Zsolt

illesi.zsolt@proteus.hu

KRITIKUS INFRASTRUKTÚRÁK HATÁS ALAPÚ MODELLEZÉSE

Absztrakt

A gazdaság dinamikus fejlődéséhez nagyban hozzájárult az informatika és a telekommunikáció térhódítása. Már nem tudunk elképzelni olyan modern munkaállomást, ahol a dolgozó munkáját valamilyen technikai vívmány ne segítené. Nincs ez máshogyan a kritikus infrastruktúrákban sem. A fenyegetések minimalizálására több módszer alkalmazható. Ezek közé tartozik a kockázatelemzés, mely valószínűségi számításokat, matematikai logikát, kvantitatív, kvalitatív módszerek tartalmazhat. A technika és az általa nyújtott szolgáltatás nem csak az adott infrastruktúrát hálózza be, hanem az infrastruktúra nyújtotta szolgáltatásai révén szoros kapcsolatban (függésben) van más infrastruktúrákkal is. A kritikus infrastruktúrák közötti függéseket, illetve egy kritikus infrastruktúrán belüli függéseket azonban ezek a modellek nem, vagy csak nagyon áttételesen érintik. Ezért cikkünkben egy olyan rendszerszemléletű modellt alkotunk meg, amely alkalmas az inter- és intradependenciák modellezésére, a függőségek tartalmának feltérképezésére.

The penetration of information technology and telecommunication contributed considerably to the dynamic development of the economy. An up to date workstation is unthinkable without technologically advanced tools helping the workers. This is the same in the critical infrastructure domain. There are multiple ways to minimise threats. One of this methods is risk assessment, which utilises probability calculations, mathematical logic, qualitative and quantitative technique. Technology and the provided services not only spreading through a given infrastructure, but via the services provided by the infrastructure it is in close links (dependence) with other infrastructures. The interdependence between critical infrastructures and internal dependencies within a critical infrastructure in these models are not included, or only superficially exposed. Therefore we are suggesting a system approach model which is applicable to prototyping inter- and intradependencies and mapping the background of dependencies.

Kulcsszavak: kritikus infrastruktúra (KI), hatás alapú modellezés, KI interdependencia, KI intradependencia ~ critical Infrastructure (CI), effect-based modelling, CI interdependence, CI intradependence

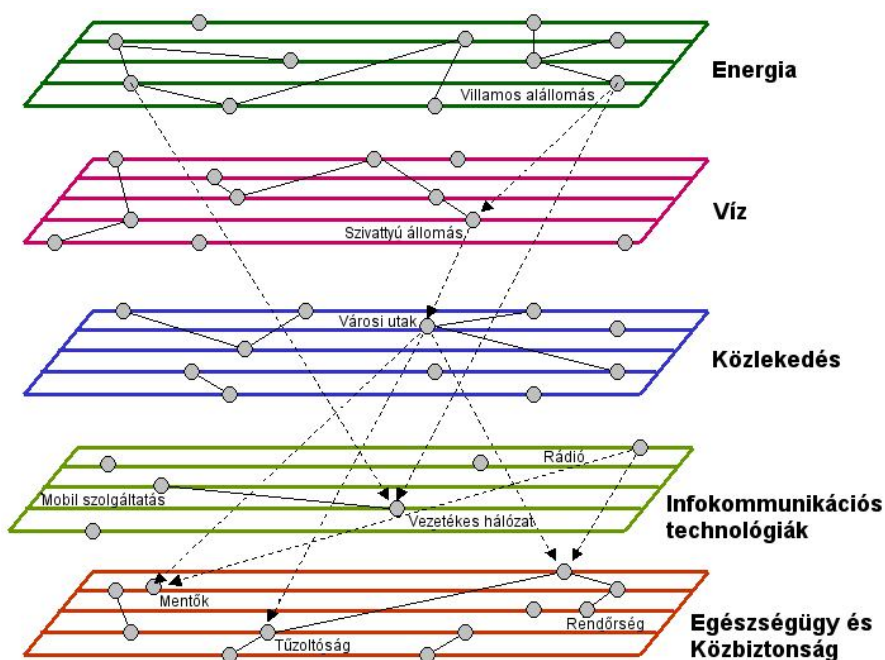
BEVEZETÉS

Az infokommunikáció térnyerése egyre nyilvánvalóbbá tette az infokommunikációs technológiák és ezzel párhuzamosan a természet- és társadalomtudományok fejlődését. A társadalomban és a gazdasági életben is egyre elterjedtebb az informatika, a telekommunikáció. A gyorsabb, intenzívebb változások megnövelték a társadalom technológiai függését, növekedtek a változásokban rejlő lehetőségek és potenciális veszélyek is. [6]

A kritikus infrastruktúrák (KI) és ezen belül a kritikus információs infrastruktúrák (KII) azonosítása, priorizálása, a veszélyeik és sérülékenységeik felmérése, a védelmi terveik meghatározása és kialakítása egyre égetőbb kérdés, és számos országban – így hazánkban is – komoly kihívást jelent.

A KI védelmének kialakításakor a kockázatok felmérésének egyik lényeges pontja a KI-KI interdependenciák (kölsönös függőség), és az egyes KI-ken belüli intradependenciák (belső rendszerelemtől való függőség) feltárása, valamint a függőség jellegének és tartalmának feltárása, hiszen ezek kezelése csak megfelelő előismeretek birtokában teszi az inter- és intradependenciát csökkentő védelmet teljes körűvé, zárttá és kockázatarányossá.

A kritikus infrastruktúrák védelmi képességeinek beazonosításakor nem minden esetben történik meg az inter- és intradependencia totális feltérképezése. Nem könnyű ezt a feladatot elvégezni, mert a modellezés során figyelembe kell venni a különböző szervezeteket, rendszereket és alrendszereket, illetve ezek kölsönös kapcsolatrendszerét. A modellezés az az első lépés, amellyel közelebb kerülhetünk a helyes megoldáshoz. Az 1. ábra New Orleans KI ágazatait és az alágazatok közti kapcsolatokat mutatja be:



1. ábra. New Orleans infrastruktúra interdependenciái [4: p 3.]

A Katrina hurrikán megmutatta, hogy az összekapcsolódó infrastruktúrákon keresztül a problémák felhalmozódhatnak, váratlanabb és lényegesen súlyosabb működésbeli zavart

okozhatnak az adott állam létfontosságú szolgáltatásaiban. Az infrastruktúrák összekapcsolódásai, és egymástól való függőségei sérülékenyebbé teszi őket támadások, zavarok, megsemmisítésre irányuló tevékenységekkel szemben. Például az energiatermelés függ a szállítástól. A szállítás függ az energiától. Mindkettő függ az infokommunikációs rendszerektől, míg az infokommunikációs rendszerek energiafüggők. [3]

A kritikus infrastruktúrák védelme elsődleges szempont minden nemzet számára. Ma Magyarországon a Zöld Könyv alapján a nemzeti kritikus infrastruktúra védelem végrehajtásának lépései a következők:

- fogalmak tisztázása, keretrendszer alapjainak meghatározása;
- szektorelemzés, ágazati fogalmak, kritériumok meghatározása;
- kölcsönös függőség (interdependencia elemzés);
- kockázat, veszély, és sebezhetőség elemzés;
- védelmi intézkedések megtétele;
- végrehajtás ellenőrzése és értékelés. [1]

Ebből a felsorolásból is jól látszik, hogy a kölcsönös függőségek elemzése, fontos pillére az infrastruktúrák védelmének. Az inter- és intradependenciák hatékony és eredményes feltárásához, értékeléséhez azonban rendszerszemléletű modell megalkotása szükséges.

Jelen cikkünkben egy ilyen lehetséges modellt szeretnénk felvázolni, azonosítva a KI függőségi rendszer modellezéséhez szükséges főbb paramétereket. A célunk továbbá az, hogy a KI függőségei modell és a kockázatelemzési modell közös illetve eltérő sajátosságaira is rávilágítsunk.

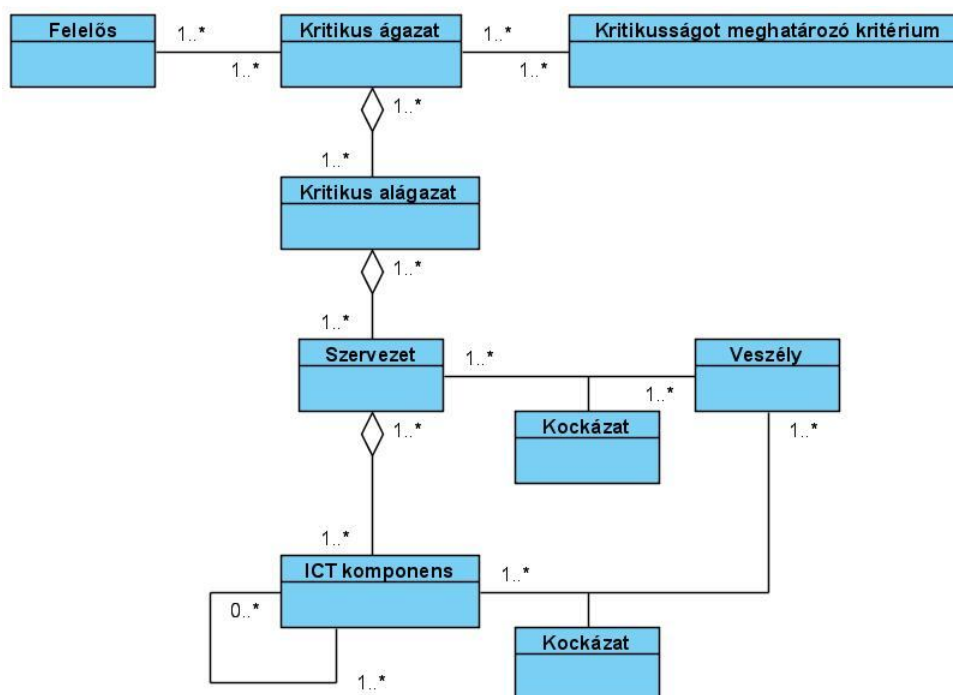
KRITIKUS INFRASTRUKTÚRA FÜGGŐSÉGÉNEK MODELL ELEMEI

A KI-KI függőségi modellben szerepelni kell a KI hierarchiának, vagyis a nemzetközi, nemzeti, EU KI elemeknek, továbbá azonosítania kell az egyedi KI szervezeteket, kapcsolódnia kell a 2080/2008. (VI. 30.) Korm. határozatban felvázolt kritikus ágazatalággaztat struktúrához. (2.ábra)

A modellnek továbbá tartalmaznia kell az egyes KI szervezeteknek a kritikusságát meghatározó kritériumokat, vagyis egy KI elvesztésének a

- hatókörét;
- nagyságrendjét és
- időbeni hatását.

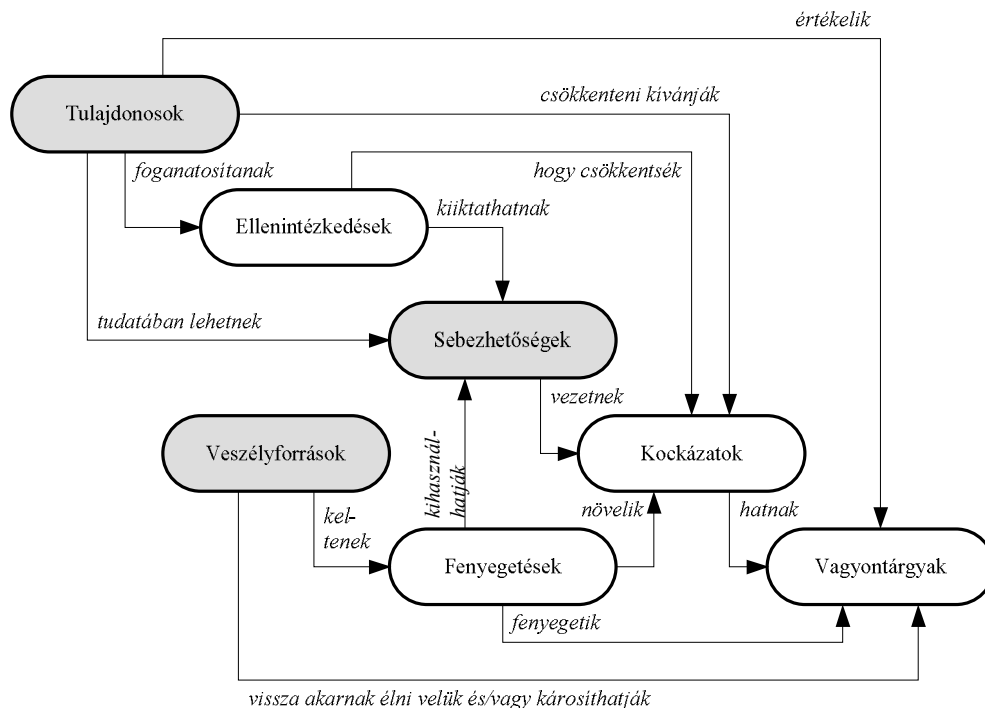
A hatókörnél meg kell vizsgálni, hogy a kritikus infrastruktúra, vagy annak részének elvesztése, elérhetetlensége milyen földrajzi kiterjedésben okoz károkat az állampolgárok gazdasági-, szociális jóléte, a közegészség, a közbiztonság, a nemzetbiztonság, a nemzetgazdaság és a kormányzat működése szempontjából. A nagyságrendnél meg kell vizsgálni, hogy a kritikus infrastruktúra vagy annak részének elvesztése, elérhetetlensége milyen mértékű hatást okoz. Az időbeni hatásnál pedig meg kell vizsgálni, hogy a kritikus infrastruktúra vagy annak részének elvesztése, elérhetetlensége milyen időtávon mennyi ideig befolyásolja az infrastruktúra újbóli működését. [1]



2. ábra. KI hierarchia modell struktúra UML objektum diagrammja
[Szerkesztették a szerzők]

A KI inter- és intradependenciáinak értékelése nem egy-egy gazdasági szervezet szintjén jelentkezik, és nem csak valamely állami szerv feladata, hanem össznemzeti védelmi feladat, ahol az államigazgatás, a nemzetvédelmi és az érintett gazdasági szervezetek hatékony és eredményes együttműködésével lehet teljeskörű, zárt és kockázatarányos védelmet kialakítani. Ennek a feltételnek a teljesítése miatt a modellnek lehetővé kell tennie a top-down elemzést (pl. a KI azonosítást és prioritizálását) és a bottom-up tervezést (pl. az egyes KI elemek függőségeinek vizsgálatát, kapcsolatainak azonosítását).

A kockázatelemzésben felhasználandó elemzendő-objektumokra és azok általános kapcsolataira „Az informatikai biztonságértékelés közös szempontjai” (Common Criteria) ad egy a gyakorlatban is tesztelt és használható modellt:



3. ábra. Kockázatelemzés fogalmi modellje
[5: p 12.]

A fenti koncepció modellből látható, hogy a szűken vett kockázatelemzéshez a

- vagyontárgy;
- fenyegető tényező;
- kockázat;
- sebezhetőség és
- ellenintézkedés

elem-ötös meghatározása és értékelése szükséges.

A fenti ábrából az is jól látható, hogy a kockázatelemzést egy-egy vagyontárgy-fenyegetés párosra kell elvégezni, általánosságban (konkrét védendő érték hiányában) nincs értelme elemzésről beszélni. A modell alapján kimondható az is, hogy egy eredményes kockázatelemzéshez részletes erőforrás leltárra van szükség, illetve célszerű mind a veszélyforrások, mind az alkalmazott védelmi intézkedések listáját is törzsadatbázis elemként felvenni.

Jelen dolgozatunkban azonban – mivel a célunk nem a KI kockázatelemzés modellezése – a továbbiakban csak a KI függőséget közvetlenül befolyásoló kérdésekkel foglalkozunk.

Modellezési szintek

Az elemzés szempontjából megállapítható, hogy a függőségeket legpontosabban az egyes erőforrás-erőforrás kapcsolatok esetében lehet a legpontosabban modellezni, tényadatokat is ilyen szinten lehet begyűjteni, illetve szakértői becsléseket is az egyes rendszerelem kapcsolatok szintjén lehet végezni.

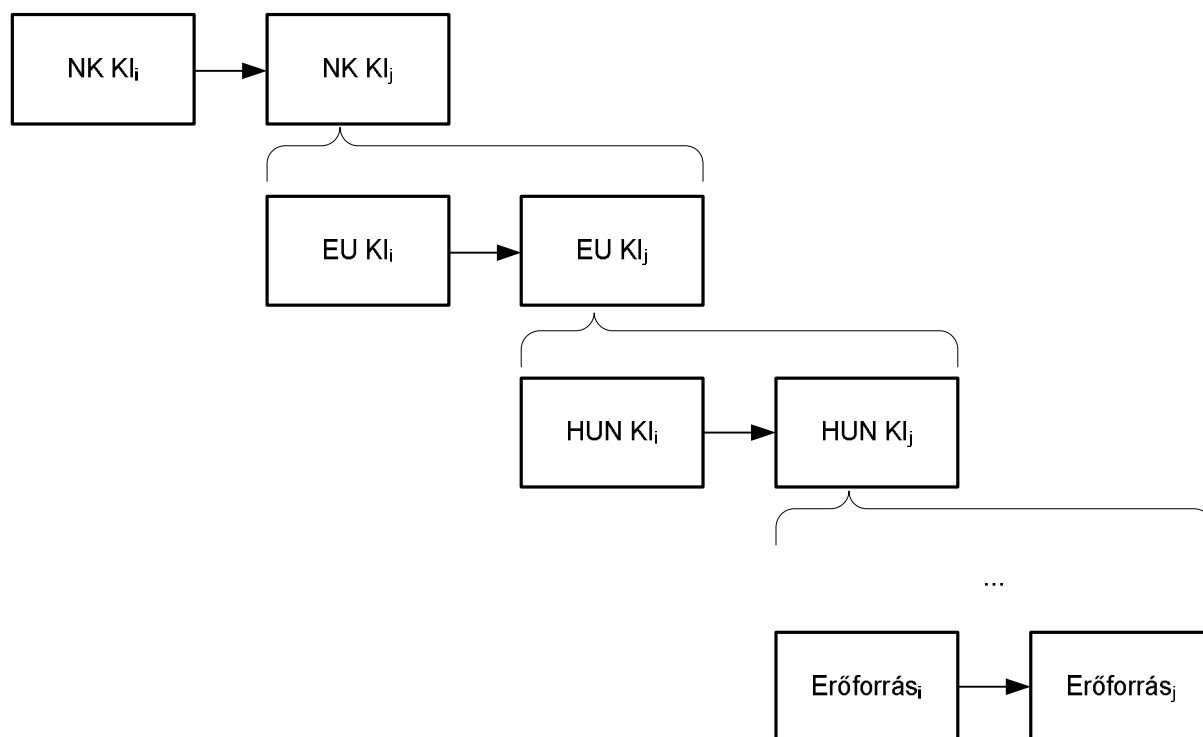
Modellezési szempontból fontos kérdés az is, hogy miként kezelhető egységes szemléletben a makro és mikro hierarchia, vagyis miként lehet azonos modell elemekkel leírni

a nemzetközi KI-KI dependenciákat, valamint egy szervezet erőforrásainak szintjén fellépő erőforrás-erőforrás dependenciákat.

A megoldáshoz az ötletet a virtuális vállalat (virtual business) koncepciója adta. [2] Ez egy olyan modellezési felfogás, amelyben egy szervezet a vele szoros kapcsolatban lévő más szervezetekkel együtt egy olyan egységet alkot, amelynek a belső kapcsolatrendszere (inter- és intradependenciái) egy külső szemlélő számára nem láthatók, az így kialakult organizáció egységes fellépése és működése helyettesíthető (és modellezhető) egy szervezettel, a tagszervezetek együtteséből felépített virtuális vállalattal.

Ilyen virtuális szervezetet alkot például az autógyár a beszállítóival együtt, ahol az együttműködés szoros keretei a JIT (just in time) módszertanra épülnek, vagy egy bank az összes kiszervezett funkciót ellátó szervezettel együtt.

Ilyen megközelítésben az egyes erőforrás kapcsolatokból felépíthető egy rendszer modellje, a rendszerek kapcsolataiból felépíthető egy szervezet, a szervezetekből felépíthető egy KI ágazat, az ágazatokból egy KI ágazat, illetve az ágazatokból, ágazatokból egy nemzeti, EU és nemzetközi KI is. Ezt a megközelítést szemlélteti a 4. ábra is.



Ahol:

NK KI – Nemzetközi kritikus infrastruktúra

EU KI – Európai Unió kritikus infrastruktúra

HUN KI- Magyarországi/Nemzeti kritikus infrastruktúra

i., j – különböző infrastruktúrák, szervezetek, erőforrások, stb.

4. ábra. KI hierarchia, mint virtuális szervezetek kapcsolata
[Szerkesztették a szerzők]

Intradependencia – interdependencia

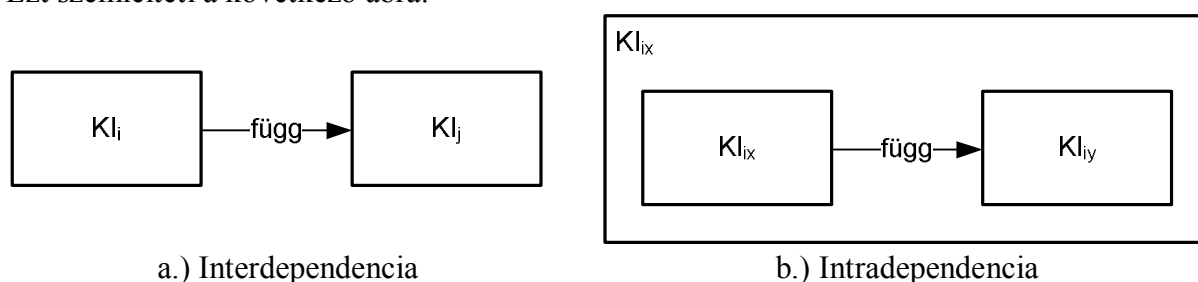
A szakirodalomban felmerül az inter- és intradependencia kérdése [3], amelyet modellezési szempontból is kezelni kell. Az interdependencia (a kölcsönös egymásra hatás) vizsgálata rendkívül fontos. Ennek során a vizsgált infrastruktúra más infrastruktúrákra gyakorolt

negatív hatását kell vizsgálni. Hangsúlyozni kell, hogy az interdependencia értékelése nagy fontossággal bír, mert ezek akár egy, akár több ágazat vagy alágazat bevonását illetve ezt követően együttes vizsgálatát követeli. A vizsgálat mennyiségi (kvantitatív) jellemzőkön alapul. [1]

Az interdependencia két KI közötti függést jelent (javasolt jelölése: $A \rightarrow B$, azaz „B” kritikus infrastruktúra elem függ „A” kritikus infrastruktúra elemtől). Az intradependencia egy adott KI önmagától való függését jelenti (javasolt jelölése: $A \rightarrow A$, azaz „A” kritikus infrastruktúra elem függ önmagától). Ez a függés rendszerint az „A” KI rendszernek saját belső al-KI rendszereinek függését jelenti.

Véleményünk szerint modellezési szempontból a KI rendszerek, alrendszerek közötti függés KI rendszerkomponensek közti függéseként értelmezhető és ábrázolható. Tehát a modell elemzési részlet finomításával az inter- és intradependencia ekvivalensként kezelhető, az intradependencia elhagyható, amit az 5. ábra b.) része szemléltet.

Ezt szemlélteti a következő ábra:



Ahol:

KI_i, KI_j – különböző kritikus infrastruktúrák

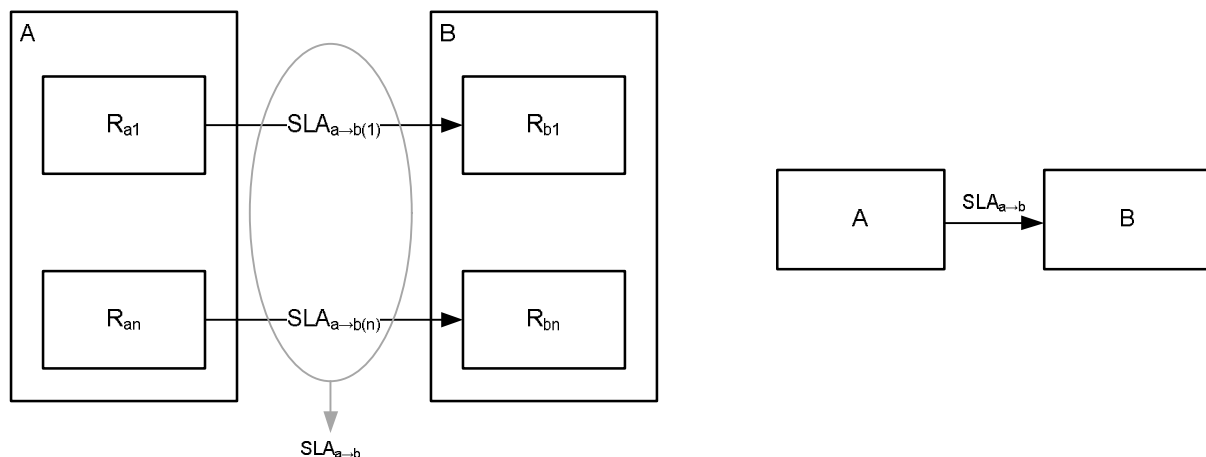
5. ábra. Inter és intradependencia helyettesítési modellje
[Szerkesztették a szerzők]

Függések modellezése

A KI-KI interdependencia vizsgálatának központi kérdése a függés. Ez a kapcsolat két rendszerelem között áll fenn, és mindkét irányból vizsgálható, egyrészt a függésben lévő rendszerelem, másrészt a függés alapjául szolgáló szolgáltatást nyújtó rendszerelem szempontjából.

Véleményünk szerint ez a függés modellezhető egy sajátos nyújtott-fogadott szolgáltatási szintmegállapodásként (SLA), amely azonban a rendelkezésre állással kapcsolatos metrikákat, valamint a szolgáltatás elmaradásának következményeit (hatás) tartalmazza. A szolgáltatás-alapú megközelítéssel kezelhető lenne az a probléma (is), hogy az alacsony modellezési szinten feltárt függőségeket egy magasabb elemzési szinten (szervezet-szervezet, alágazat-alágazat stb.) is értelmezni lehessen.

Javaslatunk alapján például egy szervezet-szervezet függőség felírható az igénybevevő szervezet számára szolgáltatást nyújtó alrendszerei szolgáltatásainak halmazaként (a két szervezet „szolgáltatási interfészén” keresztül nyújtott/fogadott szolgáltatások összegeként).



Ahol:

A,B – szervezetek

R_a, R_b – a szervezeteken belül szolgáltatást nyújtó alrendszerek

SLA – a rendszerek és/vagy szervezetek közötti nyújtott-fogadott szolgáltatási szintmegállapodások

6. ábra. KI szolgáltatási interfész egyedi függéseinek egyszerűsítése kumulált függéssel
[Szerkesztették a szerzők]

A függést leíró SLA javasolt tartalma „A kritikus információs infrastruktúrák meghatározásának módszertana” [1] alapján a következő:

	Alacsony	Közepes	Magas
Hatókör	0 1	0 1	0 1
Nagyságrend: a népességre gyakorolt hatás	0 1	0 1	0 1
Nagyságrend: a gazdasági hatás	0 1	0 1	0 1
Nagyságrend: interdependencia	0 1	0 1	0 1
Nagyságrend: politikai hatás	0 1	0 1	0 1
Időbeli hatás	0 1	0 1	0 1

7. ábra. KI SLA mátrix
[Szerkesztették a szerzők]

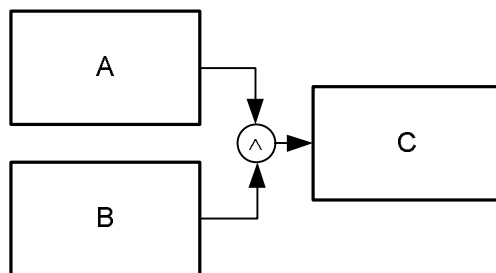
Hatás gráf felépítése

A valós életben a KI modellelemek kapcsolata rendszerint nem 1:1 típusú. Egy rendszerkomponens (pl. villamos hálózat) több más rendszerkomponens működéséhez nyújt alapvető szolgáltatást, illetve egy alkalmazás több egyéb rendszerkomponens működésétől függ (pl. az alkalmazást futtató hardvertől, operációsrendszertől, az adatokat szolgáltató adatbázis-kezelőtől, az ezek közti adatkapcsolathoz nélkülözhetetlen számítógépes hálózatoktól stb.).

A kapcsolatok n:m jellegének (azaz, hogy egy rendszerkomponenstől több más komponens is függhet, illetve, hogy egy rendszerkomponens több más komponenstől is függ) modellezéséhez hatás gráfok kialakítását javasoljuk (a támadási fákhoz hasonló szerkezetben), amelyek logikai kapcsolókkal fűzik össze az egyes rendszerelemek egymásra gyakorolt hatását. Az alapként szolgáló támadási fakkal szemben az így kialakított irányított háló (ahol az irányítást a nyújtott/fogadott szolgáltatás iránya adja meg) nem csak levél-

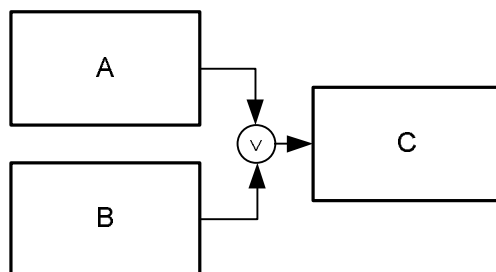
gyökér irányban járható be, hanem lehetséges valamennyi csomópont vizsgálata az abba vezető élek bejárásával.

A szolgáltatást igénybevevő rendszerkomponens funkcionalitásának, rendelkezésre állásának fenntartásához egymástól függetlenül is szükséges szolgáltatások esetére bevezettük az „és” kapcsolót, amelynek jelentése: „C” erőforrás működéséhez „A” és „B” erőforrások együttes szolgáltatása szükséges, bármelyikük kiesése „C” funkcionalitásának és rendelkezésre állásának sérülésével vagy megszűnésével jár együtt. Ezt a kapcsolatot szemlélteti a következő ábra:



8. ábra. „és” kapcsoló
[Szerkesztették a szerzők]

A szolgáltatást igénybevevő rendszerkomponens funkcionalitásának, rendelkezésre állásának fenntartásához egymást kiegészítő (redundáns) szolgáltatások esetére bevezettük a „vagy” kapcsolót, amelynek jelentése: „C” erőforrás működéséhez „A” vagy „B” erőforrások szolgáltatásai szükségesek, bármelyikük egyedüli kiesése nem jár együtt „C” funkcionalitásának és rendelkezésre állásának sérülésével. Ezt a kapcsolatot szemlélteti a következő ábra:



9. ábra. „vagy” kapcsoló
[Szerkesztették a szerzők]

Javaslatunk szerint a KI-KI rendszerelem kapcsolatok a formális logika, illetve a Fuzzy logika alapján kezelhetők, az irányított háló bejárásával. A háló bejárásával felderíthető, hogy egy adott rendszerelem mely más elemektől függ – tulajdonképpen az elemzés háló csomópontjai közti haladást jelenti a vizsgált elemtől visszafelé. A háló bejárásával azonosítható a függés tartalma és hatása, illetve áttételes függés esetén a függés „mélysége”, vagyis az, hogy hány élnyi távolságban van kritikus szolgáltatási elem az igénybevevőtől.

ÖSSZEFOGLALÁS

A kritikus infrastruktúrák, azok felmérése, kockázatelemzése napjaink egyik égető problémája. Az egyes KI ágazatok, alágazatok, szervezetek és egyedi eszközök, rendszerek kockázatelemzésének többféle módszertana létezik. Ezek lehetnek kvantitatív, kvalitatív módszerek, tartalmazhatnak több-kevesebb matematikai logikát, valószínűség számítást, lehetnek grafikusak, leíró jellegűek, egyszerűek, vagy bonyolultak. A KI-KI közötti függéseket, illetve egy KI-n belüli függéseket azonban ezek a modellek nem, vagy csak nagyon áttételesen kezelik.

Ennek a problémának a megoldására tettünk javaslatot a cikkünkben: egy olyan rendszerszemléletű modellt alkottunk meg, amely reményeink szerint alkalmas az inter- és intradependenciák modellezésére, a függőségek tartalmának feltérképezésére mind makro szinten (pl. KI ágazati vagy alágazati szinten), mind mikro szinten (az egyes rendszerelemek, alrendszerek szintjén). Az általunk javasolt megoldás a hagyományos kockázatelemzési modellek kiegészítésére is alkalmas lehet, hiszen az egyes erőforrások kockázati részmodelljét (ld. 2. és 3. ábra) egészíti ki egy félformális, a függőségeket és azok tartalmát is leíró modell.

Az általunk javasolt függőség elemzési módszert szeretnénk a jövőben egy informatikai alkalmazással fejleszteni és egy részterület modellezésével validálni, ellenőrizni, hogy valós – komplex kapcsolatokkal rendelkező – rendszerek leírására is alkalmas-e.

Irodalomjegyzék

- [1.] Dr. Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana, http://www.cert-hungary.hu/downloads/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszer_tana.pdf, (2009.12.13.)
- [2.] Virtual business. http://en.wikipedia.org/wiki/Virtual_business (2009.12.13.)
- [3.] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, http://www.gdf.hu/html/Doktorans_Klub/documentums/DK01-Muha.pdf, (2009.12.13.)
- [4.] Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, <http://www.inl.gov/technicalpublications/Documents/3489532.pdf>, (2009.12.13.)
- [5.] ISO/IEC 15408-1-3:2005: Information technology – Security techniques – Evaluation criteria for IT security
- [6.] Szádeczky Tamás: Terrorizmus a kibertérben, Infokommunikáció és jog, 2008. V. évf. 6. sz. pp. 200-205.