XXIII. évfolyam, 2014/2. szám

BOLYAI SZEMLE

A NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI TUDOMÁNYÁGI FOLYÓIRATA

A lapban megjelenő írásokat lektoráltatjuk. A közlésre szánt tanulmányokat
a bolyaiszemle@uni-nke.hu címre kérjük megküldeni magyar és angol címmel,
valamint magyar és angol összefoglalóval ellátva.

Kiadja: NKE Szolgáltató Kft.
Felelős kiadó: Hegyesi József ügyvezető igazgató
Nyomdai előkészítés: Tordas és Társa Kft.
Nyomdai munkák: NKE Szolgáltató Kft.
ISSN 1416-1443

Tartalom

E számunk szerzői

BLESZITY JÁNOS, intézetigazgató, Katasztrófavédelmi Intézet, Nemzeti Közszolgálati Egyetem

BOGNÁR BALÁZS, BM Országos Katasztrófavédelmi Főigazgatóság

HAJDU VERONIKA, a Katonai Műszaki Doktori Iskola munkatársa, Nemzeti Közszolgálati Egyetem

HORVÁTH TAMÁS, biztonságtechnikai mérnök, Magyar Villamos Művek

KÁTAI-URBÁN IRINA, MSc védelmi igazgatás szakos hallgató, Nemzeti Közszolgálati Egyetem

KÁTAI-URBÁN LAJOS DR., egyetemi docens, Nemzeti Közszolgálati Egyetem

KOVÁCS TIBOR, egyetemi docens, Óbudai Egyetem

MORVAI CINTIA, Katasztrófavédelmi Intézet, Nemzeti Közszolgálati Egyetem

MÓGOR TAMÁSNÉ, Biztonságtudományi Doktori Iskola, Nemzeti Közszolgálati Egyetem

PUSKÁS BÉLA, PhD-hallgató, Biztonságtudományi Doktori Iskola, Nemzeti Közszolgálati Egyetem

RAJNAI ZOLTÁN, egyetemi tanár, Óbudai Egyetem

SOLYMOSI MÁTÉ, a Somos Alapítvány a védelmi és biztonsági oktatásért és kutatásért kuratóriuma

SZABOLCSI RÓBERT PROF. DR., okl. mérnök ezredes, Honvéd Vezérkar, Személyzeti Csoportfőnökség

SZAMOSI BARNA, műszaki tanár, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Óbudai Egyetem

VANDERER GÁBOR, PhD-hallgató, Biztonságtudományi Doktori Iskola, Nemzeti Közszolgálati Egyetem

VASS GYULA, főosztályvezető, BM Országos Katasztrófavédelmi Főigazgatóság

ZELE BALÁZS, okleveles energetikai mérnök-közgazdász, Energiaellátás-optimalizálási munkatárs/szakértő, Tiszai Vegyi Kombinát Nyrt.; doktorandusz, Óbudai Egyetem

Hajdu Veronika

A pszichológiai műveletek megközelítése a marketing szemléletén keresztül

A pszichológiai művelet (PSYOPS) olyan tervezett módszer, mely szelektált információkat és indikátorokat közvetít egy meghatározott célcsoport részére, annak érdekében, hogy befolyásolja érzelmeiket, motivációikat, tárgyi szemléletmódjukat. Alapfilozófiájában ez a megközelítés a marketing sajátja is. Továbbá olyan eszközöket és módszereket használ fel, melyeket civil oldalon, a marketing területén alkalmaznak. A 21. században pedig mind a két terület széles palettán mozoghat, egymástól tanulva, akár a másik gyakorlatát adaptálva. Cikkemben e merőben eltérő két terület közötti összefüggéseket kívánom bemutatni néhány alapvető marketingszempont alapján, főként a pszichológiai műveletekre koncentrálva, röviden kitérve az alapjukat adó információ hasznosságára.

Kulcsszavak: pszichológia műveletek, marketing, célcsoport, információs fölény, „5M"

Bevezetés

Első megközelítésre merész feltételezésnek tűnhet egy lapon említeni a katonai műveleteket és a marketinget, mivel alapvetően két olyan területről van szó, amelyek céljukban teljesen eltérőek. A marketing egy profitorientált szemlélet tudhat magáénak, míg a pszichológiai műveletek az elmét és a lelket célozzák meg. Ha azonban távolabbról közelítjük meg a kérdést, a katonai műveletek esetében is beszélhetünk egyfajta profitmaximalizálásról, melynek tárgya nem a pénz, hanem egy sikeres hadművelet. Másik oldalról pedig a marketingnek is fontos célpontja az elme.

Ebből kifolyólag bár nem minden marketingszabály adaptálható a pszichológiai műveletek esetében, jobban elmélyedve azonban a két tudományágban, láthatóvá válnak a közös vonások, amelyek mind a két terület módszerének fejlődéséhez hozzájárulhatnak. Ismert tény, hogy a marketing eszköztára nagyban építkezik bizonyos katonai hadműveletekből, illetve előszeretettel emel át onnan kifejezéseket, meghatározásokat vagy akár stratégiai módszereket.

Gondoljunk csak a gerillamarketingre, mely nevéhez hűen nem konvencionális marketingeszközöket használ (vírusmarketing, ambient, word of mouth stb.), és így dolgozza ki a marketingstratégiát a sikeres „hadművelet" végrehajtásához.

A módszer újszerű, szokatlan, nem mindennapi és váratlan módon csap le a célcsoportra. Teszi ezt pont úgy, mint egy kötelék a gerillahadviselés során, mely meglepetésszerűen, kihasználva a területi adottságokat, kényszeríti az ellenfelet komfortzónája elhagyására.

A katonai hasonlatoknál maradva hozhatnám példaként még a marketing-megfigyelést is mint népszerű kvalitatív kutatási módszert, mely a kutató személyes megfigyeléseinek alapján végzett adatszerzés. Folyamatát tekintve pedig akár katonai felderítésként is definiálható.

A marketingben kellő mélységig megtervezett, stratégiailag átgondolt tervek kerülnek kialakításra, amelyekben célcsoportokat definiálnak, termékeket pozícionálnak, árháborúkat terveznek, erőforrásokat allokálnak és veszteségeket vesznek számba. Ehhez párosul magának a kommunikációnak a kialakítása, melynek fejlődése nagyban hozzájárult ahhoz, hogy a katonai szervezetek is egy egészen másfajta területen, más eszközökkel, de nem kevésbé hatékonyan tudjanak csatát nyerni, minimális veszteséggel.

Látható, hogy a két terület kölcsönösen hatással van egymásra, valamint közös kiindulóponttal rendelkezik, ami nem más, mint az információ megléte, illetve birtoklása esetén annak megfelelő felhasználása.

Információs hatalom

Az internet és a technológia rohamos léptékű fejlődésével a vállalatok nap mint nap új kihívásokkal szembesülnek. Más és más technikákat, módszereket kell elsajátítaniuk ahhoz, hogy életben tudjanak maradni a piacon. Újabb és újabb lehetőségeket, eszközöket, módszereket kutatnak fel, melyeket aztán minél hatékonyabban igyekeznek felhasználni a célcsoport és a piac megnyerésére, befolyásolására. Katonai aspektusból nézve a pszichológiai műveletek sem kivételek ez alól. Ugyanúgy résen kell lennie az ezen a területen működő állománynak ahhoz, hogy boldogulni tudjon a saját piacán, hadszínterén.

Az információval való gazdálkodás tehát napjaink mindennapos jelensége, nélküle létezni egyik oldal szervezete sem képes. Az információ hatalom. Aki birtokolja, versenyelőnyt szerezhet a piacon – vagy akár bővítheti azt. Területén jobb, gyorsabb, pontosabb, szakszerűbb lehet, minőségi szempontból messze kiemelkedővé válthat. A kimenetelek is kedvezőbben alakulhatnak.

Az információ a katonai oldalon szintén rendkívüli jelentőséggel bír. Erősokszorozó, hatásnövelő, integráló, illetve harci képességet javító elem. Az ellenfél oldalán pedig – információhiány esetén – ez erőcsökkentő, hatásrontó, integrációromboló, képességgyengítő és egyéb negatív tulajdonságokban tetőzhet. [1: p. 44.]

Az információ megszerzése azonban nem elég. Azt gyűjteni kell, elemezni és összehasonlítani, hogy megfelelő tendenciákat és következtetéseket lehessen levonni belőlük a jövőre nézve.

A gazdasági területen a marketingkutatás feladata ez, *„ami egy olyan objektív formális eljárás, mely a marketing döntéshozatalt a gyakorlatban is alkalmazható információkkal látja el, az adatok szisztematikus gyűjtése, elemzése, közlése révén”*, akár a piac aktív befolyásolása mellett. [2: p. 1.] A lélektani műveletekre is könnyedén adaptálható a fenti definíció, csupán a piac helyett hadszíntérről beszélünk. A két terület szerves középpontjában tehát az információ áll, mely nélkül nem születhet döntés, valamint kellően behatárolja a cselekvőképességet is a vezetés részéről.

Igaz mind a marketing, mind a katonai pszichológiai műveletekre, hogy a döntés a kognitív (tudati) dimenzióban születik meg. [3: p. 82.] Az észlelést, érzékelést, értelmezést, véleményformálást stb. célozzák meg, audio-, vizuális vagy audiovizuális eszközökkel. A végső cél a döntéshozók közvetlen módon történő befolyásolása oly módon, hogy az az információs fölénnyel elérni kívánt végső cél szempontjából optimális döntést hozzon, melynek hatása az ellenfél, illetve a versenytárs oldalán kedvezőtlen kimenetelben teljesedjen ki.

A pszichológiai műveletek, valamint a marketing hatékonyságának „sikertényezői”

„A pszichológiai műveletek azon tervezett pszichológiai tevékenységeket jelentik, amelyek békében, válságban és háborúban egyaránt alkalmazhatóak az ellenség és a saját, valamint a semleges érintettek magatartásának, szellemi beállítottságának és viselkedésének befolyásolására, a politikai és katonai célok elérése érdekében.” [1: p. 209.]

A Magyar Honvédség összhaderőnemi műveleti doktrína megfogalmazása szerint *„a lélektani műveletek elsődleges célja, hogy befolyásolja egy kiválasztott célcsoport viselkedését, magatartásformáit és véleményét az elöljáró által elfogadott lélektani műveleti célokkal összhangban, valamint hogy kiváltsa vagy megerősítse a célcsoport kívánt viselkedését az elöljáró távlati céljainak érdekében”.* [4: p. 1–36.]

A marketing az AMA[1] meghatározása alapján pedig *„olyan szervezeti funkció és eljárás, amely a vásárlók számra értéket teremt, kommunikál és közvetít, valamint az ügyfélkapcsolatokat oly módon ápolja, hogy azok a szervezet és az érdekelt személyek számára egyaránt hasznot hajtsanak”.* [5: p. 39.]

Célok és hasznok. Érintettek és vásárlók. Pszichológiai tevékenységek az egyik, kommunikáció a másik oldalon, ami magában foglalja többek között a pszichológiai hatásokat is. Nem is beszélve a befolyásolás szándékáról, mely mindkét oldal sajátja.

Ahhoz azonban, hogy az információ birtokában mind a két területen kedvező kime-

[1] AMA = Amerikai Marketing Szövetség

neteleket lehessen elérni (elérni a célokat, valamint a hasznot), azaz a befolyásolás, a kommunikáció sikeres legyen, számos faktor játszik közre, melyeket nem lehet figyelmen kívül hagyni.

Általánosságban elmondható, hogy valamennyi katonai tevékenyég rendelkezik pszichológiai hatásokkal. A katonai műveletek ugyanis nemcsak magára a célobjektumra, a célszemélyre hatnak, hanem a környezetében levő elemekre is. Befolyásolja az egyének, csoportok, vezetők magatartását, érzelmeit, motivációját, valamint viselkedését is.

A marketingben a makroökonómiai megközelítés szerint *„a fogyasztói magatartás képes befolyásolni a gazdasági folyamatokat, tendenciákat".* [6: p. 10.] Ennek fényében különböző szociológiai kutatások terjedtek el annak érdekében, hogy feltárják és körül tudják határolni a különböző fogyasztói magatartásmintákat. Ez a körülhatárolás a katonai műveletek során is hatalmas előnyt adhat, hiszen a célcsoport pontosabb ismerete egy sikeresebb érvrendszer felépítését eredményezheti.

Kotler szerint négy csoportra lehet bontani azokat a változókat, melyek valamilyen módon hatnak a fogyasztóra. Ezek a következőek:

- kulturális;
- lélektani;
- társadalmi;
- illetve személyes jellemzők. [5: p. 245.]

Ezeken a kategóriákon belül pedig olyan tényezők állnak, melyek eltérő mélységben, de hatnak a célcsoportra, befolyásolva annak viselkedését és reagálását bizonyos pszichológiai műveletekre, illetve marketingtevékenységre.

1. ábra: A célcsoportokat meghatározó ismérvek. Saját szerkesztés, 2014.

Az 1. ábrán olyan kategóriák és alkategóriák tényezői láthatóak, melyek közvetlenül hatnak az individuumra, és amelyek szépen adaptálhatók a pszichológiai műveletek előkészületeinél is.

Felsorolni és részleteiben elemezni ezeket most nem kívánom, néhány kulcstényezőt emelnék ki, melyek hatása megkérdőjelezhetetlen. Fontos megjegyezni, hogy közel sem elegendő csak az egyénre koncentrálni, hiszen ha az egyén köré csoportosuló közeg nem követi, nem tekinti magáénak a változást, akkor az egész folyamat negatívan vissza-

hat. Ebből kifolyólag egyaránt meg kell nézni az individuumot, valamint az individuumot meghatározó kultúrát, szubkultúrát és csoportot is. Azaz a szűkebb és tágabb környezetet. Ezen felül olyan lélektani (észlelés, motiváció stb.) és személyes tényezőket (életkor, személyiség, énkép stb.), melyek alapvetően határozhatják meg a célcsoport vagy az egyén cselekvését, tevékenységét, döntését.

A befolyásoló tényezők közül kiemelten fontosnak tartom a kultúrát, mely olyan tanult meggyőződések, értékek és normák összességét jelenti, amik az adott társadalomra jellemzőek, valamint erősen befolyásolják és irányítják a magatartást. [7: p. 19.] Nem lehet elmenni ennek fényében a szubkultúra fogalma mellett sem, mely nemzetiségi, vallási, faji, valamint földrajzi ismérvek mentén közvetít értékrendeket. Ezek a szubkulturális elemek a történelem folyamán jelentős hatást gyakoroltak, melyeknek jelentősége a mai napig vitathatatlan. Számos esetben találkozhattunk már olyan vallási csoportokkal, amelyek elutasítják a rajtuk kívül álló gondolkodást, nézeteket. Az ő esetükben különösen óvatosan kell eljárni minden pszichológiai művelet vagy marketinges tevékenység esetén.

Minden esetben, amikor valamilyen pszichológia műveletre készülünk vagy reklámot készítünk, és azt egy számunkra teljesen idegen közegben szükséges alkalmaznunk, feltétlenül meg kell ismerkedni a célcsoport kulturális szokásaival, normáival.

Ha elfogadjuk azt, hogy az egyénre hatnak a csoportnormák, -értékek, akkor elfogadható megállapítás, mely szerint a csoport egyedeinek pszichikumára hatva alakítható, szélsőséges esetben manipulálható a teljes közeg, csoport, tömeg viselkedése, magatartása. Ez pedig egy megfelelő művelettel mindkét oldalon kivitelezhetővé válik.

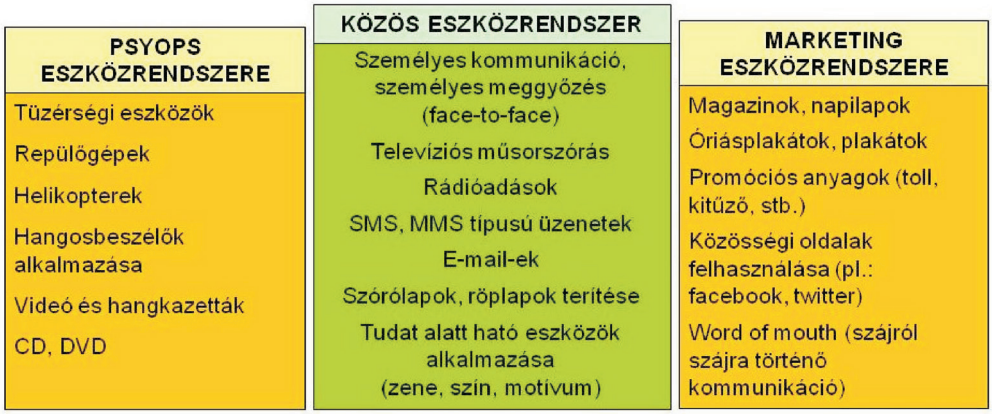
Célmeghatározás

A célmeghatározás során a nagyságrend és időtényező szempontjából specifikus célok kerülnek kialakításra, amelyek gyakorlatilag irányítani fogják a tevékenységeket. Az 1. számú táblázatban láthatóak azok a célok, melyek meghatározásra kerülhetnek a pszichológiai műveletek, valamint a marketinges reklámtevékenység során. [1: p. 209.] A vastagabban szedett részek a hasonlóságokat hangsúlyozzák a célmeghatározásukban.

A már említett információ fontosságán túl jelentősége van még azoknak a technológiájában fejlett speciális eszközöknek, amelyek segítséget nyújtanak a célok kivitelezésében. Általuk az üzenet hitelesebbé és meggyőzőbbé válhat, az üzenet a tényleges célcsoporthoz fog eljutni. Ezek az eszközök audiovizuális berendezések, tüzérségi és rakétatechnikai eszközök, repülőgépek, helikopterek is lehetnek. Továbbá ide sorolhatóak még a közvetett és közvetlen kommunikáció számos fajtája, melyekre vonatkozóan néhány példa a két terület jellemző felhasználása alapján a következő ábrán látható. [1: p. 212.]

Pszichológiai művelet célja	Marketing (reklámtevékenység) célja
Hatást gyakorolni az ellenség gondolkodására, érzelmeire, **befolyásolni** a viselkedését, szándékát.	Fogyasztói magatartás **befolyásolása** elsődlegesen, majd tájékoztatás, meggyőzés, emlékeztetés.
Erősíteni a baráti, illetve a lojális lakosság szimpátiáját a kitűzött politikai és katonai célok elérését szolgáló műveletekben.	**Fogyasztói hűség kialakítása.**
Elnyerni az el nem kötelezett vagy határozatlan népesség (**célcsoport**) támogatását és **együttműködési** készségét.	**Fogyasztók megtartása,** a potenciális fogyasztók, a célcsoport **megnyerése.**
Csökkenteni az ellenséges pszichológiai műveletek saját erőkre gyakorolt hatását.	**Válaszlépések,** illetve **megelőző lépések** megtétele a versenytársak reklámtevékenységével szemben.

1. táblázat: A pszichológiai műveletek és a reklámtevékenység céljainak összehasonlítása. Forrás: [1] alapján saját szerkesztés, 2014.



2. ábra: A PSYOPS és a marketing eszközrendszere. Forrás: [1] és [5] alapján saját szerkesztés, 2014.

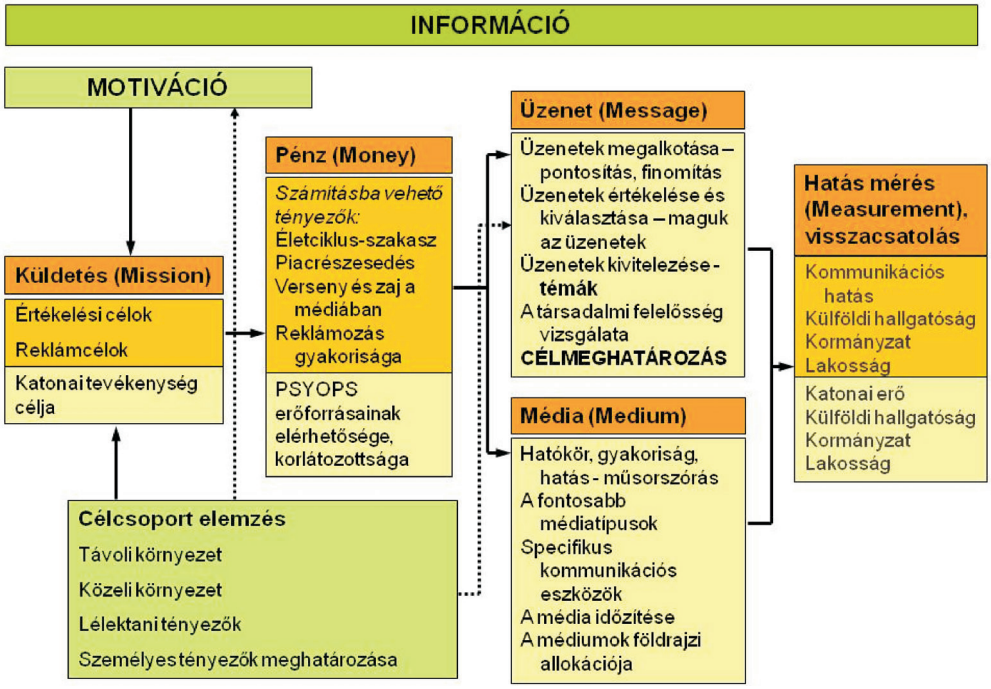
A választék széles, alkalmazásukat leginkább a területi adottság, a célcsoport összetétele, a technikai adottságok, illetve a költségkeret határozhatja meg. A pszichológiai műveletek hatékonyságát erősítik a nemzeti rádiókban, televíziókban közzétett információk is, ha van mód azt eljuttatni a célcsoport részére. Ellenkező esetben a röplap, illetve a hangosbeszélők alkalmazása a megfelelő.

Pszichológiai műveletek végrehajtása marketingszemléletű megközelítésben

Magának a műveletnek a végrehajtását egy egészen más megközelítésben szeretném ábrázolni. Mégpedig egy, a marketingben használt reklámtervezés folyamatán keresztül, melyet némileg átalakítottam és adaptáltam a pszichológiai művelet tevékenysége szerint, feltüntetve mind a két oldal résztevékenységeit a folyamat egyes lépéseiben.

A parancsnok/vezető a művelet tervezése során a döntést az úgynevezett „5M" segítségével hozza meg, mely az angol szavak kezdőbetűiből került meghatározásra: küldetés (Mission), pénz (Money), üzenet (Message), médium (Media), mérés (Measurement). [5: p. 741.]

A 3. ábra szemlélteti a teljes folyamatot, amelynek kezdőpontjaként az információt határoztam meg, ami nélkül sem pszichológiai művelet, sem pedig marketinges tevékenység nem indulhat meg.



3. ábra: A katonai pszichológia műveletek kialakítása az 5M-en keresztül. Forrás: [5] alapján saját szerkesztés, 2014.

Első lépésként elengedhetetlen a **küldetés** meghatározása, mely a már fent említett pszichológiai műveletek céljaiban definiálható, de könnyedén katonai küldetésre vonatkoztatható marketinges megközelítésben a reklámcél is, ami végső soron magának a ka-

tonai céloknak a megfogalmazott üzenetét közvetíti. Ebből következik, hogy a **célcsoport** elemzése, illetve a motivációk körvonalazása nélkül nem lehet tovább lépni.

Mind a két esetben a műveletet megelőzően alapos tervezés, adatgyűjtés történik, amit folyamatosan ellenőrizni kell. Továbbá a művelet során nem kevés idő, erőforrás (emberi, tárgyi) ráfordítása szükséges, nem is beszélve a propagandatevékenység kivitelezéséről, a reklámozás gyakoriságáról. A marketing szempontjából figyelembe kell venni, hogy mekkora piacrészesedéssel rendelkezik a vállalat, hiszen utóbbi esetében akkor nagyobb költségkerettel kell dolgozni. [8: p. 177.] Ezek biztosításához tehát elengedhetetlen feltétel a **pénz,** ami sok esetben igen szűk keretben áll rendelkezésre. A megtérülés gyorsabb és tisztább, hiszen sikeres reklámtevékenység esetében a fogyasztók a termék megvásárlásával „megtérítik" a költségeket, sőt haszon is képződik. A pszichológiai műveletek esetében azonban nincs ilyenre lehetőség. Eleve nem beszélhetünk bevételi forrásról. Hiába sikeres a művelet, anyagi haszonnal (profittal) nem jár. Közvetetten azonban úgy térülhet meg ez a ráfordítás, hogy a PSYOPS sikeres alkalmazása révén elkerülhető a jelentősebb erőforrás-veszteség, melynek haszna egy következő műveletnél jelenik meg. Fontos mind a két oldalnál, hogy külön erőforrásterv kerüljön kialakításra, mely alapján eldönthető, hogy valósítható meg a marketing (reklám) tevékenység, illetve a PSYOPS üzenetének célba juttatása.

Magának az **üzenet**nek a megalkotása szintén a célcsoport összetétele alapján kerül meghatározásra, melyben természetesen nagy szerepet játszanak a katonai célok is. Tartalma ad motivációt a célközönségnek. Fontos épp ezért mind a két területen, hogy az üzenet hihető forrásból származzon, szavahihető legyen, valamint a valóságot tükrözze. Kivételt képez ez alól a pszichológiai műveletek egyik fajtája, a fekete PSYOPS, mely hamis, csúsztatott vagy lényegesen módosított információkat tartalmazhat. Az üzenet speciális módon is célba érhet, mégpedig a tudat alatt, érzékszervek befogadásának útján (szín, hang, szimbólum).

A megfelelő **médium,** vagyis a reklámhordozó kiválasztása, annak időzítése, allokációja végső soron a fent említett kategóriák kiteljesedése, mely igyekszik a célcsoport viselkedését, attitűdjét a megfelelő irányba kormányozni, azaz befolyásolni. A marketing esetében szélesebb a paletta, hiszen az internet révén fogyasztóit a világ bármely pontján elérheti, míg a pszichológiai műveletek esetében nem mindig van lehetőség modern eszközök alkalmazására, hiszen a célcsoport elérése sok esetben csak korlátozott módon lehetséges.

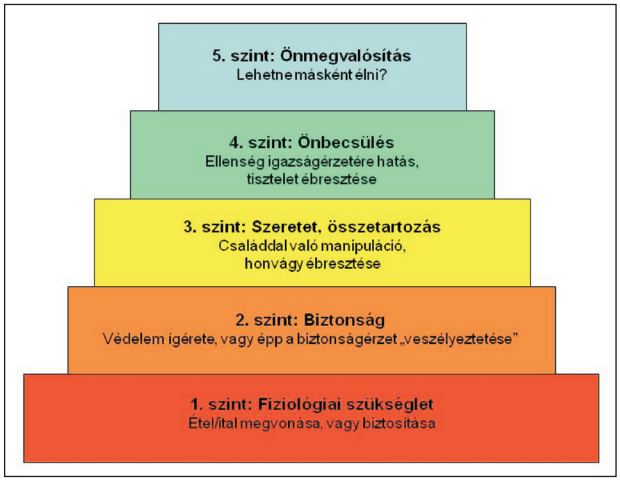
Ahhoz, hogy az egész folyamat sikeres legyen, fontos a nyomon követés és a visszacsatolás, mert így tényszerűen feltárhatóvá válnak a kommunikációs tevékenység eredményei. A célcsoport reakciójából a későbbiekben még pontosabb katonai célok fogalmazhatóak meg, még sikeresebb eredmények érhetőek el, míg a marketing esetében még nagyobb profitra van lehetőség. Visszacsatolások által megállapítható az is, hogy hol nem ért célba az üzenet, mik voltak a zavaró tényezők.

A szükséglet mint közös terület

Ha korábban hangsúlyoztam, hogy az információ a közös nevező e két terület között, akkor kiemelnék még egy ütköző pontot, mely az ember igényeit, vágyait alapvetően határozza meg. Ez egy olyan terület, melyre mind a marketing, mind a PSYOPS tud építeni, ha „termékét szeretné eladni".

Egyedi kategóriáját képezik a lélektani műveleteknek azok a tevékenységek, amelyek a különböző emberi szükségletekre hatnak. [9: p. 82.] Azért emelném ki a számos módszer közül pont ezt, mert a marketingben is használatos Maslow-piramis elvére épül.

Maslow tanulmányában hierarchikusan, 5 szintben határozta meg az emberi szükségleteket, melyeknek fő jellemzője, hogy egy magasabb szintű szükséglet elérése csak egy alacsonyabb kielégítése után valósulhat meg. Részleteiben nem térnék ki most az egyes szükségletszintekre, azonban a következő ábrán látható néhány lehetséges műveleti lépés.



4. ábra: Maslow-piramis. Forrás: saját szerkesztés, 2014

Maslow elmélete kiválóan alkalmazható a két területen, mert nem igényel jelentősebb vagy mélyebb célcsoport-, illetve környezetelemzést, hiszen ezek az alapvető szükségletek kultúrától, társadalmi osztálytól vagy épp életmódtól függetlenül mind jelentkeznek. Ezek által a befolyásolás viszonylag könnyen megvalósítható. [9: p. 82.]

Azt azonban fontos megjegyezni, hogy az egyes kultúrákban bizonyos szükségletek eltérő prioritásokkal jelentkeznek, ebből kifolyólag Maslow elméletét nem minden esetben lehet közvetlenül alkalmazni. Ez főként a keleti, illetve nyugati kultúrák szemléleti különbségében mutatkozik meg leginkább. Így szükségesnek tartok egy regionális, földrajzi behatárolást, mely az adott lélektani műveletért felelős katonai csoport szakértelmén múlik.

Ha megvizsgáljuk Maslow elméletét közelebbről, egy-egy szükséglet esetén négy alapvető manipulációs módszert lehet választani a tervezett pszichológiai műveletek területén: [10: p. 7.]

A szükséglet felkeltése – vagyis olyan propagandatevékenység kialakítása, ami valamilyen szükséglet irányában az igényfelmerülést serkenti. Sugalmaz, javasol.

1. *A szükséglet kielégítése* – van megfelelő erőforrás arra, hogy a szükséglet kielégítésre kerüljön. Talán pont egy olyan szükséglet, amit egy korábbi PSYOPS kapcsán felkeltettek.
2. *A szükséglet kielégülésének megakadályozása* – egy állapot fenntartása, vagyis a szükséglet kielégítésének megakadályozása.
3. *A szükséglet felkeltődésének megakadályozása* – vagyis a szükséglet azonnali kielégítése.

A szükséglet valami iránt minden emberben ott van, kortól, nemtől, országtól, vallástól, kultúrától függetlenül. A hangsúly a szükséglet kielégítésen van a marketing meghatározása alapján, mely történhet termék, illetve szolgáltatás útján. A PSYOPS esetében nemcsak a szükséglet kielégítéséről, hanem a célmeghatározásnak megfelelően akár a szükséglet megvonásáról is beszélhetünk. Látható tehát, hogy Maslow elmélete nemcsak a marketingben, hanem a PSYOPS által is kiválóan alkalmazható, mellyel a NATO-doktrína [9: p. 81.] is külön részben foglakozik a lélektani hadműveletek kapcsán.

Összegzés

Szun-Ce szerint nem az jelenti az igazi győzelmet, ha több száz csatát nyerünk meg, hanem ha harc nélkül győzzük le az ellenséget. [11] Ehhez pedig kiindulásképpen semmi más nem szükséges, mint információ, mely a 21. században minden hadszíntéren a boldogulás legfontosabb eleme, Legyen ez a civil vagy a katonai szférában.

A PSYOPS célja, hogy a célcsoport viselkedését befolyásolja, oly módon, hogy az a katonai célok kedvező kimenetelét támogassa, elősegítse azt. Egy sikeres művelet eredményeképpen csökkenthető a harci kedv, kedvezőbb fogadtatás, légkör alakítható ki válságreagáló műveletek alkalmával – vagy akár egy fegyveres küzdelem is elkerülhetővé válhat. [1: p. 210.] A meggyőzés és befolyásolás minden esetében a figyelem középpontjába kell állítani azt, hogy mi a fontos a célcsoportnak, és miért hoz előnyt számára viselkedésének, hozzáállásának megváltoztatása.

A marketing ugyanennek a szellemében cselekszik, felhasználva a technika adta lehetőségeket. Véleményem szerint és az eddigi kutatások alapján érdemes foglalkozni és nyomon követni a civil szférában a marketingaktivitásokat, hiszen az állandóan fejlődik, a legújabb módszereket, eszközöket vetve be a siker érdekében. Ez keretet adhat a pszichológiai műveleteknek, amely által a művelet hatékonysága is növekedhet. Továbbá nem elhanyagolható tény, hogy külön tudományterületként a marketingkutatás olyan folyamatos és széles körű szociológiai, demográfiai, technológiai, pszichológiai stb. kutatásokat végez, melyek a katonai pszichológiai műveleteknél is kiválóan alkalmazhatóvá válnak.

A marketing és a PSYOPS valóban merőben más terület, azonban az alapfolyamatok hasonlóak. A marketing részterületeként a marketingkutatás, valamint a marketing-

kommunikáció (reklámozás) olyan metodikát foglal magába, mely segítheti a PSYOPS hatékonyságát. Érdemes lenne tehát egy PSYOPS marketingstratégia kialakítása, melynek kiindulópontját a marketingkutatás alappontjai határozhatnák meg.

Irodalomjegyzék

[1] Dr. Haig Zsolt – Dr. Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, 2005, 286 oldal, ISBN: 963-327-391-9.

[2] Dr. Gyenge Balázs: Marketingkutatás jegyzet. SZIE, Gödöllő, 2007, 191 oldal.

[3] Haig Zsolt – Kovács László – Munk Sándor – Ványa László: Az infokommunikációs technológia hatása a hadtudományokra. NKE, 2013, 173 oldal, ISBN: 978-615-5305-02-3.

[4] ÁLT/38 Magyar Honvédség összhaderőnemi műveleti doktrína, 1. kiadás. A Magyar Honvédség kiadványa, 2013. 158 oldal.

[5] Philip Kotler – Kevin Lane Keller: Marketingmenedzsment. Akadémia Kiadó, 2006, 986 oldal, ISBN: 963-05-8345-3.

[6] Dr. Horváth Ágnes – Füredíné Kovács Annamária: Fogyasztói magatartás jegyzet. SZIE, Gödöllő, 2008, 131 oldal.

[7] Dr. habil Komor Levente: Gazdaságpszichológia jegyzet. Gödöllő, 2005, 250 oldal.

[8] Dr. Horváth Ágnes: Marketing jegyzet. SZIE, Gödöllő, 2007, 219 oldal.

[9] NATO-doktrína – AJP-3.10.1.(A), 2007, 106 oldal, http://info.publicintelligence.net/NATO-PSYOPS.pdf#page=82&zoom=auto,-82,737 (letöltés dátuma: 2014. április 27.)

[10] Mező Ferenc: Az emberi szükségletekre irányuló lélektani műveletek (PSYOPS). Hadtudomány, XVII. évfolyam 1. szám, 2007, 41 oldal, ISSN: 1215-4121, http://www.zmne.hu/kulso/mhtt/hadtudomany/2007/1/2007_1_15.pdf (letöltés dátuma: 2014. április 29.)

[11] Szun-Ce: A háború művészete. Carthaphilius Kiadói Kft., 2006, 176 oldal, ISBN: 978-96-3744-8546.

Marketing Approach of the Psychological Operations

Hajdu Veronika

Psychological operations (PSYOPS) are planned methods that convey selected information and indicators to a specific target group in order to influence their emotions, motivations, and approaches. The basic philosophy of marketing is very similar to this approach. In addition, PSYOPS are using tools and methods which – in the civilian sphere – are applied in the field of marketing. In the 21st century a broad range of possibilities are at the disposal of both the military and civilian fields; they can learn from each other and adapt each other's practices. In this article I intend to present the relationship between these two very different fields in the light of some basic marketing aspects, particularly focusing on the psychological operations briefly covering the usefulness of the information they are based on.

Keywords: Psychological operations, marketing, target audience, information superiority, „5M"

Zele Balázs

Tűzesetek megoszlása és az emberi tényező befolyásoló szerepe szenes erőművekben a tüzelőanyag-ellátó és elosztó rendszerek területén

Napjaink energiapolitikája egyre nagyobb hangsúlyt fektet a környezet- és az általános tűzvédelmi kérdések megvitatásának, melynek egyenes arányú vonzata, hogy fokozott figyelemmel kísérik az erőművi biztonságtechnikai előírásokat is. Ennek következtében az erőművekben és szállítórendszeren a beszállítástól az eltüzelésig terjedő úton előforduló tűzesetek, a humán erőforrás képzettsége és a biztonsági előírások fejlesztésének kérdései kulcsszereppel bírnak. Ebből kifolyólag jelen kutatásomban külföldi források segítségével kutattam egy magyarországi, lignittüzelésű erőmű példáján a tűzesetek megoszlását és az emberi tényező szerepét erőművi területen.

Bevezetés

Magyarország és a világ energiapolitikai helyzetét az elmúlt években több jelentős, nagymértékű változás és átalakulás jellemezte számos területen. Ez a megállapítás nemcsak az általános műszaki fejlesztések esetében igaz, de a környezetszennyezés visszaszorítására és az általános egészségügy színvonalának javítására is.

„Az energiapolitika egyik feladata a társadalom meggyőzése a fenntartható energetika vázolt és adottságainknak megfelelő törekvéseiről, emellett az *ellátásbiztonság érdekében a szabályozás eszközeivel való (mint pl. CO_2kvóta, tüzelőanyag-választás) minél nagyobb részarányú karbonmentes, valamint a hazai és import szénre alapozott erőművek létesítését elősegítő, a termelői átlagár minél kisebb növekedése érdekében való irányultság."*[1] Mindezek mellett kijelenthető, hogy az energiafüggőségtől való félelem nemcsak jelenünkre, de múltunkra is jelentős befolyásoló szereppel tölti be mindennapjainkat, melynek érdekében csökkenteni kell az energiafüggőséget, és ezzel együtt növelni az ellátásbiztonságot. Az energiaellátás egyik legrégebbre visszanyúló kérdése a szenes erőművekben történő energiaátalakítási folyamat. Az elmúlt években Európát, ezzel együtt Magyarországot is egyre inkább a környezetet veszélyeztető globális (kör-

[1] BME Energetikai Gépek és Rendszerek Tanszék hivatalos honlapja (online), http://energia.bme.hu/~kaszas/Energiapolitika/OszJanos/Meg%C3%BAjul%C3%B3%20energiaforr%C3%A1sok.pdf (2013. 12. 14.)

nyezeti) problémák foglalkoztatják, melynek fő irányvonala a környezetvédelem kérdéskörе.

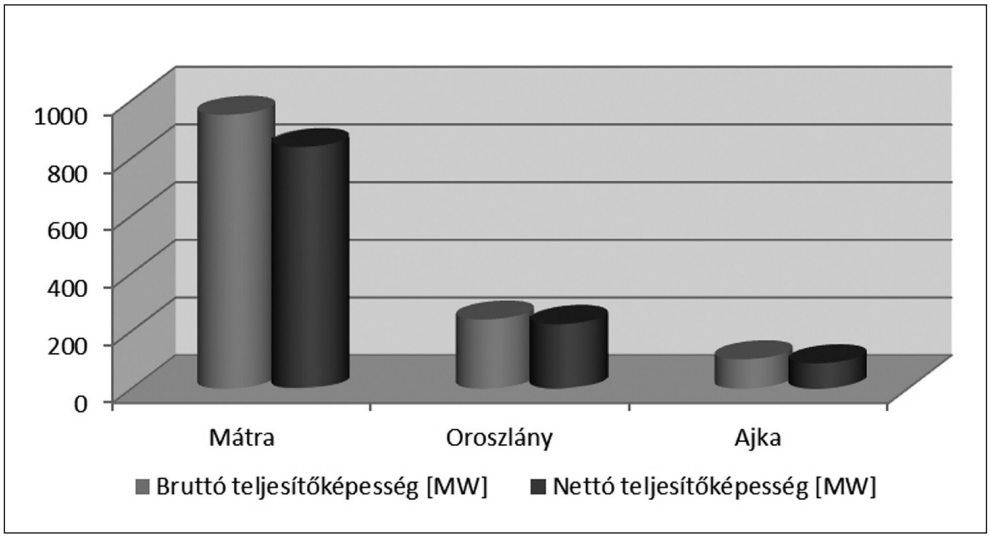
Hazánk energiapolitikáját a megújuló energiák hasznosításán túl a hazai készletek (pl. szénkészletek) minél nagyobb részben való felhasználási alternatívája is meghatározza. Ennek a szemléletmódnak az alapja, hogy hazai készletekből gazdálkodva, szénkészletünk kiaknázását előtérbe helyezve állítsunk elő energiát. Hazánk nyersanyagait tekintve a legnagyobb arányban a lignit található meg a Mátra hegyvidékén és környékén, továbbá feketekőszén-készletünk leginkább a Mecsekben és közvetlen térségében. Az utóbbi időkben bányabezárások, (pl. a mecseki), majd esetleges újbóli megnyitások visszhangjától volt hangos a köztudat. *„A bánya-erőmű integrációban működő bányák többsége is bezárásra került (2003-ban Balinka, Budaberke tároló, Sajómercse, Mákvölgy, Feketevölgy, Szuhakálló; 2004-ben a pécsi külfejtések, Mány, Ármin, Lyukóbánya, Lencsehegy). 2005-ben már csak egyedüli mélyművelésűként Márkushegy, valamint Visonta, Bükkábrány és néhány kisebb nógrádi és borsodi külfejtés működik."*[2]

Ennek ellenére bizonyos, hogy ezen erőforrások hasznosítása nemcsak a múltban volt szignifikáns, de továbbra is jövőnk egyik kiaknázatlan forrása lehet, azonban megfelelő környezetpolitikát kialakítva a már megkezdett, véleményem szerint helyes úton haladhatunk tovább a biztonságos és fenntartható energiaellátás központi szerepét alapul véve.

A jelen kutatásom alapvető célja, hogy hazánk egyik legnagyobb energiaellátó és továbbadó (a lignit felhasználására épült) erőművén keresztül bemutassam és megvizsgáljam a szabályozatlan tűzeseteket kiváltó tényezők egymáshoz való viszonyát és előfordulási arányát szénerőművi területeken – ahol alapvetően a szénporeloszlás és a technológiai veszélyek mellett leginkább az eddigi tapasztalatok alapján előforduló emberi befolyásoló szerepet vizsgáltam behatóan.

A szenes erőművek megítélése, továbbá az alkalmazhatósági technológiáik irányába való törekvés is kisebb átalakítási struktúrán ment keresztül az utóbbi időben. Egyre inkább elterjedt megoldásnak számít a lignit hasznosítása mellett a biomassza eltüzelése is, ami a szenes technológiai felhasználáshoz való hozzáadást jelenti. A technológia lényege, hogy a megfelelő fűtőértéket megtartva, a biomassza és szén megfelelő mértékben és minőségben homogenizált arányát létrehozva történik a hasznosítás. Ezek alapján a tisztán szenes technológia alkalmazása kisebb túlzással megszűnt, így a hazai beépített teljesítményadatok alapján nem csupán a szenes alkalmazás, hanem a vele együttesen alkalmazási teret nyerő biomassza hasznosítási aránya is be lett integrálva egy erőmű teljesítőképességének meghatározási értékénél (1. ábra).

[2] Kajati György, A magyar villamosenergia-ipar posztszocialista átalakulása. Doktori (PhD) értekezés, Debrecen (2008).



1. ábra: Erőműmérleg 2012. (saját szerkesztés MAVIR adatok alapján)[3,4]

A 2012-es évben döntően szénnel és bioüzemanyagok felhasználásával együttesen üzemelő létesítmények teljesítőképessége az 1. ábra szerint alakult. Ezen értékek összege alapján közel 1300 [MW] teljesítőképesség volt a rendszeren belül, ami a 2012. évi forrásoldali teljesítőképesség 13%-át vetítette előre. Ha a Paksi Atomerőmű 2000 MW-os bruttó teljesítőképességi értékét vesszük alapul – amely az ország villamosenergia-rendszer termelésének 45,9%-át mutatta az adott évre vonatkozóan –, akkor ezek az értékek az atomenergia felhasználása mellett jelentős mértékűnek tekintendőek, még ha ez többnyire a Mátrai Erőmű szerepvállalásának is volt tulajdonítható.

A 2. ábrán az ország ezen, szenes technológiára épült energia-átalakító és -hasznosító üzemeiben az energiahordozók felhasználási megoszlását tüntettem fel, melyből szintén látható a Mátrai Erőmű Zrt. kiemelkedő részesedése. Az erőmű hivatalos közleményét és megfogalmazását referenciául véve: *„…hazánk egyik legnagyobb villamosenergia-előállító egysége és egyben az ország legnagyobb szenes erőműve,”*[5] így vizsgálataim alapvetően az itt zajló folyamatokra korlátozódik. Az ország jelenlegi helyzetét elemezve egy nagyobb átalakulási folyamat zajlik, ami ezen energia-előállító, alapvetően széntüzelésű erőművi egységek termelését jellemzi. Az energiapolitikai szempontokat és az EU-s direktívákat elemezve, a megújuló energiaforrások felhasználási arányát növelve kell az elkövetkezen-

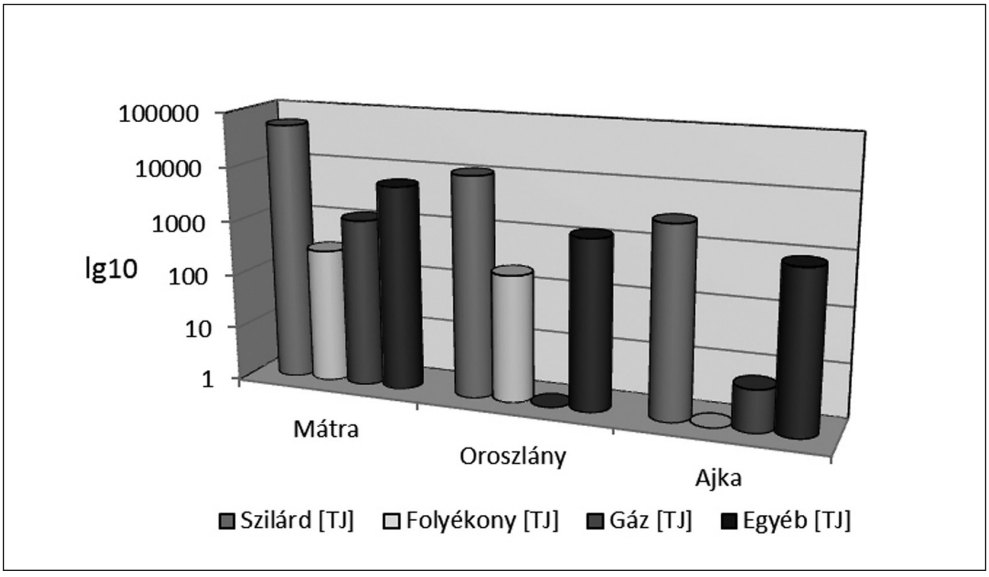
[3] MAVIR Zrt. hivatalos honlapja (online), http://www.mavir.hu/documents/10258/15461/Forr%C3%A1selemz%C3%A9s_2013.pdf/0a51f06c-73e7-4607-b582-00d3b1434837 (2014. 01. 12.)

[4] Megjegyzés: Az erőművek bruttó villamosenergia-termelésének (MWh/a) és a névleges, bruttó beépített teljesítőképességének, a BT-nek (MW) a hányadosa jelenti az egész erőműpark teljesítőképesség-kihasználását (h/a). (Dr. Stróbl Alajos: A magyar és az európai villamosenergia-ellátás változásainak elemzése, ellátás-biztonsági és kapacitáselemzési tanulmányok készítése alapján.)

[5] Mátrai Erőmű Zrt. hivatalos honlapja (online), http://www.mert.hu/hu (2014. 01. 25.)

dőkben az ország energiaellátását biztosítani, melyről az Európai Bizottság közleményében hivatalosan az alábbiakat olvashatjuk: *„Az EU jó úton halad afelé, hogy elérje célját, azaz hogy 2020-ra energiaszükségletének 20%-át megújuló forrásokból fedezze. Ez a törekvés részét képezi annak az átfogó uniós stratégiának, amely az éghajlatváltozást hivatott megfékezni. Ez mindenképpen jó hír. A szél-, a nap-, a víz-, az árapály-, a geotermikus és a biomassza-energia nagyobb arányú felhasználása csökkenteni fogja az Európai Unió energiaimport-függőségét, és ösztönzőleg hat majd az innovációra és a foglalkoztatásra."*[6]

Az ország 2012-es energiahordozó-felhasználási adatai alapján készített 2. ábra szerint –továbbra is a fent részletezett szempontokat figyelembe véve – jól érzékelhető hazánkban a Mátrai Erőmű kiemelkedő szerepvállalása, továbbá a szilárd (szén) tüzelőanyag felhasználási aránya mellett a többi energiahordozó (gáz, folyékony, egyéb) hasznosításának megoszlása is, melylyel az EU-s célokat előtérbe helyezve halad a biztonságos és környezetet védő célkitűzés felé.



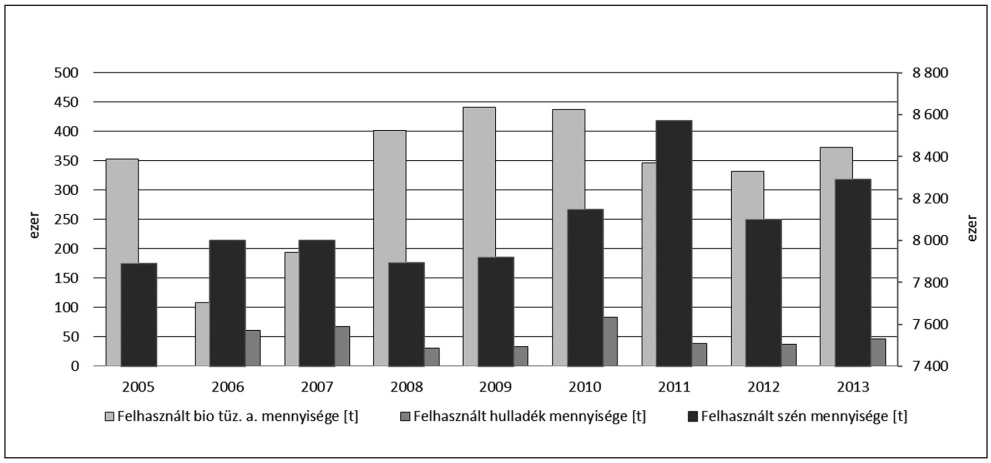
2. ábra: Energiahordozó-felhasználás „a mára megmaradt nagyobb energiaelőállító egységekben" 2012. (saját szerkesztés MAVIR adatok alapján)[7]

Az elemzés további részében az Mátrai Erőműre fókuszálva, illetve az itt történt esettanulmányt értékelve vonom le meglátásaim és megfelelő következtetéseim. A 3. ábrán az elmúlt közel tíz évben a szilárd tüzelőanyagok megoszlásában történt változás kimutatása látható, melyből szintén kiderül, hogy a közel egyenletesnek tekinthető lignitfelhasználás

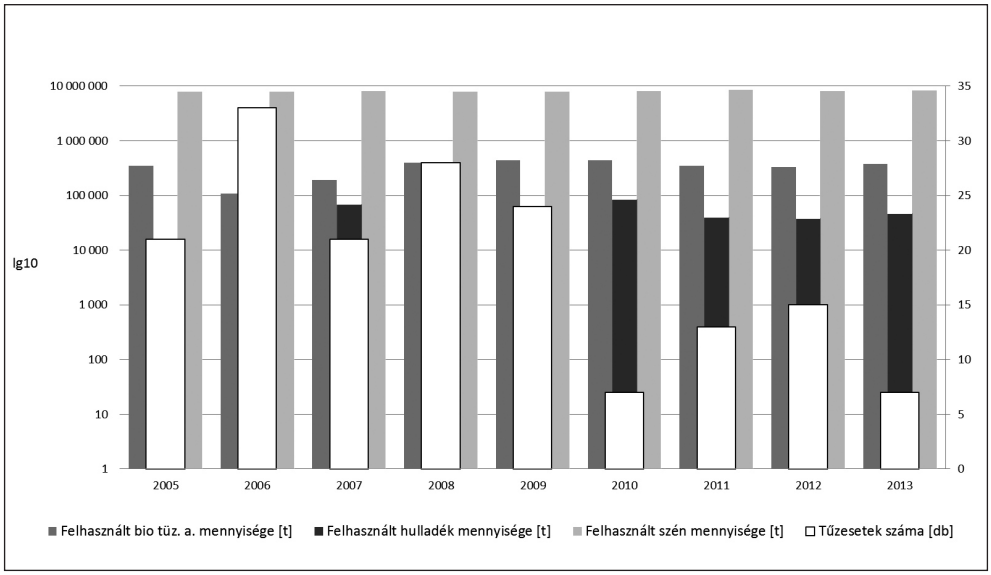
[6] Az Európai Bizottság hivatalos honlapja (online), http://ec.europa.eu/news/energy/120608_hu.htm (2014. 01. 11.)

[7] http://www.mavir.hu/documents/10258/15461/Forr%C3%A1selemz%C3%A9s_2013.pdf/0a51f06c-73e7-4607-b582-00d3b1434837 (2014. 01. 10.)

mellett a bio-, valamint a „hulladék" (egyéb) tüzelőanyagok megjelenése és ezzel együtt természetesen felhasználási aránya is jelentősen megnövekedett.



3. ábra: ME Zrt. által felhasznált szilárd tüzelőanyag megoszlása. Mátrai Erőmű Zrt. Kalorikus Osztály konzultációk, jelentések erőművi dolgozókkal alapján saját szerkesztés (2014. január–február)

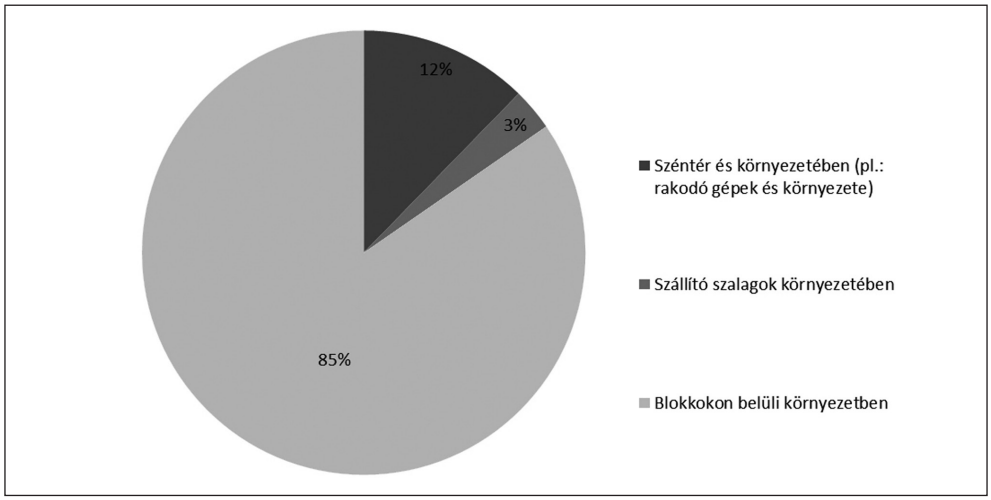


4. ábra: ME Zrt. tűzesetek a felhasznált tüzelőanyag megoszlása szerint. Mátrai Erőmű Zrt. Kalorikus Osztály konzultációk, jelentések erőművi dolgozókkal alapján saját szerkesztés (2014. január–február)

Ezzel összefüggésben viszont az erőműves jelentések alapján a vizsgált időszakban keletkezett tűzesetek száma csökkenő tendenciát mutat, vizsgálataim a továbbiakban arra irányulnak, hogy ezen adatok alapján milyen kockázati/befolyásoló tényezőkkel magya-

rázhatók az egyes esetszámok, mely esetek voltak a leggyakoribbak, illetve van-e összefüggés a mutatószámok megoszlása között.

Elöljáróban, továbbá kutatásaim és a rendelkezésemre álló erőműves jelentések alapján kijelenthető, hogy az utóbbi 10 évben *a leggyakoribb tüzesetek a szénpor kiszóródása okozta, a gépészeti meghibásodásokból adódó olajelfolyás és az emberi befolyásoló szerepből adódó esetek* voltak. Ezt a megállapítást támasztja alá további elemzésem is, melynek első részében a szénpor szabályozatlan eloszlásából adódó – a széntér és a kazán transzportvonalon előforduló – tűzesetek jellemző eseteit és mutatom be az 5. ábrán.



5. ábra: Tűzesetek megoszlása. Saját szerkesztés a Mátrai Erőmű Zrt. Biztonsági Osztály adatai alapján (2000–2012)

Az esetek 85%-át a blokkokon belüli szénpor-kiszóródás okozta/szabályozatlan eloszlás keltette tűzesetek voltak. A többi eset főleg a széntérben és környezetében keletkezett tűz volt, valamint a szállító szalagoknál és környezetében oszlott el.

A leírt tényeket szakirodalmi adatok alapján alátámasztva kívánom igazolni, illetve ezen túlmenően bizonyítani az általam megfogalmazottakat is.

Nemzetközi forrásokat kutatva, amerikai példák alapján egy előadási anyagban a szerző a vizsgált amerikai szenet „a szükséges rosszként ” említi, amivel a tüzelőanyag reakcióba lépő állapotára, vagyis a termikus égés folyamatára, a szabályozatlan szénporégés és a robbanási jelenségek veszélyes következményeire hívja fel a figyelmet. „Azokon a helyeken, ahol könnyen megtelepedhet a finom szemcsenagyságú szénpor – ilyen helyek lehetnek a szállítási transzportfolyamatoknál (szállítószalagok) és berendezéseknél is –, ezen felgyülemlett üzemanyag többletet képezve meggyulladhat.” Ezeken túl a szállítás és a kazánokba történő irányított folyamat közben is előfordulhat szénpor-kiszóródás és -eloszlás az üzemi területen belül, ami a különféle csöveken, tartályok felületein összegyűlhet, megtapadhat.

A szénporréteg vastagsága és a termikus reakció (a meggyulladás folyamata) közötti összefüggést az alábbi módon határozták meg.

$$T_{ex} = \frac{H \cdot A_{tot}}{87.5 \cdot A_{dust}}$$

ahol:

- T_{ex} = a szénporréteg vastagsága, (amely a robbanásveszélyhez hozzájárulhat)
- A_{tot} = a teljes alapterület (20 000 ft^2 [8] a felső mérési határ)[9]
- H = a terület/épület magassága (ft)
- p = lerakódott por térfogata (lb/ft^3)
- A_{dust} = a terület/épület befogadóképességén belül a porlerakódási felületek nagysága (ft^2)

Megfogalmazták továbbá az emberi szerep, a tűzvédelem fontosságát (karbantartások elmulasztása, dohányzási tilalmak, kötelező megelőző tréningek stb.) is ebben a leírásban – szintén szénpor okozta tüzeknél, szénpor okozta robbanásos eseteknél –, így a továbbiakban ezek megoszlását, befolyásoló szerepét is vizsgálom egy hazai erőműves példa alapján, azonban új tézisként a fontossági alternatívákat összevetem más tárgyi okozó esetek bekövetkező hatásával is. Mielőtt azonban ezt megkezdem, kutatásaim alapján az ebben a rendszerben előfordult leggyakoribb tűzesetek létrejöttét kiváltó okokat az 1. táblázatban foglalom össze, és így a Magyarország legjelentősebb lignittüzelésű erőművében előfordult tűzesetek képezhetik az alapot további vizsgálataimra. Ebben segítségemre volt egy namíbiai széntüzelésű erőműre – általánosságban 150-800 MW teljesítőképességre – elvégzett kockázati esettanulmány is. Ez a gépészeti meghibásodások okozta tüzek eseteit alacsony „kockázati tényező/faktor" tartományba sorolja, azonban itt inkább jelentősebb befolyásoltságról lehetne beszélni.[10] Így feltehetően a tüzelőanyag – jelen esetben szén – minősége, kora és egyéb természeti tulajdonsága alapján további elemzéseket lehetne végezni (pl. milyen további tényezők befolyásolhatják vagy befolyásolhatták ezt).

Ebből következően ugyan nem lehet egy vagy két üzem adatai és tapasztalatai alapján messzemenő és egyértelmű következtetéseket levonni, azonban egy magyarországi vagy akár a világ más területein a jövőben létesülő erőművi beruházás során az egyes tüzelőanyag-típusokra vonatkozóan alkalmazási teret nyerhetnek az itt leírtak.

A biztonsági eszközökön és megoldásokon túlmenően érdemes figyelmet fordítani az emberi tényező szerepére, megvizsgálni, ez milyen szerepet tölthetett be a tűzesetek megakadályozásában vagy a létrejött esetekben milyen befolyásoló hatással volt.

[8] USA mértékegységek (Wikipedia): köbyard = 27 ft3 ≈ 0,7646 m3

[9] INC – JUSTIN CLIFT, Hazard Control Technologies; COMBUSTIBLE DUST előadás anyaga, online, www.hct-world.com (2014. 01. 04.)

[10] NAMPOWER, Coal-Fired Power Station. Namibia Environmental, Environmental and Socio-Economic Risk Assessment Report, Reference Number: 5975; 15 MAY 2012. (2014. 02. 08.)

Az utóbbi években egyre inkább átalakult és javult az erőművek oktatási és a munkavállalók felé irányult elkötelezettsége (bizonyítja ezt az utóbbi években lecsökkent tűzesetek száma is), tehát bizonyíthatóan az emberi tényező szerepe is befolyásolta – ha közel azonos gépészeti meghibásodási arányt/rátát veszünk figyelembe – a bekövetkezett tűzesetek számát.

Tűzesetek tárgyi okozója (Mátrai Erőmű Zrt.)	**Tűzesetek száma (db) (2000–2012)**
1. Szénpor szabályozatlan eloszlása okozta tüzek (széntér, blokkon belüli környezetben keletkezett)	130
2. Gépészeti meghibásodás miatti, olajelfolyás okozta tüzek (jellemzően turbinaolaj-elfolyás)	66
3. Egyéb emberi tényezők hatása okozta tüzek (pl. karbantartási hegesztés következtében munka- és tűzvédelmi szabályzat elmulasztása – szerelőállványzat meggyulladása)	58
Összesen	254

1. táblázat: Saját szerkesztés a Mátrai Erőmű Zrt. Biztonsági Osztály adatai alapján: a 2000–2012-es időszakokban bekövetkezett tűzesetek tárgyi megoszlása [11]

A tűzesetek száma az előforduló befolyásoló tényezők alapján legnagyobb arányban a szénpor-eloszlás következtében van jelen, azonban további eseteket képeznek még a gépészeti meghibásodásból – pl.: turbinaolaj-elfolyás és a környezeti hő következtében keletkezett tüzek – és az emberi befolyásoló tényezőkből adódó esetek is, amelyek figyelmetlenségek és egyéb nem megfelelő magatartási hatások következményeként keletkeztek (pl. munkavédelmi és tűzvédelmi szabályzatok nem megfelelő alkalmazása, ezzel együtt be nem tartása).

Mivel cikkemben a bekövetkezett erőműves tűzesetek vizsgálatát tűztem ki elsődleges célul, így vizsgálom a bekövetkezett tűzesetek számát és a kiesett termelési kapacitás közötti összefüggést is (2. táblázat).

Az erőmű tűzvizsgálati jelentéseit elemezve az alábbi táblázatban foglaltam össze a különböző esetekben előforduló meghatározó emberi befolyásoltság szerepét a termelési kapacitás és a kiesési gyakoriság megoszlásával együttesen. Egy kiválasztott, több mint 5 éves időintervallumot vizsgálva, a különböző üzemi események (meghibásodási) sorozata mellett az egyén „hibájából" adódó események bekövetkezését lehet tapasztalni (1. táblázat).

A nagyobb veszélyt jelentő tűzesetek létrejöttét azonban a tűzvédelmi jelzőrendszerek és a gyors és szakszerű humánerőforrás-beavatkozás megfelelően kezelte, tehát időben megakadályozta az üzemzavart és a termelési kiesést (2. táblázat).

[11] Szabados Gábor Tamás okl. bányamérnök, jogi szakokleveles mérnök: A természeti adottságok és az emberi tényezők szerepe a bányászati veszélyekben és az azok elleni védekezésben című PhD-értekezésében (Miskolc, 2011.) leírtak mintáján.

Főbb tűzesetek (Mátrai Erőmű Zrt.)	Vizsgált év	Tűzesetek száma	Erőműves üzemzavar/ termeléskiesés (db)	Vizsgálatban megállapított indok(ok)
Szénpor szabályozatlan eloszlása okozta (széntérben és környezetében keletkezett)	2000	0	–	Felgyülemlett szénpor, öngyulladás létrejötte
	2001	3	–	
	2002	0	–	
	2003	0	–	
	2004	2	–	
	2005	4	–	
Szénpor kiszóródása okozta (blokkokon belüli, szállítószalagoknál és környezetében keletkezett)	2000	2	–	Felgyülemlett szénpor, öngyulladás létrejötte
	2001	8	–	
	2002	7	–	
	2003	9	1	
	2004	5	–	
	2005	10	–	
Gépészeti; villamos meghibásodás miatti (pl.: olajelfolyás; villamos zárlat okozta tüzek)	2000	14	–	Rendszeres felügyelet (ellenőrzések), karbantartás
	2001	10	–	
	2002	9	4/1	
	2003	2	–	
	2004	5	–	
	2005	4	–	
Egyéb emberi tényezők hatása (pl. karbantartási hegesztés következtében a munka- és tűzvédelmi szabályzat elmulasztása – szerelőállványzat meggyulladása)	2000	8	1	Emberi magatartási, mulasztási, figyelmetlenségi okok (következmény: egyénre szabott oktatási program fejlesztése, nyílt láng használatának szigorított tilalma)
	2001	2	–	
	2002	3	–	
	2003	4	–	
	2004	5	–	
	2005	6	–	

2. táblázat: Saját szerkesztés a Mátrai Erőmű Zrt. Biztonsági Osztály adatai alapján: 2000–2005-ig a tűzesetek egyes típusai és ezek megoszlása (2014. január–február)[12]

[12] Szabados Gábor Tamás okl. bányamérnök, jogi szakokleveles mérnök: A természeti adottságok és az emberi tényezők szerepe a bányászati veszélyekben és az azok elleni védekezésben című PhD-értekezésében (Miskolc, 2011.) leírtak mintáján.

Megállapítható, hogy nincs összefüggés a termelési kiesés és az emberi befolyásoltság aránya között, következésképp az erőmű biztonságtechnikailag megfelel a teljesítőképesség általános és gépészeti előírásainak, a tűzbiztonság és a védekezési mechanizmus megfelelő. Azonban az emberi tényező visszavezethetőségének szerepe akár jelentősen is befolyásolhatja a kialakult állapotok végbemenetelét pozitív és negatív értelemben egyaránt, így ez is jelentős befolyásoló hatásnak vehető.

További felvetés lehet, hogy mennyire függ össze az emberi tényező a biztonsági tűzjelző berendezések együttes működési rendszerének összehangoltságával, működésével.

Az erőműves jelentések alapján az emberi magatartási, mulasztási, figyelmetlenségi okok, amelyek következményeként egyénre szabott oktatási program fejlesztése, a nyílt láng használatának tilalmára vonatkozó felhívás és szigorítás vagy az előzetesen megfelelően felkészített tűz- és munkavédelmi oktatások voltak azok az emberi tényezők, amelyek a tűz keletkezésének létrejöttét elősegítették vagy éppen megakadályozták. Ezenkívül jellemző esetek a szénpor-kiszóródás okozta veszélyek, melyekre a jövőben is oda kell figyelni, mint ahogy a nemzetközi irodalmak is nagy hangsúlyt szentelnek a kérdésnek, habár az eltérő környezeti és műszaki befolyásoltsági szintet figyelembe kell vennünk.

Zárásként pedig azt vizsgáltam, melyek azok az emberi tényezők, amelyek a tűzesetek létrejöttekor a leginkább előfordultak.

Az ember – mint a működő rendszer egészét alkotó elem – ahogy az adott technológia irányítását és szabályozását kézben tartja, úgy kiváltó okozója/faktora is lehet egy rendszer egyensúlyát megbontó veszély vagy, súlyosabb esetben, egy baleset létrejöttének. Ezen megállapítás tudományos hivatkozásban az alábbi megfogalmazásban szerepel: az emberi teljesítmény alapvető hatást gyakorolhat a komplex műszaki rendszerek megbízhatósági és biztonsági szintjére. A megbízhatósági, illetve kockázatelemzésekben az emberi kölcsönhatások megfelelő kezelése a legfőbb tényező a balesetsorozatok és a teljes kockázatbeli relatív fontosságuk megértéséhez. Az emberi megbízhatósági vizsgálatok (HRA) céljai, hogy a kulcsfontosságú emberi kölcsönhatásokat módszeresen beazonosítva elemezzék, így ezeket nyomon követhetően építsék be a biztonsági elemzésekbe/vizsgálatokba. Ezek mellett a sikerek és kudarcok valószínűségének számszerűsítése mellett olyan kitekintést szükséges nyújtani, amely fejlesztheti az emberi teljesítményt.

Fontos kiemelni itt is a teljesítmény fejlesztésekor kiemelkedő elemeket. Ilyen lehet az ember és a gép egymáshoz illesztése, a folyamatok és az oktatási struktúra fejlesztése, a munkakövetelmények és az emberi képességek jobb összehangolása, a sikeres helyreállításra vonatkozó tanulmányok széles körű kiaknázása, illetve az egymással korreláló emberi hibák hatásainak csökkentése és javítási vonatkozásai.

Ebben a cikkben is megfogalmazódik, hogy az emberi teljesítményelemzések rendszerezése és folyamatos tematizálása mekkora jelentőséggel bír, hiszen ezzel hosszú távon kiküszöbölhető a komplex műszaki berendezések biztonságának és üzemkészségének indokolatlan, az emberi tényező általi meghibásodása és veszélyeztetése.

Az emberi tényező szerepét már az atomerőművek biztonságos üzemvitele és működése szempontjánál is elemezték, melyben megállapították, hogy *„olyan komplex rendszer, amely technológiai és emberi tényezőkre épül, a biztonság szempontjából is ezt a kettősséget mutatja”*.[13]

A fentiekben elkészített elemzésemben, a 2000-től 2005-ig terjedő időszakban vizsgált esetek számából látható, hogy a szénpor-kiszóródások (és egyéb leggyakrabban előfordult esetek) okozta tüzek milyen események kapcsán, illetve milyen események következményében oszlottak meg.

Ezek felülvizsgálatára a jövőben is sor kerülhet, illetve megakadályozásuk céljából ezeken a területeken különösen érdemes növelni a biztonsági szintet, továbbá az emberi kockázati tényező szerepét, amilyen mértékben csak lehet, csökkenteni. Ezt alátámasztja az amerikai feljegyzésben összefoglalt, a szénporrobbanásról szóló gondolatok listája is, azonban ez példának okáért a megoszlási arányokat nem írja le, ami helyileg ugyan eltérhet, de az egyes széntípusok alkalmazása esetén azonos lehet (pl. a magyarországi lignit esetében az ME-ben az alábbiak szerint alakult vagy alakulhat a jövőre vonatkozóan is hasonló erőműves beruházás utáni működés részeként).

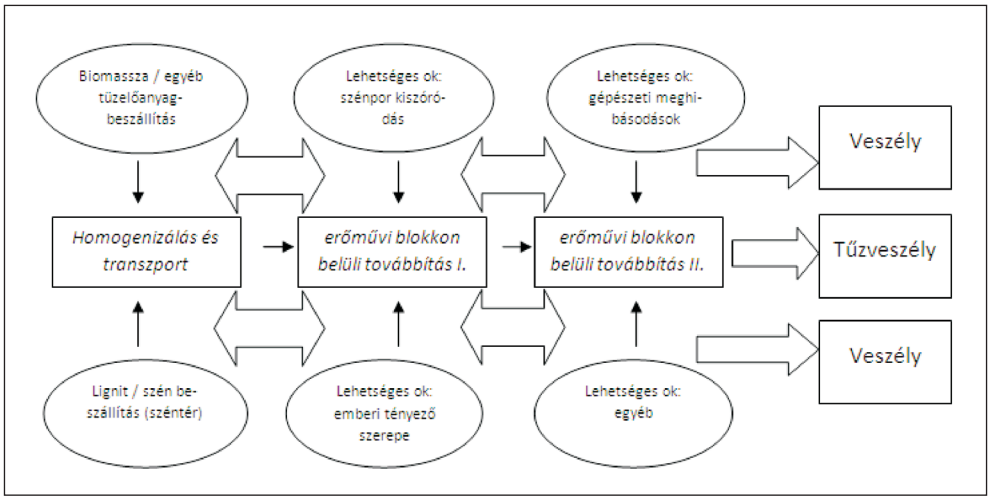
Leolvasható, hogy a széntértől a kazánokig tartó transzportfolyamat során a keletkezett, szénporeloszlás okozta tűzesetek száma nagyobb arányban a széntérben és környezetében fordult elő, továbbá a blokkok területén belül a villamos rendszerekkel együttesen okozott vagy okozhatott volna nagyobb veszélyt vagy katasztrófát.

Külföldi kockázatelemzési tanulmányokat kutatva megállapítottam, hogy több olyan kimutatás és elemzés létezik, amely az egyes erőműveknél különböző kockázati tényezőket említ és elemez. Azonban olyan kutatás, amely a transzportálási és eltüzelési folyamatok között lezajlott eseményeket – szénpor-kiporzás, gépészeti meghibásodások, emberi befolyásoló szerep – külön-külön és az ezekből keletkezett tüzeket elemezné, egymáshoz viszonyított arányát és gyakoriságát vizsgálná, nem történt. Az előzőekben bemutatott és elemzett tűzesetek bekövetkezését és ezek csökkentési alternatíváit hivatott bemutatni az általam elkészített, a lehetséges tűzkialakulási helyeket és a hozzájuk tartozó, leggyakrabban előforduló/előfordult kiváltó tényezőket bemutató ábra is, mely a lehetséges és előfordult események területét mutatja lignit erőművek esetén.[14]

A tűzesetek területi megoszlása az erőművön belüli egységeket tekintve:

[13] Kovács Judit, Az emberi tényező szerepe komplex rendszerek kockázatelemzésében. Védelmi elektronika folyóirat.

[14] Saját szerkesztés (rajz): NAMPOWER, Coal-Fired Power Station. Namibia Environmental, Environmental and Socio-Economic Risk Assessment Report,, Reference Number: 5975; 15 May 2012. Prepared by Aurecon South Africa (PTY) Ltd. (2014. 01. 09.)



6. ábra: Tűzkialakulási helyek és a hozzájuk tartozó, leggyakrabban előforduló/előfordult kiváltó tényezők az erőmű nyersanyag-szállítási és -elosztási folyamatánál (saját szerkesztés)

Összegzés

A publikáció során bemutattam és elemeztem a hazai szenes és együttes biomassza felhasználású erőművek teljesítményadatait, valamint ezeknek a hazai energia-előállítási struktúrában elfoglalt helyzetét a mai állapotok és ismeretek szerint. Véleményt formáltam, továbbá számszerű adatokkal alátámasztottam stratégiai helyüket a magyarországi energiaiparban, és ezen túlmenően bemutattam a biztonságtechnika és tűzvédelem témakörében történt eseteket, esettanulmányokat. Ezenkívül elemeztem az erőműves gépészeti működési és meghibásodási okokra visszavezethető veszélyeket, a tüzek keletkezését, emellett az emberi tényező befolyásoló szerepét is, amely alapján biztonságnövelő alternatív megoldási lehetőségeket vetettem fel.

Megvizsgáltam az emberi tényező szerepét, és elemző összehasonlítást végeztem a nemzetközi tapasztalatok alapján egy magyarországi erőmű eseteit vizsgálva. Az emberi hibák mellett azonosítottam az emberi pozitív gondolkodás, helyzetfelismerés és cselekvőképesség szerepét is.

A tűzesetek vizsgálata kapcsán el lehet mondani az összetett tényezők és többszörösen egymásra ható rendszerelemek kölcsönhatását, melyből általános érvényben a gépészeti meghibásodási tényezőkön túlmenően az ember befolyásoló és az egész rendszerre nézve kiható szerepét lehet megállapítani. Ezeken túl véleményem szerint a dominóelv (egymásra ható befolyásoló szerep) is megjelenik ezen eseteknél, amelyek a jövőben további vizsgálatok alapját adhatják, így újabb elemzéseket lehet majd készíteni a témakör kapcsán.

Összességében megállapítható, hogy ha közel azonos megoszlást mutatnak is az eset-

számok, és az ember–gép–környezet egymásra jelentős befolyásoló szereppel is bír, az adott tüzelőanyag milyenségén is múlik, hogy milyen mértékű veszély keletkezhet a tüzelési folyamatok szabályozatlan és irányítatlan lejátszódása közben. A balesetek megelőzésére és elkerülésére a már jó úton járó fejlesztések jelenthetnek megoldást, így a fokozott biztonsági és tűzvédelmi előírások, a strukturált és célzott oktatáspolitika és az erőforrás-gazdálkodás bírhat kulcsszereppel – az általános műszaki előírások betartása mellett.

Irodalomjegyzék

1. Mátrai Erőmű Zrt. hivatalos honlapja (online), http://www.mert.hu/hu (2014. 01. 25.)
2. N. K. Mohalik – D. C. Panigrahi – V. K. Singh: Application of thermal analysis techniques to assess proneness of coal to spontaneous heating. http://link.springer.com/article/10.1007%2Fs10973-009-0305-z#page-1 (2013. 12. 29.)
3. Szabados Gábor Tamás okl. bányamérnök, jogi szakokleveles mérnök: A természeti adottságok és az emberi tényezők szerepe a bányászati veszélyekben és az azok elleni védekezésben. PhD-értekezés, Miskolc, 2011.
4. Mátrai Erőmű Zrt. Biztonsági Osztály – Kalorikus Osztály adatai: konzultációk, jelentések erőművi dolgozókkal (2014. január–február)
5. MAVIR Zrt. hivatalos honlapja (online), http://www.mavir.hu/documents/10258/15461/Forr%C3%A1selemz%C3%A9s_2013.pdf/0a51f06c-73e7-4607-b582-00d3b1434837 (2014. 01. 12.)
6. BME Energetikai Gépek és Rendszerek Tanszék hivatalos honlapja (online), http://energia.bme.hu/~kaszas/Energiapolitika/OszJanos/Meg%C3%BAjul%C3%B3%20energiaforr%C3%A1sok.pdf (2013. 12. 14.)
7. Európai Bizottság hivatalos honlapja (online), http://ec.europa.eu/news/energy/120608_hu.htm (2014. 01. 11.)
8. INC – JUSTIN CLIFT, Hazard Control Technlogies; COMBUSTIBLE DUST előadás anyaga, online, www.hct-world.com (2014. 01. 04.)
9. NAMPOWER, Coal-Fired Power Station. Namibia Environmental, Environmental and Socio-Economic Risk Assessment Report,, Reference Number: 5975; 15 May 2012. Prepared by Aurecon South Africa (PTY) Ltd. (2014. 01. 09.)
10. Kovács Judit: Az emberi tényező szerepe komplex rendszerek kockázatelemzésében. Védelmi elektronika folyóirat.
11. Kajati György: A magyar villamosenergia-ipar posztszocialista átalakulása. Doktori (PhD) értekezés, Debrecen, 2008.

Distribution of fire cases and the role of human factors in coal-firing power plants in the field of fuel-supply and distribution systems

Zele Balázs

Today's energy policy places a growing emphasis on environmental and general fire safety issues, whence follows that safety regulations of power plants have increased significantly. As a result, fire cases in plants which occur from delivery to combustion, the education of personnel and the improvement of safety regulations are key issues to be addressed. In this paper I examine the distribution of fire cases and the role of human responsibility in a Hungarian lignite-fired power plant while drawing on foreign publications and researches.

Horváth Tamás
Kovács Tibor

Possibile application of thermal cameras with regard to security engineering

Not even professionals of security technology encounter thermal cameras frequently during their work experience because their usage, let alone their cost restrict them for industrial and military use. The human eye is capable of seeing only a very small part of the electro-magnetic spectrum. We are able to pick up neither UV nor IR ranges. High-tech equipment is required for that purpose. Security professionals discover more and more areas for the use of thermal images. It is worth focusing on thermal cameras and their potentials in more detail and settling for the fact that lenses can be made of metal.

Applications of thermal cameras in the field of security technology

Scientifically speaking, thermal convection has been used for thousands of years. In this respect we are very much like our ancestors. Sitting around the open fire or next to the fireplace intending to catch the warm streams looking for the hottest spots indicates that we are looking for thermal convections. Therefore it is worth knowing background of what we are doing. Our palms may be used as thermal sensors to find the most comfortable place. Today this physical phenomenon is increasingly applied by scientists with such stunning results that security protection systems installed at high-security-risks facilities may benefit from them.

General review

The reason for the first steps of development can easily be given: there were clear-cut military motives: ensuring visibility in darkness without any kind of light and becoming capable of visual observation under low visibility conditions and on battlefields.

The theory of bolometer has been known for years: the measurement of electromagnetic radiations sent by objects and living beings with the help of temperature-dependent resistance. This theory was elaborated by Samuel Pierpont Langley in 1878, which then

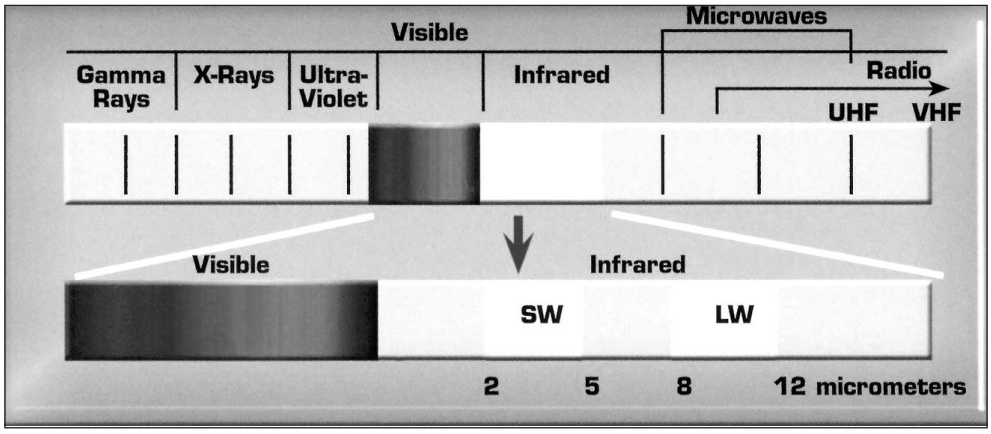
was followed by a pause of a hundred years in development. Although the theory had been invented, the electronic industry was lagging behind. The engineers had to wait for fast electronic devices which were able to process the signals of the sensor in time.

Milestones of development

→ 1960s – First sensor invented and published by Texas Instruments, Hughes Aircraft, Honeywell
→ 1980s – USA Government's program for uncooled detectors
→ 1991 – Production increased due to the Gulf War, prices decreased
→ 1994 – Invention of micro bolometer by Honeywell, new developments started by Boeing, Lockheed Martin, British Aerospace
→ 1998 – First detector introduced by Bullard for fire department

The basics

Before indulging in the details of the operation of thermal cameras, their physical basics are worth clarifying. The technology makes use of the wavelength range from 1 μm to 1 mm. The most common wavelength used for security applications are from 8 to 12 μm which is a range of LWIR[1]. There is a wide variety of military applications in which the devices operate at the longest infrared range at times (Fig, 1).



Fig, 1 Electric magnetic radiation ranges

[1] LWIR – Long Wave Infrared

The range of thermal radiation ranked in bands:

- Short Wave Infrared (SWIR), from 1μm to 3 μm
- Mid Wave Infrared (MWIR), from 3 μm to 5 μm
- **Long Wave Infrared (LWIR), from 8 μm to 12 μm**
- Very Long Wave Infrared (VLWIR), from 12 μm to 25 μm
- Far Wave Infrared (FWIR), from 25 μm to 1 mm

The sensor

A thermal sensor called microbolometer is used in thermal cameras applied in the field of security which is a bolometer made specifically for thermal cameras. The most frequent starting material is the grid of vanadium oxide (VO) or amorphous silicon. Vanadium oxide is a correct choice for sophisticated security applications as VO changes its resistance in almost all ranges used for thermal cameras. Electronically, the resistance of VO is approx. 100 kΩ making it applicable for various circuits.

Basic parameters

The comparison of thermal cameras is a sophisticated task. For professionals dealing with CCTV[2] systems it is essential to set up a standard control method to be able to compare all technical parameters correctly in the case of comparing cameras operating at visible light. We must follow correct determination but in this case we have a special built-in component called microbolometer. Its main physical parameter is the NETD[3] showing the required camera 'sensitivity' which determines the temperature difference the camera is able to detect. Obviously, this technical parameter should be checked with a fixed F Stop parameter[4].

e.g. 50 mK[5]=0,05 ^{O}C at F1.2

The resolutions of the bestselling microbolometers are the following:

→ 640 x 480
→ 320 x 240
→ 160 x 120

[2] CCTV – Circuit Closed Television System
[3] NETD – Noise Equivalent Temperature Difference
[4] F STOP – Controls the size of the aperture of the camera "lens"
[5] mK – Kelvin/103 – temperature measuring unit called Kelvin

Since 2008 the megapixel category of microbolometer (1024 x 768) has been in the market, with the 1 MP or higher resolution bolometers made for the Army.

The most common approach today is applying the highest resolution cameras for all purposes. However, in the case of thermal cameras a high resolution video analysis is generally not necessary. Therefore, it is sufficient to apply a camera with a lower pixel number.

Physical processes

After having revised different camera parameters let us focus on the operation of the bolometer sensor itself.

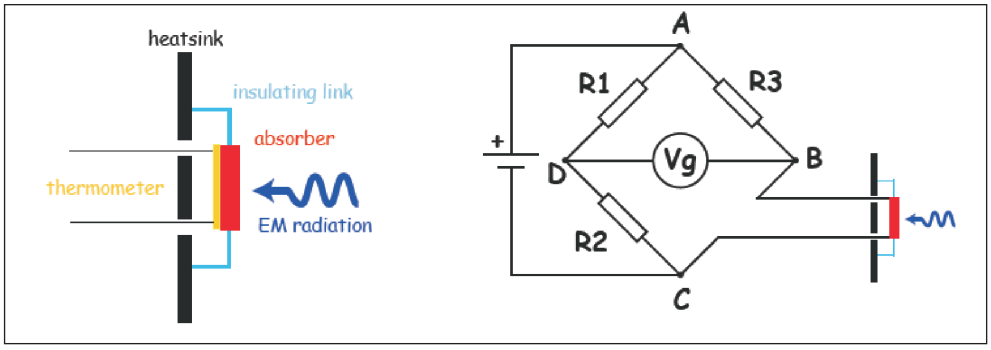


Fig. 2 Microbolometer (resistive)[6]

Fig. 2 demonstrates the physical operation of the bolometer. The type depicted is a resistive one, which adjusts its resistance to thermal radiation, making it applicable in a simple measuring circuit.

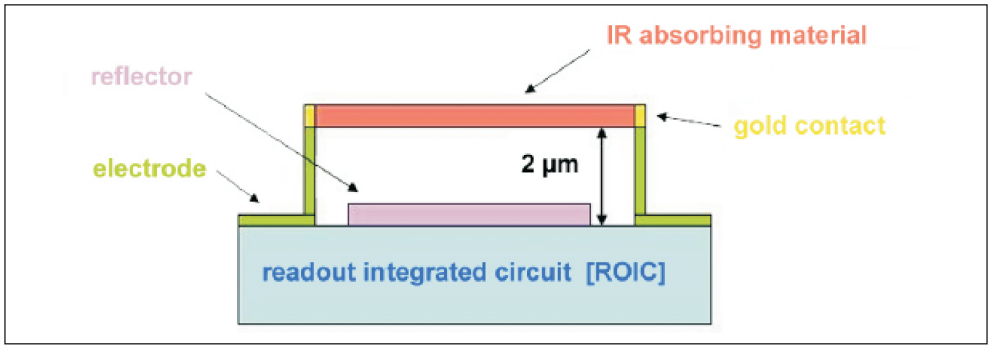


Fig. 3 Microbolometer structure

[6] J-D Ganiere – Experimental Methods in Physics (2011-2012) – course

Fig. 3 demonstrates the bolometer structure. The main goal is to set NETD as low as possible for engineers to maintain a gap between the readout circuit and the bolometer itself so that the thermal noise rate can remain at a low level.

The differencial equation of heat convection

The heat convection can be expressed by a mathematical equation. A simple equation of the heat convection can describe the heat difference which can be distinguished by the thermal detector at determined wavelengths. The most significant equations are as follows:

Differential equation of heat convection:

$$C\frac{d(\Delta T)}{dt} + G(\Delta T) = \eta P = \eta P_0 e^{j\omega t}$$

The value of the heat change:

$$\Delta T = \frac{\eta P_0 e^{j\omega t}}{G + j\omega C} = \frac{\eta P_0}{G\sqrt{1 + \omega^2 \tau^2}}$$

Time constant:

$$\tau = \frac{C}{G}$$

Where:

C: heat capacity of the bolometer membrane

G: heat draining of the bolometer and its surrounding

P_0: power of the thermal radiation touched by the bolometer

η: proportionality factor

ω: circular frequency of radiation

ΔT: temperature change of membrane

Resitive bolometer

The definition of a resistive bolometer is when the resistance of the detector changes significantly depending on the temperature of the device. Equations to be applied:

Resistant change on sensor:

$$\Delta R = \alpha R \Delta T$$

Temperature coefficient of the bolometer:

$$\alpha = \frac{1}{R}\frac{dR}{dT}$$

Temperature coefficient of metals:

$$\alpha = 0{,}002\,\frac{1}{°C}$$

Having used the equations we can determine the terminal voltage depending on the current at the working point.

Terminal voltage on the bolometer:

$$VS = \frac{i_b \alpha R \eta P_0}{G\sqrt{1+\omega^2\tau^2}}$$

Finally, terminal voltage can be determined:

$$V_s = i_b \Delta R = i_b \alpha \Delta R T$$

The electronic characteristics described by the above equations are suitable for generating video images after the necessary adjustments. There are other bolometers which work according to different physical parameters (ferroelectric, pyro electric, thermoelectric). In security technology resistive bolometers provide numerous advantages due to their accuracy of resistance being an electronic parameter.

Types of detectors

The required goals can specify the types of bolometers in which the micro bolometer would be built. In the case of military applications, the cooled micro bolometer utilisation is widely accepted. The coolant is to be used for receiving higher sensitivity, which means NETD values could be reduced to 10^{-1} compared to types used in security industry.

Cooled detectors

Advantages

- Suitable for multispectral applications
- Applicable for high speed movements detection
- Outstanding sensitivity

Disadvantages

- Expensive technology
- Considerably more sizeable than the uncooled version
- Long period of MTBF
- High energy consumption

Known applications

- IR-headed missiles (air-to-air missiles sensitivity could be extremely high, e.g. they can be applicable from 10-20 km, e.g. AIM-9M Sidewinder and FIM-92 Stinger)
- Border guard applications
- Maritime applications

Fig. 4 IRIS – T air2air missile on beam

Non-cooled detectors

The spread of non-cooled micro bolometers has been supported by the development of circuits. At first mass production was only present in military development but later economic reasons enforced the increase of production capacity. Civil applications include fire departments, civil aviation, flying in foggy weather, etc.

Fig. 5 Thermal camera in aircraft (a);

Fig. 6 Thermal camera in aircraft (b)

As it can be seen, the security risk of aviation could be reduced by an EVS[7] built-in thermal camera system.

[7] EVS – Enhanced Vision System – Extending visibility of pilots in foggy weather.

Advantages

- the small size of non-cooled micro bolometers is suitable for standard size box cameras
- Real time signal
- Low energy consumption
- Very long period of MTBF
- affordable for civil industrial production

Disadvantages

- Low sensibility compared to cooled ones
- Unsuitable for high speed movements and multispectral applications
- Thermal radiation can be shaded by glass so the lenses must be made of a special material

Applicable lenses

No cameras may be manufactured without lenses so we should also use objectives for thermal cameras. The thermal radiation must be transferred to the micro bolometer grid which can be done by lenses made of a special material. It is evident that thermo convections cannot pass through glass so developers should turn to other materials. Although there are other possibilities, one of the best kinds of material proves to be germanium for security cameras.

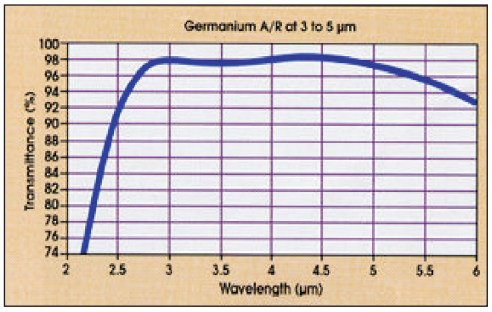


Fig. 7 Ability of thermo convection transfer by Germanium (Ge)

Base material for lenses

- germanium (Ge)
- zinc selenide (ZnSe)
- zinc sulphide (ZnS)ZnS
- zinc sulphide multispectral (ZnS MS)
- silicon (Si)
- calcium fluoride (CaF_2)
- amorphous material transmitting infrared radiation (AMTIR[8])

In accordance with the goals of applications professionals may select the best type

[8] AMTIR – amorphous material transmitting infrared radiation

of material for lenses. The transmitting ability of infrared radiation always depends on the wavelength in the IR band. If the requirements of resolution are relatively low (e.g. 320x160 pixels), amorphous plastic may also be used. There is an important parameter of germanium: the metal (Ge) itself is so soft that even nails can scrape and damage its surface. Scratched germanium lenses go wrong instantly; therefore the surface of lenses must be protected. Many thermal cameras have non-removable objectives and can only be disposed of as one piece, which raises the costs in the case of a single damaged lens.

Surface coating

- BBAR (broad band anti-reflective)
- Creep BBAR
- DLC (diamond-like carbon)

Besides surface coating, mechanical protection is quite common in the military industry, where lens covers can be removed by remote control.

Manufactures

There are a few dominant manufacturers for thermal cameras in the market, some of the most important firms are listed below:

- FLIR Systems (USA)
- OPGAL Optronics Industries (Israel)
- E.D. Bullard Corporation (USA)
- Axis Communications (Sweden)
- Tainjin SEC-EGO Electronics ltd (China)
- IRCAM (Germany)

Thermal cameras in practice

Unfortunately, professionals do not frequently encounter cases in their job where thermal cameras are applied or installed in practice. The obvious reason is they are too expensive to be widespread. However, sophisticated solutions for clients working in special industry areas (e.g. electric power plants) do require the application of these devices.

As mentioned before, the video streams provided by thermal cameras are not made for constant security guard or operator surveillance, their main function facilitates video analysis. Only in a few rare solutions should the operators control the camera pictures as a normal video stream. Instead, the video analyser software of the device induces controls switching on other subsystems or alerts security guards for operative activities following

the macro regulation set previously. It is best if the analyser program made for thermal cameras directly support the required activities.

Basic video-analysing rules[9]

Detection Rules/Behaviors	
Person	Person moving in an area
	Person crossing a line
	Crowding
	Person tailgating
	Loitering
	Grouping
Vehicle	Vehicle moving in an area
	Vehicle crossing a line
	Stopped vehicle
	Tailgating vehicle
Static Object	Suspicious object
	Traffic obstacle
	Asset protection
Counting	Count people
	Count vehicles
	Measure stickiness (dwell time)
PTZ	Preset – Person moving in an area
	Preset – Person crossing a line
	Preset – Vehicle moving in an area
	Preset – Vehicle crossing a line
	Autonomous Target Tracking

[9] Downloaded: http://www.agentvi.com/61-products-62-vi_system

Detection – recognition – identification

A few quite important parameters of thermal cameras must be prioritised when selecting a device. Their data sheets may indicate excessive distances for camera reach. Technical details must be dealt with care, bearing in mind that the phrase 'up to' in front of numbers refers a maximum, rather than a general range. As mentioned before, the one essential technical parameter is NETD. There is another one which shows what kind of pictures can be obtained from the camera in question from a certain distance. It is the DRI[10], an abbreviation explained below.

Detection

Detection is a capacity of the thermal camera which means the camera in question is able to make temperature difference between two points in its view angle. In practice this means 2 pixels / meter only. This can indicate the presence of a moving person if the camera has been installed to detect motion.

Recognition

Recognition is a capacity of the thermal camera where well-trained operators are able to determine from the provided video stream the presence of cars or people or animals in the picture. In practice this means 8-10 pixels / meter. This enables the differentiation of people in the camera image.

Identification

Identification is a capacity of the thermal camera where well-trained operators are able to conclude from the provided video stream that in the picture there are solders with guns. In practice this means 16-20 pixels / meter! This makes the users capable of recognizing people with weapons.

CCTV usually uses a specific set of guidelines for Detection, Identification & Recognition (DRI) of an object or person. This typical equates to D=10%, R=50%, I=120% of screen height.[11]

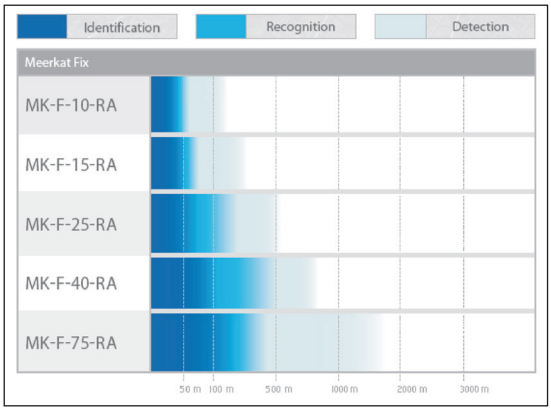


Fig. 8 DRI parameters of a few thermal cameras

[10] DRI – Detection – Recognition – Identification
[11] https://www.dedicatedmicros.com/europe/products_details.php?product_id=263

As an example, the following DRI parameters can be deduced with regard to MK-F-75-RA thermal camera produced by Xenics.

- Detection:1.800 m;
- Recognition: 450 m;
- Identification: 120 m.

An example in practise:

Fig. 9 Meaning of DRI

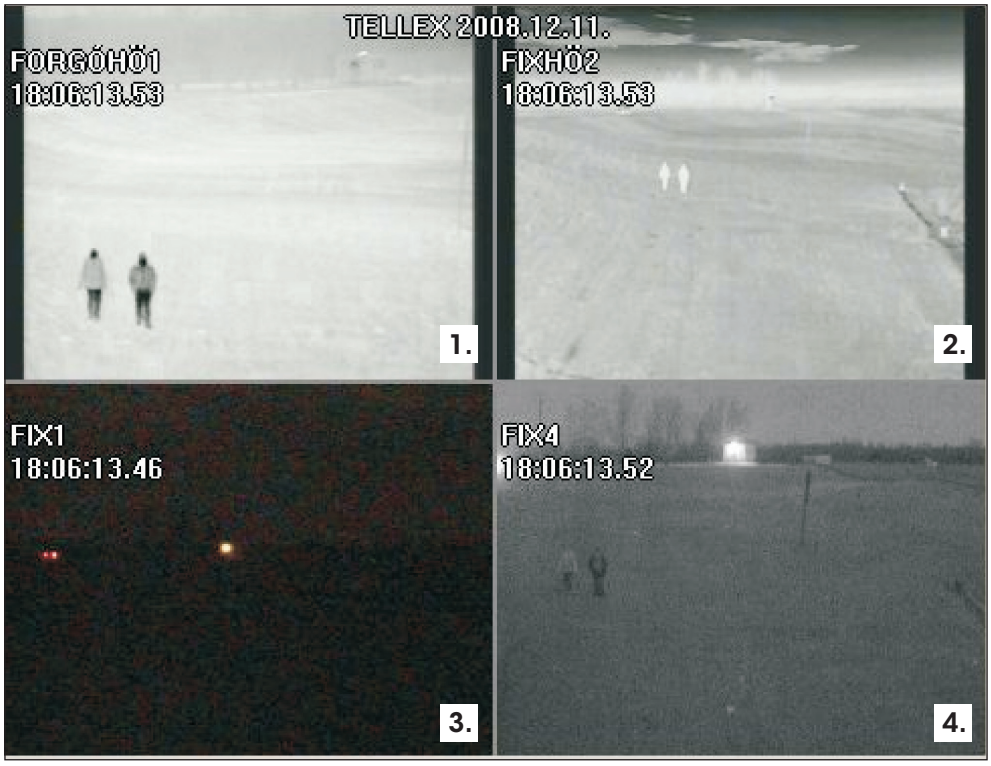
Summary

In conclusion we can say that the application of thermal cameras should considerably decrease the security risks if these applications are selected very carefully. The focus of our clients must be directed to their advantages. The prices of these cameras will shortly become low enough to be accessible and affordable for even domestic users.

A few pictures of thermal cameras

Fig. 10 Detecting and tracking down a car

Fig. 11 Detecting and tracking a moving person



1. Camera resolution: 640x480 pixel
2. Camera resolution: 320x240 pixel
3. Camera resolution:D1 quality D&N
4. Camera resolution: D1 but with special built-in software

Fig. 12 Thermal camera test

Bibliography

http://www.xenics.com/documents/20090714_LR_Meerkat_security_A4.pdf
http://www.marchnetworks.com
W. Radford; R. Wyles; J. Varesi; M. Ray; D. Murphy: Sensitivity Improvements in Uncooled Microbolometer FPAS
Peter Kornic: Selecting lenses…Janos Technology Inc.: http://www.janostech.com/thermal_image_lenses/index.html
ICU (Infrared Imaging Components for Use in Automotive Safety Applications): www.icu-eu.com
http://www.lumitron-ir.com/application_security.php
http://www.opgal.com/
http://www2.l-3com.com/irp/products/security.htm
www.flir.com
Matyi Gábor: Nanoantenna-mom dióda szenzorok elektrodinamikája 2007 (PhD thesis)
J-D. Ganiere: Experimental methods in Physics (2011-2012)

Hőkamerák lehetséges alkalmazása, tekintettel a biztonságtechnikára

Horváth Tamás – Kovács Tibor

Gyakran még a professzionális biztonságtechnikai hőkamerák sem felelnek meg egyes szakmai követelményeknek, mert alkalmazhatóságuk és nem utolsósorban költségük korlátozza az ipari és katonai feladatokra történő felhasználást. Az emberi szem az elektromágneses spektrumnak csak egy nagyon kis részét képes látni. Nem vagyunk képesek érzékelni sem UV-, sem infravörös tartományban. Ilyen feladatokra high-tech berendezések szükségesek. Biztonsági szakemberek egyre több területen használnának termikus képeket. Érdemes tehát részletesebben foglalkozni a hőkamerákkal és azok alkalmazhatósági lehetőségeivel.

Mógor Tamásné
Rajnai Zoltán

Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása

A nemzet érdekében kiemelten fontos – a napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.
Társadalmi elvárás az állam és polgárai számára elengedhetetlenül szükséges elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.[1] A publikáció a biztonságtudomány területéhez kapcsolódó kockázatmenedzsment, kockázatelemzési módszerek bemutatásáról, összevetéséről szól.

Bevezetés

Az információ megszerzése és védelme ősidők óta foglalkoztatja az emberiséget. Ez a tevékenység az emberi társadalmakkal együtt alakult ki és fejlődött.

A kezdetleges számítógépek megjelenésekor, majd később a fejlett, adatkezelő rendszerek kifejlesztésével azonban az információ megszerzésének és védelmének jelentősége, módja is megváltozott.

A 19. század végétől kezdve olyan dinamikus változások kezdődtek az egész világon, melyek az élet minden területén gyors fejlődést, átalakulást eredményeztek. Gondoljunk csak a közlekedés, a híradás, az energetika területére, melyek rendkívüli változást hoztak az emberiség életében, ugyanakkor sérült az egyén, a közösségek, a nemzetek, az országok, vagyis az egész világ biztonságérzete. Az ember nem tudta felvenni azt a dinamikát, amit a fejlődés diktált. A túlzott, gyors és hirtelen fejlődés helyett lassú, szerves, kidolgozott folyamat lenne ideális. Az 1900-as évek közepétől pedig egyre jelentősebb szerepet kapott a biztonság kérdése.[2]

[1] 2013. évi L. törvény bevezető rész.

[2] Biztonság: komplex fogalom, egy folyamatosan változó helyzet fokmérője, az egyén, társadalom komfortosságának fokmérője.

A biztonság magas szintje csak korszerű védelmi, biztonságtechnikai rendszerekkel valósítható meg. Az elvárt biztonsági szint egyre növekszik, mivel a biztonságtechnikai rendszerek egyre bonyolultabbá válnak. Az integrált, komplex biztonság a magas biztonsági szint elérésének alapvető követelménye, hogy figyelemmel kísérjük az adott rendszert, feltárjuk, elemezzük a kockázatokat, melyek veszélyeztetik a rendszer működését. Ezután próbáljuk a kockázatok szintjét és mennyiségét úgy csökkenteni, hogy a lehető legbiztonságosabb működést érjük el.

Ebben a folyamatban van egy szerves alkotóelem, maga az *ember*, hiszen ő a biztonság megteremtője és fenntartója.

Az Amerikai Egyesült Államokban már az 1970-es években teret hódított az információbiztonsági értékelés következetes rendszerének kidolgozása, előtérbe helyezése. Idővel mindez átterjedt Európába, Magyarországon pedig 1996-ban kapott jelentősebb szerepet, amikor a Miniszterelnöki Hivatal hazai ajánlást adott ki *Informatikai Rendszerek Biztonsági Követelményei* címmel.

A 2001. szeptember 11-én történt események megerősítették azt az elvárást, hogy a szakembereknek fel kell készülniük a legváratlanabb eseményekre is. Sajnos a veszélyek és kockázatok növekedése egyre hangsúlyosabb szerepet szán olyan tevékenységeknek, mint a kockázat megelőzése, a védekezés, a védelem, a biztonság.

Az EU 2002/43-as határozata arra szólít fel, hogy minden ország – ahol ez lehetséges – indítson információs oktatási kampányokat annak érdekében, hogy az információbiztonság egységessé, nemzetközileg elfogadott szabályozáson alapulóvá váljon, az elmélet és gyakorlat szintjén is megalapozott, alátámasztott legyen.

A kockázatmenedzsment mint a biztonság alapja

A bevezetőben már említettük, hogy a kockázatmenedzsment előtérbe helyeződése elsősorban a technika rendkívül gyors fejlődésének köszönhető. Napjainkban a szervezetek sikeres működése már szinte lehetetlen informatikai eszközök használata nélkül. Az elmúlt 25-30 évben az informatikai rendszerek életünk szerves részévé váltak. Jelen vannak a magán-, az állami, a védelmi, az üzleti szférában, és itt egyre inkább kitüntetett szerepet kapnak.

Az informatikai rendszerek védelme minden esetben a szervezet vezetésének a felelőssége, és ez a felelősség nem áthárítható (azonban megfelelő körülmények biztosítása esetén delegálható). A szervezet külső szervezeteket is megbízhat (például kiszervezés keretében) a védelmi rendszer kialakításával, működtetésével és a működés ellenőrzésével, de a teljes kontrollkörnyezet megfelelőségének biztosítása ez esetben is a vezetőség feladata marad.

Az IT-rendszerek központi szerepe és sérülékenysége miatt napjainkban elengedhe-

tetlen az informatikai rendszereket fenyegető veszélyek feltérképezése és a kockázatok megfelelő kezelése, menedzselése. A szervezetnek ki kell alakítania a tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét, és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.

Egyes felmérések[3] szerint a vállalati vezetők 60%-a évente minimum 1 incidensre számít, 5 évente pedig minimum 1 súlyos adatvesztéssel járóra.

A kockázatelemzés eredményeként kidolgozhatók a megfelelő védelemhez szükséges kockázatkezelési stratégiák. Az IT kockázatmenedzsmenti programok kialakítása során figyelembe kell venni a szervezet specifikus kockázati profilját, üzleti céljait az újabb kockázatok elkerülése érdekében.

A kockázatmenedzsmenteket helyesen alkalmazó szervezetek kevesebb incidensre számíthatnak. Egy átfogó szemléletmód kialakítása szoros összefüggésben és egyenes arányosságban van a hatékonysággal és az incidensek számával.

Az informatikai technológia ilyen kiemelt szerepe komoly veszélyeket is rejt magában. Minél bonyolultabb egy adatkezelő rendszer, annál nagyobb fenyegetettségnek van kitéve, a működése során fellépő hibák pedig rendkívül súlyos veszteségekkel járhatnak.

A fenyegetések, veszteségek kialakulásának megelőzésére, megakadályozására hivatott az IT-kockázatmenedzsment, amely önálló területté nőtte ki magát. Feladata, hogy a rendszert fenyegető veszélyeket felmérje, a megfelelő védelmi stratégiát kidolgozza. Csak komplex, átfogó, mindenre kiterjedő stratégiák alkalmazása segítségével küszöbölhetők ki a gyenge pontok okozta fenyegetések. Olyan szilárd rendszer kialakítására kell törekedni, amely minden pontján egyenlően erős, ezáltal hatékony védelmet képes nyújtani.

Az informatikai rendszerek biztonságának megteremtése magában foglalja a következőket:

- a számítástechnikai eszközöket, rendszereket,
- az informatikai rendszerek környezetét,
- az informatikai rendszerekkel kapcsolatba kerülő személyeket,
- a rendszerekre, üzemeltetésükre vonatkozó szabályozásokat, előírásokat, dokumentumokat.

Az informatikai rendszerek védelmét jelentősen befolyásolja, hogy ahány szervezet, annyiféle kockázati profil létezik, azonban vannak olyan általános szabályok, amelyek figyelembevétele és a kockázatmenedzsmentbe való beépítése igen fontos. Ezek a következők:

[3] Információbiztonsági helyzetkép 2011.

- *nincs tökéletes biztonság;*
- a helyes kockázatelemzés feltétele, hogy tisztában legyünk azzal, milyen elemekből áll az adatkezelő rendszer, milyen helyzetben üzemel, ki és hogyan üzemelteti;
- belátáson alapuló biztonság helyett „biztonságtudatos magatartást" tartsunk szem előtt;
- egységesítésre való törekvés – *szabványosítás;*
- saját információs vagyon értékének ismerete;
- a szervezet saját biztonságával kapcsolatos szándéka (betartás, betartatás);
- az általános és helyi szabályzók összehangolása;
- fel kell ismerni, hogy a kockázati tényezők milyen súlyúak az adott rendszer esetében, meg kell becsülni bekövetkezési valószínűségüket;
- alapelvek érvényesülése;
- hatékonyság, objektivitás;
- *a dokumentálás pontos, jól érthető, folyamatos legyen.*

A kockázatelemzés legfontosabb előnyei az alábbiak:

- a potenciális veszélyeket módszeresen azonosítja;
- kiszűri a „gyenge láncszemet"; ez azért fontos, mert minden rendszer olyan erős, mint a benne lévő leggyengébb láncszem;
- kockázati rangsort állít fel;
- mélyen képes megismerni a rendszer szerkezetét;
- lehetséges módosításokat, megoldásokat ajánl a kockázat csökkentése érdekében (feltárja a legjobb, leghatékonyabb technológiákat).

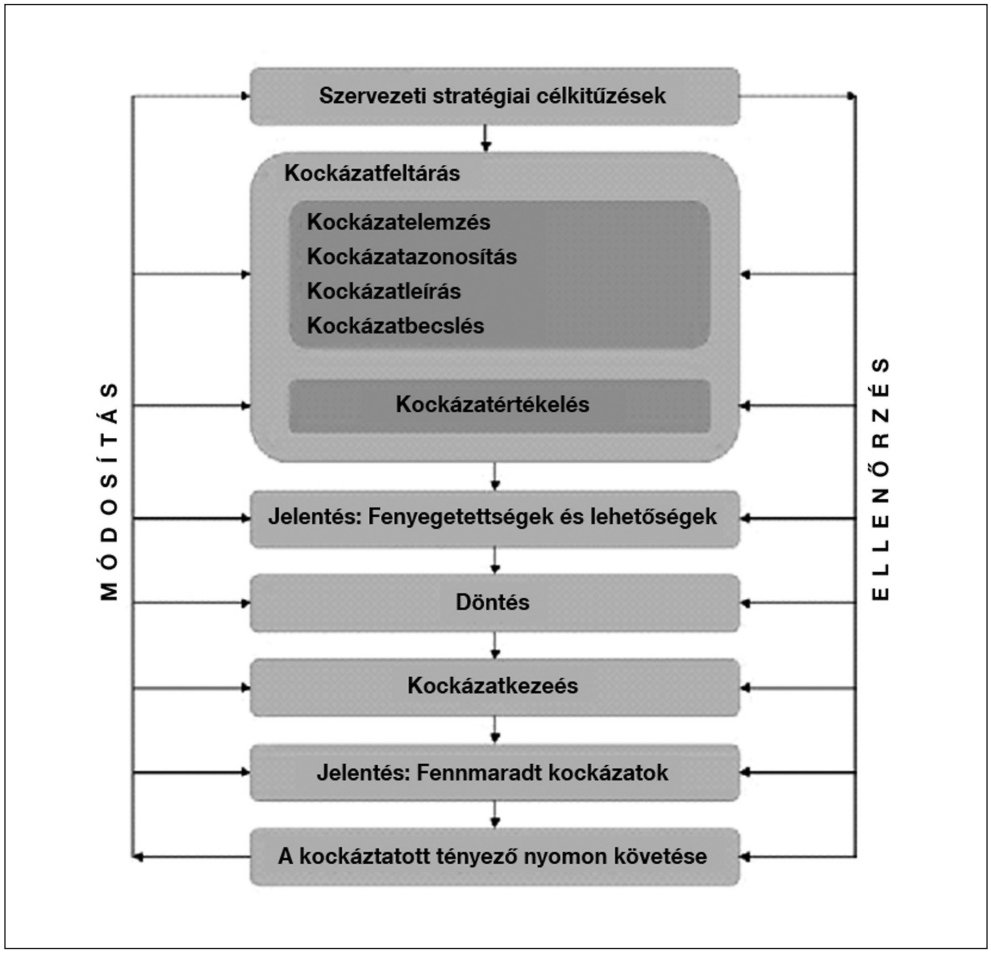
A kockázatelemzés során és az informatikai adatkezelő rendszer teljes működése során működni kell a következő alapelveknek.

Bizalmasság elve: az információ csak annak a személynek számára legyen elérhető, aki erre fel van jogosítva, mindenki más részére elérhetetlen legyen.

Sértetlenség elve: biztosítja az adat változatlanságát, a rendszernek jelezni kell, ha a benne lévő információt megváltoztatták (beszúrás, törlés, helyettesítés…)

Rendelkezésre állás elve: akinek szükséges hozzáférni az adathoz, az a személy bármikor el tudja érni, ugyanis emberéletek, anyagi javak nagymértékű biztonsága függhet ettől.

A kockázatmenedzsment folyamata[4]



1. ábra: A kockázatmenedzsment folyamatábrája. (forrás: Management Control and Compliance Control, Véry Zoltán 2008.)

A kockázatmenedzsment folyamata tudatos tevékenységsorozat, mely kockázatértő szemléletre, elemzési és kockázatkezelési módszerekre, eszközökre épül. Fontos, hogy ezt a folyamatot szabályozzuk, felügyeljük és kontrolláljuk. Ehhez elengedhetetlenül szükséges egy elemző, jól felkészült munkacsoport, melyet az adott szervezet tagjaiból is választhat a szervezet vezetője. Amennyiben a szervezet nem rendelkezik ilyen munkatársakkal, úgy külső szakértők segítségét is igénybe lehet venni. Nagyon fontos, hogy a szakértő képzettségi szintjét is éppúgy dokumentáljuk, mint bármi mást ebben a folyamatban.

[4] Kockázatelemző módszerek és eszközök (Management Control and Compliance Control), Véry Zoltán 2008.

Célszerű a működési tevékenységből származó kockázatok felismerését tudatosan, folyamatszerűen kezelni, ugyanis a fel nem ismert és nem kezelt kockázatok hatásaira, költségeire kevésbé gondolnak a döntéshelyzetben lévő vezetők, pedig azok jóval magasabb összeget és károkat eredményezhetnek, mint a kockázatelemzésbe fektetett pénz.

A kockázatelemzés kizárólag korszerű módszerek, eszközök, technikák esetén valósítható meg, amely egy szervezeti egységben végzett csapatmunka. Célja az emberi sérülések és az anyagi javak sérülésének megelőzése, a környezeti hatások szabályozása, megelőzése, csökkentése, az elviselhető kockázat mennyiségének és mértékének meghatározása.

Mivel az IT-rendszerek kiemelten fontossá váltak az elmúlt évtizedekben, fokozódik a tőlük való függőség, ennek következtében az IT-kockázat fő veszélyforrássá vált a szervezetek számára.

A fenti ábra mutatja, hogy a kockázatmenedzsment első lépése, hogy a szervezet fogalmazza meg célkitűzéseit, stratégiáját. Tárja fel azokat a tényezőket, melyek potenciális veszélyt jelentenek. Ez azért nehéz feladat, mert a károk általában nem közvetlenül fejtik ki hatásukat, hanem a velük kapcsolatban lévő rendszerelemeken keresztül az egész szervezet működésére hatással lehetnek. Például egy adatkezelő rendszerben javítást és cserét hajtanak végre, ennek hatására információvesztés, kiesés léphet fel, ami nagy kockázatot jelenthet. Következménye lehet ennek, hogy az üzleti folyamatok szintje vagy a szervezet népszerűsége csökken, illetve ezáltal bevételkiesés is előadódhat.

Különböző kárkategóriák jelentkezhetnek, melyeket három csoportba oszthatunk:

- elsődleges kár (tényleges helyreállítás költsége, javítás, adatok pótlása),
- másodlagos kár,
- harmadlagos kár (akár a szervezet teljes vesztesége).

A kockázatelemzés célja olyan megoldást találni, amely a teljes rendszer védelmét lefedi, minden elviselhető mértékű kockázatot legalább elviselhető mértékűvé csökkent vagy megszüntet. Lehetőség szerint mindez költséghatékony is legyen!

A kockázatmenedzsment egyik legfontosabb lépcsőfoka a kockázatok kezelése, melynek többféle módja lehet.

A veszélyforrások megszüntetésére csak elméletben van lehetőség, hiszen nincsen teljes kockázatmentesség, mindig adódhat váratlan esemény.

A bekövetkező valószínűség és az okozott kár csökkentése a gyakorlatban a legkedveltebb stratégia, a kettő kombinációja jelent optimális megoldást a kockázat kezelésére.

A kockázatok áthárítása azt jelenti, hogy a veszély bekövetkezte előtt, már a szerződéskötés során átruházzuk a partnerre a terhek bizonyos részét. Jó példa erre az interneten történő vásárlás, amikor az e-boltok weblapjai nagyon körültekintőek a vásárlók bankkártya-adatait illetően, de ha adatlopás történik, azért nem vállalnak felelősséget, tehát áthárítják a kockázatot.

Egy másik lehetőség a kockázatok kezelésére a *biztosítás.* Ez általában nem kifizetődő, ugyanis a biztosítási összeg általában nagyobb, mint az okozott kár mértéke lehet.

A kockázatkezelés egy másik módja a *tudatos kockázatvállalás.* Amikor a védekezésre fordítandó összeg olyan nagy, annyival meghaladja a maximális veszteség mértékét, akkor megéri tudatosan vállalni a kockázatot. Ebben az esetben viszont tisztában kell lenni a következményekkel, vagyis a lehetséges veszteség másodlagos, harmadlagos mechanizmusával.

Magyarországi helyzetkép az IT-biztonság képessége terén

2011-es adatok szerint Magyarországon átfogó biztonsági stratégia a szervezetek 61%-ánál van jelen, vagyis 4%-kal elmaradunk a nemzetközi átlagtól. Meg kell jegyezni, hogy ez az arány általánosságban magasabb a pénzintézetek esetében, hazai és nemzetközi szinten egyaránt. Lényeges adat az is, hogy míg a100%-ban magyar tulajdonú szervezetek 59%-a rendelkezik átfogó biztonsági stratégiával, addig ez az arány 82% a nemzetközi–magyar tulajdonú szervezetek esetében.

A 2011-es helyzetkép[5] alapján elmondható, hogy a hazai szervezetek vezetői 75%-ban jól informáltak az általuk vezetett cég incidenseiről (például eszközlopás, külső behatolási kísérlet stb.), szemben a nemzetközi vezetők 67%-ával.

A felelősség, a beszámoltatás terén komoly elmaradásunk van, ugyanis a szervezetek mintegy felénél nincs kinevezett informatikai biztonsági felelős. Ezen a téren is erős a pénzügyi szektor, a magánszféra is erősebb az átlagnál.

Elemzők a gazdasági válságot nagymértékben okolják azért, hogy a vezetők nem gondolkodnak az IT-biztonság támogatásáról. Az azonban hangsúlyozni kell, hogy 2010 óta a szervezetek tudatossága nőtt, emelkedtek a kockázatelemzésre fordított kiadások, szigorodtak az állami szabályozások.

Minél nagyobb egy szervezet, annál inkább ki van szolgáltatva a biztonsági kockázatoknak, ugyanakkor a pénzügyi és a távközlési szektor a leginkább kockázattudatos.

Kockázatelemzési programmal 2011-ben a szervezetek negyede rendelkezett, rendszeres mély IT-kockázatfelmérést 40% végzett, míg 34% tervezte ezt.

Kockázatelemzési módszerek

A kockázatmenedzsmenttel foglalkozó szakemberek számos módszert dolgoztak ki a kockázatelemzés korszerűsítése, szakszerűsítése érdekében. Feltehetjük a kérdést, hogy melyik a legjobb, leghatékonyabb ezek közül. Erre a kérdésre nagyon nehéz válaszolni, mert

[5] Információbiztonsági helyzetkép 2011.

nincs száz százalékos kockázatmentesség, így egyik módszerről sem jelenthetjük ki, hogy a legjobb, hiszen a különféle szervezetek profilja más és más. Az a módszer, ami kiváló a banki szférában, nem biztos, hogy például a védelmi szférában is ugyanolyan hasznos.

Vannak azonban olyan szempontok, amelyek figyelembevétele igen hasznos a kockázatelemzési módszer kiválasztásakor. Ezek a következők lehetnek.

Olyan módszert válasszunk, amely az adott adatkezelő rendszerre jól alkalmazható, és ez legyen tudományosan igazolható. A módszer kiválasztásakor figyelembe kell venni az adatkezelő rendszer életútját, kidolgozottságának fázisát. (Egy kialakítandó rendszer esetében nem szükséges részletes módszerek alkalmazása, ellenben egy bonyolult, sok adatot feldolgozó rendszer esetén a módszerek részletezhetők, finomíthatók.)

Sok esetben az „egyszerűbb több" – a helyesen alkalmazott egyszerű módszer hasznosabb eredményt hozhat, mint a bonyolultabb, kifinomultabb, de rosszul elvégzett elemzés.

Fontos megjegyezni a nyomon követhetőséget, mellyel az egész elemzést igazolni tudjuk. Ennek egyik fontos része a dokumentáltság. Az elemzés minden egyes fázisát jól érthetően, világosan kell megadni a félreértések, pontatlanságok elkerülése miatt.

A kockázatelemzési módszerek, ajánlások széles választékából néhány ismert módszert érintőlegesen említünk meg, három népszerű módszertant részletesebben jellemzünk és vetünk össze.

Fuzzy logika

A Fuzzy logika alapú kockázatbecslés lényege, hogy egy időben több logikai szabályt, szabálybázist alkalmaz, melyek kiépítését a fogalmak és kategóriák definiálásával kell kezdeni. Ez a módszer egy *kockázatbecslési mátrixot* alkalmaz.

Monte Carlo-szimuláció

Ez egy valószínűség-elemzési technika. Ebben a módszerben nagy szerepe van a megérzésnek.

Marion-eljárás

Négy szakaszból álló módszer, melynek előnye, hogy a vizsgált terület biztonsági állapotát nagyon szemléletesen ábrázolja. Európa-szerte elterjedt eljárás, az EU-ban is használják.

Courtney-eljárás

A módszert az 1970-es években fejlesztette ki az IBM Amerikában, Európában az 1980-as években kezdett népszerűvé válni.

A CRAMM-módszer

A CRAMM-módszert[6] az Egyesült Királyság kormányának Központi Számítógépes és Telekommunikációs Ügynöksége (CCTA)[7] alkotta meg 1987-ben. Ezt a kockázatelemzési és menedzselési módszert több esetben frissítették, fejlesztették. A módszertan igen nagy előnye, hogy a feladatokat következetesen, fokról fokra írja le, elkészül a kockázatok felmérése, elemzése, majd meghatározza a kockázatkezelést biztosító intézkedéseket. Ezeket az intézkedéseket az úgynevezett Informatikai Biztonsági Koncepció tartalmazza.

A CRAMM-módszer alkalmas arra, hogy informatikai kockázatokat felmérje, dokumentálja, a kockázatokat csökkentő intézkedéseket kiválassza, a fennmaradó kockázatokat egyértelműen meghatározza. Ez a módszer egy a gyakorlatban kivitelezhető eljárás, amely nem fogalmaz meg elvárást arra nézve, hogy egy szervezet szempontjából milyen kockázat fogadható el, tehát nem normatíva. A módszer alkalmazását elősegíti, hogy informatikai rendszerrel is támogatható, például vannak a CRAMM-módszertan kivitelezését elősegítő szakértői rendszerek, melyek előre beépített adatbázissal felgyorsíthatják a kockázatelemzés elkészítésének folyamatát.

A megalkotók 4 szakaszra osztották fel a módszertant.

1. szakasz: A *védelmi igény feltárása,* amely két részből áll:

- Felmérik az objektumokat, az informatikai alkalmazásokat és a feldolgozandó adatokat, melyeket védeni szándékoznak.
- Értékelik az informatikai alkalmazásokat és a feldolgozandó adatokat.

2. szakasz: A fenyegetettségek *elemzésének* szakaszában feltárják azokat a fenyegető tényezőket, amelyek az 1. szakasz adataira, alkalmazásaira veszélyesek lehetnek.

- A fenyegetett rendszerelemek felmérése.
- Az alapfenyegetettség meghatározása.
- A fenyegető tényezők meghatározása.

3. szakasz: Ebben a szakaszban vizsgálják a fenyegető tényezők *hatását* az informatikai rendszerre, meghatározzák a lehetséges károk bekövetkeztének gyakoriságát és kárértékét.

- Értékelik a fenyegetett rendszerelemeket.
- Meghatározzák a károk gyakoriságát.
- Meghatározzák a kockázatokat (kockázat = kárérték és bekövetkezési gyakoriság szorzata).

4. szakasz: Ez a feltárt kockázatok *kezelésének* szakasza.

- Kiválasztják a megfelelő intézkedéseket.
- Értékelik az intézkedéseket a lehetséges károk csökkentése érdekében.

[6] Risk Analysis and Management Method.

[7] CCTA: Central Computer and Telecommunications Agency.

- Elemzik a költség és a haszon arányát.
- Végül elemzik a maradványkockázatokat.
- Ebben a szakaszban döntenek arról is, hogy elfogadják vagy csökkentik a maradványkockázatot.

A négyszakaszos kockázatfelmérés és -kezelés után készítenek el egy biztonsági koncepciót, melyben a következők kerülnek rögzítésre:

1. A biztonsági stratégia: célok, alapelvek, felelősségi határok.
2. A jelenlegi állapot rögzítése a kockázatelemzés eredményei alapján.
3. Az intézkedések kiválasztása, meghatározása.
4. Az intézkedések kölcsönhatásainak felmérése.
5. Az intézkedéseknek a szervezet működésére gyakorolt hatása.
6. Az intézkedések elfogadhatósága a költség–haszon arány figyelembevételével.
7. A kockázatok állapotának megítélése, a maradványkockázatok mértékének tudatosítása.
8. A maradványkockázatok elviselhetőségének elemzése.

Korábban már említettük, hogy a CRAMM-módszert folyamatosan frissítették, fejlesztették. Az előző, négyszakaszos változat mellett érdemes tanulmányozni az úgynevezett 5. változatot, amely három szinten elemzi a kockázatokat, de mindegyik szint átfogó kérdéssorral és útmutatóval rendelkezik.

Az 5. változat modellje

1. szint: Az első lépésben megállapítják a biztonsági szempontokat, meghatározzák a kockázatelemzés/-kezelés elemeit. Azonosításra és értékelésre kerülnek a rendszer vagyonelemei is. Azonosítás után feltárják az üzleti hatásokat, melyek sértik a vagyonelem rendelkezésre állását, bizalmasságát és sértetlenségét.

2. szint: Ezen a szinten valósul meg a kockázat értékelése a biztonsági követelmények alapján. Megállapítják a fenyegetések fokát és típusát, amelyek megfelelő védelem nélkül potenciális veszélyt jelentenek a rendszer működésére. Meghatározzák azokat a sérülékenységeket is, amelyeken át a fenyegetés megvalósulhat. Végül összevetik a fenyegetések és sérülékenységek halmazát, majd ezekből megbecsülik a kockázati értékeket.

3. szint: Az utolsó lépésben meghozzák azokat az ellenintézkedéseket, melyekkel megfelelő védekezést lehet nyújtani a 2. szinten leírtak szerint. Nagyon fontos, hogy az ellenintézkedések mértéke kockázatarányos legyen.

A módszer gyakorlati megvalósulásának lépései

1. Vagyonleltár készítése (vagyontárgy azonosítása, értékelése).
2. Sebezhetőségi vizsgálat.
3. A lehetséges fenyegető tényezők összegyűjtése.
4. Támadható felületek (sebezhetőségek) azonosítása.

5. Kockázatértékelés: a sikeres támadás valószínűségének és a vagyontárgyakban okozott kár mértékének becslése.
6. Védelmi intézkedések meghozatala, bevezetése.
7. Védelmi intézkedések működtetése, ellenőrzése.
8. Kockázatok újraértékelése.

A CRAMM-módszer értékelése

Előnyei:

- A módszer átfogóan közelíti meg a kockázatelemzés és -kezelés feladatkörét.
- Szoftverrel és jól használható sablonnal támogatott.
- Intézkedések széles választékát ajánlja a kockázatok csökkentésére.
- Szükséghelyzetben is eszközt nyújt.
- Egy alapos biztonsági audit elvégzésére ösztönöz az informatikai rendszerben.
- Nagyon széles körben használt módszer (pl. NATO), ezáltal sok tapasztalati tényezőt beépítettek a módszerbe, így fejlődött, kikristályosodott a módszertan.
- Kockázatelemzése alapos, részletes, segítségével a kockázatok ól meghatározhatók.

Hátrányai:

- Ezzel a módszertannal hosszadalmas a kockázatelemzés, a kockázatok nem határozhatók meg egzaktul, költséges a hosszadalmas vizsgálat miatt.
- Hónapokat is igénybe vehet a rendszer elemzése, ami miatt az eredmények gyorsan túlhaladottakká válhatnak.
- A módszer kvalitatív jellege miatt nehezebb pontos értékeket meghatározni.

A COBIT nyílt szabvány

Az informatikairányítás világszerte egyre szélesebb körben elismert eszköze, egyben nyílt szabványa a COBIT (Control Objectives for Information and Related Technology), amely rendszerbe foglalja az információs, az információtechnológia és az ezzel kapcsolatos kockázatok kontrollálására alkalmas gyakorlatot. Hasznosítja az informatikairányítás korábbi eredményeit, ugyanakkor épít a korszerű vállalatirányítási módszerekre is. Hangsúlyozza, hogy az informatikának az üzleti célkitűzéseket kell szolgálnia. A COBIT alkalmazásával az üzleti területi vezetők, a működési kockázatokkal foglalkozó szakemberek, az informatikusok és az auditorok egységes szemléletben, közös fogalmi rendszert használva, hatékonyan tudnak együttműködni. Ezek az ismérvek a COBIT-ot kifejezetten érdemessé teszik a pénzügyi intézményekben való alkalmazásra. A megfeleltetés a két anyag között természetesen – keletkezésük, készítőik, céljuk, felhasználási körük stb. különbözősége miatt – nem lehet teljesen egyértelmű és megfellebbezhetetlen, de célja mindenképpen a jogszabálynak a nemzetközi gyakorlat alapján kialakított és karbantartott COBIT-

szabványhoz való igazítása és annak teljes lefedése. A nem egyértelmű megfeleltetés következtében tehát a COBIT bizonyos fejezetei több jogszabályi pontnál is megjelennek.

Történeti áttekintés, általános jellemzés

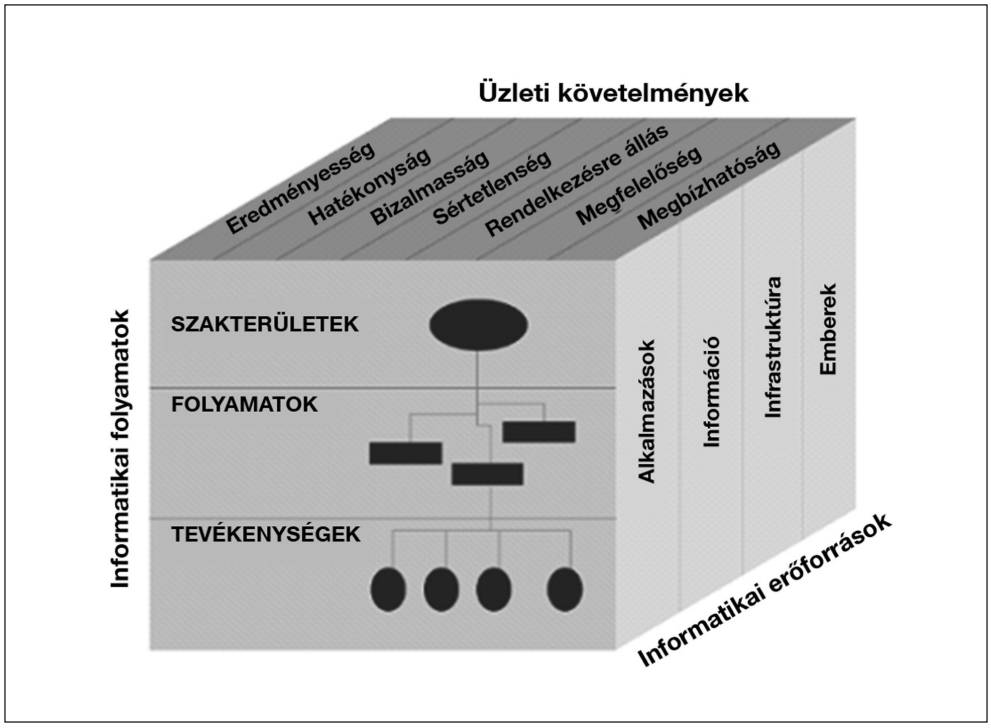
A szabványban megtestesülő kutatások motorja a világszerte kb. 35 000 tagot számláló ISACA (Information Systems Audit and Control Association), amelynek társintézménye, a COBIT-ot kiadó IT Governance Institute (USA) 1998-ban alakult. Eddig három COBIT-kiadás jelent meg: 1996-ban, 1998-ban és 2000-ben. 2003-ban megjelent egy internetes változata, továbbá egy egyszerűsített, bevezető verzió is. 2005-ben bevezetésre került a COBIT 4, de 2007-ben megtörtént ennek felülvizsgálata, mely COBIT 4.1 néven vált ismertté. A módszertan legfrissebb változata COBIT 5. néven 2012 júniusában jelent meg, melyhez kiadtak egy dokumentumot 2013 júniusában.

A COBIT növekvő nemzetközi elfogadottságához jelentősen hozzájárul részletesen kidolgozott auditálási módszertana is. A felügyelet informatikai ellenőrei az ISACA tagjai, és már több éve COBIT-szemléletben végzik a pénzügyi szervezetek informatikai rendszerének vizsgálatát. Erre épül a jelenleg használt vizsgálati módszertanuk is. A COBIT célja a nemzetközileg és általánosan elismert kontroll célkitűzések vizsgálata, fejlesztése, kiterjesztése, melyek jól használhatók biztonsági szakértők számára. Az alábbi ábrán található COBIT-kocka tetején látható „Üzleti követelmények" dimenziója tartalmazza azokat az alapelveket, amelyeket az eredmények elérése érdekében alkalmaznak az eljárás során.

- Minőségi követelmények
  1. eredményesség (az üzleti igényeknek feleljen meg)
  2. hatékonyság
- Biztonsági követelmények
  3. bizalmasság
  4. integritás (teljesség)
  5. rendelkezésre állás
- Bizalmi követelmények
  6. megfelelőség (az elvárásoknak feleljen meg)
  7. megbízhatóság

A COBIT az ellenőrizendő informatikai tevékenységekben 4 területet különböztet meg:

1. Tervezés és szervezet (PO; az informatikai stratégia megalkotása, szervezési kérdések)
2. Beszerzés és megvalósítás (AI)
3. Szolgáltatás, támogatás (DS)
4. Felügyelet (M; az informatikai folyamatok felügyelete, vizsgálata, értékelése)



2. ábra: a COBIT-kocka 3 dimenziós egysége

COBIT 5. kézikönyv

Ez az ISACA által kidolgozott kézikönyv az egyik legjelentősebb nemzetközi nyílt szabvány, amelynek alapján az IT-rendszerek menedzselését, üzemeltetését, fejlesztését, biztonságosabbá tételét és ellenőrzését meg lehet valósítani. A COBIT 5. az IT irányítási menedzselési és auditálási keretrendszert összekovácsolja az ISACA többi kézikönyvével (BMIS[8], ITAF–IT[9], Risk IT–IT RMF[10], ValIT[11]).

A COBIT 5. tehát a COBIT előző verzióira épül, továbbfejlesztve azokat. Azok a felhasználók, akik ismerik a COBIT 4.1 verzióját, könnyen át tudnak lépni a COBIT 5.-re, élvezhetik ennek a fejlett útmutatónak az előnyeit.

A COBIT 5. az alkalmazói számára több lényeges terület esetében ad iránymutatást. Természetesen központi elemként kezeli a szabályozást, de nagy hangsúlyt helyez a folyamatokra, a szervezeti struktúrára és a szervezeti kultúrára is. Emellett kiemelten foglalkozik a különféle erőforrásokkal, amelyekbe beletartoznak az információk, a szolgáltatások, az infrastruktúrák, a különféle alkalmazások ,valamint maguk az emberek is. A COBIT 5. az

[8] Business Model for Information Security.
[9] IT Assurance Framework.
[10] Risk IT–IT Risk Management Framework.
[11] Value of IT.

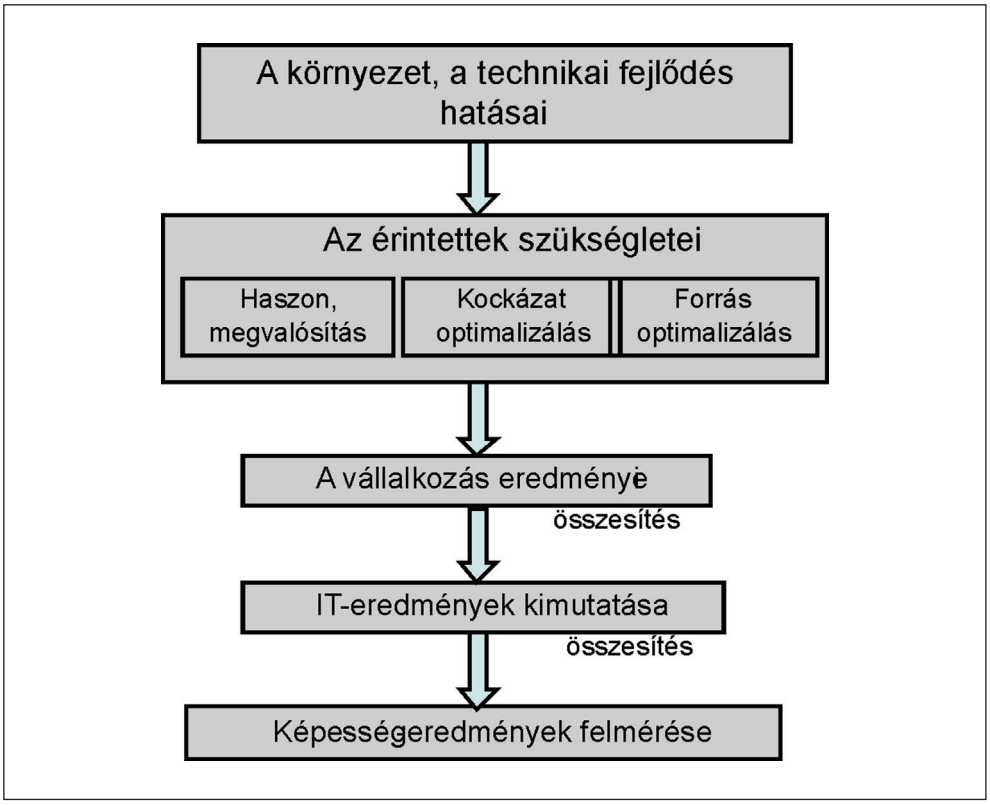
emberek képességeinek, kompetenciájának kérdéskörét is kiemeli, ami a mindennapi döntéshozatal sikerét, valamint az üzleti tevékenységek elvégzését jelentősen befolyásolhatja.

Az új COBIT kidolgozásakor fontos szempont volt az is, hogy a különféle szabványokkal való integráció, együttélés az eddigieknél könnyebben valósulhasson meg.

A COBIT 5. alkalmazása során központi szerepet kap az *értékteremtés* és az *üzleti cél.* Értéket teremteni azt jelenti: hasznot termelni egy optimális forrásköltséggel, optimalizált környezetben. Az üzleti cél maga az értékteremtés, amely az érintettek szükségleteit is képviseli.

E két fontos összetevő megteremtésekor fontos azt az alapelvet figyelembe venni, hogy az érdekeltek igényei találkozzanak. A COBIT 5. ezeket az igényeket a következőképpen hangolja össze:

- Figyelembe kell venni a környezet, a technikai fejlődés hatásait.
- Fontos szempont, hogy mik az érintettek szükségletei (haszon, megvalósítás, kockázat optimalizálása, forrás optimalizálása).
- Összesíteni kell a vállalkozás eredményeit.
- Fontos a képességeredmények felmérése.
- Az IT-vel összefüggő eredmények kimutatása.



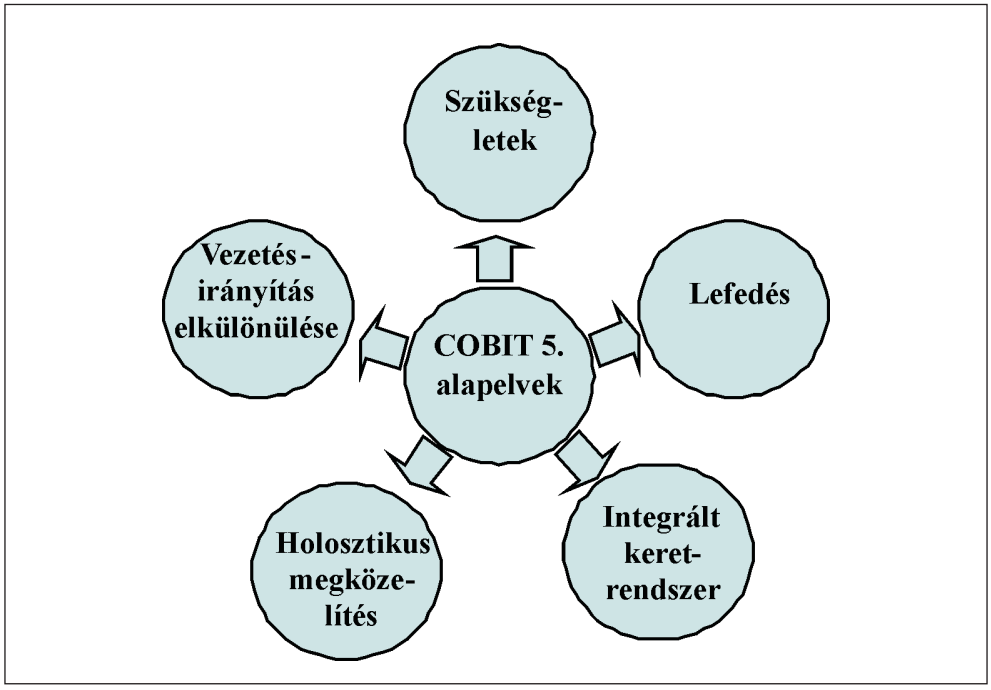
3. ábra: A COBIT 5. – igények (forrás: Cobit 5 figure 2012. ISACA)

Irányítási és vezetési meghatározás

A COBIT 5. módszere két fő területre oszlik fel: vezetésre és irányításra. A vezetés és irányítás további részekre bontható. A vezetés területe feldolgoz, értékel, vezeti és felügyeli a meghatározott gyakorlatokat. Az irányítás összhangban van a tervezés, az építés, a futtatás és a figyelemmel kísérés felelősségi területekkel.

A COBIT 5. módszertannak öt alapelve van, amelyek alkalmazása a módszert sikeressé és igen jól alkalmazhatóvá teszik:

1. Találkozzon az érintettek igényeivel.
2. Fedje le a vállalkozást az elejétől a végéig.
3. Egyetlen integrált keretet alkalmazzon.
4. Tegye lehetővé a holisztikus megközelítést.
5. Különítse el a vezetést és az irányítást.



4. ábra: COBIT 5. alapelvek (forrás: Cobit 5 figure 2012. ISACA)

A COBIT-módszer értékelése

Előnyei:

- A Governance Institute az egész világot képviselő független szervezet, ezért lehetőség nyílik arra, hogy minden kontinensen, egyre szélesebb körben fogadják el a szabványt.
- A COBIT növekvő nemzetközi elfogadottságához jelentősen hozzájárul részletesen kidolgozott auditálási módszertana.

- A módszertan kipróbált, jól bejáratott, jó alapot biztosít a kockázatok felméréséhez.
- Összpontosítás az adottságokra.
- A COBIT 5. alkalmazásakor fontos tényező, hogy olyan adottságok és források is szerepet kapjanak, mint az:
  – elvek, rendelkezések és keretek,
  – folyamatok,
  – szervezeti felépítés,
  – kultúra, etika és viselkedésmód,
  – információ,
  – szolgáltatások, infrastruktúra és alkalmazások,
  – emberek, képességek és kompetenciák.

Hátrányai:

- Jelentős kezdeti energia-ráfordítást követel meg, ebben az értelemben nem felhasználóbarát, nem kezelhető könnyen.
- Mivel jelentős anyagi befektetést igényel a módszer alkalmazása, ezért általában a jelentős és fejlett informatikával rendelkező vállalatok tudják használni.
- A COBIT elsősorban felsőszintű irányelveket tartalmaz, a technikai részletekre nem tér ki.
- Teljesen átfogó, de nem minden esetben kínál specifikus lehetőségeket.
- Kvalitatív módszer, nem tartalmaz számszerűsíthető eljárásokat.

Összegzés

Publikációnkban a kockázatelemzés legfontosabb módszereinek, eljárásainak lényegét igyekeztünk összefoglalni. Mindezekre azért volt szükség, mert napjainkban a kockázatkezelés, a kockázatelemzés és a kockázatértékelés nagy hangsúlyt kap az üzletmenet folytonosság elemzésében és tervezésében.

Mindkét bemutatott módszertan kiválóan használható a kockázatelemzés és -kezelés területén. Mind a CRAMM-módszer, mind a COBIT esetében elmondható, hogy részletes, átfogó, jól kidolgozott verzió áll rendelkezésre, melyek nemzetközi viszonylatokban is tesztelt módszerek. Külön kiemeljük, hogy az alkotók mindkét módszertan esetében – az első verziók hibáit, hiányosságait felmérve – kiküszöbölték a hibákat, pótolták a hiányosságokat annak érdekében, hogy magas szintű módszertanokat alkossanak meg. Ezek valóban lehetőséget adnak arra, hogy a napjaink információs társadalmát érő fenyegetésekkel szemben felvehessük a versenyt, ezáltal valóban a *„zéró kockázati szint”* irányába haladhassunk a kockázatok értékelése területén.

Irodalomjegyzék

Dr. Michelberger Pál – Lábodi Csaba: Vállalkozásfejlesztés a XXI. században. Budapest, 2012.
Godányi Géza: Katasztrófavédelem és üzletmenet folytonosság az információtechnológiában. (A DR/BC tervezés alapjai.) Híradástechnika, LIX. évfolyam 2004/4., pp. 47–52.
Pál Michelberger – József Beinschróth – Gergely Krisztián Horváth: The Employee – an information security risk. Acta Oeconomica Universitatis Selye, 2013, Komárno, pp. 187–200.
Tóth Tibor (szerk.): Minőségmenedzsment és informatika, Műszaki Könyvkiadó – Magyar Minőség Társaság, Budapest, 1999.
Ji-Yeu Park – Robles, Rosslin John – Chang-Hwa Hong – Sang-Soo Yeo –Tai-hoon Kim: IT Security Strategies for SME's. International Journal of Software Engineering and its Applications. Vol. 2. No. 3., July, 2008, pp. 91–98.
Lynne C. Lancaster – David Stillman: The M-Factor: How the Millennial Generation Is Rocking the Workplace. HarperCollins, 2010.
Kelemen László: Nem sztereotípiák. IT-business, 2008. szeptember 28., VI. évf. 37. sz., p. 32.
http://www.iso27001security.com/ (letöltés: 2013. december 18.)
European Network and Information Security Agency – ENISA (November 2010): How to Raise Information Security Awareness (The new users' guide, p. 140). http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide (letöltés: 2013. november)
Intrieri, Charles (10 September 2013): „Business Continuity Planning". Flevy. Retrieved 18 December 2013.
Véry Zoltán: Kockázatelemző módszerek és eszközök (Management Control and Compliance Control) 2008.
2013. évi L. törvény.

Risk Analysis of Electronic data processing systems, presentation of risk methods

Mógor Tamásné – Rajnai Zoltán

National electronic data assets are part of the national wealth, therefore their security and the security of their management information systems and of these systems' components are national priorities.
The confidentiality, integrity and availability of the state's and citizens' electronic data managed in electronic information systems is absolutely necessary. It is also indispensable to ensure the protection of the system's components, which should be closed, continuous, comprehensive and commensurate with the risk, therefore ensuring the protection of the cyberspace.

Puskás Béla
Rajnai Zoltán

The risks of network complexity

"We have built our future upon a capability that we have not learned how to protect!"[1]

"We live in an accelerated world" sounds one of the most common truisms of our age. It is mainly caused by the dynamic flow of information, globalization, fast traffic and transportation, all of which are the results of the booming technological development of the past decades. Nowadays a journey from Hungary to the United States is nothing like the risky and lengthy adventure a century ago. We can also easily keep in contact with our relatives living on another continent. Consequently, people have got closer to each other but at the same time they loosened their connections as well. We live in a virtual space and rarely meet our friends physically. This gap between individuals and their physical reality is getting so wide, that we do not realize the devastation of our environment or natural disasters.

How has the revolutionary electronic development changed our common life?

On the 4th of September in 1837 the inventor, Samuel Morze introduced his electromagnetic telegraph. In order to use it two things were essential. One of them was the Morze alphabet, while the other one was the telegraph network itself. At that time the bit rate was "only" at around 5 bit/sec.

In 1876 Alexander Graham Bell had the telephone patented. He also had to establish and operate a network, thus he founded the Bell Telephone Company in 1877. Presently it is known as the American Telephone and Telegraph Co. (AT&T).

Between 1895 and 1901[2], based on James Clerk Maxwell's theory regarding radio waves, Nikola Tesla, Guglielmo Marconi and Alexander Popov "independently" from each other invented the radiotelegraph.

In 1957 the Soviet Union launched "Sputnik", the first satellite of mankind. As a re-

[1] George Tenet, former CIA director

[2] In 1901 Marconi introduced his invention for what the Nobel Prize in Physics was awarded to him in 1909. Tesla had already introduced his patent in 1896, while Popov had done so in 1895.

sponse, the President of the USA and the Department of Defense founded ARPA[3] in 1958. In 1969 an experimental network was established and some others joined in later. Five years earlier Paul Baran had already pointed out: in order to create a minimum risk level communication channel, a partitioned network had to be established instead of the decentralized ones. According to his theory the separated packets used on the Internet had to be sent through individual nodes toward their destinations. Nevertheless his idea was rejected.

In the Seventies the Internet took on a life of its own

More and more institutions joined the network, but not the way Baran thought. Instead of the partitioned network a scale-free model was evolved. Due to its extension and rapid development the network couldn't be controlled exclusively. The original goal of an operational network, which is protected against attacks, was not taken into account any more. On the contrary THE INTERNET, which is highly resistant against random errors, was born. It is quite similar to the other networks of our life, such as social networks, networks of the human bodies (nerve system, connections between cells etc.), but it also resembles networks spreading epidemics and other things.

Do we really know what has come to life by the Internet?

The main problem is that not only the common user does not understand it, but IT professionals are also not able to clear up the matter. We do not have proper knowledge about the network structure and we cannot obtain it by our way of thinking. We have to apply the theory of networks. For example, documents are being prepared faster on the Internet than the search engines can locate and index them. Nowadays they don't even try it and only the 30-40 % of the whole document is mapped even by the most effective search engines. In case of cell phones, especially smart phones, the situation is quite the same. Their development is so fast that their effect on hardwares, softwares and other systems cannot be measured. At the time of the writing of this article 10 % of the Internet data flow is going through mobile networks.

[3] Advanced Research Projects Agency

Then how the USA, NATO or Hungary can prepare themselves for a future IT warfare and how can we protect our critical IT systems against hackers and terrorists?

Today the real task is not to understand the occurrences going on the Internet or the Internet itself as an entity. Now, that the Internet has become part of our life we have to insert it into our complex world.

Terrorist organizations and other criminal groups sometimes hide secret messages in the chaos of the Internet. They can communicate on the network or exploit its and the users' weaknesses in order to gain money.

Against whom do we have to protect our systems?

In most of the cases the attackers are completely unknown. They hide their sources and not even their homeland can be identified properly. Usually it is not the masterminds who execute the attack, but they get "innocent" prying men to carry out the dirty work. They provide only the method and pattern of the attack. The communication channels and the logistics background are also given by someone else. They rarely have particular political or economic interests, the attack is simply considered as a challenge or a prank.

I think that in the future it will be very important to get familiar with the nodes of networks and their connections. We have to realize that the network is not just one-dimensional. The connections and effects of seemingly different social and electronic networks have to be researched. Not only the threatened system has to be examined but all the other linked networks as well. Besides the structures of networks we have to know the structures and the very details of the points (e.g. cells). From this point of view the node cannot be described as a mathematical concept because if something is considered to be indivisible today, tomorrow it can be a set. According to Albert-László Barabási the XXI century is going to be the age of complexity.

What has to be studied?

The matter is not so simple. Moreover, it becomes more complex if we consider another dimension as well: the movements of nodes. The nodes can change continuously and dynamically. If the nodes are the critical infrastructures, we have to count on their perma-

nent movements. What has not been a node before can become one and vice versa. This fact especially applies to Internet nodes.

In order to determine the items of networks we have to deal with complexity as well. Traditional telecommunication – television, informatics etc. – networks and their nodes can be mentioned only within the category of electronic networks. All network items such as routers, switches, modems, hubs, repeaters, transfer medias, servers, data storages, firewalls, adapters and their features affecting system functions have to be studied. We can also test the linking "devices", for example printers, monitor-keyboard switches, different input devices, adapter interfaces (smart phones, TV, PDA, GPS etc.), medical equipment, control systems of critical infrastructures such as traffic lamps or airplanes. The device-free surveys concerning the physical and logical network topology, softwares, hardware and software settings, regulators, physical protection, the human factor, environmental effects are also key issues, of course. The parameters of these factors are quite sophisticated as well, but their mutual effects and the quality of their linkage create a complex and immense system.

The Internet has become a complex network. Since it is continuously expanding, it can be called a scale-free network as well. While studying the network, Barabási and his team noted two facts: the expansion and the popularity.

The scale-free systems are highly resistant to random errors but a targeted attack against the centres can disintegrate them easily. Many vertices, which have only a few edges, can be eliminated but it does not have a significant effect on the whole network. The destruction of the 80% of the Internet nodes leaves the remaining 20% operational nodes working as an intact network.

There is another practical question in connection with networks: Do the malfunctions of devices, eruptions of social conflicts, devastations of biological or chemical disasters happen accidentally?

The segments of the network can be paralysed by a series of chance events or a well-organized, targeted attack.

It is easy to see, that as the drawing of the lottery, the malfunction of a random device is not able to interfere with the operation of the whole scale-free network. What is the probability that I can select a particular node, which has many links or especially important for the connection? In case of the Internet and other similar networks the degree exponent is less than three. Because of this fact there is no threshold which prevents the network disintegration, when the nodes are removed continuously.

However, a targeted attack is different. If the nodes with many links are destroyed first and it is carried on with the other nodes with less and less links, the network falls apart at a certain threshold. Usually this threshold can be reached quite soon and the attacker does not have to destroy too many nodes with many links. Although our system is resistant to errors, the removal of nodes with many links (e.g. central routers) impose an almost unbearable burden onto the other important nodes and transfer medias. The other items can work for a while, but later packets are going to be lost and congestions are going to emerge, which is very similar to a DoS attack.

I am of the opinion that the nodes providing important links can cause similar problems. Although redundant connections are always installed within the systems, these connections have smaller capacity.

Perhaps if the Internet had not taken on a "life" of its own and in 1964 Baran had succeeded in implementing his basic theory concerning the primacy of distributed models, we should not be afraid of targeted attacks so much. But there is no point in asking "what if..." questions because these processes are irreversible. We could consider the particular "systems" of evolution having similar networks instead. We may owe our life to it.

Consequently, the items of the system, their mutual effects and links and the map of the network have to be known properly. I haven't mentioned the types of graphs, which make the structure of networks more difficult. For instance, whether a graph is directed or not does make a difference and the network structure modification effect of the relocation of the edge between two vertices cannot be neglected either. A complex system cannot be protected without this knowledge.

Based on databases, data storages, documents and images some modern softwares are able to graphically depict complicated networks and to map complex structures. With the assistance of these softwares false information and connections can be identified; forecasts and algorithms can be prepared. The different aspects (timeline, too many or few but highlighted connections) could reveal hidden, important information.

One of the most important part of the cognition process is the acquisition and sorting of information. The relevant data can be obtained from unclassified and classified sources, for instance, from the databases of telecommunication ventures, social sites, Internet providers, manufacturers and many other sources.

If we know our system and lead a safety-conscious life we can avoid such unpleasant events[4], which occurred to the director of MI6, Sir John Sawer. It is obvious, that the problem of mapping the complexity is not only the business of IT professionals. We have to realize that everything is linked to each other and the physical and logistical networks have mutual effects on each other as well. We can't be sure that the erased digital information really vanishes.

[4] In 2009 Sir John Sawers's wife uploaded some family images onto a social site. By these pictures hostile organizations or individuals could obtain sensitive information, which could endanger Sawers and indirectly the MI6.

Bibliography

Barabási, A.-L. (2003): *Behálózva.* Budapest, Magyar könyvklub.

University of Debrecen (without date): *Az Internet története.* Download date: 30/09/2012, source: www.inf.unideb.hu: http://www.inf.unideb.hu/~bodai/internet/internet_tortenete.html

Defense Technical Information Center (2002): *Information Technology Industry Study Final Paper.* Download date: 30/09/2012, source: www.dtic.mil: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA425460

ELTE (2006): *Az elektronikus sajtó története*. Download date: 27/09/2012, source: http://mmi.elte.hu: http://mmi.elte.hu/szabadbolcseszet/index.php?option=com_tanelem&id_tanelem=548&tip=0

National Geographic Magyarország (without date): *Samuel Morse, a távíró feltalálója*. Download date: 28/09/2012, source: www.ng.hu: http://www.ng.hu/Civilizacio/2005/04/Samuel_Morse_a_taviro_feltalaloja

Péter, B. (19/09/2012): A globális IT-rendszerek erdejében. *Computerworld*, page 4.

Komplex hálózatok kockázatai

Puskás Béla – Rajnai Zoltán

Az előző évtizedekhez képest a dinamikus információáramlás, a transzport eszközök fejlődése, a globalizáció eredményeként a műszaki fejlődés felgyorsult. Napjainkban már nem számít kockázatos és hosszú kalandnak átutazni az Egyesült Államokba, mint ahogy ez a múlt század elején volt. Mi is könnyen tarthatunk kapcsolatot rokonainkkal, ismerőseinkkel, akik akár egy másik kontinensen is élhetnek. Következésképpen az emberek az IT-hálózatok segítségével közelebb kerültek egymáshoz, de ez ugyanakkor lazított is a kapcsolatukon. Virtuális térben élünk, amit az is bizonyít, hogy csak ritkán találkozunk személyesen ismerőseinkkel, barátainkkal. Ez a különbség az egyének és a fizikai valóság egyre növekvő eltávolodását hozhatja, miközben környezetünkben jelentős változások, természeti katasztrófák játszódhatnak le.

Szamosi Barna

A kockázatelemzés módszertana

Kockázatértékelési elméletek alkalmazhatósága a kritikus infrastruktúrákra

A tanulmányban a szerző röviden összefoglalja a kockázatelemzéssel kapcsolatos tudnivalókat, illetve a kockázatértékelés munkahelyeken betöltött szerepét. A tanulmány bepillantást enged egy olyan lehetséges értékelési folyamatba, amelyik a munkahelyeken dolgozók munkavédelmi támogatásának egy speciális formája. A többször módosított 1993. évi XCIII. törvény a Munkavédelmi törvény [1] (továbbiakban Mvt.) – összhangban az Európai Közösség szabályaival – a munkáltatóknak kötelezettséget határoz meg, mely szerint ha a munkahelyi veszélyforrások a vonatkozó előírásokban nevesített műszaki, szervezési, illetve technológiai intézkedésekkel nem kezelhetők, akkor a munkahelyi veszélyforrások kockázati szintjét specifikus elemzés útján értékelni kell. A munkahelyi kockázatok értékeléséről szóló európai útmutató [4] több különböző lépésen alapuló módszert ajánl. Ez nem a kockázatelemzés elvégzésének egyetlen módszere, ugyanazon célkitűzés eléréséhez többféle módszer létezik. Ez a tanulmány ennek az elemzési folyamatnak lehetséges változatát ismerteti röviden.

Bevezetés

A munkakörülmények állapotainak veszélyforrás-elemzése a témát érintő jogszabályi rend alkalmazásán túl- és előremutató intézkedés. Az Mvt. 54. § (2) bekezdésében foglalt munkáltatói kötelezettségből fakadóan a munkáltatóknak a szervezett munkavégzés keretében keletkező egészségkárosodással és baleseti veszéllyel járó munkahelyi kockázatokat rendszerező vizsgálat keretében elemezni, értékelni kell.

A feltárt egészségkárosodással vagy baleseti veszéllyel járó kockázatok kezelése, összhangban a munkáltató preventív intézkedéseivel, megalapozza az egészséget nem veszélyeztető és biztonságos munkavégzés feltételeit.

A kockázat meghatározása

A Mvt. 87. § 1/B. értelmezésében: kockázat a veszélyhelyzetben a sérülés vagy az egészségkárosodás valószínűségének és súlyosságának együttes hatása. A kockázat fogalma az Európai Unió alapvető munkavédelmi jogforrásából, a munkavállalók munkahelyi biztonságának és egészségvédelmének javítását ösztönző intézkedések bevezetéséről szóló 89/391/EGK irányelvből került át a magyar munkavédelmi szabályozásba. Ez a fogalom bizonyos mértékben rokon a korábban használt „veszély", „veszélyforrás" fogalmakkal.

A kockázatértékelés fogalma, célja

A kockázatértékelés egyfajta becslésen alapuló veszélyelemzés. A munkavégzés körülményeinek, a munkakörnyezet kialakításának olyan értékelő, elemző áttekintése, amikor a munkáltatónak nem abból kell kiindulnia, hogy a jogszabályi követelmények megvalósultak-e vagy sem, hanem sorra kell vennie mindazokat a lehetőségeket, amelyek a munkavégzéssel összefüggésben a munkavállalók egészségét és biztonságát veszélyeztetik. Amennyiben olyan, az adminisztratív jogszabályi keretek által lefedetlen munkahelyi kockázatokat is azonosítanak, amelyek munkabaleset bekövetkezését, illetve foglalkozási megbetegedés kialakulását eredményezhetik, ezekre megelőző intézkedéseket hoznak. Ezek alapján kijelenthető, hogy a kockázatelemzés a legkorszerűbb munkáltatói megelőzési technika. Erőssége, hogy az „ember–gép–környezet" rendszer vizsgálatakor a munkavégzéskori tényállapotokból indul ki, és megkísérli meghatározni mindazokat az eseményeket, amelyek – szélsőséges körülmények között is – egy munkahelyen, a munkafeladat ellátása közben bekövetkezhetnek. [3]

A kockázatértékelés célja, hogy a munkaadó hatékony intézkedéseket hozzon és foganatosítson a munkavállalók biztonsága és egészségvédelme érdekében. Így a foglalkozási eredetű kockázatok elkerülhetővé váljanak, de legalábbis elfogadható szintűre csökkenjenek.

A kockázatértékelés végrehajtásához figyelembe veendő feltételek

A kockázatértékelés elvégzéséhez nem feltétlenül kell minden esetben laboratóriumi vizsgálatokat, illetőleg műszeres méréseket végeztetni, esetleg tudományos apparátust, költséges szolgáltatásokat igénybe venni. Általában a kockázatértékelés a meglévő munkavédelmi követelmények módszeres ellenőrzését, a hiányosságok megszűntetését jelenti, amelyben a legfőbb eszköz a széles körű munkavédelmi ismeret és a józan ész. A munkáltató akkor jár el ésszerűen, ha a kockázatértékelést és a kockázatbecslést összehangoltan szervezi meg azokon a területeken, amelyekre mindkét követelményrendszer vonatkozik, hiszen így nemcsak kisebb ráfordítással és nagyobb hatékonysággal végezheti el a felada-

tait, hanem maradéktalanul és összehangoltan elégítheti ki az ellenőrző hatóságok által számon kért követelményeket.

Az Mvt. 54. § (1) szerint az egészséget nem veszélyeztető és biztonságos munkavégzés érdekében a munkáltató köteles figyelembe venni a következő általános követelményeket:

a) a veszélyek elkerülése;
b) a nem elkerülhető veszélyek értékelése;
c) a veszélyek keletkezési helyükön történő leküzdése;
d) az emberi tényező figyelembevétele a munkahely kialakításánál, a munkaeszközök és munkafolyamat megválasztásánál, különös tekintettel az egyhangú vagy kötött ütemű munkavégzés időtartamának mérséklésére, illetve káros hatásának csökkentésére, a munkaidő beosztására;
e) a műszaki fejlődés eredményeinek alkalmazása;
f) a veszélyes helyettesítése veszélytelennel vagy kevésbe veszélyessel;
g) egységes és átfogó megelőzési stratégia kialakítása, amely kiterjed a munkafolyamatra, a technológiára, a munkaszervezésre, a munkafeltételekre, a szociális kapcsolatokra és a munkakörnyezeti tényezők hatására;
h) a kollektív műszaki védelem elsőbbsége az egyéni védelemhez képest;
i) a munkavállalók megfelelő utasításokkal történő ellátása.

Az Mvt. 54. § (2) szerint a munkáltató köteles minőségileg, illetve szükség esetén mennyiségileg értékelni a munkavállalók egészségét és biztonságát veszélyeztető kockázatokat, különös tekintettel az alkalmazott munkaeszközökre, a veszélyes anyagokra és készítményekre, a munkavállalókat érő terhelésekre, valamint a munkahelyek ergonómiai kialakítására. Az értékelés alapján olyan megelőző intézkedéseket szükséges hozni, amelyek biztosítják a munkakörülmények javulását, beépülnek a munkáltató valamennyi irányítási szintjén végzett tevékenységbe. A kockázatértékelés elvégzése munkabiztonsági és munka-egészségügyi szaktevékenységnek minősül.

A kockázatok értékelése szervesen összefügg a veszélyek megelőzésével, amelynek a kockázatok felismerésén és értékelésén kell alapulnia. Ezért a kockázatértékelés a munkáltató munkavédelmi tevékenységének központi és alapvető meghatározó fontosságú eleme, a veszélyek megelőzésének alapja.

A kockázatértékelés fő céljai:

– a megteendő intézkedések meghatározása és fontossági szempontból történő rangsorolása,
– a kockázatok elhárítása, illetve elfogadható mértékűre csökkentése.

A kockázatértékelés után a munkáltatónak képesnek kell lennie annak bizonyítására a hatóságok, a munkavállalók vagy képviselőik, illetve más érdekelt felek előtt, hogy megtett minden szükséges intézkedést a kockázatok felmérésére és elhárítására, illetve minimálisra csökkentésére. Ezért a kockázatértékeléshez hozzátartozik a folyamat és az eredmények megfelelő dokumentálása is.

A kockázatértékeléssel kapcsolatos fogalmak[1]

Kockázat a veszély megvalósulásának, azaz a káros hatás bekövetkezésének a valószínűsége, amelyet jellemez:

– a káros esemény mint következmény, amelynél figyelemmel kell leni az egyidejűleg érintett személyek számára is, valamint
– a káros esemény bekövetkezésének valószínűsége.

A kockázat számszerűsítésére használható a következő formula is: kockázat = gyakoriság x súlyosság. A gyakoriság, illetve a súlyosság megbecsülésére 1–10-ig számokat rendelnek. Az 1-es érték jelenti a kicsi vagy elhanyagolható értéket, a 10-es érték a nagyon súlyos, illetve szinte biztosan előforduló lehetőséget. Természetesen mivel becslésről van szó, itt nem lehet teljes mértékben kiküszöbölni a szubjektivitást.

Veszélyes az a létesítmény, munkaeszköz, munkafolyamat, technológia, amelynél a munkavállalók egészsége, testi épsége megfelelő védelem hiányában súlyos károsító hatásnak lehet kitéve.

Veszélyforrás a munkavégzés során vagy azzal összefüggésben jelentkező minden olyan tényező, amely a munkát végző vagy a munkavégzés hatókörében tartózkodó személyre veszélyt vagy ártalmat jelentenek.

A veszélyforrás lehet:

– fizikai,
– veszélyes anyag,
– biológiai,
– fiziológiai,
– idegrendszeri és
– pszichés igénybevétel.

Veszélyazonosítás: folyamat annak felismerésére, hogy egy veszély létezik. A veszély lehet:

– esemény vagy
– eset, amely balesethez vezetett vagy balesethez vezethetett volna.

A kockázatértékelés folyamatának lépései

1. A veszélyek azonosítása.
2. A veszélyeztetettek azonosítása.
3. A kockázatok minőségi, illetőleg mennyiségi értékelése.
4. A teendők meghatározása és a szükséges intézkedések megtétele.

[1] Az Mvt. 87. § és az MSZ EN ISO 12100-1:2004 [2] alapján.

5. Az eredményesség ellenőrzése és az értékelés rendszeres felülvizsgálata.
6. A fentieket kiegészítő és végigkísérő feladat a kockázatértékelés, valamint a felülvizsgálat írásba foglalása.

1. A veszélyek azonosítása: A veszélyek azonosítása az egész kockázatértékelés alapja. Részletesen fel kell mérni a kockázatértékelésbe bevont munkakörnyezet valamennyi munkafolyamatát, technológiáját, munkaeszközét, munkamódszerét. Ezek után kell meghatározni minden jelenlevő veszélyt, amely a munkavállalókat és más személyeket fenyegethet. Ennek során a Mvt. 54. § (2) bekezdése szerint különös tekintettel kell lenni az alkalmazott munkaeszközökre, a veszélyes anyagokra, készítményekre, a munkavállalókat érő terhelésekre, valamint a munkahelyek kialakítására. A veszélyeket (kockázati tényezőket) többféleképpen lehet csoportosítani.

2. A veszélyeztetettek azonosítása: A lehető legteljesebb körben számba kell venni azokat a személyeket, akiket veszélyek fenyegethetnek. Meg kell állapítani, hogy kik ezek, illetve hány személyt és milyen módon fenyegethetnek a veszélyek:

– A legkézenfekvőbb veszélyeztetett csoportot a munkahelyen foglalkoztatottak jelentik (például gépkezelők, karbantartók, irodai személyzet stb.), tehát azok, akik a veszéllyel járó munkafolyamatokat ténylegesen végzik, illetve ott tevékenykednek.
– A fentiek mellett különös figyelemmel kell számba venni egyrészt azokat a munkavállalókat, akiknek a munkája nem közvetlenül kapcsolódik az adott munkahelyen folyó tevékenységhez, másrészt azokat a személyeket, akik nem munkavállalóként kerülhetnek a munkavégzés hatókörébe.
– Szintén különös gondot kell fordítani az úgynevezett sérülékeny munkavállalói csoportok jelenlétére, akik egyrészt veszély előidézői is lehetnek, másrészt a veszélyek fokozottan fenyegethetik őket.

3. A kockázatok minőségi vagy mennyiségi értékelése: A kockázat végső értékelésében figyelembe kell venni egyrészt a veszély súlyosságát, vagyis az okozható kár mértékét és kiterjedését, ide értve a veszélyeztetettek számát is, másrészt a veszély bekövetkezésének valószínűségét. A munkahelyi kockázatértékelés legnagyobb feladatát a felismert veszélyek áttekintése és a kockázatok rangsorba állítása jelenti annak érdekében, hogy a munkáltató meghatározhassa a szükséges intézkedéseket. A kockázatok értékelésének nem célja és nem követelménye a számszerűsítés. A megfelelő értékeléshez célszerű a gyakorlatban használható kategóriákat felállítani. Erre nincsenek kötelező szabályok, de a besorolás alapjai lehetnek például a károsodás jellege, súlyossága, ezen belül is:

– Személyi sérülés.
– Kisebb személyi károsodás (horzsolás, zúzódás, múló egészségkárosodás).
– Súlyos személyi károsodás (törés, csonkulás, krónikus egészségkárosodás).
– Halálos (életveszélyes) baleset vagy egészségkárosodás.

Az értékeléshez figyelembe kell venni az érintett személyek számát is.

Másik szempont lehet a veszély bekövetkezésének valószínűsége, ezen belül is:

– Valószínűtlen.
– Lehetséges, de nem valószínű.
– Valószínű.
– Szinte elkerülhetetlen (csak idő kérdése).

A szempontok alapján a kockázatokat súlyossági (fontossági) sorrendbe célszerű állítani. A legsúlyosabb (legsürgősebb intézkedést igénylő) kockázatok természetesen azok, ahol a veszélyek a legsúlyosabb kárt okozhatják, a legtöbb személyt érinthetik és a legnagyobb valószínűséggel következhetnek be.

Gyakoriság/ kockázat	Kevésbé ártalmas (3)	Ártalmas (5)	Rendkívül ártalmas (10)
Valószínűtlen 1	Minimális kockázat 3	Elviselhető kockázat 5	Mérsékelt kockázat 10
Lehetséges 2	Elviselhető kockázat 6	Mérsékelt kockázat 10	Lényeges kockázat 20
Valószínű 4	Mérsékelt kockázat 12	Lényeges kockázat 20	Elfogadhatatlan kockázat 40
Elkerülhetetlen 5	Mérsékelt kockázat 15	Lényeges kockázat 25	Elfogadhatatlan kockázat 50

1. táblázat: A kockázat mértékének lehetséges értelmezése[2]

Ezután kell a munkáltatónak eldöntenie:

– A jelenlegi helyzet kielégíti-e a munkavédelemre vonatkozó szabályok követelményeit?
– A kockázatok megfelelő ellenőrzés alatt vannak-e?
– A jelenlevő kockázatok milyen módon szüntethetők meg?
– Milyen intézkedéseket kell tenni a kockázatok megelőzése vagy csökkentése érdekében?

[2] Az 1-es táblázatban szereplő kategorizálás, illetve az egyes kategóriákhoz rendelt számok, szorzatok a gyakoriság, valamint a kockázat mértékével kapcsolatban a szerző lehetséges gondolkodásmódját tükrözik.

Kockázat	Kockázat mértéke	Intézkedés
Minimális	1–4	Nem szükséges
Elviselhető	5–9	Amennyiben viszonylag egyszerűen, kis költséggel megvalósítható, intézkedés szükséges. Amennyiben nem, akkor a munkahelyi események további figyelemmel kísérése szükséges.
Mérsékelt	10–19	Intézkedés a kockázatcsökkentésére, ill. megszüntetésére. határidő kitűzésével
Lényeges	20–30	Azonnali intézkedés szükséges.
Elfogadhatatlan	31–50	A tevékenység leállítása szükséges a kockázat megszüntetéséig, vagy csökkentéséig.

2. táblázat: Lehetséges intézkedések a kockázat mértékének függvényében[3]

A jelenlevő kockázatok megszüntetése, megelőzése vagy csökkentése a Mvt.-ben foglalt elvekkel összhangban történhet:

- Ha lehetséges, a kockázatot teljes mértékben ki kell zárni.
- A kockázatos dolgot (pl. veszélyes anyag, technológia) kevésbé kockázatossal kell helyettesíteni.
- A kockázatot a keletkezési helyén kell megszüntetni, hogy minél kisebb helyen kelljen védekezni ellene, és minél kevesebb munkavállalót érintsen.
- Mind a kevésbé kockázatos dologgal (anyaggal, technológiával, munkaeszközzel stb.) történő helyettesítéskor, mind pedig a kockázat keletkezési helyén történő megszüntetésekor gondot kell fordítani arra, hogy ez ne eredményezzen újabb, esetleg észrevétlenül maradó kockázatot.
- A kollektív műszaki védelmet előnyben kell részesíteni az egyéni védőeszközök alkalmazása helyett.
- Alkalmazni kell a műszaki fejlődés eredményeit.

4. A teendők meghatározása és a szükséges intézkedések megtétele: Az előzőek elvégzése után a fenti szempontok alkalmazásával a munkáltatónak konkrét intézkedési tervet kell készítenie a kockázatok megelőzése vagy csökkentése érdekében.

A Mvt. 54. § (2) bekezdése szerint „az értékelés alapján olyan megelőző intézkedéseket szükséges hozni, amelyek biztosítják a munkakörülmények javulását, beépülnek a munkáltató valamennyi irányítási szintjén végzett tevékenységbe".

[3] A 2-es táblázat az 1-es táblázat kategóriáival és értékeivel összhangban került kialakításra.

Az intézkedéseknek mindig az adott munkahelyhez, munkavállalókhoz és munkakörülményekhez kell igazodniuk. A szükséges intézkedéseket célszerű sürgősségi sorrendbe állítani, amelyek lehetnek:

– azonnali,
– rövid- vagy középtávú,
– hosszú távú intézkedések.

5. Az eredményesség ellenőrzése és az értékelés rendszeres felülvizsgálata: A munkáltatónak ellenőriznie kell, hogy a kockázatértékelés következményeként a kockázatok csökkentése érdekében meghatározott és végrehajtott intézkedések valóban hatásosan és stabilan csökkentették a kockázatokat.

A kockázatértékelést legalább évente felül kell vizsgálni akkor is, ha nem történik különösebb változás. Ha azonban jelentősebb változás következik be a munkakörülményekben, a technológiában, a munkaeszközökben, a felhasznált anyagokban, a munkaszervezésben, a munkavállalói állományban, a munkavédelmi követelményekben, a műszaki fejlődésben vagy a rendelkezésre álló ismeretekben, akkor szükségessé válik a kockázatértékelés ismételt elvégzése, illetőleg felülvizsgálata.

6. A kockázatértékelés és a teendők, valamint a felülvizsgálat írásba foglalása: A munkáltatónak be kell tudnia bizonyítani a munkavédelmi hatóságok (Állami Népegészségügyi és Tisztiorvosi Szolgálat, Magyar Bányászati Hivatal, Országos Munkabiztonsági és Munkaügyi Főfelügyelőség), a munkavállalók vagy képviselőik, illetve más érdekelt felek előtt, hogy megtett minden szükséges intézkedést a kockázatok felmérésére és elhárítására, illetve minimálisra csökkentésére.

Ezen túlmenően a Mvt. szerint a munkáltató köteles tájékoztatni a kockázatértékelés tapasztalatairól a következőket:

– a munkáltatónál munkabiztonsági szaktevékenységet ellátó személyt,
– az általa foglalkoztatott, munkavédelmi szakképesítéssel rendelkező személyt,
– a foglalkozás-egészségügyi szolgálatot,
– a munkavédelmi képviselőt vagy bizottságot.

A kockázatértékelés eredményeként a munkáltató felelőssége legalább a következők dokumentálása:

– a kockázatértékelés időpontja, helye és tárgya, az értékelést végző azonosító adatai,
– a veszélyek azonosítása,
– a veszélyeztetettek azonosítása, az érintettek száma,
– a kockázatot súlyosbító tényezők,
– a kockázatok minőségi, illetőleg mennyiségi értékelése, a fennálló helyzettel való összevetés alapján annak megállapítása, hogy a körülmények megfelelnek-e a munkavédelemre vonatkozó szabályoknak, illetve biztosított-e a kockázatok megfelelően alacsony szinten tartása,
– a szükséges megelőző intézkedések, a határidő és a felelősök megjelölése,

– a tervezett felülvizsgálat időpontja,
– az előző kockázatértékelés időpontja.

A kockázatértékelés dokumentumát a munkáltató köteles a külön jogszabályban foglaltak szerint, de legalább 5 évig megőrizni.

Összegzés

A munkahelyi kockázatértékelés végrehajtása – a jogszabályi háttér figyelembevételével – elsősorban a munkáltatóra ró felelősséget. Az kiderült, hogy az elemzés módszertana tartalmaz szubjektív elemeket. Nem véletlenül fogalmazza meg a Mvt. is, hogy a munkahelyi kockázatelemzés elvégzése munkabiztonsági és munka-egészségügyi szaktevékenységnek minősül. A tanulmányban ismertetett elvek mentén, továbbá megfelelő szakember alkalmazása esetén azonban megalkotható egy olyan kockázatelemzés, amely valóban szolgálja a munkáltató és a munkavállalók érdekeit, illetve biztonságát egyaránt.

Irodalomjegyzék

1993. évi XCIII. törvény a munkavédelemről.
MSZ EN ISO 12100-1:2004.
Kis-Pál Ágnes: Munkavédelem biztonságtechnikája. Jegyzet. Budapest, 2011. július.
Guidance on risk assessment at work, European Comission Directore-General of Employment, Industrial Relations And Social Affairs.
Dr. Rajnai Zoltán – Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army. Academic and Applied Research in Military Science 9: (1) pp. 15–23., Budapest, 2010.

Risk Analysis Methodology

Szamosi Barna

In the study the author briefly explains risk assessment and the role of risk assessment in the workplace. The study provides insight into a possible assessment process, which is a special form of OSH of the workers.
In accordance with the rules of the European Community, the 1993 Occupational Health and Safety Act, which has been amended several times, lays down certain obligations for the employers; i.e., if the occupational hazards cannot be treated by the relevant standards named in the technical, organizational, and technological measures, the level of occupational hazards must be assessed by specific analysis.
The European guidance on risk assessment at work recommends a method based on a number of different steps. This is not the only method of risk analysis; there are several methods to achieve the same objective. This study describes briefly one of the possible variants of this analysis process.

Vanderer Gábor
Rajnai Zoltán

Applicability of risk-evaluation theories in crtitical infrastructures

Business (and governmental, municipal, non-profit etc.) organizations have long been paying attention to safeguarding their information assets and information infrastructure. On the one hand, it is getting more and more important with the development of an information society, and on the other hand, it is a response to the growing external threats jeopardizing the operation of enterprises. By now, there are many regulations, procedures and industry standards that have been developed for organizations to handle these threats, but these methods mostly use a traditional, business-based approach.

Information wealth

Information has always had a great value. Owners have been interested in defending their treasure since the beginning of times. Many kings and generals relied on a network of intelligence and communication and all of them were aware of the consequences if this information should fall into unauthorized hands. That was a call for the development of the art of cyphering (and decoding) while also increased the value of storing and transmitting information in a secure way. Safeguarding information has never been the monopoly of the state: civilian traders or even the church wanted to safeguard their information as well, even if they did not have the same resources.

Our world has changed a lot since those times, but it is still very true that information is the key factor for success in today's knowledge-based society. It has a value that can easily decide between success and failure in the life of a company. It is self-evident that information needs to be safeguarded.

As more and more companies entered into the information security market, the general concepts for an effective approach have crystallized. This helped to establish the standards for information security (ISO/IEC 27001) which includes:

- Confidentiality (information should be accessed by authorized people only)
- Integrity (information should be full and accurate)
- Availability (information should always be accessible for authorized people)

Information security and IT security

Information security is a much more complex problem than IT security (Michelberger–Lábodi, 2012). Firewalls, virus protection, 0-day prevention (and all the things usually categorized as IT security) are forming only the technical background. Obviously, it is not enough. These systems are being used by people. The confidentiality, integrity and availability of this information is jeopardized by the slothful attitude of the inside users and the people outside the company authorized to use this data (suppliers, partners, etc.)

As Pál Michelberger said (Michelberger – Lábodi, 2012, p 243), the weak link is always the human part. In his opinion (and I can only agree with it), information security is more of a journey than a destination. If we investigate IT security, it becomes clear that not even a well-secured system can persist forever. New vulnerabilities unravel every time, new software bugs emerge, which should be addressed. Safeguarding the information vault depends not on the (currently) state-of-the-art technical implementation, but on the permanent inspection and development of the existing systems. And feedback, obviously.

Organizations usually regulate the usage of information-barriers and the information itself to safeguard their information-wealth (ISO 27001). Safeguarding can be successful if they define:

- information elements to be secured
- inside and outside threats
- the probability of each threat
- regulations and instruments required for protection (ISO 27002)

The aim of information security is to maintain business continuity in a regulated way and to moderate the damage caused by security accidents. Parts of these regulations are regulations describing the processes of the organization and the rules for the use of IT devices and systems. Organizations have to concentrate on the information management system instead of buying equipment in order to ensure long-term secure operation.

We can define different levels of protection within information security (Ji-Yeu Park et.al. 2008):

- Information technology infrastructure (hardware, software and network protection)
- Information handling (data entry, modification, deletion and access)
- Procuration (process regulation, workflow)
- Organization (information security strategy, risk management)

A good example for this is a „holistic" approach (Michelberger – Lábodi, 2012, p 244) where authorization has to be implemented on all 4 levels:

- *IT level* – user authentication
- *information handling* – guarantee that only the required data will be accessed

– *process level* – sharing of critical processes, personal and workplace-based access control
– *organization level* – risk avoidance, group-based authentication, regulating the permanent supervision of the authentication system.

It is commonly accepted today that the first stage of security is a written security policy. It is impossible to set goals without the definition of tasks and responsibilities (and the human and financial resources required). Information security – as a process – can only be ensured after having this done.

Risk management

The aim of risk-management is to identify threats that could jeopardize the operation of the organization. They may exist inside or outside of the organization (a typical external example is the market of a company). In traditional risk-management we usually assign amounts of money to each detected risk (calculated damage caused be the event), associated with the probability of occurrence. The cost of defence against each threat is compared with this, and a cost-benefit analysis is made to decide on security investments. There are situations where factors for the calculations above can only be assessed with an extremely low precision. In these situations professionals talk about vulnerability and describe only the threats to the operation (and do not use numbers). Organizations operating critical infrastructure elements have to use the second approach. These organizations also use cost/benefit-based analysis for decisions (obviously); but when critical infrastructures enter the picture it is not reasonable to define damage in monetary value. Organizations simply have to be prepared against the threats.

Standards and recommendations

People say that an engineer can find a standardized solution for almost everything. The only problem is to find the relevant standard. This applies to the area of information security as well. There are several de facto and de jure standards related to information security. The latest standards commonly use a process-based approach, but each one concentrates on different areas. However, most of them cover the area of security. A commonly used information security management system is the British-originated ISO/IEC27k standard-group. (www.iso27001security.com). Organizations working with it define security requirements and corresponding actions based on organizational strategies. This standard places a special emphasis on information security (integrity, confidentiality, availability). It has no part dedicated especially to critical infrastructure systems (however

„ISO 27799 - ISO27k for healthcare industry" covers one critical infrastructure). It has a framework typically suitable for defining information security for critical infrastructures. It is an interesting thing that being process-based, the standard is not dependable on any kind of technical solution. However, it contains some parts on network security (ISO/IEC 27033). It was a common procedure to prohibit internet connection for critical infrastructure elements, but nowadays it is not always sustainable. A typical example is the banking system. All organizations use the Internet for bank transfer (and they have to use bank transfer by governmental regulations), but only a fraction of them is able to implement some kind of workaround (transfer money by phone, for example). Not even banks are prepared for this in the required volume. Using the Internet is sometimes mandatory, so some calculated risks have to be taken. The ISO/IEC 27032:2012 standard addresses Internet Security specifically.

Another interesting regulation is addressing cloud services. The ISO/IEC 27017 is currently existing in a draft version only (the final version is scheduled for 2015). There are no plans for auditing the cloud providers at all. As I have already mentioned, the weak link is always the human part. It is reasonable to create rules for employees on how to act in different situations. One of the most important standards is the British-originated MSZ ISO/IEC 20000-1, -2, targeting operational issues based on the recommendations of ITIL (Information Technology Infrastructure Library, www.itsmfi.org). It contains a formal system of requirements about the acceptable level of information services, a guideline about service controls and one more for auditing.

Service management activities are connected to the currently popular PDCA model, which is applied in several standards. In addition to the management system, the issues of planning and implementation of information technology systems, and the planning and creation of new services, there are five basic areas of complete service management:

1. Service security (service level, service reporting, capacity, service continuity, availability, information security, budgeting and accounting for IT services)
2. Management processes (configuration and change management)
3. Release (documents, operational description distribution management, the documentation of approved modifications)
4. Solution processes (incident and problem management)
5. Relationship (customer service, business and supplier relationship management)

ITIL is widely used by IT outsourcing companies for SLA definitions; however, the specialties of critical infrastructures can be fitted into MSZ ISO/IEC 20000-1 based specifications. See later in the paper about BCP and DRP plans. ITIL takes a process-based approach. It defines activities which are segmented into processes. All processes have 3 levels:

– Strategic level: Organizational objectives are defined, together with the outline of methods to achieve these objectives.

– Tactical level: Strategy is translated into organizational structure and plans which describe the processes to be executed, assets to be deployed and outcome(s) of the processes.
– Operational level: The execution of tactical plans to achieve strategic objectives within a specified time frame.

ITIL does not have a separate topic for information security. It targets the subject as part of all the processes. For example Data and information management (ITIL v3 Service Design Chapter 5.2) or Roles and responsibilities (ITIL v3 Service Design Chapter 6.4) have details on information security control, and there is a separate process on Information security management and service operation (ITIL v3 Service Operation Chapter 5.13).

ISACF (Information Systems Audit and Control Foundation) also developed a recommendation, the widely used COBIT (Control Objectives for Information and related Technology) (www.itgi.org/cobit). It is an internationally developed and accepted framework (mainly for business organizations), which helps to understand and handle the risks around the areas of information and information security. COBIT is aimed at harmonising information technology services and the operational processes of the organisation as well as facilitating the measurability of the security and management features of information technology services.

COBIT starts from business targets. Achieving these targets requires information to be available and resources to be allocated to the information systems. All of these processes should be handled under coherent processes. ITIL helps to fill the gap between business risks, verification needs and technical problems. COBIT concentrates specifically on creating a cost-effective security.

ISO/IEC 38500 is a high level, principles-based, advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of IT. The objective of the standard is to provide a framework of principles for directors to use when evaluating, directing and monitoring the use of IT in their organizations. It also targets human behaviour.

Based upon the standard, a GRC model can be developed:

Governance – Corporate goals and processes, the organizations running the processes with special emphasis on the supporting information technology systems

Risk management – Identifying the probabilities of expected events and defining an acceptable level of security for the processes and their supporting information systems

Compliance – Organizations have to meet internal regulations and external (governmental) regulations and standards.

The outcome of the model is a list of requirements continuously following the changing conditions. Thus the management of the company is aware of the risks and risk-based decision-making. The ISO/IEC 38500 builds on consciously undertaken risks, so its use is contraindicated for the operation of a critical infrastructure. In this scenario, core operation allows negligible risks only, so decision-making based on calculated risks seems unfeasible.

Integrated control systems

All of the above-mentioned integrated management systems use a process-based approach. All of them follow the schemes of the unavoidable ISO 9001. All of the other management systems (ISO 14001 for environmental control, ISO 27001 for information security, and so on) are usually integrated into ISO9001. It is easy to state that transparent operation is important for every organization and not just for those operating critical infrastructures. Companies have a recognized right to keep their internal processes secret (as part of the competitiveness). Another natural need is to be sure that their partners (suppliers, resellers, etc.) are trustworthy. It is easy to see that data handled by a partner should be just as safe as the data handled by ourselves. If our partner is ISO27001 certified, we are sure that it can meet these expectations and the organization places importance on information security even if we do not see the exact inside processes.

BCP and DRP

Maintaining normal operations in any circumstance requires a written documentation defining how operations are to be re-established after an unexpected event. The main purpose of this document is to define all necessary tasks in advance to possibly prevent ad-hoc decision-making in a stressful situation. In this way the re-establishment of service (ideally) becomes an automatic step-by-step process. It has some clear advantages:

- As the re-establishment (or the implementation of a workaround) becomes a step-by-step process with clear checkpoints, the possibility of making a mistake is substantially decreased
- All the necessary and only the necessary underlying infrastructure elements will be restored to maintain core business processes.

- Prioritizing among processes of the company is not the decision of the staff operating the underlying technical infrastructure (and doing the actual restoration). Predefined priorities eliminate the need of communication between different sub-organizations: the technical staff are able to restore business on their own.

Business Continuity Planning (BCP), sometimes also called Business Continuity and Resiliency Planning (BCRP), helps a company to continue operations under adverse conditions, such as a disaster afflicting the company's headquarters. It does this by identifying the core underlying processes of the organization which directly affect the bottom line and by finding alternate or back-up processes in the event of disruption. The business continuity plan itself is exactly what it looks — it is a plan or roadmap for the business to follow in a situation which threatens the continuity of business. (Charles Intrieri, 2013)

Business Impact Analysis (BIA): This analysis is for collecting the relevant features of business processes in order to assess the damage caused by any disturbance in each of the processes. The result of the analysis:

- list of processes
- their monetary and non-monetary value
- allowed maximum downtime
- list of the resources required by the process
- interdependencies of processes

The Disaster Recovery Plan (DRP) is supposed to define procedures to follow in case of an unexpected event. It typically provides alternatives which enable the IT system to serve business processes, at some (even reduced) level. Its basic concept is to minimise damage coming from the stoppage of business processes defined according to BCI/BIA. When creating a DRP, it is a typical mistake to concentrate on the information serving infrastructure only. In this case all business processes are considered equal, everything is equally important, everything must work. The order of restoration is not based either on the business impact of the processes served or interdependencies. However, it is much better than nothing, and it can even be sufficient in some cases when the only purpose is the restoration of the required service in the shortest possible time. In an ideal case, DRP relates to the BCP plan: it is exploring organizational processes and considers their connections and the effects they make on each other. A really good DRP plan requires the exploration of all organizational processes.

Information security and the human factor

The need for information security in an organization usually comes from IT, and during organizational evolution, remains on this level for a long time. This approach is usually the technocratic kind: strongly concentrates on data storage, regular backup, firewalls and virus protection. On the other hand, it typically neglects the risks of the human factor, and physical protection is also reduced to an alert and entry system for the office building. On this level, information has two classification categories: important (with backup save) and not important. In a less than ideal case, everything is backed up and no classification is done. It is a common mistake with critical infrastructures, too. ("everything is important, no need for classification"). However, at this point we must already see that this approach is essentially wrong: it does not allow the detection of effects exerted on procedures and thus precludes risk handling. However, risks are mostly caused by the human factor. Even though standards and regulations are placing emphasis on both physical defence and the human side, this issue is usually neglected. As Pál Michelberger states: "They [the errors coming from the human factor] cannot be fully eliminated, but it is possible to reduce them by a good human resources policy. Information security considerations can and should be integrated into the regulation of selecting, admitting and dismissing employees." The training and awareness of employees (mostly employees involved in operating and emergency response) is very important; however, in my opinion, it is much more effective to build a system which requires only a minimal amount of thinking in the case of a catastrophe, during the implementation of a DRP plan. Of course, there are events not covered by the DRP, and in these cases the effectiveness of salvaging depends heavily on the knowledge and routine of employees. However, in general, a system which is covering events by written procedures has a much better stability.

If we set aside special cases and concentrate on normal business, we still find that a significant part of threats to information infrastructure are caused by employees (Michelberger et al., 2013). These threats cannot be fully eliminated, but they should be minimalised. The training of users is vital. The danger caused by a negligent administrator is totally different from that of a vengeful system administrator. It is an interesting issue that generation gap might play some role in information security as a part of the human factor. According to sociologist and marketing professionals, employees may fall into any of the following five characteristic categories by date of birth (Lancaster-Stillmann, 2010):

- veterans
- „baby boom" generation (born between 1946 and 1965)
- generation X (born between 1965-1980)
- generation Y (born between 1980-1995)
- generation Z (born after 1995)

There are no general rules, and there are a lot of exceptions; however, each group has a specific approach to information technology, so categorization might be useful for IT security purposes in case of a large number of employees. Veterans were born a long time ago and they were already quite old when information technology became widespread. Using modern communication and information technology is a challenge for them. Most of them are already retired. Members of the baby-boom generation are usually loyal to their employer, but it is difficult for them to follow the constant development of information technology. They may also have deficiencies in their technical knowledge so they can create damage by mistake. The typical member of generation X is independent. They usually throw away the security regulations ("They know it better"). They have the knowledge so they may create damage by malice. The members of Generation Y are the children of the Information Age. They are the people who rather use Google instead of waiting for a call center in Bangladesh. They frequently download, without encryption, confidential corporate information to their private mobile devices. The members of generation Z are born into the world of internet, they expect and require a constant online presence. A traditionally high-security workplace is tearing them out of their natural medium. Generation differences and age group characteristics must be considered when regulating information security (Kelemen, 2008).

Training and education

As I have already pointed out, the technical staff operating the information technology are usually aware of threats, even if they do not acknowledge its non-technical side. The biggest threat for the information vault of an organization is usually not deliberate sabotage but the lack of security awareness and prudence. Improving information security awareness is vital. Internet has become the primary source of information and paper-based catalogues have practically disappeared. Information comes from the manufacturer's web page but even supply chains rely heavily on Internet (e.g. webEDI). Nowadays it is almost impossible for an organization to exclude the internet, even without the protest of X and Z generation members.

The most neglected part of information technology investments is the education of users. Trainings rarely consider the special needs of organizational units, and system administrators who typically manage internal trainings are not necessarily prepared in training methodologies. Follow-up trainings are usually forgotten too. It is very common to try handling basic problems with technology: too simple and rarely changed passwords with authentication hardware and single-use passwords; logging-in with someone else's user by biometric identification, etc. However, these methods are only aimed at the symptoms. They might help to force users to use secure passwords but they do very little to improve awareness.

Conclusions

In my study I have reviewed the widely used de facto and de jure standards in the field of information security while also investigated the experience with them. It can be stated that today's process-based approach is able to cater for the special requirements of critical infrastructures. However, they might need a little adjustment: It is not always reasonable to handle some types of costs as „infinite" (e.g. COBIT's smallest harm). It is a much better solution to create categories for the needs and place each of them into the right category. (ISO/IEC 14598). The future belongs to process-based, integrated quality control systems. I think that information security can be handled well within the scope of existing information security standard ISO/IEC 27xxx, while we can handle critical infrastructures with special BCP / DRP plans which are more detailed than the usual ones.

Bibliography

Dr. Michelberger Pál – Lábodi Csaba: Vállalkozásfejlesztés a XXI. században. Budapest, 2012.
Godányi Géza: Katasztrófavédelem és üzletmenet folytonosság az információtechnológiában. (A DR/BC tervezés alapjai.) Híradástechnika, LIX. évfolyam, 2004/4, pp. 47–52.
Pál Michelberger – József Beinschróth – Gergely Krisztián Horváth: The Employee – An Information Security Risk. Acta Oeconomica, Universitatis Selye, 2013, Komárno, pp. 187–200
Tóth Tibor (szerk.): Minőségmenedzsment és informatika. Műszaki Könyvkiadó – Magyar Minőség Társaság, Budapest, 1999.
Ji-Yeu Park – Robles, Rosslin John – Chang-Hwa Hong – Sang-Soo Yeo –Tai-hoon Kim: IT Security Strategies for SME's. International Journal of Software Engineering and its Applications, Vol. 2. No. 3., July. 2008, pp. 91–98.
Lynne C. Lancaster – David Stillman: The M-Factor: How the Millennial Generation Is Rocking the Workplace. HarperCollins, 2010.
Kelemen László: Nem sztereotípiák,. IT-business. 2008. szeptember 28., VI. évf. 37. sz., p. 32.
http://www.iso27001security.com/ (retrieved 18 December 2013)
European Network and Information Security Agency – ENISA (November 2010): How to Raise Information Security Awareness (The new users' guide p. 140). http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide (retrieved november 2013)
Intrieri, Charles (10 September 2013). "Business Continuity Planning". Flevy (retrieved 18 December 2013)

Kockázatértékelési elméletek alkalmazhatósága a kritikus infrastruktúrákra

Vanderer Gábor – Rajnai Zoltán

Az üzleti (és a kormányzati, önkormányzati, nonprofit stb) szervezetek már régóta nagy figyelmet fordítanak az informatikai infrastruktúra és az információs eszközök védelmére. Egyrészt az információs társadalomban egyre fontosabb ezen eszközök és rendszerek fejlesztése, másrészt a vállalkozások működésében ez egy válasz is a növekvő külső fenyegetésekre, veszélyekre. Napjainkban több rendelet, eljárás és ipari szabvány segít, hogy a különböző szervezetek kezelni tudják ezeket a fenyegetéseket, de ezeket a módszereket leginkább a hagyományos, üzleti alapú megközelítés jellemzi.

Szabolcsi Róbert

UAV automatikus repülésszabályozó rendszer típus- és légi alkalmassági tanúsításának megfelelési kritériumai – oldalirányú mozgás

A szerző célja, hogy az UAV[1]/UAS[2] automatikus repülésszabályozó rendszerek oldal- és keresztirányú irányítási csatornájában megvalósuló mozgások minőségi jellemzőiről átfogó képet adjon, és a minőségi jellemzőket olyan módon írja le, hogy e jellemzők alapjául szolgálhassanak egy adott UAV típus- és légi alkalmassági vizsgálatainak. Tekintettel a hazai és a nemzetközi szabályozás részleges hiányára, a cikkben közölt eredmények hiánypótlóak, a hatósági tanúsításban részt vevő szakemberek számára pedig megfontolásra ajánlottak.

Kulcsszavak: UAV, UAS, oldalirányú/keresztirányú mozgás, UAV robotpilóta, UAV automatikus repülésszabályozás, UAV hatósági tanúsítás

Bevezetés

A modern UAV/UAS-rendszerek aerodinamikai elrendezése meglehetősen sokszínű, ezért e cikk csak a hagyományos tervezésű, hagyományos aerodinamikai elrendezésű, kisméretű UAV-k (SUAV[3]) automatikus repülésszabályozási kérdéseivel foglalkozik.

A szerző célja, hogy összefoglalja az UAV tanúsítási folyamatok eljárásrendjére vonatkozó és jelenleg is rendelkezésre álló szabályokat. Az UAV/UAS-rendszerek légi és földi üzemeltetési jellemzői közül a szerző a fedélzeti automatikus repülésszabályozó rendszerre fektet hangsúlyt. Tekintettel a jelenlegi szabályozás sajátosságaira, a szerző bemutat és alkalmazásra javasol egy merőben új minőségi követelményrendszert, amely alkalmas lehet a kisméretű, pilóta nélküli légi járművek fedélzeti automatikus repülésszabályozó rendszerének típus- és légi alkalmassági megfelelési vizsgálata során.

[1] Unmanned Aerial Vehicle – pilóta nélküli légi jármű.
[2] Unmanned Aerial System – pilóta nélküli légijármű-rendszer.
[3] Small Unmanned Aerial Vehicle – kisméretű pilóta nélküli légi jármű.

Előzmények, motiváció, problémafelvetés

A szerző egyik cikkében azt vizsgálta, hogy a légügyi hatósági tanúsítás eljárási folyamatai „barát vagy ellenség"-ként kezelhetőek-e. [4] A cikkben a szerző igazolta, hogy a hatósági eljárásnak gyakorlatilag nincs hátránya, míg előnye számos mutatkozik.

A szerző egy másik cikkében részletekbe menően foglalkozik az UAV/UAS-rendszerek légi alkalmassági tanúsítási sajátosságaival. [5] A szerző bemutatta, hogy a hazai tanúsítási rendszer számos eleme egyelőre nem teljes részletességgel kidolgozott, számos terület vár szabályozásra vagy éppen a meglévő szabályok módosítására.

A szerző egy további cikkében ismertette a hazai fejlesztésű METEOR-3MA pilóta nélküli célrepülőgép és a részére kifejlesztett C4S-HMEI OSD fedélzeti robotpilóta típus- és légi alkalmassági tanúsításának eredményeit. [6] A szerző mint szakértő vett részt és vesz részt mind a mai napig a Nemzeti Közlekedési Hatóság Légügyi Hivatala által vezetett hatósági tanúsítási folyamatban, amely ez év során sikerrel kecsegtet.

A szerző szakkönyvében már foglalkozott a légi járművek automatikus repülésszabályozó rendszereinek minőségi jellemzőivel. [3] A szerző rámutatott, hogy a jelenleg ismert minőségi jellemzőket alapvetően az utasok vagy a személyzet komfortérzetét szem előtt tartva határozták meg. Könnyű belátni, hogy az emberközpontú minőségi jellemzők, amelyekről [1] is számot ad, az UAV-k esetében közvetlenül, újragondolás és esetleges módosítás nélkül nem használhatóak.

A nemzetközi gyakorlatban rendelkezésre álló szabályozók közül a NATO STANAG 4671 katonai szabvány az egyedüli, amely pilóta nélküli légijármű-rendszerek légi alkalmassági tanúsításával foglalkozik. [2] A szabvány a több mint 150 kg és legfeljebb 20 000 kg maximális felszálló tömegű, nem elkülönített légtérben közlekedő UAV-kra vonatkozik.

A NATO STANAG 4671 szabvány hatálya tehát közepes és nagy felszállótömegű UAV-kra terjed ki. Ez a NATO-szabvány tehát nem alkalmazható a kisméretű UAV-kra. Mindezeken túl, az UAV repülésszabályozása szempontjából fontos dinamikus minőségi jellemzőket a szabvány „Flight Characteristics"/„Controllability and Manoeuvrability" fejezet, „145 Longitudinal control" és a „147 Directional and lateral control" alfejezetei „Not applicable" („Nem alkalmazandó") megjegyzéssel jelöli. Más szóval, a vizuális látótávolságon túl repülő, pilóta nélküli légi járművek, amelyek nem elkülönített légtérben repülnek, sokszor automatizált üzemmódokon, a NATO STANAG 4671 szabvány hatálya szerint nem rendelkeznek a zárt automatikus repülésszabályozó rendszerekre vonatkozó minőségi előírásokkal.

A hazai és a nemzetközi szabályozási környezet bemutatása

Az állami célú repülésben használt légi járművek típus- és légi alkalmassági követelményeit a 21/1998. (XII. 21.) HM rendelet taglalja. Megemlíteni szükséges azonban, hogy a jogszabály inkább a légi alkalmassági tanúsítás rendjét adja meg, mint az eljárás módszertanát vagy éppen műszaki előírásait, követelményeit. Könnyű belátni, hogy az UAV/UAS típus- és légi alkalmassági tanúsítási rendszerében a hazai jog meglehetősen hiányos.

A NATO STANAG 4671 katonai szabvány kifejezetten az UAS-rendszerek légi alkalmassági tanúsítási követelményeiről szól. [2] A szabvány 1. változata 2007-ben készült el, 2008-ban hazánk is ratifikálta, de a hazai jogrendbe nem vezették be. A STANAG 4671 katonai szabvány 3. változatát a NATO 2009-ben léptette hatályba.

Új ösztönzést adhat az Európai Bizottság 2014. április 8-i keltezésű, COM(2014)207 közleménye, amely 2016-tól előírja az UAV/UAS/RPAS-rendszerek fokozatos és folyamatos integrációját a légi közlekedésbe a nem elkülönített légterekben végrehajtott repülések során is. A megfogalmazott új irányok és ezen irányokban sikeresen megoldott feladatok felszabadítják az utat az UAV/UAS-technológiák elterjedése előtt: kitörési pont lehet ez úgy az európai, mint a világpiacon az UAV-tervezők, a fejlesztők, a gyártók és az üzemeltetők részére is. [7]

UAV térbeli, oldalirányú mozgásának dinamikus repülési modellje és jellemzői

A vizsgált UAV térbeli, oldalirányú mozgásának többváltozós, állapotteres modelljét zavarásmentes esetben az alábbi állapot (vektor-differenciál) egyenlettel írhatjuk le [1] [3]:

$$\dot{\boldsymbol{x}}=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{B}\boldsymbol{u}, \quad (3.1)$$

ahol: $\boldsymbol{x}$ – állapotvektor, $\boldsymbol{u}$ – bemeneti vektor; $\boldsymbol{A}$ – állapotmátrix; $\boldsymbol{B}$ – bemeneti mátrix.

A továbbiakban feltételezzük, hogy az $\boldsymbol{x}$ állapotvektor rendezői, más szóval az oldal-/keresztirányú mozgás repülési paraméterei az alábbiak [1] [3]:

v – kereszt(oldal)irányú repülési sebesség (m/s);

p – orsózó szögsebesség (rad/s vagy °/s);

r – legyező szögsebesség (rad/s vagy °/s);

ϕ – bedöntési szög (rad vagy °);

ψ – irányszög/legyezőszög (rad vagy °).

Az UAV $\boldsymbol{u}$ bemeneti vektorának rendezői, más szóval a kormányzás/irányításhoz használt bemeneti jellemzői az alábbiak [1] [3]:

δ_A – a csűrőlapok szöghelyzetének változása;

δ_R – az oldalkormány szöghelyzetének változása.

Az UAV oldalirányú forgómozgása két tengely körül valósul meg. A hossztengely körüli forgás az orsózó mozgás, míg a függőleges tengely körüli forgás a legyezőmozgás. A légi járművekre jellemző, hogy e két tengely körül a forgómozgás más és más dinamikával bír, és a repülési jellemzők minőségi jellemzői is lényeges mértékben térnek el egymástól. [1] [3]

Az UAV orsózó mozgásának dinamikus repülési modellje és annak jellemzői

Az UAV orsózó mozgásának dinamikus viselkedését az alábbi reprezentatív átviteli függvényekkel adhatjuk meg [1] [3]:

$$W_1(s) = \frac{p(s)}{\delta_A(s)} = \frac{sK_\phi(s^2+2\xi_\phi\omega_\phi s+\omega_\phi^2)e^{-\tau_{ep}s}}{(s^2+2\xi_D\omega_D s+\omega_D^2)(s+1/T_S)(s+1/T_R)}, \qquad (3.2)$$

vagy

$$W_2(s) = \frac{\phi(s)}{\delta_A(s)} = \frac{K_\phi(s^2+2\xi_\phi\omega_\phi s+\omega_\phi^2)e^{-\tau_{ep}s}}{(s^2+2\xi_D\omega_D s+\omega_D^2)(s+1/T_S)(s+1/T_R)}, \qquad (3.3)$$

ahol:

– $\delta_A(s)$ – a csűrőlapok szöghelyzet-változásának Laplace-transzformáltja;
– p(s) – az orsózó szögsebesség Laplace-transzformáltja;
– ϕ(s) – a dőlési szög Laplace-transzformáltja;
– K_ϕ – az UAV erősítési tényezője;
– s – Laplace-operátor (komplex frekvencia);
– $1/T_R$ – az orsózó mozgás időállandója;
–$1/T_S$ – a spirálmozgás időállandója;
– ω_D – a keresztirányú csillapítatlan lengésének (Holland-orsó) sajátfrekvenciája;
– ω_ϕ – az UAV komplex zérusának körfrekvenciája;
– ξ_D – a keresztirányú csillapítatlan lengésének (Holland-orsó) csillapítási tényezője;
– ξ_ϕ – az UAV komplex zérusának csillapítási tényezője;
– τ_{ep} – holtidő.

A (3.2) és a (3.3) átviteli függvények alapján megállapítható, hogy a dinamikus rendszer modellje negyedrendű és holtidős. Ha azonban teljesül a

$$\omega_\phi \cong \omega_{ph}; \xi_{\phi\cong}\xi_{ph} \qquad (3.4)$$

feltételrendszer, és a spirálmozgás időállandója nagyon nagy értékű az orsózó mozgás időállandójához képest, valamint az UAV kisértékű holtidővel bír, akkor a (3.2) és a (3.3) egyenletek az alábbi egyszerűbb alakban adhatók meg:

$$W_1(s) = \frac{p(s)}{\delta_A(s)} \cong \frac{sK_\phi}{(T_R s+1)}, \qquad (3.5)$$

vagy

$$W_2(s) = \frac{\phi(s)}{\delta_A(s)} \cong \frac{K_\phi}{(T_R s+1)}. \qquad (3.6)$$

Ha az UAV repülési paramétereit automatikus repülésszabályozó rendszer stabilizálja vagy változtatja előre megadott algoritmus szerint, akkor a zárt automatikus repülésszabályozó rendszer minőségi jellemzőire megfogalmazhatunk elvárásokat, amelyeket a zárt repülésszabályozó rendszernek teljesítenie kell.

Az UAV orsózó mozgását irányító zárt automatikus repülésszabályozó rendszer tranziens válaszfüggvényein számos minőségi jellemzőt definiálhatunk. Tekintettel a (3.5) és a (3.6) átviteli függvények alakjára, kínálkozik, hogy ez a minőségi jellemző legyen az orsózó szögsebesség időállandója. Számos esetben célszerű a megadott dőlési szög eléréshez szükséges időt is meghatározni mint minőségi jellemzőt.

A fenti megfontolások alapján, az UAV zárt repülésszabályozó rendszereinek tervezésekor az orsózó mozgás átmeneti függvényein értelmezett és figyelembe veendő minőségi jellemzőkre javaslatom a következő:

– T_{Rcl} – az UAV zárt automatikus repülésszabályozó rendszere csillapított lengéseinek időállandója;
– t_s – az UAV zárt automatikus repülésszabályozó rendszere csillapított lengéseinek tranziens (átmeneti) ideje;
– Δ – az UAV zárt automatikus repülésszabályozó rendszere csillapított lengéseinek dinamikus pontossága.

Az UAV zárt repülésszabályozó rendszereinek tervezésekor az orsózó mozgás felnyitott szabályozási körének frekvenciafüggvényein (Bode-diagram, Nyquist-diagram) értelmezett és figyelembe veendő minőségi jellemzőkre javaslatom a következő:

– G_m – az UAV felnyitott automatikus repülésszabályozó rendszerének erősítési tartaléka;
– ϕ_m – az UAV felnyitott automatikus repülésszabályozó rendszerének fázistartaléka.

A fent megadott minőségi jellemzők megfelelőek és elégségesek a zárt szabályozási rendszerek tervezéséhez, a megtervezett rendszerek stabilitás- és minőségvizsgálatához. A hatósági tanúsítások során a fenti paraméterek és jellemzők messzemenően elegendőek az UAV repülésszabályozó rendszer előírások megfelelésének megítéléséhez.

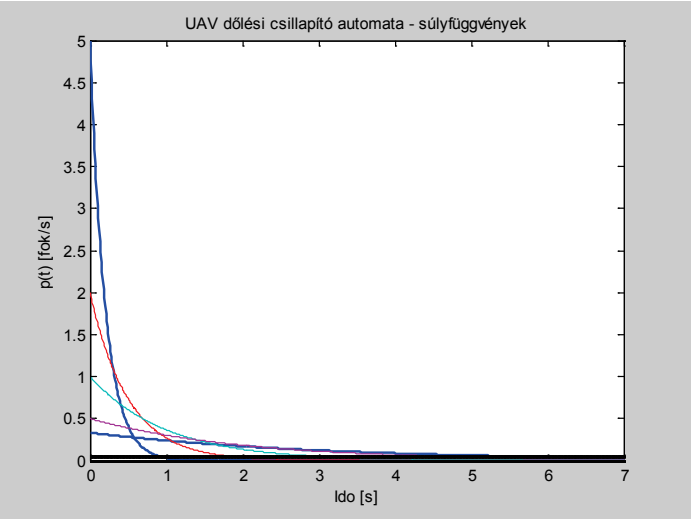
Az UAV zárt, dőlési csillapító automata rendszerének az orsózó szögsebesség referencia bemeneti jelére vonatkoztatott eredő átviteli függvénye legyen tehát a következő alakú:

$$W_{cl}(s) = \frac{p(s)}{p_{ref}(s)} = \frac{K_{cl}}{(T_{\mathrm{Rcl}} s+1)} \qquad (3.7)$$

ahol K_{cl} és T_{Rcl} implicit módon fejezi ki a nem irányított UAV és a repülésszabályozó rendszer paramétereinek kapcsolatát. A továbbiakban vizsgáljuk meg egy hipotetikus UAV tranziens viselkedését, az alábbi paraméterek mellett:

$$K_{cl}=1;\ 0{,}2\mathrm{s} \leq T_{Rcl} \leq 3s \qquad (3.8)$$

A (3.7) átviteli függvénnyel leírt dőlési csillapító automata időtartománybeli viselkedése a (3.8) adatok figyelembevételével az 1., a 2. és a 3. ábrákon látható.



$T_{R_{min}} = 0{,}2s$; $T_{R_{max}} = 3s$; $T_R = 0{,}5s$; $T_R = 1s$; $T_R = 2s$

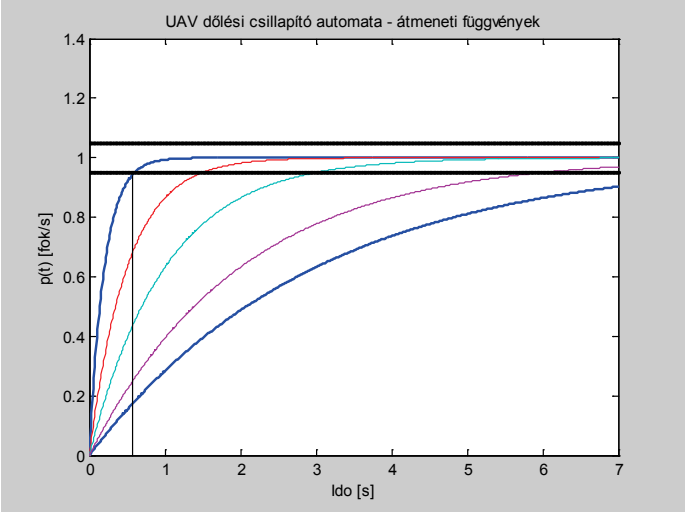
1. ábra: UAV dőlési csillapító automata súlyfüggvényei

Az 1. ábrán jól látható, hogy az UAV hossztengely körüli forgómozgásnak fontos minőségi jellemzője a T_{Rcl} időállandó, amely alapvetően befolyásolja a tranziens időt. A vizsgálatok során bemenetnek tekintett egységimpulzus dőlési szögsebesség inkább matematikai, mint fizikai jellegű: a gyakorlatban ilyen jelet előállítani nem lehetséges, csak közelíteni tudjuk a bemeneti jel idősorát. A válaszfüggvényt viszont nagyon jól használhatjuk az UAV zárt automatikus repülésszabályozó rendszerének stabilitásvizsgálata során is.

A 2. ábrán az UAV dőlési átmeneti függvényei a T_{Rcl} időállandó értékében paraméterezve láthatóak.

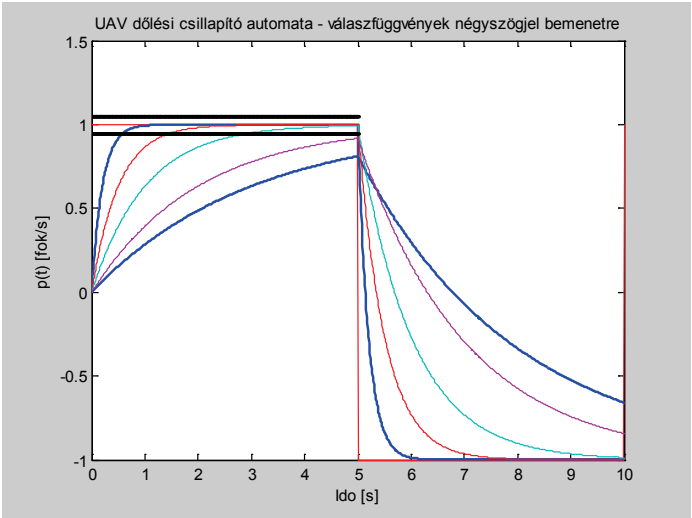
A 2. ábrán függőleges vonallal jelölve a Δ=±5% dinamikus pontosság mellett meghatározott tranziens idő, amely jelen esetben közel 0,5 s. A dinamikus pontosság jelen esetben átlagos, ±5% értékű. Igényes, pontos szabályozásokban, mint például precíziós navigációs feladatok megoldása, ez lehet kisebb értékű is. Mindazonáltal kisebb pontosságot igénylő, kevésbé igényes szabályozások esetén akár nagyobb is lehet az értéke, mint 5%.

A 3. ábrán az UAV előjelváltó négyszögjelre adott válaszfüggvényei láthatóak



$T_{R_{min}} = 0{,}2s$; $T_{R_{max}} = 3s$; $T_R = 0{,}5s$; $T_R = 1s$; $T_R = 2s$

2. ábra: UAV dőlési csillapító automata átmeneti függvényei



$T_{R_{min}} = 0{,}2s$; $T_{R_{max}} = 3s$; $T_R = 0{,}5s$; $T_R = 1s$; $T_R = 2s$

3. ábra: UAV dőlési csillapító automata válaszfüggvényei egységnyi, négyszögjel bemenetre

A 3. ábra alapján könnyen belátható, hogy nagy értékű T_{Rcl} időállandó esetén az UAV válaszjele nem éri el a kívánt dőlési szögsebesség értéket, így a megadott értékű dőlési szög létesítése is kérdésessé válik.

Az UAV legyezőmozgásának dinamikus repülési modellje és annak jellemzői

Az UAV legyezőmozgásának dinamikus viselkedését az alábbi reprezentatív átviteli függvényekkel adhatjuk meg [1] [3]:

$$W_3(s) = \frac{\beta(s)}{\delta_A(s)} = \frac{A_\beta(s+{}^1/_{T_{\beta_1}})(s+{}^1/_{T_{\beta_2}})(s+{}^1/_{T_{\beta_3}})e^{-\tau_{ep}s}}{(s^2+2\xi_D\omega_D s+\omega_D^2)(s+{}^1/_{T_S})(s+{}^1/_{T_R})}, \tag{3.9}$$

$$W_4(s) = \frac{\beta(s)}{\delta_R(s)} = \frac{A_\beta(s+{}^1/_{T_{\beta_1}})(s+{}^1/_{T_{\beta_2}})(s+{}^1/_{T_{\beta_3}})e^{-\tau_{ep}s}}{(s^2+2\xi_D\omega_D s+\omega_D^2)(s+{}^1/_{T_S})(s+{}^1/_{T_R})} \tag{3.10}$$

és

$$W_5(s) = \frac{r(s)}{\delta_R(s)} = \frac{A_\beta(s+{}^1/_{T_{\beta_1}})(s+{}^1/_{T_{\beta_2}})(s+{}^1/_{T_{\beta_3}})e^{-\tau_{ep}s}}{(s^2+2\xi_D\omega_D s+\omega_D^2)(s+{}^1/_{T_S})(s+{}^1/_{T_R})}, \tag{3.11}$$

ahol:

– $\delta_R(s)$ – az oldalkormány szöghelyzet-változásának Laplace-transzformáltja;
– $\delta_A(s)$ – a csűrőlapok szöghelyzet-változásának Laplace-transzformáltja;
– $r(s)$ – legyező szögsebesség Laplace-transzformáltja;
– β(s) – a legyezőszög (keresztirányú lineáris sebesség) Laplace-transzformáltja;
– A_β – az UAV erősítési tényezője;
– s – Laplace-operátor (komplex frekvencia);
– $1/T_R$ – az orsózó mozgás időállandója;
– $1/T_S$ – a spirálmozgás időállandója;
– ω_D – a keresztirányú csillapítatlan lengésének (Holland-orsó) sajátfrekvenciája;
– ξ_D – a keresztirányú csillapítatlan lengésének (Holland-orsó) csillapítási tényezője;
– T_{β_1}; T_{β_2}; T_{β_3} – transzmissziós zérusok időállandói;
– τ_{ep} – holtidő.

A (3.9)–(3.11) átviteli függvények negyedrendű, három transzmissziós zérussal bíró és általános esetben holtidős dinamikus rendszert írnak le, függetlenül a bemenet jellegétől. A gyakorlatban sokszor eltekintünk a holtidőtől, és a (3.9)–(3.11) átviteli függvények zérusai és valós pólusai kiejtik egymást, ezért a (3.9) és (3.11) egyenletekkel megadott átviteli függvények holtidőmentes esetre az alábbi közelítő alakban is felírhatóak:

$$W_3(s) \cong \frac{\beta(s)}{\delta_A(s)} = \frac{A_\beta(s+{}^1/_{T_\beta})}{(s^2+2\xi_D\omega_D s+\omega_D^2)}, \tag{3.12}$$

$$W_4(s) \cong \frac{\beta(s)}{\delta_R(s)} = \frac{A_\beta(s+{}^1/_{T_\beta})}{(s^2+2\xi_D\omega_D s+\omega_D^2)}. \tag{3.13}$$

$$W_5(s) \cong \frac{r(s)}{\delta_R(s)} = \frac{A_\beta(s+{}^1/_{T_\beta})}{(s^2+2\xi_D\omega_D s+\omega_D^2)}. \tag{3.14}$$

A (3.12)–(3.14) modellek meghatározása lényeges, mert az UAV identifikációja során meg kell adnunk, hogy egyváltozós (átviteli függvény) vagy többváltozós (állapotteres modell) modellben gondolkodunk, az lineáris vagy nemlineáris, tartalmaz-e holtidőt az identifikálandó modell vagy sem.

Az oldalirányú mozgást irányító zárt automatikus repülésszabályozó rendszer tranziens válaszfüggvényein számos minőségi jellemzőt definiálhatunk. Általában többhurkú repülésszabályozó rendszert építenek az UAV-k fedélzetére. Az első visszacsatolás szögsebesség szerint valósul meg, és ezt a hurkot bólintó csillapító automatának szokás nevezni [1] [3].

Az UAV zárt repülésszabályozó rendszereinek tervezésekor az oldalirányú mozgás átmeneti függvényein értelmezett és figyelembe veendő minőségi jellemzőkre javaslatom a következő:

– ξ_{cl} – az UAV zárt automatikus repülésszabályozó rendszere csillapított lengéseinek csillapítási tényezője;
– σ_{cl} – az UAV zárt automatikus repülésszabályozó rendszere csillapított lengéseinek túlszabályozása;
– t_p – az UAV zárt automatikus repülésszabályozó rendszere csillapított lengéseinek csúcsideje;
– t_s – az UAV zárt automatikus repülésszabályozó rendszere csillapított lengéseinek tranziens ideje;
– Δ – az UAV zárt automatikus repülésszabályozó rendszere csillapított lengéseinek dinamikus pontossága.

Az UAV zárt repülésszabályozó rendszereinek tervezésekor tervezési kritérium lehet a zárt repülésszabályozó rendszer pólusainak és zérusainak értéke, illetve helye a komplex síkon. E minőségi előírások szolgálnak alapul domináns póluspárra történő tervezés során is [1] [3]:

– p_i – az UAV zárt automatikus repülésszabályozó rendszer pólusai;
– z_i– az UAV zárt automatikus repülésszabályozó rendszer zérusai.

Az UAV zárt repülésszabályozó rendszereinek tervezésekor a hosszirányú mozgás felnyitott szabályozási körének frekvenciafüggvényein (Bode-diagram, Nyquist-diagram) értelmezett és figyelembe veendő minőségi jellemzőkre javaslatom a következő:

– G_m– az UAV felnyitott automatikus repülésszabályozó rendszerének erősítési tartaléka;
– ϕ_m– az UAV felnyitott automatikus repülésszabályozó rendszerének fázistartaléka.

A fent megadott minőségi jellemzők megfelelőek és elégségesek a zárt szabályozási rendszerek tervezéséhez, a megtervezett rendszere stabilitás- és minőségvizsgálatához. A hatósági tanúsítások során a fenti paraméterek és jellemzők messzemenően elegendőek az UAV repülésszabályozó rendszer előírásoknak megfelelése megítéléséhez.

Az UAV zárt, legyezőcsillapító automata rendszerének referencia bemeneti jelre vonatkoztatott eredő átviteli függvénye legyen a következő alakú:

$$W_{cl}(s) = \frac{r(s)}{r_{ref}(s)} \cong \frac{\omega_{cl}^2}{(s^2+2\xi_{scl}\omega_{cl}s+\omega_{cl}^2)} \qquad (3.15)$$

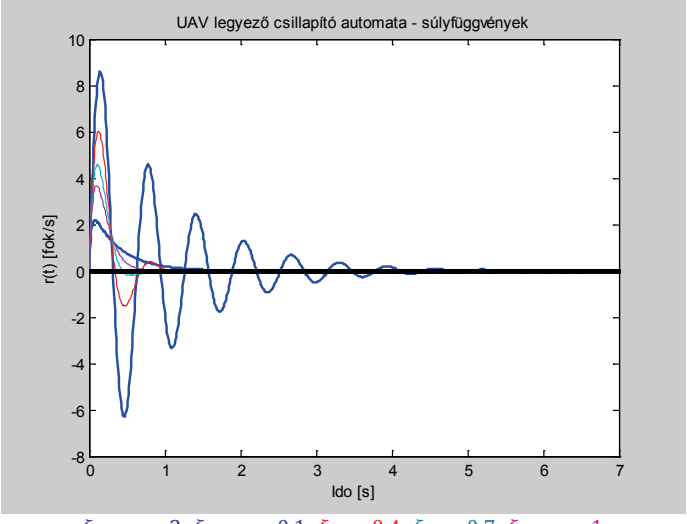
ahol ω_{cl} és ξ_{cl} implicit módon fejezi ki a nem irányított UAV repülésdinamikai jellemzőinek és a repülésszabályozó rendszer paramétereinek kapcsolatát.

A (3.15) átviteli függvény nevezője a zárt automatikus repülésszabályozó rendszer egy domináns póluspárjának modellje. Feltételezzük, hogy tetszőleges bonyolultságú UAV repülésszabályozó rendszer esetén is tudunk olyan szabályozót tervezni, ami a zárt szabályozó rendszer karakterisztikus egyenletének gyökeit úgy helyezi el a komplex síkon, hogy a függőleges tengelyhez legközelebb egy komplex konjugált, más néven domináns póluspár helyezkedik el. A zárt repülésszabályozó rendszer karakterisztikus egyenletének többi gyöke ettől a póluspártól nagy távolságra, balra helyezkedik el a komplex síkon. Ennek megfelelően, az UAV zárt repülésszabályozó rendszer dinamikáját a domináns póluspár határozza meg, a többi gyök érdemben nem befolyásolja a zárt szabályozás dinamikáját. E szabályozótervezés megvalósítását a MATLAB Control System Toolbox programjának *acker.m* és a *place.m* segédfüggvényei is támogatják. [3]

A továbbiakban vizsgáljuk meg egy hipotetikus UAV tranziens viselkedését, az alábbi paraméterek mellett:

$$\omega_{cl}=10 \text{ rad/s}, \quad 0{,}1 \leq \xi_{cl} \leq 2 \qquad (3.7)$$

Az UAV legyezőcsillapító automata tranziens analízisének eredményeit a 4., 5. és a 6. ábrák mutatják be.

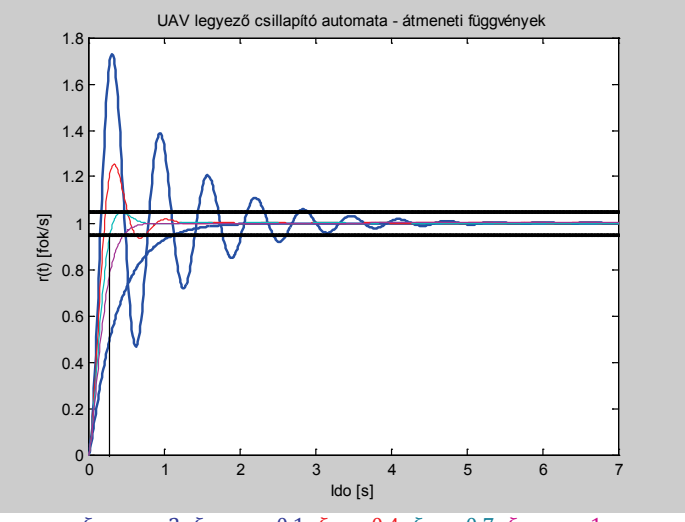


$\xi_{clmax} = 2$; $\xi_{clmin} = 0{,}1$; $\xi_{cl} = 0{,}4$; $\xi_{cl} = 0{,}7$; $\xi_{clkrit} = 1$

4. ábra: UAV legyezőcsillapító automata súlyfüggvényei

A 4. ábrán jól látható, hogy az UAV függőleges tengely körüli legyezőmozgása az erősen lengőtől az aperiodikus viselkedésig terjed, mindeközben a minőségi jellemzők is széles határok között változnak. A vizsgálatok során bemenetnek tekintett, egységimpulzus jelleggel viselkedő legyező szögsebesség inkább matematikai, mint fizikai jellegű. A számítógépes szimuláció eredményeként kapott válaszfüggvényeket jól használhatjuk az UAV zárt automatikus repülésszabályozó rendszerének stabilitásvizsgálata során.

Az 5. ábrán bemutatott átmeneti függvények Δ=±5% dinamikus pontosság mellett mutatják az UAV zárt repülésszabályozó rendszerének tranziens viselkedését. A leggyorsabb tranziens folyamat a ξ_{cl}=0,7 csillapítási tényezővel bíró zárt UAV repülésszabályozó rendszer. Könnyű belátni, hogy a dinamikus pontosság értékének csökkentésével igényesebb, pontosabb szabályozást kapunk, míg a dinamikus pontosság növelése kevésbé igényes, kevésbé pontos szabályozást jelent a gyakorlatban. Az UAV repülésszabályozó rendszerei egyes üzemmódjain az is előfordulhat, hogy más és más dinamikus pontossággal kell számolnunk.

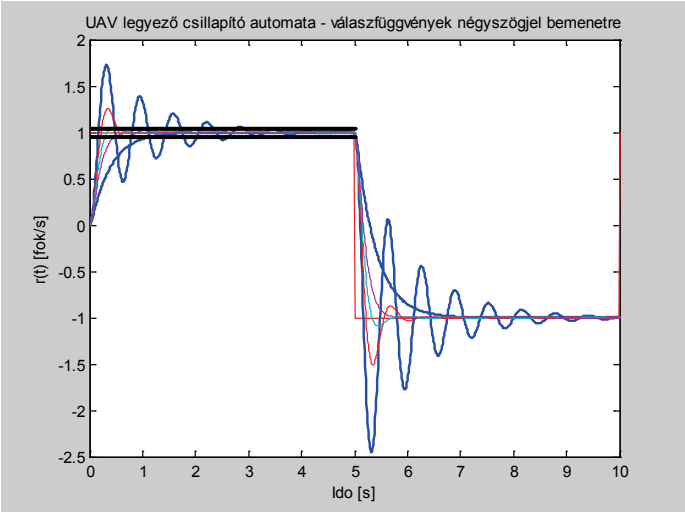


$\xi_{clmax} = 2$; $\xi_{clmin} = 0{,}1$; $\xi_{cl} = 0{,}4$; $\xi_{cl} = 0{,}7$; $\xi_{clkrit} = 1$

5. ábra: UAV legyező csillapító automata átmeneti függvényei

A 6. ábrán az UAV legyezőcsillapító automata előjelváltó, egységnyi amplitúdójú négyszögjel bemenetre adott és a zárt szabályozási rendszer ξ_{cl} csillapítási tényezőjében paraméterezett időfüggvényeket láthatjuk.

A 6. ábrán jól látható, hogy az egyes egységnyi bemenetekre az UAV csillapító automata lengő vagy aperiodikus válaszfüggvényekkel válaszol. Az előjelváltáskor az UAV gyorsan átáll az ellentétes előjelű válaszfüggvényre. A csillapítási tényező minimális és maximális értékei között számos más csillapítási tényező érték is választható, amely érdemben befolyásolja a dinamikus viszonyokat.



$\xi_{clmax} = 2$; $\xi_{clmin} = 0{,}1$; $\xi_{cl} = 0{,}4$; $\xi_{cl} = 0{,}7$; $\xi_{clkrit} = 1$

6. ábra: UAV legyező csillapító automata válaszfüggvényei az előjelváltó bemeneti négyszögjel bemenetre

Összegzés, eredmények, következtetések

A cikkben a szerző bemutatta az UAV típus- és légi alkalmassági megfelelés mérése során alkalmazható hazai és nemzetközi szabályozókat. A szerző igazolta, hogy a hazai jogszabályi környezet meglehetősen hiányos e tekintetben, míg a nemzetközi környezet alapvetően az UAV elkülönített légterű, katonai alkalmazásaival foglalkozik. E területen is az UAV fedélzeti automatikus repülésszabályozó rendszere alkalmazásának kérdésköre meglehetősen hiányos követelményrendszerrel bír, így a hazai jogalkotóknak még a jogszabályok, szabványok átvétele sem jelent megoldást, hiszen jelenleg csak töredékes és hiányos szabályozás áll rendelkezésre. A szerző bemutatta azokat a dinamikus modelleket, amelyek segítségével az UAV oldalirányú térbeli mozgása leírható. Az UAV típus- és légi alkalmassági tanúsítása során a szerző javasolja az egyváltozós, átviteli függvényekkel megadott, holtidőmentes modell alkalmazását. Megemlíteni szükséges azonban, hogy a gyakorlatban a MATLAB System Identification Toolbox programja úgy a lineáris (egyváltozós, átviteli függvénnyel adott; többváltozós, állapotegyenlettel adott), mint a nemlineáris rendszerdinamikai modell identifikációját képes végrehajtani.

A szerző összefoglalta a zárt automatikus repülésszabályozó rendszerek minőségi jellemzőit, bemutatta azok sokszínűségét. E minőségi jellemzők halmazából a szerző összeállította azon minőségi jellemzők körét, amely alkalmas lehet egy adott UAV-típus hatósági tanúsítása során a megfelelés értékelésére.

A szerző javasolta, hogy az egyes esetekben a minőségi jellemzőket (pl. csillapítási tényező) egyenlőtlenségi korlátozással adjuk meg, és hagyjunk tág teret a legkisebb és a legnagyobb megengedett értékekre, hiszen a fedélzeten az egyes tranziens folyamatok élettani hatásai nem relevánsak. Az alulcsillapított UAV csillapító automaták tervezésekor azonban figyelembe kell venni a sárkányszerkezet kritikus pontjainak (pl. szárnyak bekötési helye, kormányfelületek bekötési pontja) terhelhetőségét is. Nyilvánvaló, hogy a lengő rendszerek esetében az alulcsillapítás azt is jelenti, hogy az UAV élettartama csökken, földi és légi üzemeltetése nagyobb odafigyelést követel.

Irodalomjegyzék

1. McLean, D.: Automatic Flight Control Systems. Prentice-Hall International Ltd., New York–London–Toronto–Sydney–Tokyo–Singapore, 1990.
2. NATO STANAG 4671 Unmanned Aerial Vehicles Systems Airworthiness Requirements (USAR), NSA/0976(2009)-JAIS/4671, 2009.
3. Szabolcsi R.: Modern automatikus repülésszabályozó rendszerek. ISBN 978-963-7060-328, p. 415, Zrínyi Miklós Nemzetvédelmi Egyetem, 2011.
4. Szabolcsi R.: UAV és UAS rendszerek légialkalmassági tanúsítása: barát vagy ellenség?! Műszaki Tudomány az Észak-kelet Magyarországi Régióban 2013 tudományos konferencia kiadványa. Elektronikus műszaki füzetek, XIII, ISBN 978-963-7064-30-2, pp. 1–10., MTA Debreceni Akadémiai Bizottság, 2013.
5. Szabolcsi R.: Pilóta nélküli légijármű rendszerek légialkalmassági jellemzői és a légialkalmassági tanúsítás követelményei. Szolnoki Tudományos Közlemények, XII. évf., 1. szám, ISSN 1419-256X (2060-3002), pp. 64–75., 2013.
6. Szabolcsi R.: TUAV automatikus repülésszabályozó rendszer típus- és légialkalmassági tanúsítása. Hadmérnök, 2013/4. szám, p. 26–32., http://www.hadmernok.hu/134_03_szabolcsir.pdf
7. http://ec.europa.eu/transport/modes/air/doc/com(2014)207_en.pdf (letöltve: 2014. május 9.)

Criteria for the compliance of the UAV automatic flight control system with type and airworthiness certification – lateral/directional motion

Szabolcsi Róbert

The purpose of the author is to derive a new set of dynamic performances for the lateral/directional motion of the UAV's spatial motion that could be applied to measure and test the type and airworthiness of the UAV. Due to the missing or not properly defined flying qualities of UAVs, the importance of this article is undoubted. The article will fill the gap in the regulations, and its results are recommended for consideration to experts and authority staff in their work to measure the compliance of the UAV flying characteristics.

Keywords: UAV, UAS, lateral/directional motion, UAV autopilot, UAV automatic flight control, UAV certification

Solymosi Máté

Tehetséggondozás a katonai műszaki tudományokban

Cikkemben bemutatom a *Somos Alapítvány a védelmi és biztonsági oktatásért és kutatásért* tevékenységét a katonai műszaki tudományok tehetséggondozása területén. Ismertetem az alapítvány által alapított díjakat, amelyek ösztönözték a hazai tehetségeket kiemelkedő teljesítményeik elérésében a BSc, MSc és PhD-képzésben, és egy közel sem teljes felsorolást magukról a díjazottakról. Továbbá bemutatom az ELTE Eötvös Kiadóval közösen kiadott szakkönyveket.
Kulcsszavak: oktatás, tehetséggondozás, alapítvány, szakkönyvek kiadása

Bevezetés

A *Somos Alapítvány a védelmi és biztonsági oktatásért és kutatásért* közhasznú szervezetet (a továbbiakban: alapítvány) 1998. április 27-én alapította Dr. Solymosi József. Az alapítvány célja az oktatási és a tudományos érdeklődés felkeltése, illetve a műveltségi, az oktatási és a tudományos színvonal fejlesztése a nemzet-, a környezet-, munkavédelem és -biztonság, azaz összefoglalóan a biztonságvédelem szakterületei iránt.

Az alapítvány cél szerinti közhasznú tevékenysége, hogy a megcélzott szakterületeken elősegítse Magyarország euroatlanti integrációját oly módon, hogy kutatási-oktatási programokat szervez (melyek során felnőtt- és egyéb oktatást, ismeretterjesztést, természettudományi műszaki, társadalomtudományi, humán kutatást, fejlesztést végez, műszaki vizsgálatokat, elemzéseket készít), illetve azokat előmozdítja. [1]

Az alapítvány a céljával egyező területeken díjak alapításával, könyvek kiadásával támogatja a tudományos kutatásokat és a hazai kutatás-fejlesztést. Az alapítvány a katonai műszaki tudományok területén elsősorban a következő tudományos területeket támogatja: nukleáris biztonság, radiokémia és sugárvédelem és a katasztrófavédelem.

A hazai tehetségek támogatására alapított díjak:

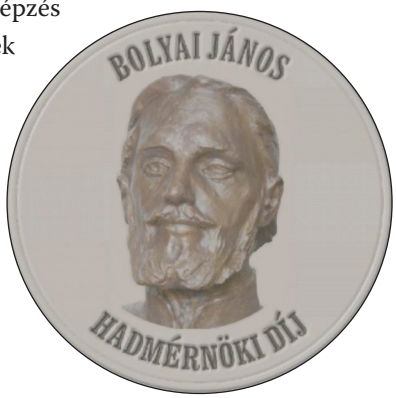
- Bolyai János Hadmérnöki Díj;
- Hevesy György-díj a Nukleáris Biztonságért;
- Sugárvédelmi Nívódíj;
- Katasztrófavédelmi díj.

Az alapítvány támogatásában az alábbi könyvek jelentek meg:

- Sugárvédelem (2010)
- Prométheusz magyar unokái (2013)
- Atomrektorok biztonsága (2013)

Bolyai János Hadmérnöki Díj

Az alapítvány, együttműködésben a Nemzeti Közszolgálati Egyetem jogelőd intézményével, a Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Karával (2010-től Bolyai János Hadmérnöki Karával; a továbbiakban: ZMNE BJHMK) a két fél közérdekű kötelezettségvállalása alapján a hadmérnöki képzés és kutatások területén elért, kiemelkedő eredmények méltó elismerésére díjat alapított *„Bolyai János Hadmérnöki Díj"* elnevezéssel 2008-ban. A Bolyai János Hadmérnöki Díj *kilenc kategóriában ítélhető oda,* kizárólag magyar adóazonosító jellel rendelkező, a ZMNE BJKMK-n jelesre végzett hallgatóknak és a Katonai Műszaki Doktori Iskolában (a továbbiakban KDMI) Katonai műszaki tudományok tudományágban summa cum laude végzett doktoroknak.



1. kép: Bolyai János Hadmérnöki díj, bronzplakett [2]

- Arany fokozat: PhD Doktori I. Díj és Különdíj
- Ezüst fokozat: Diplomás I. Díj és Különdíj
- Bronz fokozat: PhD hallgatói TDK I. Díj és Különdíj
- Bronz fokozat: hallgatói TDK I. Díj és Különdíj
- IX. Kategória: Gyémánt fokozat: Témavezetői/Konzulensi Díj.

A díjazottaknak valamennyi kategóriában bronzplakett és emlékérem jár, továbbá *az I.–VIII. kategóriához pénzjutalom.* amelyet az alapítvány mint kifizető ad, illetve utal át a díjazottnak, aki azt oktatási intézményekben folytatott tanulmányokra, kutatásra vagy külföldi tanulmányútra köteles fordítani. A díj egyes kategóriáihoz tartozó pénzjutalom összege *100 000–300 000 Ft*-ig terjedt. [3] Sajnálatos módon a díj a ZMNE átalakulása miatt 2011-ben megszűnt.

A díj fennállása alatt *mintegy 40 fő részesült díjazásban,* illetve témavezetői díjban. *Díjazottjaink* (a teljesség igénye nélkül): Földi Ferenc mk. ezredes, Zelenák János mk. ez-

redes, Németh András mk. főhadnagy, Hegedűs Ernő mk. százados, Miskey Tamás tü. őrnagy, Petőfi Gábor, Nagy Gábor.

Témavezetői díjban részesültek többek között: Dr. Ungvár Gyula, Prof. Dr. Turcsányi Károly, Prof. Dr. Kovács László, Dr. habil. Rajnai Zoltán, Dr. habil. Cziva Oszkár, Dr. Seres György, Dr. Földi László, Prof. Dr. Halász László, Dr. Ványa László, Dr. habil. Vincze Árpád. [3] [4] [5]

Hevesy György-díj a Nukleáris Biztonságért

A Magyar Tudományos Akadémia, az MVM Paksi Atomerőmű Zártkörűen Működő Részvénytársaság és a Somos Alapítvány a nukleáris biztonság területén folyó kutatások kiemelkedő eredményeinek méltó elismerésére *Hevesy György-díj a nukleáris biztonságért* elnevezéssel díjat alapított *2006-ban.*

A díjat két kategóriában ítélik oda. *A díj az I. kategóriában odaítélhető* annak a magyar állampolgárságú személynek, aki Magyarországon, illetve Magyarország érdekében alkotásaival a nukleáris biztonság területén legalább húsz éve tevékenykedve kimagasló eredményt ért el. *A díj a II. kategóriában* annak a legfeljebb 35 éves magyar személynek adományozható, aki a nukleáris biztonság témakörében, magyar nyelven készítette vagy készíti PhD-dolgozatát. A Somos Alapítvány pénzdíjban részesíti a díjazottakat.

Díjazottak, akik a katonai műszaki tudományokban szereztek kiemelkedő érdemeket:

I. kategóriában a díjazottjaink (a teljesség igénye nélkül): Rónaky József, Cserháti András, Gadó János, Fehér István, Gimesi Ottó, Vajda Nóra, Deme Sándor.

II. kategóriában a díjazottjaink: Horváth Kristóf. [3]

Sugárvédelmi Nívódíj

A Somos Alapítvány az Eötvös Loránd Fizikai Társulat (ELFT) Sugárvédelmi Szakcsoportjával együttműködésben a sugárvédelem területén folyó kutatások kiemelkedő eredményeinek méltó elismerésére *ösztöndíjat* alapított *Sugárvédelmi Nívódíj* (továbbiakban: nívódíj) elnevezéssel. A nívódíjak idén kerülnek hetedik alkalommal átadásra a XXXIX. Sugárvédelmi Továbbképző Tanfolyamon Hajdúszoboszlón. [6]

A Nnívódíj három kategóriában kerül kiosztásra. Azoknak a kutatóknak adományozható, akik a sugárvédelem szakterületén végzett kutatásaikkal kimagasló eredményt értek el, továbbá az eredeti, új tudományos eredményt az adott formában *első alkalommal adják közre,* és tudományos közlemény kéziratként benyújtják. A kutatók a benyújtott pályázatokat az ELFT Sugárvédelmi Szakcsoportjának a szervezésében évente zajló *„Sugárvédelmi Továbbképző Tanfolyam*" elnevezésű konferencián, nyilvános előadás keretében

ismertetik. A konferencia résztvevőinek a díj odaítélésről – a konferencia résztvevőinek a közönség szavazatát is figyelembe véve – Sszakértői Kkuratórium dönt.

I. Általános kategória: magyar állampolgárságú kutatóknak adományozható.

II. Ifjúsági kategória: az általános kategóriában nem díjazott magyar állampolgár kutatóknak adományozható, akik a konferencia kezdő napjáig még nem töltötték be a 35. életévüket.

III. Különdíj kategória (Általános és Ifjúsági).

Díjazottak, akik a katonai műszaki tudományokban szereztek kiemelkedő érdemeket: Dr. Eigemann Gábor, Dr. Nagy Gábor, Molnár Kolos. [6]

Katasztrófavédelmi díj

A Magyar Tudományos Akadémia elnöke, a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság főigazgatója, a Nemzeti Közszolgálati rektora, valamint a Somos Alapítvány kötelezettségvállalása alapján, az iparbiztonság, a polgári védelem és a tűzvédelem mint a katasztrófavédelem kiemelten fontos területén elért hazai eredmények méltó elismerésére díjat alapított *Katasztrófavédelmi díj* elnevezéssel.

A Katasztrófavédelmi díjról, annak az immáron két éves eredményes működéséről Dr. Kátai Urbán Lajos tű. alezredes, az NKE Katasztrófavédelmi Intézet egyetemi docense – mint a szervezői munka kimagasló egyénisége – egy másik cikkben számol be, így az jelen cikkben nem kerül részletezésre. [7]

Sugárvédelem, 2010

„A könyv áttekintést ad az ionizáló sugárzások elleni védelem legfontosabb elméleti kérdéseiről és gyakorlati módszereiről, eredményeiről. Tárgyalja a tudományszak fejlődését, a sugárvédelem dozimetriai alapjait, az ionizáló sugárzás emberre gyakorolt károsító hatását, a külső és belső sugárterhelés mechanizmusát, az ellenük való védekezés módszereit. Külön fejezetek foglalkoznak a sugárvédelmi szabályozással, a radioaktív anyagok biztonsági kérdéseivel és szállításuk szabályozásával, továbbá a radioaktív hulladék kezelésének és elhelyezésének kérdéseivel. A sugárvédelmi ellenőrzési módszereket, így a személyi dozimetriai, a

2. kép: Sugárvédelem (2010) [8]

munkahelyi ellenőrzési és a nukleáris környezet-ellenőrzési módszereket feldolgozó fejezetek mellett a sugárvédelmi metrológiai követelményeket bemutató rész is kimerítő ismeretanyagot nyújt az olvasónak. A lakosság különböző forrásokból származó sugárterhelése és a nukleárisbaleset-elhárítás kérdései zárják az általános ismeretek anyagát. Az utolsó fejezet, az előzőekben leírtak alkalmazási példájaként, áttekinti a paksi atomerőmű sugárvédelmi rendszerét." – mutatja be a könyvet rendkívül szemléletesen az ELTE Eötvös Kiadó saját honlapján. [9][10]

Prométheusz magyar unokái, 2013

A könyv Maróthy László szerkesztésében, az ELTE Eötvös Kiadó kiadásában 2013-ban, a Paksi I. blokk indulásának 30. évfordulójára jelent meg. A 20. század egyik legnagyobb magyarországi beruházását, a Paksi Atomerőmű megépítése mutatja be: hogy miben tért el a hazánkban korábban létesült erőművek építéséhez képest, mik voltak a felmerülő akadályok és milyen feladatokkal kell manapság az üzemeltetőknek és háttérintézményeinek szembesülniük. [11]

3. kép: Prométheusz magyar unokái (2013) [12]

Atomreaktorok biztonsága, 2013

A könyv hazai szerzői a világon elsőként adták közre egyetlen könyvben összefogottan ezt a komplex tudásanyagot. Az elméleti kérdések mellett a könyv betekintést nyújt abba a folyamatba, hogy miként kezelik a szakemberek a gyakorlatban az atomerőművek, atomreaktorok biztonsági kérdéseit. Aktualitása és egyben a fontossága mindenképpen elismerésre méltó, hiszen hazánkban a villamosenergia-termelés több mint 40%-át az MVM Paksi Atomerőmű Zrt. szolgáltatja, folyamatosan garantálva az ellátás biztonságát. Ugyanakkor napjainkban elengedhetetlenné vált az energiaellátás növelése, amelynek egyik fontos és környezetbarát módja lehet a Paksi Atomerőmű bővítése a jelenleg tervezett két új blokk építésével. A bővítéshez is tudást meríthetnek a könyvből a fiatal szakemberek, de az adott szakterületen tanuló egyetemi hallgatók, oktatók és dolgozók is. [14]

Az alapítvány által alapított díjak keretében kiosztott összeg *meghaladja a 15 millió forintot.*

Hevesy György-díj: a díjak eddigi összege mintegy 10 millió forint.

Hevesy György Ifjúsági Nívódíj: a díjak eddigi összege mintegy 750 ezer forint.

4. kép: Atomreaktorok biztonsága I–II. (2013) [14]

Bolyai János Hadmérnöki Díj: a díjak eddigi összege mintegy 1 millió 500 ezer forint.
Sugárvédelmi Nívódíj: a díjak eddigi összege mintegy 800 ezer forint.
Pro Patria et Scientia díj: a díjak eddigi összege mintegy 2 millió 250 ezer forint.

Összefoglalás

Az alapítvány továbbra is küldetésének tekinti a tehetséggondozást, és a jövőben is folytatni kívánja ezt, a hazai szakembereket ösztönző díjak fenntartásával, esetlegesen új díjak alapításával és további szakkönyvek kiadásával.

„A tehetség egy különleges természeti kincs, a világ fejlett államainak legfontosabb alapanyaga, és hazánk ebben egyedülállóan gazdag. Ez egy olyan kincs, ami csak akkor ér valamit, ha felfedezik, hasznosítják és gyarapítják." – emelte ki a Talentum Díj 2010. évi díjátadó nyitóbeszédében Pálinkás József, az MTA elnöke. [15]

Irodalomjegyzék

[1] Az Alapítvány bejegyzése és tevékenysége, http://www.sugarvedelem.hu/referenciak.htm (letöltve: 2014. 02. 25.)
[2] http://www.zmne.hu/ETDT/XXIXOTDK/DOCS/Bolyai_Dij_alapito.pdf (letöltve: 2014. 02. 14.)
[3] Solymosi J. – Borszuk V. – Pintér I. – Vincze Á.: A Somos Alapítvány a védelmi és biztonsági oktatásért és kutatásért közhasznú tevékenység a sugárvédelem érdekében. Előadás, ELFT XXXVII. Sugárvédelmi Továbbképző

Tanfolyam, Hajdúszoboszló, 2012. április 24–26. http://www.sugarvedelem.hu/sugarvedelem/docs/kulonsz/2012sv/Pinter_Istvan_a%20vedelmi%20%C3%A9s%20biztonsagi.pdf (letöltve: 2014. 02. 25.)
[4] Az alapítvánnyal és díjaival kapcsolatos 2011-es hírek oldala, http://www.sugarvedelem.hu/index2011.htm (letöltve: 2014. 02. 25.)
[5] 2003–2010 között az alapítvány által díjazásban részesült személyek listája, http://www.sugarvedelem.hu/dijak.htm (letöltve: 2014. 02. 25.)
[6] *Atomerőmű*, XXXVI. évfolyam 5. szám, 2013. május, 5. oldal, http://www.atomeromu.hu/download/10387/2013.%20m%C3%A1jus.pdf (letöltve: 2014. 02. 25.)
[7] http://www.vedelem.hu/letoltes/tanulmany/tan483.pdf (letöltve: 2014. 02. 25.)
[8] 2. kép: [9] felhasznált irodalom borítója
[9] Sugárvédelem: Szerkesztette: Fehér István, Deme Sándor (2010)
[10] Rövid ismertető a Sugárvédelem könyv tartalmáról, http://eotvospontok.hu/termeszettudomany/sugarvedelem (letöltve: 2014. 02. 25.)
[11] Maróthy László (szerk.): Prométheusz magyar unokái. Dr. Aszódi Attila, Bajsz József, Bilecz Ferenc, Budy Gábor, Cserhát András, Dr. Elter József, Kiss István, Lovass Gyula, Ördögh József, Dr. Szatmáry Zoltán, Dr. Trampus Péter, Láczai Szabó Tibor (2013)
[12] 3. kép: [11] felhasznált irodalom borítója
[13] 4. kép: [14] felhasznált irodalom borítója
[14] Elter József – Gadó János – Holló Előd – Lux Iván: Atomreaktorok biztonsága I–II., (013
[15] MTA hírei 2010. 02. 15.: A tehetség a legfontosabb természeti kincs, http://mta.hu/mta_hi rei/a-tehetseg-a-legfontosabb-termeszeti-kincs-91421/ (Letöltve: 2014. 02. 25.)

Talent management in Military Engineering

Solymosi Máté

In the article I would like to give an overview of the Somos Foundation's activity. The Foundation is carrying out an exemplary work managing talent in the military engineering sciences and in the defence and security education and research. I present the scholarships founded by the Foundation, which have motivated Hungarian talents to reach their BSc, MSc and PhD degrees and I also provide an incomplete list of the awardees. In addition, I give a short description of the specialized textbooks published in cooperation with Eötvös Publishing House, ELTE.

Keywords: Education, talent management, foundation, edition of handbooks

Bognár Balázs
Kátai-Urbán Lajos
Vass Gyula

A létfontosságú rendszerek és létesítmények védelméről szóló szabályozás végrehajtása Magyarországon

Magyarországon az új katasztrófavédelmi szabályozás 2012. évi bevezetésével egyedülálló iparbiztonsági hatósági és felügyeleti rendszer létesült nemzeti, területi és helyi szinten. A jelen cikk bemutatja a létfontosságú rendszerek és létesítmények azonosításával, kijelölésével, védelmével kapcsolatos hazai szabályozás végrehajtásának helyzetét és tapasztalatait.

Kulcsszavak: iparbiztonság, létfontosságú rendszerek és létesítmények védelme, katasztrófavédelem, Magyarország

1. Az európai jogi szabályozás megalkotása

Napjainkban különösen fontos és komplex feladatot jelent a lakosság és a környezet magas szintű védelmének biztosítása. Az iparbiztonság négy szakterületet foglal magába, így a veszélyes üzemek felügyeletét, a veszélyesáru-szállítmányok ellenőrzését, a létfontosságú rendszerekkel és létesítményekkel, valamint a nukleáris baleset-elhárítással kapcsolatos katasztrófavédelmi feladatok végrehajtását. [1] [2]

A kritikus infrastruktúra védelmére (Critical Infrastructure Protection, CIP) vonatkozó uniós jogi háttér első, jelentős mérföldkövének tekinthetjük az Európai Tanács 2004 decemberében elfogadott dokumentumát, a Létfontosságú Infrastruktúrák Európai Programjának (European Programme for Critical Infrastructure Protection – EPCIP) kialakítására vonatkozó előterjesztést. Ezt követően 2005 novemberében az Európai Bizottság kiadta az ún. létfontosságú infrastruktúrák védelmére vonatkozó európai programról szóló Zöld Könyvét, amely a későbbi jogi szabályozás alapjának tekinthető alapvető definíciókat, megállapításokat, folyamatokat és eljárásrendeket rögzítette. [3]

Ezt követően megszületett az uniós jogi szabályozás is az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről: a 2008/114/EK irányelv (továbbiakban: irányelv). A bizottság az irányelvet főként a Zöld Könyv alapján, az ágazati specifikumok figyelembevételével és az EU hosszú távú politikai célkitűzéseivel összhangban alkotta meg. Az irányelv mellett kiadtak egy

„nem kötelező iránymutatást", amely a tagállami feladatok részletes levezetésével törekszik megkönnyíteni a megvalósítást.

Az irányelv alapvető rendelkezése, hogy a kihirdetéstől számított két éven belül a megvalósításhoz szükséges intézkedéseket a tagállamoknak végre kell hajtaniuk. A tagállamok évente készítenek jelentést az ágazatonkénti, európainak kijelölt infrastruktúraelemek mennyiségéről; valamint kétévente küldenek általános adatokat tartalmazó összefoglaló jelentést a kritikus infrastruktúrák védelme érdekében tett intézkedéseikről.

Az irányelv rendelkezései alapján a tagállamok kidolgozzák az ágazati kritériumaikat. Az irányelv külön nevesíti az energia- és a közlekedési ágazatot, így az ezekre vonatkozó ágazati kritériumok előtérbe kerülnek a végrehajtás során. Fentiek mellett horizontális kritériumok szerint is vizsgálni szükséges az adott tagállamban található, potenciálisan kritikus infrastruktúrákat. A veszteségek, a gazdasági és a társadalmi hatások kritériumára vonatkozó küszöbértékeket a tagállamok eseti alapon határozzák meg, függően az adott infrastruktúra által biztosított szolgáltatás jellegétől.

A tagállamok meghatározzák azokat a potenciális kritikus infrastruktúrákat, amelyek európai szintűek lehetnek. A tagállam köteles tájékoztatni a hatás alatt álló más tagállamokat a beazonosítással kapcsolatos információkról, és egyeztetést folytatni velük a potenciális hatásokról. A kijelölés csak akkor történhet meg, ha az érintett tagállamok arról megállapodást kötnek.

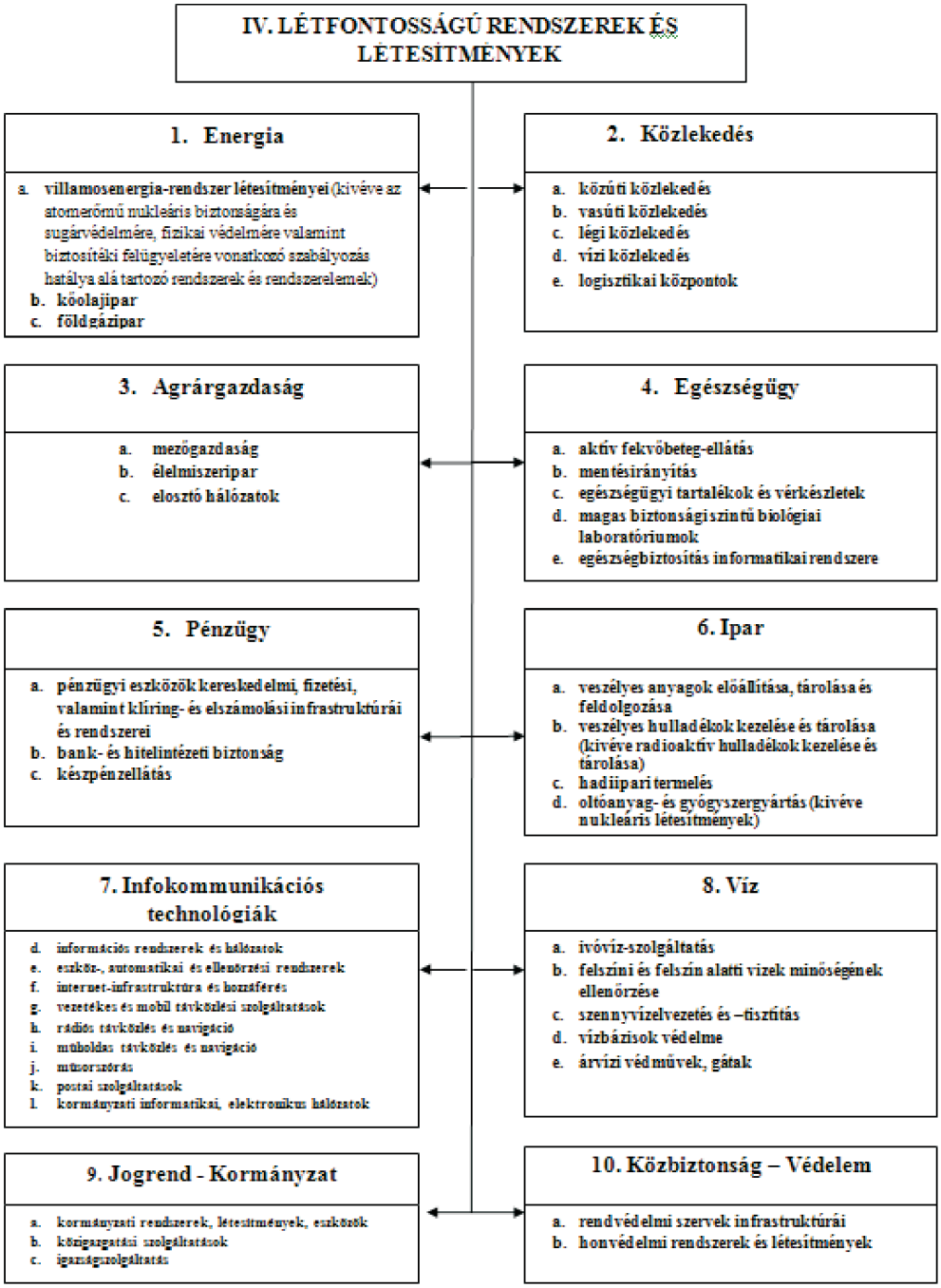
Az üzemeltetők a kijelölést követő egy éven belül dolgozzák ki az üzemeltetői biztonsági tervet és jelölik ki a hatósággal kapcsolatot tartó biztonsági összekötő személyt. [4]

2. A hazai szabályozás megalkotása

A kritikus infrastruktúra védelmi rendszer kialakításának első magyarországi lépése volt a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat elfogadása. A nemzeti programról szóló Zöld Könyv a kormányhatározat mellékletét képezi. [5]

Az irányelv szabályozási irányvonalát követő, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényt (a továbbiakban: Lrtv.) célja egyrészt a létfontosságú rendszerelemek azonosítása, másrészt a kijelölés megtörténte után a védelem biztosítása. A Lrtv. 2013. március 1. napján lépett hatályba. A szabályozás hatálya alá a következő ábrán látható szektorok tartoznak. [6]

A törvény a tárgykör szempontjából alapvető fogalmakat határoz meg, így a nemzeti és európai létfontosságú rendszerelem, üzemeltető, ágazati és horizontális kritérium definícióit. A nemzeti és az európai létfontosságú rendszerelem kijelölése szempontjából külön eljárási procedúráról is rendelkezik. Közös szabályokat tartalmaz mind a nemzeti, mind az európai létfontosságú rendszerelem tekintetében a nyilvántartásra, az adatvéde-



1. sz. ábra: A létfontosságú rendszerek és létesítmények ágazati és alágazati besorolása

lemre, az ellenőrzésre, az üzemeltetői biztonsági tervre, a biztonsági összekötő személyre, a szankcionálásra vonatkozóan.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról rendelkező 65/2013. (III. 8.) kormányrendelet (a továbbiakban: végrehajtási rendelet) 2013. március 11-én lépett hatályba. [3]

A végrehajtási rendelet a jogalkalmazást elősegítő, a törvényben nem meghatározott értelmező rendelkezéseken (lásd azonosítás, kockázatelemzés fogalmai) túl szabályozza a nemzeti létfontosságú rendszerelemek üzemeltető általi azonosítását. Az azonosítási eljárás keretében az üzemeltető – a jogszabályban rögzített követelményeknek megfelelő – azonosítási jelentését megküldi az ágazati kijelölő hatóságnak, amely azt véleményezés céljából továbbítja az ágazati javaslattevő hatóságnak. Az ágazati javaslattevő hatóság a jelentés vizsgálatát követően megküldi a javaslatait a kijelölő hatóságnak.

Az ágazati kijelölő hatóság, az illetékes hivatásos katasztrófavédelmi szerv szakhatósági állásfoglalására figyelemmel, határozatban dönt a nemzeti vagy európai létfontosságú rendszerelem kijelölése tárgyában. A kijelölés feltétele az, hogy az ágazati kritériumok és a horizontális kritériumok közül legalább egy bekövetkezésének lehetősége fennáll. A kijelölő határozat rendelkezik a kijelölésről, a kijelölt rendszerelem nyilvántartásba vételéről, az üzemeltetői biztonsági terv készítésének kötelezettségéről, a biztonsági összekötő személy foglalkoztatásáról, a hálózatbiztonsági központba való bekötésről, továbbá egyéb feltételeket határozhat meg a létfontosságú rendszerelem védelme érdekében. [6]

A biztonsági összekötő személy képesítési követelményei tekintetében a végrehajtási rendelet a műszaki, védelmi igazgatási, katasztrófavédelmi, rendészeti ismereteket preferálja. Meghatározza továbbá az üzemeltetői biztonsági terv követelményeit, az ellenőrzés egyes szabályait, a rendkívüli esemény során követendő általános eljárási szabályokat, az üzemeltetővel szemben kiszabható közigazgatási bírság összegét.

Az azonosítási jelentést az üzemeltetőnek első alkalommal a végrehajtási kormányrendelet hatálybalépését követő 180 napon belül kell benyújtania.

A szabályozás a kritikus infrastruktúra védelme területén a katasztrófavédelem részére elsődleges felelősségi köröket határozott meg, amelyek a következők:

- szakhatósági feladatok ellátása valamennyi szektor esetében a horizontális kritériumok vizsgálata érdekében: Vhr. 4. § (2), 13. § (1);
- létfontosságú rendszerek és létesítmények nyilvántartó hatósága: Vhr. 12. § (1);
- javaslattevő hatóság a feladatkörében rendelt szektor esetében: Vhr. 3. §;
- hatósági ellenőrzések koordinálása: Vhr. 8. §, 13. § (3);
- Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ működtetése: Vhr. 10. §;
- rendkívüli események kezelése: Vhr. 11. § (6);
- CIP POC kapcsolattartó ponti feladatkör: Kat. Vhr. [7]

Az ún. koordinált ellenőrzések tartására és az európai és nemzeti létfontosságú rend-

szerelemekre vonatkozó nyilvántartás vezetésére a hivatásos katasztrófavédelmi szerv központi szerve (a továbbiakban: BM OKF) kapott jogosultságot. A végrehajtási rendelet a BM OKF-et bizonyos szempontok (így közrend, közbiztonság, lakosságvédelem, alkotmányvédelem, nemzetbiztonság, terrorelhárítás) tekintetében javaslattevő hatóságként is kijelöli.

A hálózatbiztonsággal kapcsolatos szabályokat az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) kormányrendelet tartalmazza.

A BM OKF a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenység ellátása érdekében eseménykezelő központot működtet Létfontosságú Rendszerek és Létesítmények Eseménykezelő Központja elnevezéssel. A központ felügyeletét a katasztrófák elleni védekezésért felelős miniszter látja el. A 2012. január 1. óta a BM OKF szervezetében működő Országos Iparbiztonsági Főfelügyelőség feladatkörén belül kiemelt helyet foglal el a kritikus infrastruktúra védelmi (KIV) szakterület.

Az európai kritikus infrastruktúra védelmével kapcsolatos ügyekben a nemzeti kapcsolattartó és koordinációs feladatokat – mint ECIP kapcsolattartó pont – a belügyminiszter látja el. A belügyminiszter ellátja továbbá a polgári válságkezelési, a katasztrófavédelmi és a kritikus infrastruktúra védelmi feladatok kormányzati koordinációját, illetve előkészíti különösen az infrastruktúra kritikus elemeivel kapcsolatos feladatokról szóló jogszabályokat. [8]

Az Lrtv. felhatalmazó rendelkezéseire tekintettel az azonosítási, kijelölési és a hatósági ellenőrzés ágazatokra vonatkozó különös szabályokat, valamint az ágazati kritériumokat külön ágazati kormányrendeletek állapítják meg.

2014. március végéig a következő ágazati szabályozás került Magyarország kormánya által elfogadásra:

- 360/2013. (X. 11.) kormányrendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
- 512/2013. (XII. 29.) kormányrendelet az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) kormányrendelet módosításáról;
- 540/2013. (XII. 30.) kormányrendelet a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről;
- 541/2013. (XII. 30.) kormányrendelet a létfontosságú vízgazdálkodási rendszerelemek és vízi létesítmények azonosításáról, kijelöléséről és védelméről. [7]

A fenti rendeletek már hatályosak, és megkezdődött az üzemeltetői feladatok teljesítésének időszaka. A végrehajtási rendeletek főként az adott szektorra jellemző ágazati azono-

sítási kritériumokat jelenítik meg. Ezeken túl a biztonsági összekötő személy képzettségére, az üzemeltetői biztonsági terv tartalmára vonatkozóan adnak meg részletszabályokat. A többi ágazat tekintetében a végrehajtási kormányrendelet még szabályozási szakaszban van.

3. A végrehajtásban érintettek felkészítése

A végrehajtási rendelet alapján 2014. szeptember 1-től a biztonsági összekötő személynek az adott ágazatnak megfelelő szakirányú végzettséggel kell rendelkeznie. A biztonsági összekötő személynek az adott ágazatnak megfelelő szakirányú végzettség mellett rendelkeznie kell védelmi igazgatási vagy rendészeti igazgatási szakon szerzett felsőfokú végzettséggel; tűzvédelmi, iparbiztonsági, polgári védelmi szakmai irányú rendészeti szervezői szakképesítéssel vagy ezzel egyenértékű végzettséggel; iparbiztonsági szaktanfolyami végzettséggel; iparbiztonsági szakon szerzett felsőfokú végzettséggel vagy a katasztrófavédelem hivatásos szerveinél legalább 5 év iparbiztonsági szakterületen szerzett gyakorlattal.

2018. július 1-ét követően a biztonsági összekötő személynek az adott ágazatnak megfelelő szakirányú végzettség mellett rendelkeznie kell iparbiztonsági szakon szerzett felsőfokú végzettséggel vagy a katasztrófavédelem hivatásos szerveinél legalább 5 év iparbiztonsági szakterületen szerzett gyakorlattal. [9] [10]

Az iparbiztonsági végzettséget a 2012. január 1-én létrehozott Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézeténél 2013-ban először indított katasztrófavédelmi alapszak iparbiztonsági szakirányán lehet megszerezni. E szakirányon az általános katasztrófavédelmi, tűzvédelmi és védelmi igazgatási ismeretekeken kívül ún. iparbiztonsági ismereteket is oktatnak. Az iparbiztonsági szakismeretek kiterjednek a veszélyes üzemek és a veszélyes szállítmányok biztonságára, a veszélyes anyagok jelenlétében bekövetkező események elhárítására, a létfontosságú rendszerek és létesítmények védelmére, valamint a nukleárisbaleset-elhárítási feladatok teljesítésére. [11]

4. Összegzés

A létfontosságú rendszerek és létesítmények védelméről szóló nemzeti szabályozás megfelelő alapot biztosít ahhoz, hogy Magyarország komoly lépések megtételéről adjon számot a létfontosságú rendszerek és létesítmények védelme érdekében, megvédve azokat az infrastruktúraelemeket, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához.

A kritikus infrastruktúra védelmének szabályozásával a lakosság alapvető ellátása, a potenciálisan veszélyes tevékenységek környezetében élők védelme is hatékonyabban

garantálható. Fokozható a lakosság életének és vagyonának biztonsága, a kiemelkedő társadalmi jelentőségű közszolgáltatások folytonosságának biztosítása, valamint a meglévő közfeladatok, a közbiztonság hatékonyabb ellátása.

Irodalomjegyzék

[1] Kossa, Gy.: Industrial safety – tasks and challenges to protect the future. Iparbiztonság – feladatok és kihívások a jövő védelmében. Védelem-, Katasztrófa-, Tűz-, és Polgári Védelmi Szemle (ISSN: 1218-2958) 18., (6) pp. 49–50. 2011.

[2] Bognár Balázs – Vass Gyula – Kozma Sándor: A BM OKF Országos Iparbiztonsági Főfelügyelőség szakterületeinek bemutatása. Új Magyar Közigazgatás, 2012/6. szám, pp. 19–27., Budapest

[3] Tünde Bonnyai – Balázs Bognár: The process of critical infrastructure protection. Academic and Applied Research in Military Science, Vol. 8., issue 3. pp. 499–513. 2009., Budapest

[4] Balázs Bognár – Judit Mógor: Concept and development of regulations on protection of critical infrastructures (Chapter). The Best Practice of Training Handbook Critical Electric Energy Infrastrucures Protection. EU-ExTraH project: HOME/2009/CIPS/AG/C1-010, pp. 9–20., 2011., Budapest.

[5] Bognár Balázs: A létfontosságú rendszerek és létesítmények védelme. Katasztrófavédelmi Szemle, 2012. XIX. évfolyam, 4. szám pp. 13–17., Budapest

[6] Bognár Balázs – Kossa György – Kozma Sándor – Szakál Béla – Vass Gyula – Kátai-Urbán Lajos (szerk.): IPARBIZTONSÁGTAN I.: Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. Budapest, Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 564 p. (ISBN:978-615-5344-12-1)

[7] Bognár Balázs: Létfontosságú rendszerek és létesítmények védelmével kapcsolatos szabályozás kialakítása és hazai alkalmazása. In: Iparbiztonsági Szakmai Nap. NKE Katasztrófavédelmi Intézet, Budapest, 2014. március 11.

[8] Endrődi István: A közlekedési ágazat kritikus infrastruktúra elemei, kapcsolatuk a katasztrófavédelemmel, figyelemmel az Európai Unió Kritikus Infrastruktúrák Azonosításáról és Kijelöléséről szóló 2008. évi 2008/114/EK Tanácsi Irányelvében megfogalmazottakra. In: Fejezetek a kritikus infrastruktúra védelemből I. Budapest,: Magyar Hadtudományi Társaság, 2013, pp. 238–267.

[9] Bleszity János: Подготовка дипломированных специалистов по чрезвычайным ситуациям в Венгрии (Education of Disaster Management Officers in Hungary). «ПОЖАРЫ И ЧС» 2012. № 4 С. 9. (FIRE AND EMERGENCIES: PREVENTION ELIMINATION) 4:(12) pp. 9–13. (2012)

[10] Bleszity János – Joó Bálint: NKE katasztrófavédelmi egyetemi képzés született. Katasztrófavédelmi Szemle XX., (5) pp. 38–40. (2013)

[11] Grósz Zoltán: Egyetemi képzések a katasztrófavédelem számára. Bolyai Szemle XXII., (3.), pp. 9–16.

Implementation of the regulation on the protection of critical systems and installations in Hungary

Bognár Balázs – Kátai-Urbán Lajos – Vass Gyula

After the New Disaster Management Regulations entered into force in 2012, a unified Industrial Safety Supervising Authority was established at a national, regional and local level in Hungary.This paper introduces the state and experiences of the implementation of the nat ional regulations about the identification and protection of Critical Infrastructure in Hungary.

Keywords: industrial safety, critical infrastructure protection, disaster management, Hungary

Kátai-Urbán Irina
Bleszity János

Hazardous establishments as national risks

The experts of the National Disaster Management Organisation actively participate in the elaboration of the "National Risk Assessment Report and Methodology". The goal of this work is to elaborate a method suitable for the analysis of a broad range of events related to significant risks for Hungary, both in terms of probabilities and consequences. An important output of the analysis is the risk chart with the scenarios posing significant risks, broken down according to their relative probability and the severity of their consequences. In the present article the authors report on the results of their professional scientific activities carried out in connection with hazardous establishments. Keywords: industrial safety, industrial accidents, dangerous substances, hazardous activities, vulnerability.

Preface

The experts of the National Disaster Management Organisation actively participate in the elaboration of the document "National Risk Assessment Report and Methodology" (hereinafter: Report). [1] The goal of the workgroup, with the participation of more than 20 professional state organizations, is to elaborate a method suitable for the analysis of a broad range of events related to significant risks for Hungary, both in terms of probabilities and consequences.

On the basis of the guides of the European Union the planned method considers the aspects of the adaptation to climate change, the effects of the individual scenarios on critical systems and installations and handles cross-connections and interdependencies that can be assumed between the scenarios through the concept of individual/multiple risks.

An important output of the analysis is the risk chart with the scenarios posing significant risks, broken down according to their relative probability and the severity of their consequences.

In the present article the authors report on the results of their professional scientific activities carried out in connection with hazardous establishments.

Identification of disaster events

Regarding hazardous establishments, in the present phase of the analysis disaster events with the most severe consequences for major geographic areas of the country, for the people living there, for the economy and natural treasures have been identified. It was a fundamental goal that in line with the Seveso guideline one scenario shall be selected in connection with toxic, explosive and flammable hazardous substances and with hazardous substances causing environmental damage.

The most severe scenarios are selected on the basis of the exposure to dangers as presented in the safety documentation of the individual hazardous establishments, using a scientific approach, by the implementation of the so-called „modified Preliminary Hazard Assessment" (hereinafter: modified PHA). [2]

The aspects of the modified PHA have been selected to be suitable for the screening of the risks occurring in various fields, in accordance with the special aspects listed above and specified by the EU. In the course of the modified PHA the experts of the national disaster management authority have analyzed which of the several thousands of major accident scenarios that can be assumed in the territory of the 700 hazardous establishments in Hungary are probable to occur within 5 or 20-25 years, respectively and which scenarios are affected by the climate change. In the course of the screening a further aspect was that the scenario shall affect critical systems and installations and that the management of the situation and the coordination of damage control tasks shall require government intervention. In addition, the analysis has also checked if the assumed scenario affects our social values, like human health/life, the environment/nature, finances/economy, social stability, governing ability and the territorial manageability of the country.

As a result of the modified PHA the damage event of a container storing 146 tons of liquefied chlorine gas was selected. As a consequence of the damage the toxic gas cloud could endanger some 7,800 people. The damage to a container resulting in the release of 300 tons of acrylonitrile was also selected, which can cause major environmental damage in the vicinity of the Danube River and – because of the toxicity of the substance – can endanger the health of those staying in the surrounding residential and industrial area. Furthermore, the catastrophic damage of a propane/propylene distillation column was also selected, which might trigger air shock waves and heat effects destroying not only the plant but also the surrounding industrial areas, causing economic and human damage. [1]

Evaluation of the effects of climate change

In the course of the preparation of the report the consideration of the effects of climate change was one of the priorities. The effects of climate change, such as heat waves, floods, landslides, cavities can damage industrial installations (including establishments involving hazardous substances, nuclear installations) and equipment storing, processing hazardous substances, thus increasing the probability of major accidents, and the exposure of those living in the surroundings of hazardous installations to hazards. [3]

Due to climate change the weather conditions influence the propagation of hazardous substances potentially released and thus can change the size and location of the area endangered by the harmful effects. On the basis of the climate adaptation strategy of the EU (Brussels, April 16, 2013) the experts of the national disaster management authority determined the effects of climate change that can affect the industry. The most significant effects that might increase the chances of the occurrence and/or consequences of a potential major accident are the following:

Extreme temperature, heat waves. In the summer of 2012 the operators of hazardous establishments announced 11 incidents involving hazardous substances. A part of the incidents could be traced back to technical-technological reasons resulting from extreme environmental parameters (e.g. high temperature).

The disaster management authority received notifications of 14 incidents and further events in the winter of 2012. Technological equipment fail is typically in the period between January and February, most of such failures can be traced back to extreme weather conditions, to the low outdoor temperature. The increased stress of the technological elements resulting from the outdoor temperature and the reduction of the number of periodic maintenance mainly due to financial reasons highly increase the probability of the occurrence of major accidents.

With regard to the consequences, extremely low temperature together with stable atmospheric conditions are an extremely unfavorable condition for human health in the event of the propagation of toxic gases. Gas propagates slowly under such weather conditions and is able to stay in the vicinity of the ground for a long time, thus significantly increasing the risks humans are exposed to.

Flood. As it can be seen in the figure below, there are 121 hazardous establishments operating in Hungary in areas endangered by floods. Sites need increased monitoring; before flood waves actions shall be taken to remove the hazardous substances, wastes and the containers used for their storage, and to transfer them to a safe place, as the water can lift up, sweep away containers and hazardous wastes, thus seriously jeopardizing environmental safety.

Landslide, cavities. There are some 10 such hazardous establishments in Hungary located on young, sedimentary soil creating increased risk of landslide. In addition, mines

under hazardous establishments can also pose a long-term problem due to the collapse of mine cavities. Such data are not all-comprehensive at the present, further analysis is necessary.

Lack of surface waters. In Hungary there are several hazardous industrial establishments in need of high amounts of water (e.g. for technological processes, cooling, firefighting). Due to the engineering reserves their water abstraction structures are able to supply the water quantity needed for normal operation at present; however, in the long run bridging and managing intervals of temporary surface water shortage is a strategic challenge.

In the territory of the plants there are water reserves which are sufficient for simultaneous firefighting and for the safe shutdown of the technologies available. However, in consideration of the fact that these installations supply feedstock (petrochemical products, industrial gases) to other players of the industry in Hungary and they play a special role in the supply of the public (production of disinfectants, medicine, medical gases) and that the loss of their function could cause serious disturbances in the supply chain, it is justified to create the conditions needed for the function of the plants even in case of permanent water shortage. [1]

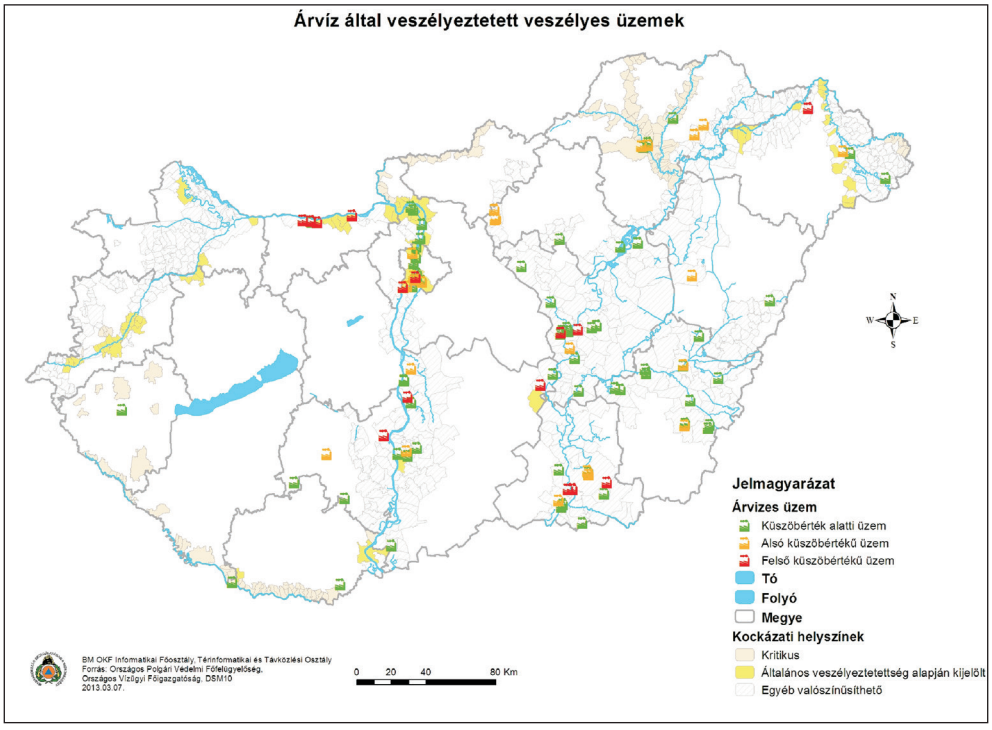


Table No. 1. Hazardous establishments endangered by flood (Source: Hungarian Disaster Management Authority)

Checking the vulnerability of the elements of critical infrastructure

In the course of the preparation of the Reports the experts of the national disaster management authority evaluate to what extent the major accident scenarios selected (on local, regional or national level) can interfere with the operation of the critical infrastructure sectors listed in the legal regulations of Hungary. It can be stated that the consequences of events assumed in the territory of hazardous establishments can, due to the release of toxic substances, impair the quality of surface and subsurface waters and contaminate arable land.

Through the expectedly high number of injuries and fatalities they can overload the healthcare system and can interfere with the road, rail and water transportation system during the emergency response. The loss of the function of hazardous installations can lead to the shutdown of other plants due to reasons listed above. [4]

Emergency response tasks to handle the consequences of major accidents

In the course of the preparation of the Report it is an important aspect that the mitigation of the consequences of the major accident scenarios selected requires the intervention of the government. The tasks related to the mitigation of the consequences of major accidents selected for analysis have been defined in the external and internal emergency plan and in the water emergency response plans.

After the activation of the plans, the staff of the operator, the local and regional organizations of the disaster management authority, jointly with the other state organizations concerned and with the mayors of the settlements endangered carry out the damage mitigation activities, under the management of the central organization of the disaster management authority.

In case of the occurrence of the major accidents selected, the intervention of the government is a precondition to efficient damage control, as it is absolutely necessary for the mobilization of other state organizations (police, ambulance service, military and water experts) and for the harmonization of their activities.

The disaster management authority and its experts specializing in training and in industrial safety explain in detail these legal requirements in their leading scientific works. [5] [6]

Conclusions

In the next stage of the preparation of the Report the detailed analysis of effects and probabilities will be completed (and expressed in figures) and the cross-connections and interdependencies between the scenarios selected as the result of the modified PHA will be mapped. The necessary preparations (definition of the criteria of the effects, setting up probability classes) for these working processes have already been completed.

In the course of the work, the experts of the Hungarian Disaster Management Authority have seen a high number of fields and as a result of further research and the development of these fields, the efficiency of the prevention of major accidents can be improved. E.g. the renewal of the risk analyses is underway at present, the review of models used for the avoidance of hazardous substances and for the analysis of their propagation with regard to the effects is changing, as described above. The long-term objective is to further improve public safety by reducing the risks resulting from climate change as much as possible.

Bibliography

[1] Kockázatértékelési Jelentés és Módszertan. BM Országos Katasztrófavédelmi Főigazgatóság, Budapest, 2013. (National Risk Assessment Report and Methodology, National Directorate General for Disaster Management of the Ministry of the Interior, Budapest, 2013.)

[2] Kátai-Urbán Lajos – Révai Róbert: A veszélyes anyagokkal kapcsolatos katasztrófák lehetséges környezetet, emberi életet és egészséget károsító hatásai. (Possible Effects of Disasters Involving Dangerous Substances Harmful to the Environment, Human Life and Health), Bolyai Szemle XXII., (2) pp. 151–158. (2013)

[3] Szakál Béla – Cimer Zsolt – Kátai-Urbán Lajos – Sárosi György – Vass Gyula: Iparbiztonság I. Veszélyes anyagok és súlyos baleseteik az iparban és a szállításban. (Industrial safety I. Dangerous substances and major accidents in industry and transportation.) Budapest, Korytrade, 2012., 113 p. ISBN 978-963-89073-3-2

[4] Endrődi István: A közlekedési ágazat kritikus infrastruktúra elemei, kapcsolatuk a katasztrófavédelemmel, figyelemmel az Európai Unió Kritikus Infrastruktúrák Azonosításáról és Kijelöléséről szóló 2008. évi 2008/114/EK Tanácsi Irányelvében megfogalmazottakra. (The elements and their disaster management aspects of critical infrastructure protection of the transport sector, taking into account the Council Directive 2008/114/EC on the identification and designation of the Critical Infrastructure of European Union.) In: Fejezetek a kritikus infrastruktúra védelemből I. (Chapters of Critical Infrastructure protection I.) Budapest, Magyar Hadtudományi Társaság, 2013. pp. 238–267.

[5] Bognár Balázs – Juhász István – Kátai-Urbán Lajos (szerk.) – Kossa György – Kozma Sándor – Szakál Béla – Vass Gyula: Iparbiztonságtan I. Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. („Industrial safety I." Manual for the completion of industrial safety tasks of operators and authorities".) Budapest, Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 564 p. ISBN: 978-615-5344-12-1

[6] Szakál Béla – Cimer Zsolt –Kátai-Urbán Lajos – Vass Gyula: Iparbiztonság II. A veszélyes anyagokkal kapcsolatos súlyos balesetek következményei és kockázatai. (Industrial Safety II. Consequences and Risks of Major Accidents involving Dangerous Substances.) Budapest, TERC Kereskedelmi és Szolgáltató Kft., 2013., 182 p. ISBN 978 615 5445 002

Veszélyes tevékenységek nemzeti kockázatai

Kátai-Urbán Irina – Bleszity János

A magyar katasztrófavédelmi szakemberek aktívan részt vesznek a Nemzeti Kockázatértékelési Jelentés és Módszertan című dokumentum kidolgozásában. A munka célja olyan módszer kidolgozása, amely alkalmas az ország szempontjából jelentős kockázattal bíró események széles spektrumának elemzésére mind a valószínűségek, mind a következmények tekintetében. Az elemzés egyik fontos végkimenete a kockázati diagram, amely a figyelembe vett jelentős kockázatú eseménysorokat mutatja azok relatív valószínűsége és a következményeik súlyossága szerint. Jelen cikkben a szerzők beszámolnak a nemzeti jelentés elkészítése során a veszélyes üzemekkel kapcsolatosan végzett szakmai tudományos tevékenységük eredményeiről.

Kulcsszavak: iparbiztonság, ipari balesetek, veszélyes anyagok, veszélyes tevékenységek, veszélyeztetettség

Morvai Cintia

Toronyházak mentő tűzvédelme – esettanulmány

A magas épületek mentő tűzvédelme a tűzoltóságok számára is mindig kiemelkedő feladat volt. A gyöngyösi toronyház tűzvédelmével foglalkozó esettanulmányból kiderül, hogy mintegy 40 év telt el a toronyház építésétől, amely alatt a mentésre szolgáló eszközök jelentős mértékű technikai fejlődésen mentek keresztül. Jelen cikkben a toronyház tűzvédelmi fejlesztésének irányvonalait is elemzem, konkrét tűzvédelmi hiányosságokra is kitérek, valamint új tűzvédelmi eszközök beépítésének alkalmazására is javaslatot teszek.
Kulcsszavak: toronyház, mentő tűzvédelem, technikai fejlődése, magas épület, mentés

Bevezetés

Az urbanizáció hatására az utóbbi évtizedekben egyre több középmagas és magas épület épült. Az elmúlt 20-25 évben ezek száma rohamosan nőtt. Számos iparilag fejlett ország modern építészetére jellemző a magas építkezés. A városok szempontjából jellemzővé válik a beépíthető szabad területek hiánya. Az élet- és vagyonbiztonsági, a biztonságtechnikai és a tűzbiztonsági szempontok elemzésekor azonban már több megoldatlan műszaki, építészeti, gazdasági és szervezési kérdés merülhet fel. Különösen fontos, de kiemelt figyelmet érdemlő probléma a tűzesetek megelőzése és a bekövetkezett tüzek esetén az emberi élet és egészség, illetve az anyagi javak hatékony védelme.

Mentő tűzvédelem

A magas épületek mentő tűzvédelme a tűzoltóságok számára mindig kiemelkedő feladat volt. Ezek az épületek 30 méternél magasabbak, így a felső szintek megközelítése csak a lépcsőházon keresztül oldható meg. Számos szakirodalom foglalkozik ezen épületek tűzoltás-taktikai jellemzésével. Ebben a fejezetben ismertetem a toronyház mentő tűzvédelmével kapcsolatos legfontosabb szempontokat, a toronyház kivitelezésekor használt tűzoltó eszközöket, járműveket és a jelenleg használatos felszereléseket, továbbá a magas épületek mentő tűzvédelmének markáns tűzoltó-taktikai előírásait.

A hatályos jogszabályban olvasottak alapján a tűzoltási, felvonulási terület kiépítését és műszaki paramétereit, szélességét, teherbírását, az épülettől való távolságait, valamint azt, hogy ezt az épület melyik oldalán szükséges kialakítani, az építési engedélyezési eljárás keretében a tűzvédelmi szakhatóság állapítja meg. Az engedélyezési tervdokumentációban szereplő helyszínrajzon a felvonulási területet jól felismerhető módon kell jelölni. A felvonulási területet úgy kell kialakítani, hogy a szélessége 6 méter legyen, és 7,5 méter széles kitalpalási hely legyen a mentési helyek előtt, aminek felismerhetőnek és jól láthatónak kell lennie. A hosszanti tengely távolsága 8-14 méter kell, hogy legyen a mentési homlokzattól számítva. Ha a felvonulási területen fasor vagy villanyvezeték található, akkor az egymás közötti távolságuk minimum 15 méter kell, hogy legyen. Magas épületek felőli oldalon a felvonulási területen közvilágítási szabadvezetékek vagy közúti villamos járművek vezetékei nem helyezhetők el. A felvonulási terület felé eső homlokzatán szintenként és tűzszakaszonként minimum két, mentésre alkalmas, 1 méter magasságú erkélyt, loggiát vagy ablakot kell kialakítani. Magas épületek esetén a vízellátást úgy kell megoldani, hogy 50 méterenként legalább két tűzcsapnak kell lennie. [1]

A magas épületekben, ha szintenként van kettő vagy több tűzszakasz, akkor legalább egy-egy lépcsőházat kell kiépíteni. Ha a felvonulási épület felől lévő homlokzatától való mélysége 45 méternél több, akkor két füstmentes lépcsőházat kell kialakítani. Hő- és füstelvezetésre alkalmazni lehet nyílászárókat is, nem csak szellőztető berendezéseket. A nyílászáró tervezésénél figyelni kell, hogy ne nyíljon rá a menekülési útvonalra, és azok nyitási módját érthetően és láthatóan jelölni kell. Amennyiben füstelvezető nem alakítható ki a magas épületben, akkor a füstelvezetést légtechnikai berendezésekkel kell megoldani.

Korabeli eszközök

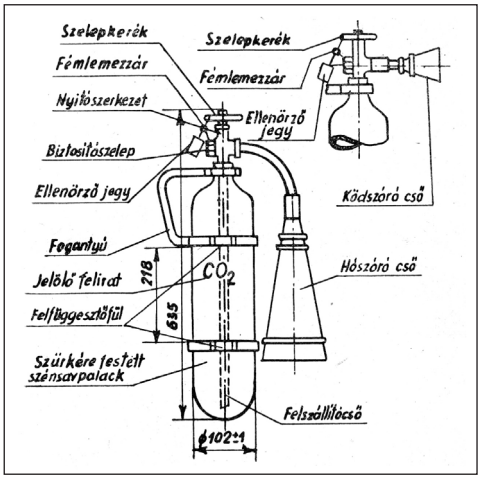
A toronyházat az építéskori (1970-es éveknek megfelelő) eszközök alkalmazási lehetőségeihez mérten tervezték és építették meg. Ebben az időszakban több jelentős tűzeset is történt. A főváros egyik legnagyobb tűzesete volt a Csertő utcai, 1972. május 18- án történt baleset. Ez az épület Larsen–Nielsen (dán) típusú épület volt, mint a Gyöngyösi toronyház is. A tragédia bebizonyította, hogy az ezen épületeknél történt tűzesetek súlyos károkat okoznak, és emberi életeket követeltek a hibás tervezés miatt.

Kihúzós létra

A kihúzós létra három egymásba kapcsolódó, nem szétszedhető, de elcsúsztatható támasztólétra részből áll. Ez a létra a szerkezetéből kifolyólag könnyen megszerelhető a különböző magasságok elérésére. Alumíniumból sajtolt rúdanyagból készült, hegesztett módszerrel. A létra két részből áll: az alaptagból és a mozgótagból. A létra alaphossza 5,3 méter, a teljes hossza 9,6 méter, a tömege 44 kg, a támrudakkal együtt pedig 54 kg. [2]

Kézi tűzoltó készülékek

A kézi tűzoltó készülékek jellemzője, hogy egyszerű szerkezetűek, a kézben könnyen szállíthatóak, és üzemképes állapotban nem haladják meg a 20 kg-ot. Ezek a készülékek könnyen és rövid idő alatt üzembe helyezhetőek, a keletkezett tüzet azonnali beavatkozással el lehet velük oltani. A készülékeket az épületek folyosói mentén úgy helyezték el, hogy a legtűzveszélyesebb helyek közelében legyenek. Az 1960-as években használt készülékek: vízzel oltó kézi tűzoltó készülékek; szénsavval oltó kézi tűzoltó készülékek; gázzal oltó kézi tűzoltó készülékek; Tetra oltókészülékek; bromidoltó készülékek; porral oltó kézi tűzoltó készülék; vegyi habbal oltó kézi tűzoltó készülék. [3]



1. ábra: Szénsavval oltó kézi tűzoltó készülék [3]

Szűrőbetétes gázvédő eszközök

A szűrőbetétes gázvédő eszközök, azaz a szűrőbetétes gázálarcok közül kettőt használtak: a keretgázálarcot és a sisakgázálarcot. A gázálarc az arcot vagy a fejet is beborító, légmentesen záródó, gázáthatatlan anyagból készült védőeszköz. A rendeltetése, hogy megvédje a légzőszerveket és a szemet a levegő ártalmas szennyeződéseitől. Az eszköz segítségével a légzés biztonságossá válik a szennyezett légtérben is, mivel a szűrőbetét áttisztítja a levegőt, mielőtt az eljut az eszköz használójához. Ezek a gázvédő eszközök biztonságot nyújtanak a sugárzó hő és a szúróláng hatása ellen.

Füst- és gázelszívó készülék

Zárt térben keletkezett tűzesetnél az egyéni gázvédő eszközökön kívül szükséges olyan készülék is, amely a füsttel, gázzal telt helyiségekből eltávolítja a füstöt vagy a gázt, esetleg friss levegőt juttat oda. Ez a berendezés a tűzben dolgozó tűzoltók egészségének megóvásában és a munkájuk megkönnyítésében játszik szerepet. Ezentúl a zárt térben lévő értékes anyagok, felszerelések megóvása céljából is használatosak. A tűzoltóságok használatában lévő készülékek mind hordozhatóak.

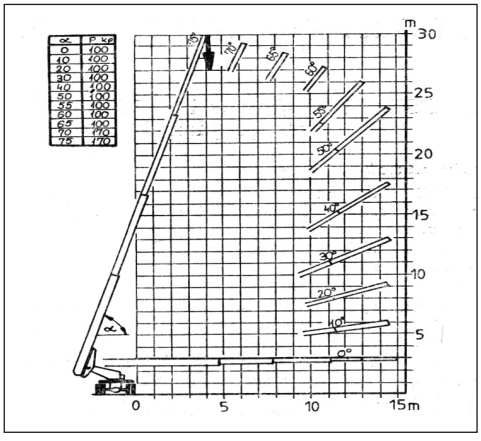
Járművek

A tűzoltási feladatokat és a műszaki mentést általában egyszerre kell megoldani, egymást kiegészítve. Ennek megfelelően lett kialakítva az alkalmazott technika, a tűzoltó gépjárművek többségében mindkét tevékenység végzéséhez találunk eszközöket.

Gépjárműfecskendők. A gépjárműfecskendők általános célú tűzoltójárművek. Ezeket elsősorban a tűzoltók szállítására és a vízzel oltásra alakították ki, a szabvány szerint a habbal oltásra is képesek. A gépjárműfecskendők a felszereléseik révén még a műszaki mentéseknél is alkalmazhatók. A tűzoltójárművek több típusát alkalmazták, például a GF-I. 10 12-TÜ. 2. típusút, a GF-II. 20 15-p-TÜ. 1. és az IFA W 50 TLF 16 típusú gépjárműfecskendőt. [4]

Létrás gépjárművek. A létrás gépjárművek nélkülözhetetlen eszközei a tűzoltóságnak. Mivel a középmagas és magas épületek száma egyre növekedett már az 1970-es, 1980-as években is, így készenlétben tartásuk egyre fokozódott. Az épületek magasabb szintjeit kívülről a létrás járművekkel vagy az emelőkosaras járművekkel lehetett megközelíteni. Sajnos ezeknek a járműveknek is korlátozott volt az elérhető magasságuk. Az 1980-as években épített legnagyobb létra körülbelül a 60 méteres magasságot érte el. A magasság növelésével stabilitási problémák léptek fel. A hazánkban alkalmazott létrák 30, 37 és 44 méter hosszúságúak. Ilyen jármű például az IFA W 50 L DL 30, a CSD 710 Magarius DL 30-h és a Magarius DL 44-h típusú létrás gépjármű. Az IFA W 50 L DL 30 típusú létrás gépjárműnek négyhengeres motorja van, 92 kW, vízhűtéses, dízel, a gördülőtömege 9500 kg. A szállítható személyek száma 1+5 fő. A létrakészlet legnagyobb magassága 30 méter, és négy darab létratagból áll. Ezt a létrakészletet nem szerelték fel személyszállító berendezésekkel, így tipikus mászólétra.

A tűzoltás 40–70°-os szögállásban végezhető, a sugárcsövet kötéllel kell mozgatni függőleges irányba. Terhelhetősége szabadon álló helyzetben 65° szögállás alatt 1 kN egy fő, 70-75° között 1,7 kN két fő, feltámasztott létravéggel 3 méterenként 1 fő. Daruüzemben legfeljebb 10 kN terhelés adható az alaptagra 60°-os szögállásnál.



2. ábra: IFA W 50 L DL 30. típusú, létrás gépjármű használati mezője [4]

A jelenlegi felszerelések

A toronyház építését követő tűzoltó eszközök és a jelenleg használt felszerelések között nagy különbségek lelhetők fel, hiszen a ma használt eszközök nagyon sokat fejlődtek az akkoriakhoz képest.

Létraszer

A létrák alkotják a tűzoltók számára az egyik nélkülözhetetlen eszközcsoportot. Ezt az eszközt mind az életmentéshez, mind a támadáshoz felhasználhatják, különösen, ha a felhatolási utak járhatatlanok vagy azok egyáltalán nincsenek. A tűzoltóságok célszerűségi okokból különböző kivitelű és alakú létrákat használnak, de minden létrának ki kell elégítenie az általános műszaki követelményeket.

„A tagokba 19 létrafokot építettek be, teljesen kihúzott állapotban az átfedés 5 foknyi. A létra működése megegyezik a régi típusú kihúzós létra működésével." [5] Az új típusú kihúzólétre az F 619-es. A létra alaphossza 5810 mm, kihúzható hossza 10 méter, a tömege 41 kg, és támrudakkal nem rendelkezik.

A Gyöngyösi Katasztrófavédelmi Kirendeltség tulajdonában található – csak a toronyház kivételes magassága miatt – egy IVECO MAGIRUS DLK, ami 37,5 méterig használható.

Kézi tűzoltó készülékek

Kézi tűzoltó készülékek azok az eszközök, amelyek oltóanyagot tartalmaznak nyomás alatt, így a tűzre tudjuk juttatni az oltó anyagot úgy, hogy irányítani tudjuk azt. Úgy tudjuk eldöntetni, hogy mikor melyik készüléket használjuk egy adott helyen, hogy mindig az adott funkciót kell figyelembe venni. Ezek a kézi készülékek működési elveik szerint két csoportra oszthatók. Az egyik ilyen csoport, mikor az égést tápláló oxigént zárja el a kiáramló oltóanyag; ilyen a porral oltó, a vízzel oltó és a habbal oltó készülék. A másik pedig, mikor a gyulladási hőmérséklet alá csökkenti az égő anyag hőmérsékletét; ebbe a csoportba tartozik a szén-dioxiddal oltó és a halogéngázzal oltó készülék. Csoportosítani tudjuk ezeket a készülékeket az oltóanyag, a hajtóanyag, a hajtóanyag tárolása alapján és nagyság szerint. A jelenleg használt kézi tűzoltó készülékek: vízzel oltó tűzoltó készülékek; porral oltó tűzoltó készülékek; habbal oltó tűzoltó készülékek; halonnal oltó tűzoltó készülékek; szén-dioxiddal oltó tűzoltó készülékek.

Szűrőbetétes gázvédő eszközök

A mai gázálarcok már komfortos anyagból készülnek és nagyon alacsony súlyúak, ami megkönnyíti a viselésüket. Alacsony légzési ellenállásúak, és a beszélgetés is sokkal érthetőbb az álarcokban, mint az elődeik esetében. A beavatkozásnál is nagy előnyt jelent, hogy párásodásmentes kialakítású az ablaka, ezért a látás is tökéletes az álarcban.

Járművek

A legalapvetőbb eszközök, amelyek segítségével a tűzoltóegységek a helyszínre érkeznek. Számos változatuk ismert: a különböző terepekre, célokra más és más járművek léteznek. Jelenleg számos gyártó kínálja a legkülönfélébb felépítményeket a tűzoltóságok számára, ezek kiválasztása a szakemberek feladata, ám több esetben gátat jelenthetnek az anyagiak.

„A tűzoltószivattyúk motorizációjának és kerekekre építésének hőskorában fecskendő, ezt követően kocsi fecskendő, napjainkban gépjárműfecskendő, köznapi nyelven tűzoltó autó." [6] A mai tűzoltó járműveket két kategóriába sorolhatjuk: gépjárműfecskendők és különleges rendeltetésű tűzoltó gépjárművek. A gépjárműfecskendőkön megtalálható minden elsődleges beavatkozáshoz szükséges eszköz, így például a műszaki mentéshez szükséges eszközök, a védő- és mászóeszközök és az oltóanyagok is fellelhetőek az autón.

A gépjárműfecskendőket négy kategóriába sorolhatjuk az oltás intenzitása szerint: könnyű, közepes, nehéz és félnehéz. Egy gépjárműfecskendőbe 6 fő fér el, így ez egy teljes rajnak felel meg. A különleges gépjárművek két fővel állnak készenlétben. Ezek a járművek az emelőkosaras gépjármű, a porral és habbal oltó és a műszaki mentőszer. Az ilyen autók kezeléséhez speciális szakmai képzettség szükséges. A porral oltó gépjárművek oltási távolsága 4-5 méter pisztollyal, ágyúval pedig a 30-50 métert is eléri. A habbal oltó gépjármű a tartályában csak habképző anyagot szállít, ezáltal az annak előállításához szükséges vizet az oltás helyszínén kell biztosítani. A por- és habszereket a tűzoltóságok tartályparkok védelmére, veszélyes anyaggal vagy áruval foglalkozó ipari tevékenységek védelmére is használják. [7]

A műszaki mentési és a tűzoltási feladatokat gyakran együtt kell megoldani, egymást kiegészítve vagy egymást követve. Az alkalmazott technika is ennek megfelelően kerül készenlétbe helyezésre, így a gépjárművek többsége mindkét tevékenység végzésére használható. A műszaki mentőszeren található szükséges eszközök: hidraulikus vágó-feszítő mentőkészülék; pneumatikus emelőpárna; benzinmotoros gyorsdaraboló; benzinmotoros láncfűrész; benzinmotoros kőfejtő kalapács; hegesztő- és vágókészülék; univerzális kézimentő szerszámkészletek; emelőgépek, csörlők; légzőkészülék és védőruha.

Magas épületek tűzoltó-taktikai jellemzése

Amikor fellendült a középmagas és magas házak építése, a tűzvédelmi műszaki követelmények is kidolgozásra kerültek. A szabvány előírásait azonban esetenként a beruházók gazdaságossági okokra hivatkozva csak részben hajtották végre.

Ebből súlyos tűzvédelmi hiányosságok keletkeztek. Ilyenek például, hogy többek között

- a lépcsőházi füstelvezetésről nem gondoskodtak,
- a menekülési útvonalakon éghető anyagú beépített szekrényeket létesítettek,
- éghető anyagú technológiai csatornákat és falakat alkalmaztak,

- tűzjelzési lehetőség az újabb lakóépületeknél nem lett biztosítva,
- a tűzoltáshoz, mentéshez szükséges felvonulási területekre gépjárműparkolót terveztek és létesítettek,
- a használatbavétel után sem biztosították a tűzoltó gépjárművek részére az épületek megközelítési lehetőségét.

A fentiekben említett hiányosságok általában a használatbavételi eljárások során derültek ki. Az engedélyezési eljárásokban többségében mellőzték a tűzvédelmi hatóságok közreműködését. E problémákat akkor oldották meg, mikor Csertő utcai baleset bekövetkezett. Ezt követően több szabványrendelet került kiadásra, ami a hiányosságokra világított rá, ezért a kiadott rendeleteknek megfelelően mindenütt megtörtént az utólagos tűzvédelmi munkák felmérése. Az állami tűzoltóságoknak viszont további erőfeszítéseket kellett tenniük a korábbi években elkövetett hibák, hiányosságok végleges felszámolására. A magas épületeknél még jelenleg is megtalálható főbb tűzvédelmi hiányosságokról szólunk a következőkben.

A kiszolgáló úthálózatok vezetése akadályozza a mentésre érkező gépjárműveknek az adott helyzethez szükséges mozgását. A parkolóhelyek helytelen kijelölése miatt a parkoló gépjárművek akadályozzák a tűzoltási terület megközelítését, elfoglalását és a tűzcsapok igénybevételét. A speciális tűzoltó gépjárművek mozgatása és üzemeltetése is akadályba ütközhet, például lépcső közbeiktatása vagy lejtős út miatt. A villamos elosztók, a fogyasztást mérő szekrények a menekülési útvonalakon éghető anyagokból vannak kialakítva. A terepadottságok miatt a különleges mentő erők, helikopterek, gépjárművek alkalmazása nem lehetséges. Az épületekben elhelyezett fali tűzcsapok, a száraz vezetékek sok esetben hozzáférhetetlenek, a rendszeres karbantartásukat nem teljesítik. A füstmentesre tervezett lépcsőházak ajtói nem önműködően záródnak. A lépcsőházak és a lakások csatlakozása nincs úgy megtervezve, hogy az kizárja a lakásokból kiáramló füst közvetlen bejutását a lépcsőházba. Gyakran tapasztalható, hogy a lépcsőházakban, pincékben a rendeltetéstől eltérő a használat. Nagy problémát okoz a magas házak esetén, hogy sok ember jelenlétével kell számolni.

A tűz alatti szinteken a számításba vehető menekülési útvonalak a lépcsőházon keresztül vezetnek lefelé,. A tűz feletti szinteken a mentés bonyolultabb, viszont a lépcsőházon keresztül történő menekülés is csak a tűz keletkezését követő néhány percben lehetséges, mivel egy idő után a lépcsőház telítődik füsttel, és a benn uralkodó hőmérséklet is elviselhetetlené válik.

A magas épületekben keletkezett tüzek alapvető sajátossága a nagy sebességű füstképződés és az épület füsttel történő telítődése. A beépített műanyagok és egyéb éghető anyagok égése során felszabaduló égéstermékek mérgezőek, ezért az esetek nagy részében a tűz feletti szintekről is mentenek a tűzoltók. A gyakorlat igazolja, hogy az emberi életre a legveszélyesebb a füstképződés. A füstképződés esetén romlik a látótávolság is, ezáltal pánik is keletkezhet.

Következtetések és javaslatok

A világ állandóan fejlődik, ezáltal napjainkban is folyamatosan épülnek újabb és újabb technikával magas épületek, amit még a 1960-as és 1970-es években is hatalmas megdöbbenéssel és figyelemmel kísértek az emberek, manapság pedig természetes a számunkra, hogy a fejlődő világ minden részén épülnek monumentális építmények.

Mivel a gyöngyösi toronyház az 1970-es években épült, ebből adódóan az épület az akkori követelményeknek megfelelően került kivitelezésre. Ez bizonyos mértékben lefedi a jelenleg hatályos jogszabályi előírásokat, azonban a tűzvédelmi jogszabályok jelentős változása miatt komoly eltérések vannak az akkori és a jelenleg hatályos jogszabályi előírások között. A ház építésénél a középmagas és magas épületek tűzrendészeti előírásáról szóló 5/1965. számú BM TOP ágazati szabványt alkalmazták. Az ágazati szabványban megtalálhatóak a külföldi tapasztalatok figyelembevételével azok a tűzvédelmi követelmények, amelyeket a fontos élet- és vagyonvédelmi szempontok megfontolása után, tervezéskor, építéskor és üzemeltetéskor figyelembe kell venni.

A fejlesztésére a pénzügyi források igen szűkösek, ezért a lakók több esetben háttérbe helyezik ezeket a felújításokat. Megfelelő pénzügyi hátteret véleményünk szerint állami pályázatokon való részvétellel lehet elősegíteni. Ilyen témájú pályázatok jelenleg nincsenek. A legutolsó ilyen jellegű pályázat – melynek tűzvédelmi vonatkozásai is vannak – a panelprogram volt, amelynek során az épületek külső homlokzati hőszigetelésére lehetett pályázni. Több példa mutatja, hogy ezen pályázatoknál az aktív tűzvédelmi rendszerek felújítására is jutott a pénzügyi erőforrásokból.

Figyelemmel kell lenni az ajtók működésére is, mivel logikus, hogy a nyitott tűzgátló ajtó nem teljesíti feladatát. Ezáltal szükség van hidraulikus csukó szerkezetre, ami vezérléssel képes bezárni az ajtót. Tehát a fentiekben olvasottak alapján erre a fejlesztésre is szükség lenne. [8]

Jelentős fejlesztést lehetne még a tűzjelző berendezések felújítása, mivel az elavultnak számító MMG-rendszer helyett egy korszerűbb, intelligens tűzjelző központ és berendezés létesítése lenne indokolt. A korszerű rendszerek a tűz pontos helyét is képesek megmutatni, továbbá közvetlen jelzés leadása is lehetséges lenne a tűzoltóság ügyeletére, amivel a riasztási idő jelentősen csökkenhetne. A tűzjelző rendszerrel lehet vezérelni a hő- és füstelvezetést, azaz a ventillátorokat, a hő- és füstelvezető ablakokat. Ilyen például a SUTTY és a GST5000. A GST5000 központot az EN 54-2 szabvány követelményeinek betartásával fejlesztették ki, és figyelembe vették az egyszerű telepítés, üzemeltetés és karbantartás szempontjait. A központot két hurokkal szállítják, a hurkok száma modelltől függően maximum 4-ig, illetve 20-ig bővíthető. Az első hurokra 237, a többi hurokra pedig 241 címezhető eszközt lehet csatlakoztatni, ilyenek lehetnek például a hőérzékelők, a füstérzékelők és a kézi jelzésadók. [9]

A toronyházba beépíthetők lehetnének még a hagyományos optikai füstérzékelők is, ezek már két vezetéken keresztül kommunikálnak a tűzjelző központtal.

A kézi jelzésadók beépítése is nagy előrelépést jelente a toronyház számára. Ezek a

berendezések nagyon egyszerűen kezelhetőek. A legelterjedtebbek a KAC kézi jelzésadók, működésük egyszerűségéből adódóan. [10]

A hangjelzés fontosságáról sem feledkezhetünk meg, mivel ha éjszaka történik egy tűzeset, a lakóknak erről mielőbb értesülniük kell, hogy időben elhagyhassák az épületet. Napjainkban már újabbnál újabb típusú, hangjelzéseket előállító eszközök, berendezések léteznek.

Sajnos ezeket a fejlesztéseket a közeljövőben nem lehet megoldani, mivel jelentős költséggel járó beruházások lennének, amit nem támogatnának a lakók. A lehetséges megoldás a már említett pályázatok, illetve az állami erőforrások alkalmazása lehetne.

Irodalomjegyzék

[1] Az „új" Országos Tűzvédelmi Szabályzat. Védelem.hu, http://www.vedelem.hu/files/UserFiles/File/konf2008/otsz/otsz_beav.pdf (letöltés: 2012. 04. 06.)

[2] Tűzoltásnál alkalmazott létrás szerek. Kalászi Tűzvédelmi Kft., http://kalaszituzi.uw.hu/muszakiismeret.pdf (letöltés ideje: 2012. 04. 05.)

[3] Biczó István – Minárovics János – Polgár Mihály – Szőke István – Tarján Rezső: Tűzoltófelszerelések. Belügyminisztérium Országos Tűzrendészeti Parancsnoksága, Budapest, 1960.

[4] Zemplén István: Műszaki mentések. BM Könyvkiadó, h. n.,1988, ISBN: 963-7703-276

[5] Tűzoltásnál alkalmazott létrás szerek. Kalászi Tűzvédelmi Kft., http://kalaszituzi.uw.hu/muszakiismeret.pdf (letöltés ideje: 2012. 04. 05.)

[6] Tűzoltó gépjárművek. Lánglovagok on-line, http://www.langlovagok.hu/html/azs/43.shtml (letöltés ideje: 2012. 04. 05.)

[7] Bognár Balázs – Kátai-Urbán Lajos – Kossa György – Kozma Sándor – Szakál Béla – Vass Gyula: Iparbiztonságtan I. Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. Szerk.: Kátai-Urbán Lajos. Budapest, Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 564 p., ISBN:978-615-5344-12-1

[8] Építészeti tűzvédelem – elméleti kérdések, http://dio.uw.hu/letott/kidodozva.pdf (letöltés: 2012. 04. 12.)

[9] GST5000 Intelligens tűzjelző központ telepítési kezelési leírása. Multialarm Kft., http://multialarm.hu/pdf/kereskedelem/termekek/tuzjelzo/GST5000_v1_hun.pdf (letöltés ideje: 2012. 04. 12.)

[10] Tűzjelző kézi jelzésadók és kézi oltásindítók. Elektrowill Kft., http://www.elektrovill.hu/download/KAC_kezi.pdf/KAC_kezi.pdf (letöltés ideje: 2012. 04. 13.)

The rescue fire protection of tower blocks – case study

Morvai Cintia

The rescue fire protection of high-rise buildings has always been a major task of fire departments. The case study of the tower block in the town of Gyöngyös shows that rescue equipment and gear has undergone considerable technological development in the last 40 years since the tower block was built. In this article I lay down guidelines for the development of the fire protection system in the high-rise building specifying certain fire safety deficiencies, while also making suggestions for the installation of new fire protection equipment.

Keywords: tower block, rescue fire protection, technical development, high building, rescue