Óbudai Egyetem

Doktori (PhD) értekezés tézisfüzete

Elektronikus megfigyelő-, és ellenőrző rendszerek objektumorientált kialakítása különös tekintettel a biztonsági kockázatok rendszerére

Témavezető:
Prof. Dr. Kovács Tibor CSc / PhD

Biztonságtudományi Doktori Iskola

Budapest, 2018.

Tartalomjegyzék

Mechatronikai és Biztonságtechnikai Szimpózium, ISBN: 978-615-5018-10-7

6. HORVÁTH T., KOVÁCS T.: Possible application of thermal cameras with regard to security engineering; Hírvillám = Signal Badge 4: pp. 17-31., 2014, ISSN 2061-9499

7. HORVÁTH T., KOVÁCS T.: A hőkamerák alkalmazási területei, kiemelten a biztonságtechnikai felhasználásokban; International Engineering Symposium at Bánki – Bánki Kari Tudományos Konferencia; Konferencia helye, ideje: Budapest, Magyarország, 2011. november 15-16., Óbudai Egyetem, 13. oldal, ISBN: 978-615-5018-15-2

Szimpózium 2013., Budapest, Magyarország, 2013. április 10., Óbudai Egyetem, 10. oldal (ISBN: 978-615-5018-53-4)

6.2. További tudományos közlemények

További saját publikációk listája, folyamatos számozással.

2. HORVÁTH T., KOVÁCS T.: Létfontosságú rendszerek és létesítmények védelme, üzemeltetői biztonsági terv a gyakorlatban; Biztonságtechnikai Szimpózium a Magyar Tudomány Ünnepe 2013 keretében: Bánki közlemények, Konferencia helye, ideje: Budapest, Magyarország, 2013. november 12-19., Óbudai Egyetem, 1-10. oldalak, ISBN: 978-615-5018-89-3

3. HORVÁTH T.: Kábelek, hálózatok, CCTV rendszerek; Hadmérnök VI: (3), 5-13. oldalak, 2011, ISSN 1788-1919

4. HORVÁTH T.: Korszerű kerítésvédelem; Hadmérnök VI: (3), 14-21. oldalak, 2011, ISSN 1788-1919

5. HORVÁTH T., KOVÁCS T.: Zsetonok és IP kamerák – a játéktermek biztonságtechnikájának egyes kérdései, Konferencia helye, ideje: Budapest, Magyarország, 2010. november 10-11., Óbudai Egyetem, 11 oldal, Nemzetközi Gépész,

SUMMARY

Object oriented design of electronic surveillance and control systems with special regard to structure of the physical security risks

PhD thesis

by Tamás Horváth

Existing protection systems have to be occasionally and regularly reviewed and audit by owners and operators due to dynamically changing security risks and environments. These revisions are usually completed by the leading companies and nationally and commercially firms and institutions whom really work with sensitive data. However they do not have a uniformly agreed system of policies in above of this they should rely on security experts' advice meanwhile the balanced and risk-based security requirements can't really be controlled. Lack of specialized standards and design principles could also make difficult situations for professionals in convincing owners and operators to improve of the existing physical protection systems meanwhile not any the company representatives charged in security activities, corporate security officers, can't find real reason for the improvement of it which means that senior financial officers of the companies would decide on security questions focusing on immediate financial interest of

them only. In long run these only economy-based decisions could make difficulties for physical protection systems.

During my work, I have found that the evaluation of the suitable security systems (intrusion detection, access control and video surveillance systems) which should be installed or have already been installed at different security risk level facilities are not uniformly solved today. The question is whether these systems meet professional-client expectations while also being able to handle the safety risks of facilities. It is possible to make out various security audits, but checks and reviews, notably from a security point of view, are not the same. No general-purpose object-specific design and implementation principles are available. Development of a unified system of requirements could provide a determined support for both the clients and the designers at the same level of expectations. At the same time it is a useful help to the operators to identify possible modifications, security enhancements, directions and details as a result of updating the security risks.

One of my main motivations for my research is that for those facilities for which security risks require it, I should work out a well-traceable and usable risk assessment method related safety engineering system directly. The system and assessment proposal I worked out it would be familiar with the flexibility market needs and the expectations.

23. Uptime Institute LLC. Datacenter Site Infrastructure Tier Standard: Topology
LLC UPTIMEINSTITUTE – 2012
pdfs.semanticscholar.org
letöltve: 2016. február 10. **[23]**

24. Az IEC/ISO 31010:2009 Risk management. Risk assessment techniques magyar nyelvű változata, MSZ EN 31010 (2010), Kockázatkezelés. Kockázat felmérési eljárások. **[24]**

25. HARMADOS Gy.: Gazdasági hírszerzés és ipari kémkedés, Detektor Plusz 2006/8-9.
www.detektor.siteset.hu/fajl.php?id=8277
letöltve: 2017. február 20. **[25]**

26. 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1100190.kor
letöltve: 2017. február 20. **[26]**

6.1. A téziskehez kapcsolódó tudományos közlemények

1. HORVÁTH T., KOVÁCS T.: Kockázatértékelési módszerek, azok alkalmazási lehetőségei a fizikai védelem területén; Tavaszi Biztonságtechnikai

19. MOTEFF, J., PARFORMAK, P.: Critical Infrasturcture and Key Assets: Definition and Identification; October 1, 2004 file:///C:/Users/B5596/Downloads/ADA454016.pdf letöltve: 2016. szeptember 30. **[19]**

20. IZSÓ L.: SOL. Safetyafety through Organizational. Learningearning. Tengelic, november pszichológia előadás 2. http://docplayer.hu/33819749-Sol-safetyafety-through-organizational-learningearning-tengelic-november-pszichologi-az-eload-2.html letöltve: 2016. október 15. **[20]**

21. Skálatípusok. http://ramet.elte.hu/~kún.adam/oktatas/biometria8.pdf letöltve: 2017. március 1. **[21]**

22. TATAY T., PATAKI L.: Kockázatelemzés, Kockázatértékelés, cselekvési tervek; 2008. december, Raabe Kiadó www.spek.hu/letoltes.php?fajl=anyagok/Tatay-Pataki-kockazatelemzes.pdf letöltve: 2016. szeptember 4. **[22]**

During my work, at first I created a risk assessment methodology which could provide the required support for the design of security systems.

At second I could prove that each of the facilities can be classified in for security risk levels or categories.

I have proved that the method I had developed is object-oriented in design of the physical protection system and the classification corresponding to each security risk category.

1. A kutatási előzményei

A munkámból adódóan, hosszú évek óta kerülök szembe azzal a problémával, hogy a biztonságtechnikával foglalkozó szakemberek, a megbízásaik során vagy nem készítenek, vagy nem kapnak az adott létesítmény biztonsági kockázatait értékelő irányadó dokumentációt, amely pedig tervezéskor szükséges. Amennyiben mégis akad ilyen, akkor az általában az elkészítés időpontjában lehetett aktuális és nélkülözi a könnyen „up-to-date” szinten tartás lehetőségét (az elkészített tervek, iránymutatások „kőbevésettek” és rugalmatlanok). Ipari és kereskedelmi létesítmények esetén igen gyakran még egy megalapozott objektumvédelmi tervet sem lehet fellelni, főként akkor, ha arra semmilyen hatósági rendelkezés nincs, vagy nem volt.

A kutatásom egyik fő motivációja az, hogy azon létesítmények számára, amelyek esetében a biztonsági kockázatok azt megkövetelik, egy jól követhető és használható kockázatértékelési módszert és ahhoz közvetlenül kapcsolódó biztonságtechnikai rendszerkialakítási elvet fogalmazzak meg, valamint az általam szolgáltatott rendszer és értékelési javaslat kellő rugalmassággal le tudja követni a piaci igényeket, elvárásokat.

További motivációt jelentett számomra az a lehetőség, hogy egy, a nemzetközi piacon is tevékenykedő nagyvállalat környezetében az általam kialakított követelményrendszer tesztelhető és bevezethető lehet.

Nem feledkezhetem meg arról sem, hogy a kutató munkám során összeállított rendszer informatikai támogatással akár piaci termékké is fejleszthető, hiszen a követelményrendszer adatbázisba szervezhető, szükség esetén bővíthető.

14. MABISZ Betöréses lopás- és rablásbiztosítás technikai feltételei (Ajánlás)
Telephelyek és létesítmények, helyiségek őrzésének, vagyontárgyak tárolásának, szállításának szabályai: 2015. április 24.-módosítás
http://www.pluto.hu/_A/A2.html
letöltve: 2016. február 15. **[14]**

15. IAEA International Training Course on the Physical Protection of Nuclear Material and Nuclear Facilities (2016. november 11.-22.), Albuquerque, NM, USA **[15]**

16. HORVÁTH T., KOVÁCS T.: Kockázatértékelési módszerek, azok alkalmazási lehetőségei a fizikai védelem területén; Tavaszi Biztonságtechnikai Szimpózium 2013., Budapest, Magyarország, 2013. április 10., Óbudai Egyetem, 10. oldal (ISBN: 978-615-5018-53-4) **[16]**

17. Mark-Recapture Maximum Likelihood Estimators adapted from Seber et al. 1982 (page 200) and Burnham et al. 1987 (page 114) for CJS models
studylib.net/.../calculation-of-detection-probabilities-adapted-from-bu..
letöltve: 2017. július 3. **[17]**

18. WHITH, J. M.: Security Risk Assessment, Managing Physical and Operational Security, ISBN: 978-0-12-800221-6; 206. oldal **[18]**

http://uni-nke.hu/downloads/bsz/bszemle2006/2/06%20Utassy-Barkanyi.pdf
letöltve: 2016. október 12. **[10]**

11. The evolution of access control systems
http://securecomminc.com/2014/06/19/the-evolution-of-access-control-systems/
letöltve: 2017. augusztus 1. **[11]**

12. The evolution of access control
https://www.isonas.com/news-education/the-evolution-of-access-control/
letöltve: 2017. augusztus 2. **[12]**

13. HORVÁTH T., KOVÁCS T.: Kockázatértékelési módszerek és lehetőségeik a fizikai védelem területén
http://www.securinfo.hu/termekek/biztonsagi-szolgalat-az-eloero-eszkozei/978-kockazatertekelesi-modszerek-es-lehetosegeik-a-fizikai-vedelem-teruleten.html
letöltve: 2017. július 1. **[13]**

2. Célkitűzések

a. Létrehozni egy olyan, a biztonsági kockázatokat értékelő módszert, amely elsősorban a biztonságtechnikai rendszerek tervezéséhez ad támogatást.

A létező kockázatértékelési módszerek közül olyan módszer kiválasztásának van létjogosultsága, amely a megbízó és a megbízott számára is könnyen követhető, jelentős véleményeltérésre okokat nem szolgáltat. Az elsődleges szempontok között kell szerepelnie a generális látásmódnak, amely az adott létesítményeket struktúrában vizsgálja, és a tágabb környezet, társadalmi beágyazódottság ugyanakkora súllyal jelenik meg az értékelésben, mint a belső működési struktúra, személyi feltételek és a minősített adatállomány, vagy a specifikus informatikai hálózat.

b. Az egyes létesítmények biztonsági kockázatok alapján történő besorolása egy olyan rendszerbe, amelyben ezek biztonsági kockázatai megjelennek egy létesítményi együttható formájában.

A biztonsági kockázatok alapján történő létesítmény-besorolás egységes módszere jelenleg nem létezik. Az elszigetelt, egyedi kockázatértékelések nem teszik összehasonlíthatóvá az egyes létesítmények biztonsági kockázatait, így a biztonságtechnikai rendszerek kivitelezésére felhasznált pénzügyi erőforrások felhasználása sem hatékony.

Egy adott létesítmény biztonsági besorolása jelentős támogatást biztosíthat más biztonsági szakterület (például a munkavédelem) számára is. Létesítményi jellemzőként figyelembe véve a besorolást a nagyvállalatok esetében a munkavédelmi tevékenység összehasonlíthatóvá válhat a különböző veszélyességi környezetben tevékenykedő társaságok esetén is.

c. ***Megalkotni egy objektív, a biztonsági kockázatokra épülő tervezési segédletet, amely támogatást adhat a biztonságtechnikai rendszerek tervezéséhez, kialakításához.***

Egy felhasználóbarát tervezési segédletet mind a megbízó, mind a megbízott könnyen értelmez, a tervezett költségvetés tételeinek ellenőrzése ezáltal áttekinthetővé válik.

3. Vizsgálati módszerek

A primer kutatás során áttekintettem azokat a fellelhető szakkönyveket, amelyek a számomra releváns információkkal szolgálhattak a téma feldolgozásában.

Kutatási munkámat a szekunder fázisban kiterjesztettem a szakkönyvek mellett a szakirodalmi hivatkozások felkutatására. Ennek során elsősorban az Internetes minősített szakanyagokat és természetesen magát a hivatkozott publikációkat tekintettem át, majd a nagyobb külföldi könyvforgalmazók szakkönyv kínálatát, illetve a

5. The history of Home security
https://www.livewatch.com/history-of-home-security
letöltve: 2017. június 30. **[5]**

6. The history of the alarm system
https://www.abus.com/eng/Guide/Break-in-protection/Alarm-systems/History-of-the-alarm-system
letöltve: 2017. június 2. **[6]**

7. KISS S.: A biztonságtechnika kialakulásának történetéről; Hadmérnök, X. évfolyam, 4. szám, 2015. december, 24-29. oldalak, ISSN 1788-1919 **[7]**

8. SANS Institute InfoSec Reading Room: The history and evaluation of Intrusion detection, SANS Institute 2001
https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344
letöltve: 2017. április 15. **[8]**

9. PAPP P.: IP a biztonságtechnika világában
http://www.detektor.siteset.hu/fajl.php?id=8267
letöltve: 2017. július 1. **[9]**

10. UTASSY S., BÁRKÁNYI P.: IP alapú kommunikáció az elektronikus vagyonvédelmi rendszerekben;

6. Irodalmi hivatkozások listája

A felhasznált szakirodalmi hivatkozások.

1. GARCIA, M. L. (Sandia National Laboratories): Vulnerability and assessment of physical protection systems, ISBN13 978-0-7506-7788-2 (2001) **[1]**

2. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No.13 (INFCIRC/225/Rev.5) http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf letöltve: 2015. február 18. **[2]**

3. GARCIA, M. L.: Design and Evaluation of Physical Protection System (PPS), ISBN-13: 978-0-08-055428-0 (Kindle Location 230), Elsevier Science, Kindle Edition **[3]**

4. Interagency Security Committee Guide 2015 December *https://www.dhs.gov/.../isc-planning-managing-physical-security-reso...* letöltve: 2016. február 20. **[4]**

szakmai tevékenységem során ismertté vált társaságok nyilvánosan fellelhető anyagait.

A szakmai publikációk és szakkönyvek felkutatása és tanulmányozása mellett lehetőségem volt - a kockázatértékelési módszerek között válogatva - a fizikai védelmi rendszerek számára jól használható módszert kiválasztanom és bemutatnom a társaságunk által szervezett szakmai ülésen, a kritikus infrastruktúra fizikai védelmének gyakorlati megvalósításáról tárgyban „Üzemeltetői Biztonsági Terv[1], de a gyakorlatban hogyan?” címmel.

A tercier kutatási szakaszban, lehetőségem volt a nem publikus, az üzleti szempontból érzékeny adatokat tartalmazó, az MVM Magyar Villamos Művek Zrt. vállalatcsoportban érvényben lévő szabályozási rendszert is áttanulmányozni.

4. Új tudományos eredmények

a) Elsőként létrehoztam egy biztonsági kockázatokat értékelő módszert, amely biztonságtechnikai rendszerek tervezéséhez ad támogatást.

---

[1] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.) az a jogszabály, amely az Üzemeltetői Biztonsági Terv tartalmi követelményeit tárgyalja.

b) Bebizonyítottam, hogy az egyes létesítményeket elegendő négy biztonsági kockázati kategóriába sorolni.

c) Igazoltam, hogy az általam kidolgozott módszerrel objektumorientált módon van lehetőség - az egyes biztonsági kockázatoknak megfelelő besorolás mellett - az adott létesítmények fizikai védelmi rendszerének tervezésére, kialakítására.

5. Az eredmények hasznosítási lehetősége

Értekezésem kidolgozása során jól láthatóan körvonalazódott az a védelmi probléma, amely szerint a fizikai védelmi rendszerek működtetése minősített időszakban milyen módon változik.

Fontos lenne kidolgozni annak módszerét, hogy a normál (közhasználati kifejezéssel élve „békeidőben") időszakban meglévő biztonsági kockázatok kezelését milyen módon kellene módosítani, ha minősített időszakot jelent be a kormányzat, vagy akár a társaság biztonsági szervezetének vezetője, illetve ezen időszakban az adott létesítmény milyen biztonsági kockázatokkal szembesül és ez a változás milyen módon kezelhető az általam kidolgozott rendszerben.

Egy másik, napjainkban egyre akutabb biztonsági problémát okozó ún. drónok[2], az azok elleni védekezés fontos tanulmányozási terület lehet. Az elmúlt néhány év robbanásszerű technológiai fejlődése rendkívüli biztonsági kihívásokat állít a létesítmények fizikai védelmét üzemeltető, tervező és kivitelező társaságok elé. Nem kell sokat vizsgálódni az Internet végeláthatatlan hálóján, hogy a rengeteg nagyszerű felhasználási példa mellett néhány a robbanóanyagok, vagy kisméretű géppisztolyok szállítására és alkalmazására is megfelelő mintát találjunk. Ezek olyan eszközök, amelyek már kiemelkedő biztonsági kockázatot jelentenek. E veszélyek feldolgozása, az erre alapozott kockázatkezelési módok rendszerbe illesztése további kutatási célokat ad.

Végeredményben: a közeli jövő újabb lehetőséget teremthet egy még komplexebb, valamennyi körülményt figyelembe vevő kockázatkezelési és fizikai védelmi rendszer kidolgozásához, amelyhez ez az értekezés megfelelő alapot szolgáltat.

---

[2] „Drone" angol elnevezésből átvett szóhasználat, amely valójában egy pilóta nélküli repülőszerkezet – UAV: Unmanned Aerial Vehicle -, amely felhasználása szerint a hobbitól az ipari, hadiipari területekig megtalálható.