ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM
BOLYAI JÁNOS KATONAI MŰSZAKI KAR
KATONAI MŰSZAKI DOKTORI ISKOLA

Utassy Sándor

Komplex villamos rendszerek biztonságtechnikai kérdései

Doktori (PhD) értekezés

Témavezető: Prof. Dr. Zsigmond Gyula, egyetemi tanár

2009. BUDAPEST

TARTALOMJEGYZÉK

1. BEVEZETÉS

Komplex villamos rendszereknek nevezzük azokat a villamos rendszereket, amelyek erősáramú, gyengeáramú és irányítástechnikai alrendszereket tartalmaznak.[1] Konvencionálisan a villamos rendszerek biztonságtechnikája a túlfeszültség-védelem, villámvédelem, érintésvédelem, túláramvédelem, vonal- és hurokimpedanciák összetevőire vonatkozó méréstechnikai és kivitelezési előírásokat foglalja magába.[1]
Napjainkban a biztonságtechnika fogalma – a fentieken túl – kiterjed az objektumok (épületek) diszjunkt és integrált biztonságtechnikai (vagyonvédelmi) összetevőire, alrendszereire is.[2]
A komplex villamos rendszerek többféle aspektusból vizsgálhatóak. Az értekezés az objektumok diszjunkt és integrált biztonságtechnikai alrendszereivel foglalkozik, az ezekkel kapcsolatos kérdéseket tárgyalja.

1.1. A KUTATÁSI TÉMA IDŐSZERŰSÉGE

Az utóbbi években ugrásszerűen megnőtt és a jövőben tovább nő az új beruházások, rekonstrukciók villamos rendszereinél a biztonságtechnikai alrendszerek jelentősége és fokozódnak a velük szemben támasztott követelmények. Nagy megbízhatóságú, intelligens, széleskörű szolgáltatásokat nyújtó, az üzemeltetés, biztonságosságát és gazdaságosságát segítő rendszerekre van igény a katonai objektumoknál is.

A biztonság kérdése a rendszer determináló tényezőjévé prioritásává vált nemcsak a nagy területű, több épületből álló katonai objektumoknál, hanem egyes épületeknél is.

Egy felmérés szerint 2008-ban mintegy 73 milliárd dollárt költöttek világszerte biztonságtechnikai beruházásokra és az előrejelzések szerint ez az összeg a következő öt évben 55-60%-kal növekedni fog. Mindezek következtében az integrált

[1] A villamos biztonságtechnika megnevezése az angol nyelvű szakirodalomban „Electrical Safety”. A „safety” kifejezést az emberi életet, egészséget, környezetet fenyegető kockázatokkal kapcsolatos biztonság fogalmaként használjuk.

[2] Elektronikus biztonságtechnikai (vagyonvédelmi) rendszerek – angolul „Electonic Security Systems”. A „security” kifejezés a magántulajdon, közösségi tulajdon védelmével, biztonságával kapcsolatban használt fogalom.

biztonságtechnikai rendszerek fejlesztése jelentősen felgyorsult, külön iparággá vált. A fejlett országokban a biztonságtechnikai piac bevételének 40%-a ma már integrált biztonságtechnikai rendszerek eladásából származik.

Az integrált biztonságtechnikai rendszerekkel olcsóbban, hatékonyabban és egyszerűbben lehet garantálni a biztonságot és emellett több járulékos előnyük is van. Egy integrált rendszerrel megvalósított intelligens épület a felhasználónak nagyfokú biztonságot, gazdaságos üzemeltetést, komfortot és presztízst jelent. [2]

Az intelligens épület koncepció magába foglalja a fejlett vagyonvédelmi, tűzvédelmi szolgáltatásokat, az integrált videó és audió rendszert, a teljes körű klimatizációt, az automata nyílászárókat és árnyékoló elemeket, a digitális telefonhálózatot, az Internet elérést bárhonnan lehetővé tevő számítógép hálózatot, szelektált fogyasztásmérést-, illetve szabályozást, az automatizált szaniter készülékeket és további egyedi igényeket kielégítő szolgáltatásokat. Mindezt az erősáramú, gyengeáramú, informatikai, kommunikációs alrendszereknek komplex villamos rendszerré integrálásával lehet optimálisan megvalósítani. [3]

Az integrált épületfelügyeleti rendszerek - mint komplex villamos rendszerek - biztonságtechnikai alrendszerei különös fontossággal bírnak a katonai létesítmények, objektumok esetében.

Az épületfelügyeleti rendszer korábban az épületgépészeti rendszerek, azon belül is elsősorban a szellőzési, fűtési és klíma rendszerek felügyeletét jelentette. Ma épületfelügyeleti rendszeren integrált épületfelügyeleti rendszert értünk, amely a fentieken túl magába foglalja az épület biztonságtechnikai és kommunikációs alrendszereit is. Nagyobb objektumok egyes alrendszereinél az üzembiztonság növelése, az intézkedések gyorsítása, az események, adatok naplózása, feldolgozása, kiértékelése céljából esetenként számítógépes felügyeleti központokat alkalmaznak. Korábban az egyes alrendszerek felügyeleti számítógépei többnyire nem voltak (nincsenek) kapcsolatban egymással. Az alrendszerek között szükséges átjelzés, vezérlés napjainkban is általában adatpont szinten, feszültségmentes (relés) kontaktusokkal történik.

Az épületek erősáramú és gyengeáramú alrendszereinek integrálása több irányból is megindult.

Egyik oldalról az egyes alrendszerek gyártói, fejlesztői igyekeznek más alrendszereket beintegrálni felügyeleti rendszereikbe.

- Korábban épületfelügyeleten többnyire az épületgépészeti automatikai rendszerek felügyeleti szoftverét értették. Ezek a szoftverek ma már nemcsak az adott gyártó cég berendezéseinek felügyeletét látják el, hanem más („vendor") cégek eszközeinek, berendezéseinek integrálására is képesek. [4]
- Ugyancsak integrátor (protokoll konverter) modulok alkalmazásával több épületautomatikai cég is alkalmassá tette az épületgépészeti automatikai rendszerek felügyeletére készült szoftverét más, többnyire tűzjelző központok beintegrálására is. [5]
- A vagyonvédelmi, biztonságtechnikai rendszerek gyártói előbb a nagyobb, moduláris, de ma már a kisebb behatolás jelző központoknál is beépítenek beléptető rendszer funkciókat, egyetlen rendszerbe integrálva a behatolás jelző és beléptető alrendszereket. Ezekhez a központokhoz számítógépes felügyeleti szoftverek is tartoznak.
- A zártláncú TV rendszerek telepítésekor gyakran felmerül más biztonságtechnikai alrendszerekkel (tűzjelző, beléptető, áruvédelmi) történő összekapcsolás igénye. Ilyen jellegű integrálás is megfigyelhető.
- Egyes cégek más célra fejlesztett, például tűzjelző rendszerüket és felügyeleti szoftverüket fejlesztették tovább más, például behatolás jelző vagy beléptető rendszer kezelésére is.

Másik oldalról az információ technológiával foglalkozó, szoftver rendszereket fejlesztő cégek kínálnak univerzális intelligens épületmenedzselő megoldásokat.

- Ezek a felügyeleti rendszerek többnyire valójában nem integrált rendszerek, hanem különböző cégek egyedi alrendszereit fogják össze, többnyire az alrendszerek központjaival kommunikálva. Az egyes alrendszerek egyedi, de általában szabványos kommunikációs interfészekkel rendelkeznek. [6]

- Más cégek komplex „facility management” rendszereket kínálnak, amelyeknek része az egyes gyengeáramú alrendszerek felügyelete is. [7]

Az „igazi” intelligens épület koncepciót, amelynél az egyes alrendszerek már nem elkülönülve, hanem valóban integrálva jelennek meg, ma még kevés „integrált épület-felügyeleti rendszer” valósítja meg.

1.2. A TUDOMÁNYOS PROBLÉMA

A különböző gyártók által kifejlesztett biztonságtechnikai alrendszerek egzakt módon történő minősítése, összehasonlíthatósága a tervező, a beruházó és a felhasználó számára egyaránt fontos. Különösen a tervezési fázisban, főleg már meglévő biztonságtechnikai rendszerek bővítésekor, integrálásakor lenne fokozott jelentősége az egyes tervezési alternatívák összehasonlíthatóságának.

A minősítés, összehasonlítás alapvető jellemzőinek, például az egyes diszjunkt biztonságtechnikai alrendszerek komplexitásának, vagy az integrált rendszerek integráltság fokának és ezzel korrelációban a megbízhatóságra, gazdaságosságra, biztonságra vonatkozó paramétereknek a meghatározására a szakirodalomban nincsenek kidolgozott eljárások, eszközök.[3]

Hiányoznak az alrendszerek komplexitásának meghatározásához szükséges kvantitatív és kvalitatív paraméterek, sőt eddig a biztonságtechnikai elemek, összetevők átfogó klasszifikálása sem történt meg.

Mindezek következtében hiányoznak a szakirodalomból az integrált rendszerek tervezéséhez, minősítéséhez kimunkált, ajánlott algoritmusok, modellezési eljárások.

[3] Sem a biztonságtechnikai alrendszerek, sem az integrált vagyonvédelmi rendszerek, mint komplex villamos rendszerek integráltsági fokának mutatója nincs definiálva sem a polgári, sem a katonai szakirodalomban. Ebből adódóan nincs sem számítási, sem becslési modell az integráltsági fok számítására.

A komplex rendszerek leírására, ezen belül a komplexitás modellezésére más területeken korábban kidolgozott elvek, módszerek adaptálása a specifikus biztonságtechnikai alrendszerekre csak részben lehetséges. [4]

A bonyolult gráf/mátrix leképzések a különböző rendszerek összehasonlításánál – többek között a biztonságtechnikai ajánlások, szabványok változásai miatt – a gyakorlatban nem igazán használhatók.[5]

(Azok az egyszerűsített makroszintű vizsgálati modellek viszont, amelyek a rendszer-architektúrák kvantitatív paramétereiből határozzák meg a vizsgált alrendszer determináló tulajdonságát, a komplexitást, a kutatómunka során a gyakorlatban is alkalmazhatónak bizonyultak. A diszjunkt alrendszerek komplexitásának ismeretében pedig a két vagy több alrendszerből álló integrált rendszer integráltsági jellemzője viszonylag könnyen meghatározhatóvá vált. A tudományos problémát és a kutatási célkitűzéseket a közel húsz évet átfogó biztonságtechnikai oktatói és tervezői tevékenységem elméleti és gyakorlati tapasztalatai alapján fogalmaztam meg.)

[4] Ilyenek elsősorban a számítógépes programok bonyolultságának, komplexitásának számítására kidolgozott modellek.

[5] A MABISZ (a Magyar Biztosítók Szövetsége) biztonságtechnikai ajánlásai, amelyek a biztonságtechnikai tervezők alapvető kiindulási dokumentumai, 2007-ben alapvetően megváltoztak. Az addigi technikai/gazdasági jellegű kritériumokat a biztonságtechnikai szabványokkal jobban összhangban lévő ajánlás váltotta fel. [8]

1.3. KUTATÁSI CÉLKITŰZÉSEK

Az értekezés célja olyan makroszintű vizsgálatokat lehetővé tevő matematikai modell kidolgozása (felállítása), amellyel lehetővé válik a diszjunkt biztonságtechnikai alrendszerek komplexitásának számítása, valamint a két vagy több alrendszer integrálásával létrejött komplex rendszer integráltsági jellemzőjének meghatározása.

A kutatási cél elérése érdekében az alábbi részcélokat jelöltem meg:

1. A komplex villamos rendszerek specifikus biztonságtechnikai összetevőinek, alrendszereinek áttekintő rendszerezése.

2. A biztonságtechnikai alrendszerek integrálási lehetőségeinek, az integrált rendszerek tervezési folyamatának leírása, a rendszerek integrációs típusainak osztályozása.

3. Matematikai modell kidolgozása a biztonságtechnikai alrendszerek komplexitásának meghatározására, és a biztonságtechnikai alrendszer-modellekben szereplő eszközök kvantitatív és kvalitatív jellemzőinek definiálása, gyakorlati értékeik meghatározása.

4. Próbaszámítások végzése katonai és polgári objektumok biztonságtechnikai alrendszereinek komplexitás-meghatározására.

5. Definíció adása és matematikai modell kidolgozása az integrált biztonságtechnikai rendszerek integráltsági jellemzőjének meghatározására.

1.4. KUTATÁSI HIPOTÉZISEK

A kutatási téma vizsgálatánál az alábbi hipotéziseket állítottam fel:

1. A komplex villamos rendszerek biztonságtechnikai alrendszereinek leírására, ezen belül a komplexitás számítására matematikai eljárások alkalmazhatók.

2. A biztonságtechnikai alrendszer-architektúrák kezelésére meghatározhatók olyan specifikus (kvantitatív és kvalitatív) mutatók, amelyek figyelembevételével az alrendszerek komplexitása számolható.

3. Az integrált biztonságtechnikai rendszereknél az integráltság foka meghatározható, számszerűsíthető.

4. Adott katonai és polgári objektumok biztonságtechnikai rendszereinél az alrendszerek integrálásával a rendszer komplexitása csökkenthető.

1.5. KUTATÁSI MÓDSZEREK

A kutatási célok eléréséhez az alábbi kutatási módszereket alkalmaztam:

1. Tanulmányoztam a témával kapcsolatos írott és elektronikus szakirodalmat, szabványokat, ajánlásokat, esettanulmányokat. Ezek feldolgozása, rendszerezése során alapvető módszerként az adaptációt alkalmaztam.[6]

2. A komplex villamos rendszerek specifikus biztonságtechnikai összetevőinek, alrendszereinek áttekintő rendszerezéséhez felhasználtam a több évtizedes

[6] A tématerületen rendelkezésre álló szabványokra, a magyar és főként a külföldi nyomtatott és elektronikus (Internetes) szakfolyóiratokra, a tervező, gyártó, telepítő, üzemeltető, őrző-védő cégek, illetékes hatóságok által közzétett esettanulmányokra, felmérésekre, valamint a szakmai és tudományos konferenciák anyagaira lehetett támaszkodni.

oktatói és kutatói tevékenységem során szerzett elméleti és gyakorlati ismereteimet, ennek során a taxonómiai csoportosítás, illetve összegzés eljárásait alkalmaztam.

3. A kutatómunka során megismert, feltárt, rendszerezett ismereteket, részeredményeket konferenciákon, szaklapokban és a katonai műszaki felsőoktatásban a biztonságtechnikai mérnökképzés egyes tantárgyaiban is ismertettem.[7]

4. Az ismert matematikai modellek elemzése és a biztonságtechnikai alrendszereknél alkalmazható modell kidolgozása során az analízis és szintézis módszerét alkalmaztam.

5. Folyamatos szakmai konzultációkat folytattam a szakterület hazai művelőivel.[8]

1.6. A DOKTORI ÉRTEKEZÉS FELÉPÍTÉSE

Az értekezés a kutatási téma célkitűzéseinek, a feldolgozás logikájának megfelelően épül fel.

A bevezetőben áttekintést adok a komplex villamos rendszerek biztonságtechnikai alrendszereinek integrálási folyamatáról, bemutatva a dolgozat tárgyának időszerűségét. Itt ismertetem a tudományos problémát, leírom a kutatási célkitűzéseket, hipotéziseket, az alkalmazott kutatási módszereket és végül ismertetem az értekezés felépítését.

A második fejezetben ismertetem a komplex vagyonvédelem felépítését, összetevőit és rendszerezett összefoglalását adom a komplex villamos rendszerek biztonságtechnikai alrendszereinek, azok összetevőinek.

[7] A Biztonságtechnikai mérnök szak „Személy és vagyonvédelmi rendszerek tervezése”, „Személy és vagyonvédelmi rendszerek kialakításának módszerei”, „Személy és vagyonvédelem rendszertana”, „Intelligens épületek” tantárgyak előadójaként hasznosítottam a kutató munka részeredményeit.

[8] A szakterület képviselői közül elsősorban témavezetőmmel, Dr. Zsigmond Gyula professzor úrral folytattam rendszeres konzultációkat, mellette a Tóth Attila, Móré Attila és Tóth Levente uraktól kapott szakmai információk bizonyultak igen hasznosnak.

A harmadik fejezetben átfogó ismertetést adok a biztonságtechnikai rendszerek integrálási lehetőségeiről és az integrált biztonságtechnikai rendszerek tervezési folyamatáról, elvégzem a biztonsági alrendszerek integrációs lehetőségeinek klasszifikációját.

A negyedik fejezetben elemzem a komplex villamos rendszerek integráltsági fokának becsléséhez szükséges rendszer-komplexitás leíró modelleket, kiválasztva az alkalmazható módszereket, paramétereket. Meghatározom a leggyakrabban alkalmazott biztonságtechnikai rendszerek (a behatolás jelző rendszerek és a beléptető rendszerek) komplexitásának modellezéséhez a gyakorlatban is alkalmazható paramétereket, elvégzem az egyes alrendszerek eszközeinek, moduljainek táblázatos klasszifikációját és elvégzem az egyes eszközök interfész komplexitás szorzó értékének meghatározását

Az ötödik fejezetben ismertetem az integrált biztonságtechnikai rendszerek integráltsági fokának általam adott definícióját, számítási modelljét, majd egy katonai ügyeleti objektum behatolás jelző- és beléptető rendszerének példáján bemutatom a komplexitás-mutatók és integráltsági fok meghatározásának menetét.

Az egyes fejezetek végén leírom az adott fejezetben ismertetett kutatómunka részkövetkeztetéseit.

Az összefoglalás tartalmazza a fő fejezetekben megállapított részkövetkeztetések főbb gondolatait, s azok szintéziseként a kutatás eredményeit. Itt jelöltem ki azokat a területeket, amelyek további kutatómunkát igényelnek, vagy részletes kidolgozásra alkalmasak.

A publikációs lista a témakörhöz kapcsolódó publikációimat sorolja föl, az **irodalomjegyzék** pedig részletesen tartalmazza a hivatkozott szakirodalmat.

2. KOMPLEX VILLAMOS RENDSZEREK BIZTONSÁGTECHNIKAI ALRENDSZEREI

2.1. A KOMPLEX VAGYONVÉDELEM

A komplex (erős-, gyenge-, irányítástechnikai-, informatikai- alrendszereket tartalmazó) villamos rendszerek biztonságos működése, üzemeltetése többféle aspektusból vizsgálható. Jelen dolgozat az objektumok integrált biztonságtechnikai rendszereivel (és érintőlegesen épületgépészeti rendszereivel), mint komplex villamos rendszerekkel foglalkozik.

Az egyes objektumok, épületek területén működő berendezések, szervezetek működését több kockázati tényező befolyásolja:

- A technológiai paraméterek.
- A környezeti paraméterek, hatások (hőmérséklet, nedvesség, katasztrófák).
- Emberi tényezők (hozzá-nemértés, gondatlanság).
- Szándékos károkozás (lopás, szabotázs, terrortámadás).

A dolgozat tárgyához a szándékos károkozások kockázatának csökkentésére szolgáló biztonságtechnikai alrendszerek és érintőlegesen a környezeti kockázatok csökkentésében szerepet játszható épületgépészeti rendszerek integrálási lehetőségeinek vizsgálata tartozik.

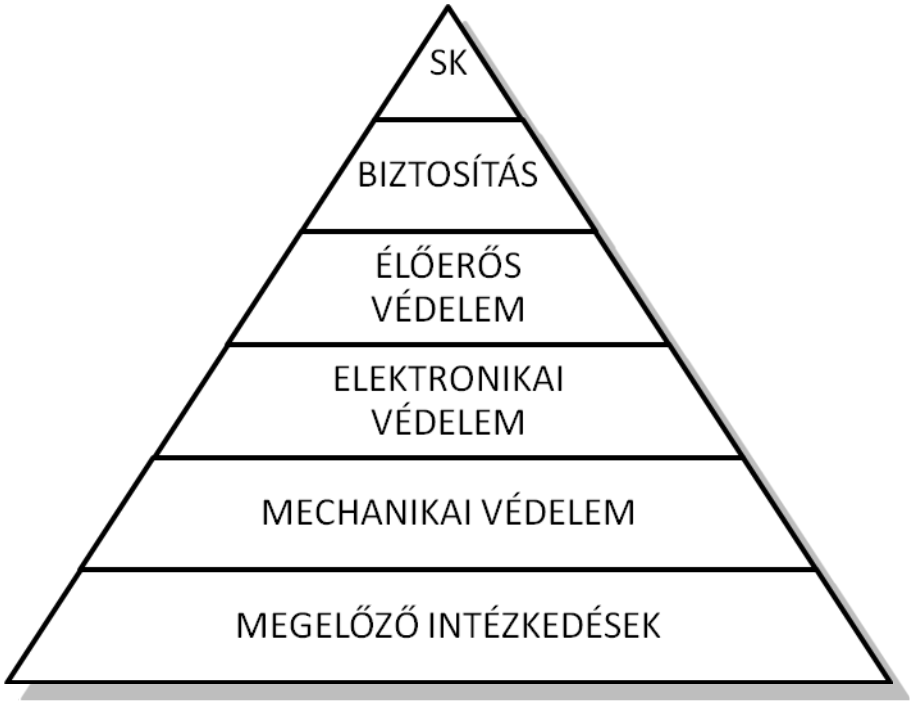
Nem foglalkozom a nem megfelelő technológiai paraméterek és a nem szándékos emberi károkozó tényezők kockázataival.

A szándékos károkozások hatékony kockázatcsökkentésének eléréséhez komplex vagyonvédelem megvalósítása szükséges.

A komplex vagyonvédelem egymásra épülő összetevőkből álló, piramisszerű rendszer. Célja a kockázatok előfordulási valószínűségének és az egyes, mégis bekövetkező kockázati események káros következményeinek minél nagyobb mértékű csökkentése,

Összetevői:

- Megelőző intézkedések.
- Mechanikai védelem.
- Elektronikai védelem.
- Élőerős védelem.
- Biztosítás.
- Saját kockázat (SK).



2.1. ábra. A komplex vagyonvédelem összetevői

A megelőző intézkedések célja a kockázatok előfordulási valószínűségének és az egyes, mégis bekövetkező kockázati események kárkövetkezményeinek minél nagyobb mértékű, átszervezéssel, rezsim- intézkedésekkel történő csökkentése.[9]

A megfelelő megelőző intézkedésekkel a komplex védelem további összetevőinek költségei nagymértékben csökkenthetők.

[9] Például készpénz-kezelés helyett elektronikus pénzátutalásra történő áttérés, vagy hozzáférési jogosultságok korlátozása.

A mechanikai védelem elsődleges célja a behatolás késleltetése, az elektronikai védelem jelzőrendszerei által értesített élőerős védelem helyszínre érkezéséig, beavatkozásáig. Másodlagos funkciója az elriasztás, elrettentés az impulzív, alkalmi elkövetők szándékának befolyásolása.

Az elektronikai védelem komplex fogalom, több, önállóan telepíthető, önálló funkciókat ellátó biztonságtechnikai alrendszert foglal magába:

- Behatolás jelző rendszer.
- Beléptető rendszer.
- Videó felügyeleti rendszer.
- Áruvédelmi rendszer.
- Járőrkövető rendszer.
- Tűzjelző rendszer.[10]

Az elektronikai védelem elsődleges funkciója az élőerős védelem értesítése a behatolási kísérletekről, rendkívüli eseményekről. Másodlagos funkciója az elriasztás, elrettentés bűnmegelőzési céllal. Harmadlagos funkciója az események rögzítése, naplózása későbbi feldolgozások, elemzések céljából.
Az egyes rendszerek integrálásával, a szinergia hatás kihasználásával az egyes funkciók hatékonysága nagymértékben növelhető.

Az élőerős védelem célja a vagyon- és életbiztonság védelme helyszínen telepített erőkkel, vagy távfelügyeleti központokon keresztül értesített járőrök helyszínre irányításával. Az élőerős védelem hatékonysága alapvetően a komplex vagyonvédelmi piramis egyes összetevőinek hatékonyságától és megfelelő egymásra épülésétől, ezen belül az elektronikai védelem jelzőrendszereinek megfelelő működésétől függ.

[10] Sok esetben, mint esetünkben is a tűzjelző rendszereket is az elektronikai védelem rendszerei közé soroljuk.

A biztosítás célja a védelmi intézkedések ellenére mégis bekövetkező kockázati események kárkövetkezményeinek csökkentése káráthárítási szerződésekkel. A vagyonvédelmi szakember számára a védelmi koncepció kialakításánál a biztosítási lehetőségek, portfóliók számbavétele fontos szempont a megfelelő kockázati szint/védelmi költségek megtervezésénél. A biztonságtechnikai tervező számára pedig a rendszerterv kialakításánál elengedhetetlen az adott biztosítás feltételeinek, követelményeinek figyelembevétele.

A saját kockázat a minden erőfeszítés ellenére fennmaradó kockázat, amire a biztosítás sem nyújt mindenre, így a vagyonvédelmi koncepció kialakításánál a saját kockázatot is figyelembe kell venni.

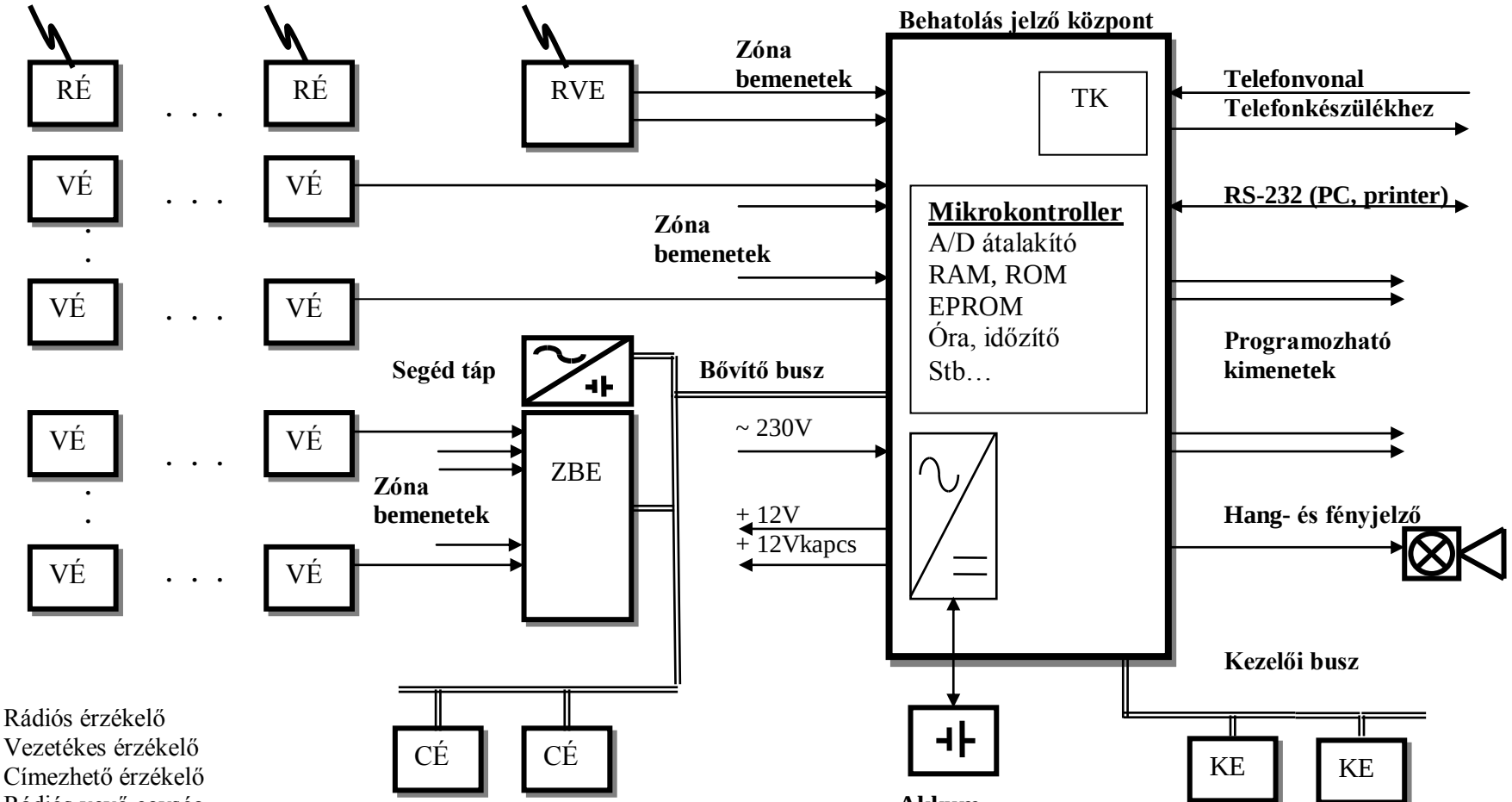
2.2. BEHATOLÁS JELZŐ RENDSZEREK

A behatolás jelző rendszerek elsődleges célja az élőerős védelem értesítése az illetéktelen behatolásról, behatolási kísérletről. A megfelelően tervezett és telepített rendszer, a mechanikai védelem eszközeire közvetlenül ráépülő érzékelői segítségével már a mechanikai védelem megsértésének kezdetén helyszíni hang- és fényjelzőkkel, illetve távjelzéssel - a távfelügyeleti központon keresztül, vagy közvetlenül - értesíti az élőerős védelmet. [9]

Egy behatolás jelző rendszer érzékelőket, helyi jelzésadókat, központot, kezelőegységeket, tápegységeket, kiegészítő/bővítő modulokat, távjelzés-átviteli modulokat és az eszközöket összekötő helyi kommunikációs hálózatot tartalmaz.
A helyi kommunikációs hálózat általában vezetékes kialakítású, de egyre inkább terjednek a vezeték nélküli, rádiós megoldások.

A 2.2. ábra egy vezetékes behatolás jelző rendszer blokkvázlatát szemlélteti.[11]

[11] Az ábra az „Új vagyonvédelmi nagykönyv” [10] általam írt „Behatolásjelző központok” alfejezetéből származik.



RÉ Rádiós érzékelő
VÉ Vezetékes érzékelő
CÉ Címezhető érzékelő
RVE Rádiós vevő egység
ZBE Zónabővítő egység
KE Kezelő egység
TK Telefon kommunikátor

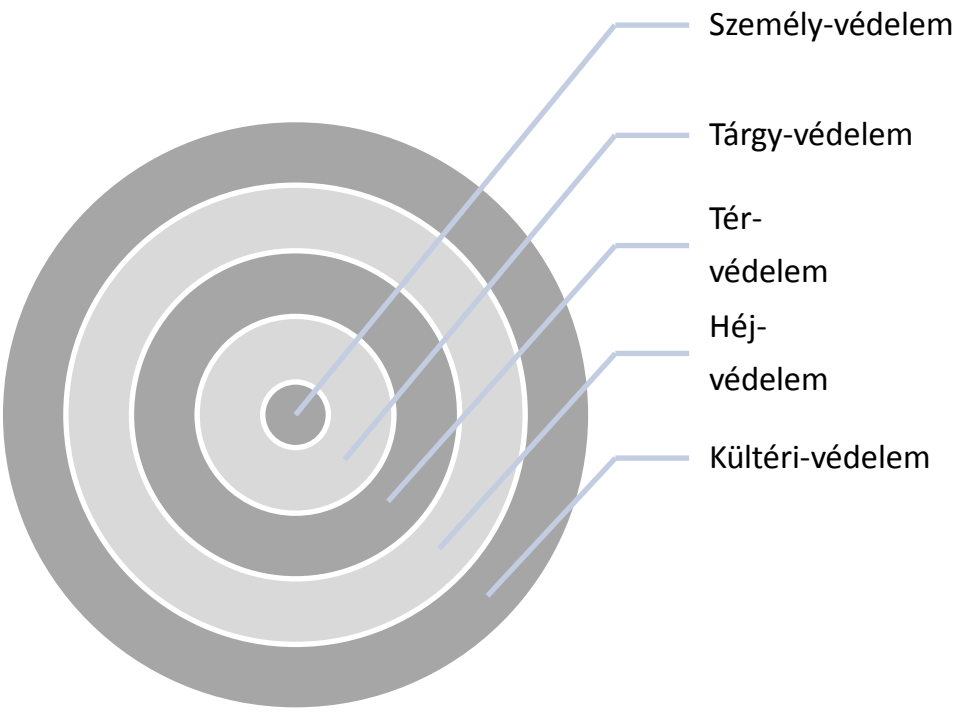
2.2. ábra Vezetékes behatolás jelző rendszer blokkvázlata

A BEHATOLÁS JELZŐ RENDSZEREK ÉRZÉKELŐI

A behatolás jelző rendszer érzékelőit hagymahéj-szerű elrendezésben, „védelmi körökben”, több rétegben helyezzük el.

Az egyes védelmi körök:

- Kültéri védelem.
- Felület (héj) védelem.
- Térvédelem.
- Tárgyvédelem.
- Személyvédelem.



2.3. ábra. Behatolás jelző rendszer védelmi körei

A kültéri védelem érzékelői mozgás, rezgés, nyomásváltozás, elektromos tér változás és egyéb érzékelési módokon működő eszközök. Ezeknél az eszközöknél fokozottan figyelembe kell venni a környezeti jellemzők hirtelen, nagymértékű változásának lehetőségét, emiatt az eszközök telepítésekor a megfelelő IP[12] védettségét, valamint szükség esetén fűtésüket-hűtésüket is biztosítani kell. [11]
A leggyakrabban alkalmazott kültéri eszközöket a 4.1. táblázat tartalmazza.

A felületvédelem („héjvédelem") érzékelői biztosítják a védendő objektum falazatán, padozatán, mennyezetén, nyílászáróin, üvegportáljain át történő behatolási kísérletek érzékelését. A nyitható ablakokat, ajtókat nyitásérzékelővel kell ellátni, az üvegfelületek betörésének jelzésére üvegtörés érzékelőket kell telepíteni, a nem megfelelő mechanikai szilárdságú falszerkezeteket falbontás érzékelőkkel kell védeni. [13]
A felületvédelem leggyakrabban alkalmazott érzékelőit a 4.2. táblázat tartalmazza.

A térvédelem érzékelői a passzív infravörös, a mikrohullámú (Doppler[14]), az ultrahangos és a kombinált[15] mozgásérzékelők a védendő objektumon belül történő mozgások jelzését biztosítják. Az alkalmazott eszközöket a 4.3. táblázat tartalmazza.

A tárgyvédelem érzékelői a védendő objektumon belül elhelyezkedő védendő tárgyak, illetve tároló eszközök megközelítését, elmozdítását, nyitását, rongálását jelzik. Az alkalmazott eszközöket a 4.4. táblázat tartalmazza.

[12] Az IP (Ingress Protection) jelentése behatolás elleni védelem, az elektronikát védő tokozás (készülékház) környezeti behatások elleni védettségét jelzik vele. Az IP besorolást az IEC 60529 szabvány írja le, amelyet gyakorlati tesztek alapján határoztak meg. Az első számjegy a szilárd testek elleni, a második a vízzel szembeni védettségre vonatkozik. A magasabb szám mindkét esetben jobb védettséget jelent.

[13] A felületvédelem eszközeinek követelményeit az MSZ EN 50131-2-6, és 2-7 szabványsorozat tartalmazza. [13], [14]

[14] A közeledő vagy távolodó testről visszaverődő hullámok hullámhossza (és frekvenciája) megváltozik; ezt alkalmazzuk a Doppler elven működő érzékelőknél a mozgás érzékelésére.

[15] A passzív infravörös-, a mikrohullámú és a kombinált mozgásérzékelők követelményeit az MSZ EN 50131-2-4.:2009 szabvány tartalmazza. [12]

A személyvédelem eszközei a védendő objektumon belül dolgozók személyi biztonságát szolgálják. Ezek az eszközök támadás esetén lehetőséget biztosítanak csendes riasztás aktiválására. A leggyakrabban alkalmazott kültéri eszközöket a 4.5. táblázat tartalmazza.

HELYI JELZÉSADÓK

Céljuk a környezet és a helyi élőerős védelem figyelmének hang- és/vagy fény-jelzéssel történő felhívása a behatolási-, rablási kísérletre, támadásra. [15] Az alkalmazott eszközöket a 4.6. táblázat tartalmazza.

KEZELŐEGYSÉGEK

A behatolás jelző rendszerek kezelőegységei biztosítják a felhasználó/telepítő és a behatolás jelző rendszer közötti kapcsolatot. Lehetővé teszik a kezelői beavatkozást, a rendszer üzemállapotainak átváltását, működési paramétereinek megváltoztatását, átprogramozását, megjelenítik a rendszer és a rendszer elemeinek állapotait. [16]

A kezelőegységek kialakításuk szerint lehetnek:

- LED-es kezelőegységek.[16]
- LCD-s kezelőegységek.[17]

A vezetékes rendszerek kezelőegységei adatbuszon, a „kezelői buszon” keresztül kommunikálnak a behatolás jelző központtal. A vezeték nélküli kezelőegységek digitális „táviratokkal” kommunikálnak a behatolás jelző központtal.

Az adatátvitel mind a vezetékes, mind a vezeték nélküli kezelőegységek esetében nem szabványosított, gyártó-specifikus egyedi protokollokkal történik.

[16] LED - A fénykibocsátó dióda vagy LED neve az angol Light Emitting Diode rövidítéséből származik.

[17] LCD - Liquid Crystal Display, folyadékkristályos kijelző.

KÖZPONTOK

A behatolás jelző rendszerek központjait több szempont szerint osztályozhatjuk.

A központ által egyedileg kezelhető, megkülönböztethető érzékelők által lefedett „zónák” száma (Z) alapján:

- Kis központ ($Z \leq 16$).
- Közepes központ ($16 < Z \leq 64$).
- Nagy központ ($64 < Z$).

A központ által külön kezelhető, élesíthető, kikapcsolható területek „partíciók” száma alapján:

- Egy partíciós („nem partícionálható”).
- Több partíciós.

A központ és az érzékelők közötti kommunikációs hálózat alapján:

- Vezetékes központok.
- Rádiós központok.
- Hibrid (vezetékes és rádiós) központok.

A kis központok általában kompakt felépítésűek, egy áramköri panelen tartalmazzák valamennyi, az érzékelők bekötéséhez, a jelzésadók vezérléséhez, a távátviteli jelzések továbbításához és a rendszer eszközeinek tápellátásához szükséges elemeket. [17]

A közepes- és nagy vezetékes központok moduláris felépítésűek, adatbuszon keresztül kommunikálnak a bővítő- és kiegészítő modulokkal. A közepes moduláris központoknál a bővítő- és kiegészítő modulok a kezelői buszra csatlakoznak. Nagyobb központoknál a kezelőegységek számára külön „kezelői busz”, a bővítő- és kiegészítő modulok számára pedig „bővítő buszok” vannak kialakítva. Egyes központoknál a bővítő buszokra címezhető érzékelők is felrakhatók. [18]

KIEGÉSZÍTŐ/BŐVÍTŐ MODULOK

A moduláris felépítésű központok az érzékelők jeleinek fogadására bemeneti zónabővítő modulokat, a jelzésadók és más eszközök vezérlésére kimeneti bővítő modulokat, a távátviteli jelzések továbbításához kommunikációs modulokat és a rendszer eszközeinek elosztott tápellátásához segédtáp modulokat alkalmaznak. Ezeken kívül egyéb kiegészítő modulok is beilleszthetők a rendszerekbe (pl. rádiófrekvenciás érzékelők csatoló modulja, hangmodul, X10 épületautomatikai modul[18]).

A moduláris behatolás jelző központoknál alkalmazott bővítő- és kiegészítő modulokat a 4.8. táblázat tartalmazza.

TÁVJELZÉS-ÁTVITELI (KOMMUNIKÁTOR) EGYSÉG

A központ riasztás, szabotázs, hiba jelzéseinek és egyéb (SMS[19], hang) üzeneteknek a távfelügyeleti rendszer-központokba és/vagy egyedi telefon és e-mail, internet címekre történő átvitelére, a központ távvezérlésére, távprogramozására távjelzés-átviteli (kommunikátor) modulokat használunk.
A riasztás, szabotázs, hiba jelzések kódolása többnyire szabványosított protokoll alapú, maga az átviteli protokoll az alkalmazott kommunikációs módtól függően szabványosított (pl. GSM[20]/GPRS[21], TCP/IP[22]), vagy gyártó-specifikus lehet.

[18] Az X10 protokoll lehetővé teszi az egyes épületautomatikai eszközök világítási hálózaton keresztüli vezérlését.

[19] SMS (Short Message Service, szó szerint „rövid üzenet-szolgáltatás”), mobiltelefonnal küldött rövid terjedelmű, meghatározott karakterszámú üzenet.

[20] GSM (Global System for Mobile communications) a mobil telefon kommunikáció elterjedt jelölése.

[21] A GPRS (General Packet Radio Service) egy csomagkapcsolt, IP (Internet Protocol) alapú mobil adatátviteli technológia, amelyet a GSM mobiltelefon hálózatok használnak.

[22] A TCP/IP betűszó az angol Transmission Control Protocol/Internet Protocol (átviteli vezérlő protokoll/internet protokoll) rövidítése, mely az interneten alkalmazott protokollstruktúrát jelenti.

2.3. BELÉPTETŐ RENDSZEREK

A biztonságtechnikai célokból telepített beléptető rendszerek elsődleges célja a védendő objektumba történő belépés/kilépés, valamint az objektumon belüli mozgások jogosultság szerinti szabályozása.
A fentieken kívül a beléptető rendszer felhasználható különböző bemeneti állapotváltozások hatására történő vezérlések elvégzésére, munkaidő nyilvántartásra, kombinálható különböző gépjármű beléptető rendszerekkel (például rendszám felismerő rendszer). Elláthat továbbá olyan speciális funkciókat is, mint például elektronikus pénztárca funkció (szállodai, közlekedési alkalmazásoknál). [19]

BELÉPTETŐ RENDSZEREK OSZTÁLYOZÁSA

A beléptető rendszereket több szempont szerint osztályozhatjuk.

Aszerint, hogy személyek, járművek, vagy állatok, esetleg tárgyak mozgását szabályozzák, léteznek:

- Személybeléptető rendszerek.
- Gépjármű beléptető rendszerek.
- Egyéb beléptető rendszerek.

Az egyes belépési pontok egymással és/vagy központi számítógéppel való kapcsolata szempontjából a beléptető rendszer lehet:

- Off-line (önálló belépési pontok, számítógépes kapcsolat nélkül).
- On-line (belépési pontok kommunikációs hálózattal, számítógépes kapcsolattal).

BELÉPTETŐ RENDSZEREK FELÉPÍTÉSE

A beléptető rendszerek alapvető eleme az objektumok, helyiségek, területek bejáratainál telepített belépési pont. Az on-line rendszereknél a belépési pontok helyi kommunikációs hálózaton keresztül számítógépes központhoz kapcsolódnak. [20]

A belépési pont elemei:

- Mechanikai áthaladás-gátló szerkezet.
- Nyitottság/zártság érzékelők.
- Rácsukás érzékelők.
- Áthaladás érzékelők.
- Speciális érzékelők (fémdetektor, súlyérzékelő).
- Vésznyitók.
- Olvasók.
- Visszajelző eszközök.
- Vezérlő egység.
- Szünetmentes tápegység.

A mechanikai áthaladás-gátló szerkezet akadályozza meg a nem engedélyezett belépéseket az adott területre. Az egyszerű, csak jelzésértékű, könnyen leküzdhető forgóvillától az elektromágneses ajtózárakon át egészen a nagybiztonságú zsilipekig sokféle, az adott alkalmazáshoz megfelelő szerkezet létezik.

A mechanikai áthaladás-gátló szerkezetre **nyitásérzékelőket** és a reteszelő szerkezet zártságát jelző **zártság érzékelőket** telepítenek.

A **rácsukás érzékelők** az áthaladó személyek, járművek épségének biztosítására szolgálnak, jelzésükkel megakadályozzák a mechanikai áthaladás-gátló szerkezet rácsukódását az áthaladó személyekre, járművekre.

Az **áthaladás érzékelők** a belépési ponton történő áthaladás tényét és irányát érzékelik. Személybeléptetésnél infravörös fénysorompók, dupla-érzékelős passzív infravörös

mozgásérzékelők, gépjármű beléptetésnél induktív hurkok az általánosan használt eszközök.

A **speciális érzékelők** alkalmazására ritkán, csak nagybiztonságú helyeken (trezorok, sugárveszélyes objektumok) kerül sor.

A **vésznyitók** kétféle funkció ellátására szolgálnak. Egyik fajtájuk az azonosítást nem igénylő áthaladási irányban a vezérlőegységen keresztül, vagy a-nélkül nyitja a mechanikai áthaladás-gátló szerkezetet. Másik típusuk az elektronikai rendszer meghibásodása esetén lehetővé teszi az áthaladás-gátló szerkezet mechanikai úton történő nyitását.

Az **olvasó egységek** az áthaladási jogosultságot jelző kódok, azonosítók, jellemzők érzékelésére, beolvasására és a a vezérlőegységhez történő továbbítására szolgálnak. Egy belépési pontnál több olvasó elhelyezésére is szükség lehet, akár a két irányban történő azonosítás céljából, akár többféle azonosítási technológia alkalmazása esetén.

A **visszajelző eszközök** hang és fényjelzésekkel, szövegkiírással-, vagy bemondással jelzik a beolvasott azonosítók érvényességét, elfogadását/elutasítását.

A **vezérlő egység** a belépési pont minden elemével kapcsolatban van. Az olvasókról beolvasott azonosítókat összehasonlítja a memóriájában tárolt jogosultsági listával és ennek alapján, valamint az áthaladás érzékelők, a speciális érzékelők, a rácsukás érzékelők jelei alapján vezérli a visszajelző eszközöket és a mechanikai áthaladás-gátló szerkezetet.
Eseménynaplóban rögzít minden sikeres áthaladást és sikertelen kísérletet. Az on-line rendszereknél üzenetet küldhet minden eseményről a központnak.

A **szünetmentes tápegység** gondoskodik a belépési pont elemeinek tápellátásáról.

A **beléptető terminálok** kompakt kialakítású, a vezérlőegységet, olvasókat, visszajelző és egyéb kezelő eszközöket egy modulban tartalmazó berendezések. Speciális fajtája a **munkaidő-nyilvántartó terminál**.

AZONOSÍTÁSI MÓDOK

A személybeléptető rendszereknél a belépési jogosultság igazolására többféle módszert használunk [21]:

- Tudás alapú azonosítás.
- Birtoklás alapú azonosítás.
- Tulajdonság alapú azonosítás.
- Viselkedés alapú azonosítás.

A **tudás alapú azonosításnál** azonosító kóddal, jelszóval igazoljuk jogosultságunkat. Az adatok bevitelére billentyűzet, vagy (hangbemondásos jelszónál) szöveg- és hang-felismerő modul szolgál olvasóként.

A **birtoklás alapú azonosítási** mód a legelterjedtebb módszer. Itt különböző eszközök által hordozott kódok szolgálnak a jogosultság igazolására. Sokféle adathordozó és ennek megfelelően sokféle olvasó létezik.

A leggyakrabban használt típusok:

- Vonalkódos azonosítók.
- Mágnes-csíkos (kártyás) azonosítók.
- Proximity (közelítéses) azonosítók.
- Mikrohullámú („Hand-free” és „Long-range”) azonosítók.
- Intelligens kártyás („Smart-card”) azonosítók.
- Dallas gombos azonosítók.

A **tulajdonság alapú azonosítás**nál a személyek egyedi, személy-specifikus biometriai jellemzőit használják a jogosultság igazolására. Itt is sokféle jellemzőt és ennek megfelelően sokféle olvasót alkalmazhatunk.

A leggyakrabban használt azonosítási módok:

- Ujjlenyomat azonosítás.
- Kézgeometria azonosítás.
- Arc-hőtérkép azonosítás.
- Arcfelismerés, azonosítás.
- Írisz (szivárványhártya) mintázat letapogatás, azonosítás.
- Retina mintázat letapogatás, azonosítás.
- Hangminta azonosítás.

A **viselkedés alapú azonosítás**nál a személyek egyedi, személy-specifikus dinamikus biometriai jellemzőit használják a jogosultság igazolására. Ilyen azonosítási mód lehet:

- Beszédhang azonosítás.
- Kézírás azonosítás.
- Gépírás azonosítás.

A gépjárművek azonosítására használt eszközök:

- Mágneshurkos transzponder.
- Rendszám leolvasó kamera.

A különböző azonosítási módokhoz használt olvasók az egyedi, gyártó-specifikus adatátviteli protokollok mellett általában a szabványként elfogadott Wiegand protokollt is tudják alkalmazni.

2.4. ÁRUVÉDELMI RENDSZEREK

Az elektronikus áruvédelmi rendszerek (**EAS** - **E**lectronic **A**rticle **S**urveillance) telepítésének célja az árusított termékek fizetés nélkül történő kivitelének jelzése.
A kereskedelem, hasonlóan minden más iparághoz, a tevékenysége folyamán óhatatlanul elszenved bizonyos veszteségeket. Ezeket a veszteségeket maradéktalanul megszüntetni nem lehet, viszont a lehető legalacsonyabb szinten kell tartani. A veszteségforrások az alábbiak lehetnek:

- Az áruk minőségromlása.
- Adminisztrációs hibák.
- Beszállítói tévedések.
- Alkalmazotti lopások.
- Vásárlói lopások.

Az összes veszteségeknek általában a kétharmadát teszik ki az alkalmazotti és a vásárlói lopások. Ezek számát csökkentheti hatékonyan egy megfelelően megtervezett és jól működtetett áruvédelmi rendszer.

ÁRUVÉDELMI RENDSZEREK FELÉPÍTÉSE, MŰKÖDÉSE

Az üzlethelyiségek kijáratánál, vagy a kasszáknál elhelyezett áruvédelmi szenzorok, „kapuk” érzékelik a közöttük átvitt, még aktív áruvédelmi címkével ellátott árucikkeket és jelzést adnak. A jelzés lehet helyi hang- fényjelzés, vagy/és távjelzés.

Az áruvédelmi rendszerek elemei:

- Áruvédelmi kapuk, szenzorok.
- Áruvédelmi etikettek, címkék.
- Hatástalanító, deaktiváló/reaktiváló eszközök.

A védendő árucikkeket, az áru fajtájától függően címkékkel, vagy etikettekkel kell ellátni. Ruházati termékek védelmére leggyakrabban úgynevezett kemény etiketteket használnak. Az etikettet egy edzett acéltüskét a szöveten átszúrva kell rögzíteni, eltávolítani viszont csak speciális célszerszámmal lehet. Felhelyezése és eltávolítása a célszerszámmal néhány másodperc alatt elvégezhető. Léteznek olyan kemény etikettek is, amelyek önmagukban is képesek riasztás jelzés adására, ha megpróbálják őket erőszakkal eltávolítani. Az etikettek eltávolításához különféle speciális célszerszámokat alkalmazunk.

Az áruvédelem másik fajta eszközei a címkék. A címkék előnye, hogy kicsi az előállítási költségük és kis méretüknek köszönhetően kicsi a helyigényük. Több színben, áttetsző burkolattal és álcázott (ál-vonalkódos) kivitelben is gyártják őket, ez segíti a rejtett felhelyezésüket. Léteznek egyszer használatos és többször használható, többször aktiválható és hatástalanítható típusok is.

A címkék hatástalanítására szolgáló elektromágneses eszközök felületre szerelhető, beépített, vagy akár futószalag alá szerelhető változatban is elérhetők.

Nagymértékben növelheti a biztonságot, ha az áruvédelmi rendszerrel összekapcsoljuk, integráljuk a videó megfigyelő rendszert és az áruvédelmi rendszer jelzésére rögzítésre kerül a videó megfigyelő rendszer adott kamerájának képe.

ÁRUVÉDELMI RENDSZEREK OSZTÁLYOZÁSA

Az áruvédelmi rendszereket az alkalmazott érzékelési technológiák szerint osztályozhatjuk.

- Rádiófrekvenciás (RF) rendszerek.
- Elektromágneses (EM) rendszerek.
- Akuszto-magnetikus (AM) rendszerek.

A rádiófrekvenciás rendszerek a 2-10 MHz-es frekvencia tartományban működnek. A rendszerben használt címke egy hangolt rezgőkört tartalmaz, amely az antenna által

kisugárzott rádiófrekvenciás jel hatására rezegni kezd. Ezt a jelet érzékeli a vevőantenna, majd továbbítja egy kiértékelő egységbe.
A címkék minden esetben jeleznek, ha átviszik őket a kapuk között, ezért ha a téves riasztásokat el akarjuk kerülni, a címkét a pénztárnál el kell távolítani, vagy tönkre kell tenni. A címkék tönkretételére egy úgynevezett „deaktivátor" tekercset használunk, amely olyan nagy energiájú elektromágneses erőteret hoz létre, amely a címke rezgőkörét tönkreteszi.

Az elektromágneses rendszerek címkéit aktiválni és deaktiválni is lehet. Ezek a címkék általában lágy-mágneses anyagból készülnek. Fő alkalmazási területeik a különböző könyvtárak, kölcsönzők.

Az akuszto-magnetikus rendszerek címkéiben két fémlemez van. Az egyik lágy-mágneses, a másik kemény-mágneses anyag. A méretüket úgy állítják be, hogy fizikai rezgésük frekvenciája megegyezzen az antenna frekvenciájával. Az antenna kisugárzott mágneses impulzusai megmozdítják a fémlemezkéket, amelyek rezgéseit egy ultrahang-mikrofon érzékeli. Ezeknek a rendszereknek a rezgési frekvenciája 50-70 kHz közötti tartományban van. Egyszerű a címkék felépítése, azonban az antenna teljesítménye akár a 150 Wattot is meghaladhatja. A címkék aktiválhatók és deaktiválhatók, ez a kemény-mágneses lemez felmágnesezésével, illetve lemágnesezésével történik.
Az akuszto-magnetikus elven működő áruvédelmi rendszerek antennái ötször-hatszor kisebb méretűek a hagyományos RF rendszerekben alkalmazott antennáknál, ezáltal nagyobb helyet hagynak a kijáratnál, esztétikusabban helyezhetők el. Az akuszto-magnetikus technológia nagy teljesítménye révén képes érzékelni a címkéket és etiketteket többféle folyadékon, fémes csomagoláson és a bevásárló kocsin keresztül is.

2.5. ŐRJÁRAT ELLENŐRZŐ RENDSZEREK

Az őrjárat ellenőrző rendszerek célja, funkciója az élőerős védelmet a helyszínen ellátó őrjáratozó személyek tevékenységének ellenőrzése. Segítségükkel ellenőrizhető, hogy a járőrök a járőrútvonal minden előzetesen kijelölt állomását, ellenőrzési pontját bejárták-e, ezt mennyi időközönként tették meg és mennyi idő alatt értek egyik helyről a másikra.

OFF-LINE ELLENŐRZŐ RENDSZEREK

A járőr tevékenységének utólagos ellenőrzését, kiértékelését teszik lehetővé. Ezeknél a rendszereknél a járőr egy, az ellenőrző pontokon elhelyezett azonosítók leolvasását és a kódok és időpontok letárolására szolgáló eszközt hordoz. A járőrözés befejeztével a tárolt adatokat számítógépbe lehet leölteni. A letöltött adatok utólag kerülnek kiértékelésre.

Az ellenőrzőpontokon elhelyezett azonosítók típusa szerint lehetnek:

- **Vonalkódos ellenőrzőpontok**
  Az ellenőrzőpontokon vonalkódok kerülnek felragasztásra, kültéri alkalmazásoknál vízálló kivitelben.
- **Mágnescsíkos ellenőrző pontok**
  A mágneskártyás beléptető rendszerek kártyáiéhoz hasonló mágnes csík kerül felragasztásra az ellenőrzési pontokon, amelyet a járőrnél lévő leolvasó szerkezet végighúzásával lehet leolvasni.
- **Proximity ellenőrző pontok**
  A mágnes-csíkos rendszerhez hasonló felépítésű, de itt a kihelyezett eszközök nem mágnes-csíkos, hanem proximity azonosító kártyák.
- **Dallas-gombos ellenőrző pontok**
  Az ellenőrzési pontokon Dallas-gombos azonosítókat helyeznek el, amelyet a járőrnél lévő leolvasó szerkezettel lehet leolvasni.

ON-LINE ELLENŐRZŐ RENDSZEREK

A járőr tevékenységének folyamatos, „real-time” ellenőrzését, kiértékelését teszi lehetővé. Ezeknél a rendszereknél a járőr útvonala folyamatosan nyomon követhető, az eredeti járőr-útvonal tervtől való eltérés azonnal jelezhető. A központ számítógépes programja által a járőrök véletlenszerű időpontokban, változó útvonalakon történő indítása hatékonyabb, nehezen kijátszható járőrözést valósíthat meg.

Az alkalmazott megoldások:

- **GPS helymeghatározó rendszerrel**[23]
  A járőrnél lévő GPS eszköz pozícióját GSM, vagy más rádiós berendezés segítségével a központ folyamatosan lekérdezi és megjeleníti.
- **Kiépített ellenőrzési pontokon elhelyezett olvasó terminálokkal**
  A járőrőr saját azonosító eszközével megy végig a megadott útvonalon,. Az ellenőrzési pontokon a6zolvasó terminál a járőr azonosító kódját leolvassa, és továbbítja az őrjárat ellenőrző központhoz
- **Beléptető rendszer segítségével**
  A járőrőr saját azonosító eszközével megy végig a megadott útvonalon, amely az átjárókon történő áthaladást lehetővé teszi. Egyéb belépési pontoknál nem nyitja az bejáratokat. de olvastatáskor az olvasás helyét, idejét és a kártya azonosítóját a rendszer eltárolja, kijelzi.
- **Az elektronikus behatolás jelző rendszerhez kapcsolva**
  Ennél a megoldásnál az ellenőrzési pontoknál erre a célra telepített passzív infravörös mozgásérzékelők automatikusan – esetleg a szintén e célra telepített nyomógombok működtetésével – jelzést adnak a központ felé, amely az megfelelően programozva nem riasztásként, hanem egyéb információként érzékeli és eltárolja az eseménymemóriájába.
- **Videó megfigyelő rendszerrel**
  Az útvonalra célszerűen telepített kamerák alkalmazásával a vagyonőr járőrözés közben megfigyelhető, a járőrözés folyamatát képrögzítő tárolja.

[23] A GPS (Global Positioning System) az egész világon használható műholdas helymeghatározó rendszer.

2.6. VIDEÓ MEGFIGYELŐ RENDSZEREK

A videó megfigyelő rendszerek ismertebb elnevezése, a zártláncú videó megfigyelő rendszerek (ZTV) neve az angol Closed Circuit Television (CCTV) névből ered. A zárt láncú televízió rendszereknél, ellentétben a műsorszóró rendszerekkel, a telepített kamerák által közvetített képeket csak egy előre meghatározott célcsoport nézheti. Egyes felhasználóknak lehetősége van a vezérelhető kamerákat vezérelni, valamint a rögzített képeket visszanézni, lemásolni.[24]

Zártláncú videó megfigyelő rendszereket alkalmaznak kültéri térfigyelő rendszerekben, épületek környezetének megfigyelésére, parkolókban. Beltéri kivitelben pénzintézetekben, bevásárlóközpontokban, irodaházakban alkalmazzák őket. CCTV rendszereket telepítenek akkor is, ha egy területen az üzemvitel zavartalanságát akarják ellenőrizni forgalomfigyelő kamerákkal. Ezeket a kameraképeket sok esetben nem is rögzítik. [23]

Máshol a rendszer telepítésének célja a személyek követése, cselekvésük pontos megfigyelése, rögzítése, például bevásárlóközpontok eladó terébe telepített kamerák, közterületi térfigyelő kamerák segítségével. Ezeknél a rendszereknél lényeges a kamerák gyors vezérlése, a felügyelő személyzet jó kiképzése, a kameraképek nagy felbontású, nagy sebességgel történő rögzítése. [24]

A videó megfigyelő rendszerek elemei:

- Kamerák + objektívek.
- Adatátviteli eszközök.
- Videójel kapcsoló eszközök.
- Képrögzítők.
- Monitorok.

[24] A videó megfigyelő rendszerek eszközeinek ismertetése magyar nyelven a „CCTV magyarul” szakkönyvben részletesen megtalálható. [22]

KAMERÁK

- A kamerák kialakításuk szerint lehetnek: beltéri/kültéri kamerák.
- A szolgáltatott kép alapján lehetnek: fekete-fehér/színes képet adó kamerák.
- Mozgathatóság alapján: fix/forgatható/„cső”/célkövető kamerák.

OBJEKTÍVEK

Az objektívek, más néven optikák, a kamera képfelbontó eleme (például CCD[25]) elé rögzített képalkotó eszközök. Az objektív egy lencserendszer segítségével képezi le a tárgy képét a képfelbontó elemre. Az objektívekbe beépítenek egy – a fotó technikában is ismert – blendét, vagy más néven íriszt, amely segítségével szabályozható a képfelbontó elemre beeső fény mennyisége.

- Írisz szempontjából lehetnek: fix/manuál/auto íriszes objektívek.
- Fókusztávolság szerint lehetnek: fix/változtatható fókusztávolságú/zoom objektívek.

ADATÁTVITELI ESZKÖZÖK

Az adatátviteli eszközök, utak kiválasztása a kamera által szolgáltatott jel, valamint a kamera és képfeldolgozó eszköz (videó központ, vagy monitor) közötti távolság figyelembevételével történik. [25]

- Koaxiális kábel.
- Csavart érpár.
- Optikai kábel.
- Rádiós képátvitel.
- Mikrohullámú képátvitel.

[25] A CCD (Charge Coupled Device, azaz töltés-csatolt eszköz) a fényt elektronikus jelekké alakító eszköz.

- Infravörös képátvitel.
- Lézeres képátvitel.
- LAN hálózaton történő képátvitel.

VIDEÓJEL KAPCSOLÓ ESZKÖZÖK

- Képléptetők

A képléptetők vagy más néven „switcher”-ek olyan két-, vagy több bemenetű videotechnikai eszközök, amelyek a bemenetükre kapcsolt videojeleket – legtöbbször digitalizálás nélkül – egymás utáni sorrendben jelenítik meg a kimenetükre kapcsolt monitoron.

- Képosztók

A képosztók a képléptetőkkel ellentétben a bemenetükre kapcsolt kameraképeket osztott kép formájában, akár egyszerre is meg tudják jeleníteni a kimenetükön.

- Video-multiplexerek

A video-multiplexerek a képléptetők és a képosztók hiányosságainak megszüntetésére hivatott eszközök. Képesek a bemenetükre kapcsolt képek szekvenciális, vagy osztott képes (többféle osztásban), illetve teljes képes megjelenítésére.

- Video-mátrixok

A mátrixok olyan több bemenetű és több kimenetű készülékek, amelyek bármelyik kimenetükön bármelyik bemenetükre kapcsolt kamera képét meg tudják jeleníteni.

- Távvezérlők

A távvezérlők a multiplexerek, mátrixok, valamint a mozgatható kamerák távkezelését, távvezérlését teszik lehetővé.

VIDEÓ RÖGZÍTŐK

- „Time-lapse” [26] videó magnetofonok

A „time-lapse” videó magnetofonok vagy más néven időosztásos videó magnetofonok alkalmazásával egy 180 perces videó szalagra 12, 24, 48, 72…, vagy akár 960 órányi felvételt is tudunk készíteni. A time-lapse videó magnetofonok alkalmazását napjainkra háttérbe szorították a digitális képrögzítők.

- Digitális képrögzítők

Az analóg kameraképeket fogadó digitális képrögzítő először a rákapcsolt kameraképet egy analóg/digitális átalakítóval digitalizálja, majd a digitalizált anyagot valamilyen tömörítési eljárással tömöríti. Ezt a tömörített információt rögzíti a beépített merevlemezre, memória kártyára vagy más egyéb tárolóeszközre. Az alkalmazott tömörítési eljárás nagymértékben befolyásolja a rögzített kép minőségét és méretét, ezáltal az egységnyi területen tárolható képek mennyiségét is. [26]

MONITOROK

A monitorok a zártláncú televízió rendszer képmegjelenítő eszközei. Lehetnek katódsugárcsöves monitorok, vagy más néven CRT[27] monitorok, LCD[28] monitorok, vagy plazma-kijelzők.

Míg korábban legelterjedtebben színes, vagy fekete-fehér katódsugárcsöves monitorokat használtak a biztonságtechnikai rendszerekben, mára egyre nagyobb teret hódítanak az LCD és a plazma monitorok.

[26] Időben hosszan elnyúló mozgások, folyamatok képi rögzítése.
[27] CRT - Catode Ray Tube – katódsugárcső.
[28] LCD - Liquid Crystal Display – folyadékkristályos kijelző.

2.7. TŰZJELZŐ RENDSZEREK

Az automatikus tűzjelző rendszerek telepítésének célja a keletkező tűz korai észlelése, a beavatkozó szervek mielőbbi értesítése az emberéletek és az anyagi javak hatékony mentésének érdekében. Az automatikus tűzjelző rendszerekkel szemben elvárás, hogy a helyi riasztás-jelzésen túl automatikus vezérlési feladatokat is képesek legyenek elvégezni. Ilyen vezérlési feladat például a légtechnikai berendezések ki-, illetve bekapcsolása, a felvonók vezérlése, tűzszakaszok lezárása, automatikus oltórendszerek vezérlése.

TŰZJELZŐ RENDSZEREK FELÉPÍTÉSE, MŰKÖDÉSE

Az automatikus tűzjelző rendszerek központi egységből, a hozzá csatlakoztatott automatikus érzékelőkből, kézi jelzésadókból, valamint vezérelt jelzőeszközökből állnak. [27]

A tűzjelző rendszer elemei:

- Tűzjelző központ.
- Automatikus érzékelők.
- Kézi jelzésadók.
- Bemeneti-, kimeneti modulok.
- Akusztikus jelzőeszközök.
- Átjelző eszközök

Az érzékelők és a központ közötti kommunikáció, feladatmegosztás alapján többféle tűzjelző rendszer létezik [28]:

- Hagyományos, más néven hurkos kialakítású rendszerek.
- Hagyományos címzett rendszerek.
- Analóg intelligens címzett rendszerek.

Hagyományos rendszerek

Hagyományos rendszereknél az automatikus érzékelők és manuális jelzésadók érzékelő hurkokon helyezkednek el, a hurkok végén egy lezáró elemmel (ellenállás vagy kondenzátor). A hagyományos rendszerek érzékelői a tápáram-felvétel megváltoztatásával (általában több nagyságrenddel történő megnövelésével) jelzik a tűzriasztás állapotot. Ezeknél a rendszereknél a központ nem tudja megállapítani, hogy melyik érzékelő jelzett, csak az érzékelő-hurok számát tudja azonosítani. Az érzékelő eszközökbe beépített LED-ek csak a helyszínen jelzik az érzékelő riasztás-állapotát Emiatt egy érzékelő hurokra 20-25 db érzékelőnél több nem telepíthető.

Hagyományos címzett rendszerek

A hagyományos címzett rendszereknél a hagyományos érzékelők foglalatába épített címző-egység segítségével a központ egyenként lekérdezheti az érzékelők, jelzésadók állapotát és így azonosíthatja a jelzésadó eszközt. Ezeknél a rendszereknél egy érzékelő-hurokra központ típustól függően 32 – 64 érzékelő telepíthető. Mind a hagyományos, mind a hagyományos címzett rendszereknél az érzékelők szintjén dől el a tűz-riasztás állapot jelzése. Adott mértékű környezeti változás hatására az érzékelők generálnak riasztás-jelzést.

Analóg intelligens rendszerek

Az analóg intelligens rendszerekben címzett érzékelőket és jelzésadókat alkalmazunk. Ezeknél a rendszereknél az érzékelők nem riasztás-jelzést generálnak, hanem a központ ciklikusan lekérdezi az érzékelő eszközök által mért mérési eredményeket (hőmérséklet, füst-koncentráció). Az érzékelők az általuk mért fizikai jellemzők értékének megfelelő, azzal „analóg” értékeket küldenek a központnak, innét ered az „analóg rendszer” elnevezés.
A központ a mérési eredményeket összehasonlítja a telepítő/programozó által megadott küszöbértékekkel és ez alapján a központ dönt a tűzriasztás állapot generálásáról.

TŰZJELZŐ RENDSZEREK ÉRZÉKELŐI

A tűzjelző rendszerek érzékelői az általuk lefedett térszegmens alapján lehetnek:

Pontszerű érzékelők:

- Optikai füstérzékelő.
- Ionizációs füstérzékelő.
- Hő-maximum (hőküszöb) érzékelő.
- Hő-sebesség érzékelő.
- Kombinált érzékelők.
- Kézi jelzésadók.

Vonali érzékelők:

- Infravörös vonali füstérzékelő.
- Hő-érzékelő kábel.

Síkbeli érzékelők:

- Aspirációs füstérzékelő.

Térbeli érzékelők:

- Lángérzékelők.

RÉSZKÖVETKEZTETÉSEK

A komplex villamos rendszerek biztonságtechnikai összetevőinek, alrendszereinek felmérése, rendszerezett összefoglalása elengedhetetlen feltétel az egyes alrendszerek, valamint az integrált rendszerek komplexitásának, majd integráltsági fokának megállapításához.

A fejezet elején vázoltam a komplex vagyonvédelem felépítését, összetevőit, majd elvégeztem az általam vizsgált elektronikus biztonságtechnikai alrendszereknek, mint az elektronikai védelem összetevőinek a pozicionálását, meghatároztam a komplex vagyonvédelemben elfoglalt helyüket, funkcióikat, relációikat.

A továbbiakban a komplex villamos rendszerekben legtöbbször alkalmazott behatolás jelző rendszerek részletes rendszertechnikai vizsgálatát végeztem el. Egy rendszer blokkvázlat alapján ismertettem a behatolás jelző rendszerek felépítését, összetevőit, védelmi körök szerint csoportosítva az alkalmazott érzékelők fajtáit, funkcióit. Osztályoztam a behatolás jelző központokat, kezelőegységeket, kiegészítő/bővítő modulokat.

A behatolás jelző rendszerek vizsgálatát követően a beléptető rendszerek klasszifikációját, rendszertechnikai leírását végeztem el. Ismertettem a beléptető rendszerek alap moduljának a belépési pontnak a felépítését, egyes elemeinek funkcióit, majd a beléptető rendszereknél alkalmazott azonosítási módokat.

Az áruvédelmi rendszerek céljának, felépítésének, működésének áttekintése után elvégeztem az áruvédelmi rendszerek alkalmazott technológia szerinti osztályozását is.

Az őrjárat ellenőrző rendszereknél külön osztályoztam az off-line és külön az on-line rendszereket.
A videó megfigyelő rendszerek alkalmazási céljainak, funkcióinak ismertetése után a rendszerelemek (kamerák, objektívek, videójel kapcsolók, képrögzítők, monitorok) vázlatos klasszifikációját végeztem el.

A fejezet végén az elektronikus vagyonvédelmi rendszerként is tekintett tűzjelző rendszereket írtam le. A rendszerek céljának, funkcióinak ismertetése után a rendszerek osztályozását végeztem el, majd röviden felsoroltam a tűzjelző rendszerek érzékelőit.

A tématerület részletes feldolgozása során feltárt ismereteket jó hatásfokkal tudtam alkalmazni a felsőfokú MSc szintű biztonságtechnikai képzésben is, az egyes, általam oktatott szakmai tárgyakban.[29]

Ebben a fejezetben rendszerezett leírását adtam a vizsgált terület biztonságtechnikai összetevőinek, alrendszereinek, ami megalapozta az egyes alrendszerek komplexitásának, integráltsági fokának modellezését, a későbbi fejezetek interfész táblázatainak kialakítását.

Ezzel teljesítettem a kutatási célkitűzések 1. pontját, a „Komplex villamos rendszerek specifikus biztonságtechnikai összetevőinek, alrendszereinek áttekintő rendszerezése" részt.

[29] Szakmai gyakorlat I.-II., Intelligens épületek, Biztonságtechnikai rendszerek tervezése I.-II., A személy és vagyonvédelem rendszertana, Személy és vagyonvédelmi rendszerek kialakításának módszerei, Személy és vagyonvédelmi rendszerek üzemeltetése, üzemfenntartása I.-II. [29]

3. INTEGRÁLT RENDSZEREK VIZSGÁLATA

3.1. INTEGRÁLT VAGYONVÉDELMI RENDSZEREK

A biztonságtechnika, az élet- és vagyonvédelem egyre nagyobb szerepet játszik globalizálódó és egyre kevésbé biztonságos világunkban. A cégek, hogy biztonságban tudják létesítményeiket, eszközeiket, alkalmazottaikat, ügyfeleiket, egyre többet fordítanak biztonságtechnikai eszközökre, rendszerekre.
Az integrált vagyonvédelmi rendszerekkel olcsóbban, hatékonyabban és egyszerűbben lehet garantálni a biztonságot és emellett több járulékos előnyük is van.[30]

A hagyományos vagyonvédelmi rendszerek az egyes kockázati tényezők és fenyegetések csökkentésére szolgáló megoldásokat különálló behatolás-jelző-, beléptető-, zártláncú TV-, őrjárat-ellenőrző- és egyéb alrendszerekkel valósítják meg. Az egyes alrendszereket többnyire különböző gyártók eszközeivel, sokszor különböző cégek telepítik. Az üzemeltetés során a rendszereket kezelő személyzet oktatását, továbbképzését, a rendszerek karbantartását, szervízelését is több cég látja el.

A felügyeletet ellátó személyzetnek többféle, teljesen különböző kezelőfelülettel rendelkező berendezéseket, számítógépes programokat kell megismerniük, kezelniük. Az egyidejűleg bekövetkező eseményekre való reagálás sorrendisége személyfüggő, a prioritási sorrendet nem a rendszer dönti el. Az egyik rendszerben bekövetkező esemény (például egy behatolás-jelzés) nincs hatással más (például a CCTV) rendszerekre, egy másik rendszer funkciójának (például adott kamerakép rögzítésének) indítása a kezelőszemélyzet feladata.

Egy „hagyományos" épület gyengeáramú alrendszereit különböző tervezők tervei alapján, különböző gyártók berendezéseiből, különböző alvállalkozók telepítik.

Egy épület gyengeáramú alrendszereit funkcióik szerint több csoportba sorolhatjuk:

[30] A fejlett országokban a biztonságtechnikai piac bevételének 40%-a ma már integrált vagyonvédelmi rendszerek eladásából származik. (Az egyedi CCTV rendszerek mintegy 19%-kal, a beléptető rendszerek 14%-kal részesednek a piacból.)

Épületgépészeti automatikai alrendszerek:

- Szellőzés, fűtés, klíma.
- Világítás, vészvilágítás.
- Liftek, mozgólépcsők, mozgójárdák.
- Automata nyílászárók, árnyékolók.
- Energia-ellátás, mérés, korlátozás (elektromos, víz, gáz).

Tűzjelző és oltó rendszerek:

- Automatikus tűzjelző rendszerek.
- Automatikus oltó rendszerek, sprinkler.
- Tűz-gátló ajtók, toló-kapuk, tűzvédelmi csappantyúk.
- Füstmentesítő rendszerek.
- Hang- és fényjelzés, átjelzés.

Vagyonvédelmi, biztonságtechnikai alrendszerek:

- Behatolás jelző rendszer.
- Személy beléptető és követő rendszer.
- Gépjármű beléptető (parkoló, garázs) és követő rendszer.
- Áruvédelmi rendszer.
- Őrjárat ellenőrző rendszer.
- CCTV (zártláncú TV), videó felügyeleti rendszer.

Kommunikációs alrendszerek:

- Telefonhálózat.
- Számítógép hálózat.
- Épülethangosítás.
- Rádió és TV műsor elosztó hálózat.

AZ INTEGRÁCIÓS FOLYAMAT

Az „integráció” alapszinten azt jelenti, hogy az egyik rendszerben bekövetkező esemény valamilyen válasz-reakciót generál egy másik rendszerben. Az egyes alrendszerek a hagyományos kialakítású épületekben is (többnyire adatpont szinten, feszültségmentes relé kontaktusokkal) több ponton kapcsolódhatnak egymáshoz.

Kötelező jogszabályi és hatósági előírások szabályozzák például a tűzjelző rendszerek és az épületgépészeti automatikai alrendszerek kapcsolatát.

A tűzjelző rendszer hatása más alrendszerekre:

- Szellőzések, klímarendszerek kényszervezérlése.
    - Légkezelők leállítása.
    - Füstmentesítés indítása.
- Tűzszakasz ajtók, tűzcsappantyúk vezérlése.
- Liftek kijárati szintre vezérlése, leállítása, mozgólépcsők vezérlése.
- Kijáratok nyitása, nyílászárók vezérlése.
- Elektromos elosztók, főkapcsoló vezérlése.
- Vészvilágítás, evakuációs információk biztosítása.
- Tűzoltók értesítése.

Az integrált vagyonvédelmi rendszerek előnyeinek kihasználásához a vagyonvédelmi funkciók mellett épületautomatizálási, vezérlési funkciókat is meg kell valósítani a rendszerekben.

Behatolás jelző rendszer jelzésének hatása más alrendszerekre:

- CCTV kamera felvétel indítása.
- Liftek blokkolása.
- Világítás felkapcsolása.
- Nyílászárók zárása.

Beléptető rendszer jelzésének hatása más alrendszerekre:

- Tűzjelző érzékelők jelzésszint állítása.
- Klíma komfort fokozat kapcsolása.
- Behatolás jelző partíciók élesítése/lekapcsolása.
- Lift engedélyezése/blokkolása.
- Nyílászárók zárása/nyitása.
- Világítás kapcsolása.

Őrjárat-követő rendszer jelzésének hatása más alrendszerekre:

- CCTV kamera felvétel indítása/leállítása.
- Lift engedélyezése/blokkolása.
- Világítás fel/le-kapcsolása.
- Nyílászárók nyitása/zárása.

Az egyes alrendszerek más alrendszerekre történő hatását a 3.1. interdependencia táblázatban foglaltam össze.

A táblázat soraiban lévő alrendszerek hatását a függőleges oszlopokban jelölt alrendszerekre a táblázat celláiban „X” jellel jelölöm. Az egyes alrendszerek saját magukra történő hatását „O” jel mutatja.

3.1. táblázat. ALRENDSZEREK INTERDEPENDENCIA TÁBLÁZATA

	I. Épületgépészet					II. Tűzjelző és oltó r.					III. Biztonságtechnikai alr.						IV. Komm.		
	1.	2.	3.	4.	5.	1.	2.	3.	4.	5.	1.	2.	3.	4.	5.	6.	1.	2.	3.
I. Épületgépészeti automatikai alrendszerek																			
1. Szellőzés, fűtés, klíma	O																		
2. Világítás, vészvilágítás		O																	
3. Liftek, mozgólépcsők, mozgójárdák			O																
4. Automata nyílászárók, árnyékolók				O															
5. Energia-ellátás, mérés, korlátozás					O														
II. Tűzjelző és oltó rendszerek																			
1. Automatikus tűzjelző rendszerek	X	X	X	X	X	O	X	X	X	X		X	X			X			X
2. Automatikus oltó rendszerek, sprinkler							O												
3. Tűz-gátló ajtók, csappantyúk								O											
4. Füstmentesítő rendszerek									O										
5. Hang- és fényjelzés, átjelzés										O									
III. Biztonságtechnikai alrendszerek																			
1. Behatolás jelző rendszer		X	X	X	X						O	X	X		X	X	X	X	X
2. Személy beléptető és követő rendszer	X	X	X	X	X	X					X	O	X	X	X	X	X	X	X
3. Gépjármű beléptető és követő rendszer		X	X	X	X	X					X	X	O		X	X			
4. Áruvédelmi rendszer.		X	X	X							X	X	X	O	X	X			X
5. Őrjárat ellenőrző rendszer		X	X	X		X	X	X		X	X	X	X		O	X	X	X	X
6. Videó felügyeleti rendszer		X	X	X		X	X	X	X		X	X	X	X	X	O		X	X
IV. Kommunikációs alrendszerek																			
1. Telefonhálózat										X	X	X			X		O	X	X
2. Számítógép hálózat	X	X	X	X	X	X				X	X	X	X	X	X	X	X	O	X
3. Épülethangosítás																			O

A vagyonvédelmi rendszerek integrációja az 1960-as évektől figyelhető meg. A fejlődés tendenciái az alábbiak szerint alakultak:

- A behatolás jelző rendszerek gyártói előbb a nagyobb, moduláris, majd a kisebb behatolás jelző központokba is beépítettek beléptető rendszer funkciókat, egy rendszerbe integrálva behatolás jelző és beléptető alrendszereket. Ezekhez a központokhoz általában számítógépes felügyeleti szoftverek is tartoznak.

- A CCTV rendszerek egyes elemeit (switcher-ek, time-lapse rögzítők, képosztók) riasztás bemenetekkel látták el, amelyek a behatolás jelző rendszer jelzéseinek hatására különböző vezérléseket generáltak a CCTV rendszerben.

- A beléptető rendszerek monitorjain a belépési pontnál lévő CCTV kamera képe is megjelent az azonosító kódhoz tartozó személy archivált képe mellett.

- Az épületautomatizálással foglalkozó nagyobb cégek (Honeywell, Siemens, Johnson Controls) épület-gépészeti felügyeleti szoftverei már régóta alkalmasak más alrendszerek, többnyire tűzjelző központok „beintegrálására" is. Ma ezek az épület-felügyeleti szoftverek már többféle vagyonvédelmi alrendszert (behatolás, beléptetés, CCTV) is kezelnek.[31]

- Egyes szoftver-fejlesztő cégek, rendszer-integrátorok, létesítmény menedzsment programokat fejlesztő cégek is megjelentek vagyonvédelmi rendszerek integrálására is alkalmas programokkal.

Az IP alapú rendszerek rohamos térhódításával az elektronikus vagyonvédelem és az információ-technológia (IT) gyorsuló **konvergenciája** figyelhető meg.

[31] A vagyonvédelmi piac koncentrálódásával a nagyobb vagyonvédelmi, vagy azzal is foglalkozó cégek (ADT, Bosch, GE, stb.) kihozták saját integrált vagyonvédelmi rendszereiket.

Ma a korszerű integrált vagyonvédelmi rendszerek általában moduláris behatolás jelző rendszert, személy- és gépjármű beléptető- és követő rendszert, digitális videó-megfigyelő rendszert, őrjárat-követő rendszert és tűzjelző rendszert képesek kezelni. Legtöbbjük bizonyos épületautomatikai funkciókat (liftvezérlés, világításvezérlés, nyílászáró vezérlés) is képes ellátni.

A nagyobb méretű, integrált épület-felügyeleti rendszerek a fentieken túl elsősorban az épületgépészeti rendszereket felügyelik és integrálhatók vállalatirányítási és létesítmény-gazdálkodási („Facility Management") rendszerekbe is.

A legtöbb integrált rendszer kliens/szerver felépítésű. Az egyes alrendszerekhez, funkciókhoz külön szerverek (videó, beléptető, adatbázis) tartoznak, a felügyeletet ellátó személyzet pedig különböző jogosultságú kliensként kijelölt munkaállomásokról, vagy akár Interneten keresztül tetszőleges helyről, tetszőleges eszközről férhet hozzá a rendszerhez.

Ezek a mai, még a múlt évszázad filozófiájára és technológiájára alapozó felügyeleti szoftverek valójában még nem igazi integrált rendszerek, hanem különböző cégek egyedi alrendszereit összefogó, többnyire az alrendszerek központjaival kommunikáló programok.

A jövő „valódi" integrált rendszerei hálózatba szervezett érzékelő és beavatkozó elemeket fognak alkalmazni, adaptív, öntanuló, elosztott intelligenciájú virtuális alrendszerekbe szervezve. Az integráció már az érzékelők szintjén megvalósul, egy érzékelő több virtuális alrendszer részeként működhet. Egy-egy virtuális alrendszer sokféle érzékelőt alkalmazhat, kihasználva a szinergia-hatás előnyeit.

3.2. IP (INTERNET PROTOCOL) ALAPÚ INTEGRÁCIÓ

ÚJ GONDOLKODÁSMÓD, ÚJ LEHETŐSÉGEK

Az IP (Internet Protocol), ez a – már nem is annyira új - technológia nagy lehetőségeket kínál az integrált vagyonvédelmi megoldások számára is.

A korábbi években az elektronikus vagyonvédelem és az intelligens épület menedzsment területén jó néhány szakember hiányolta az eszközök és rendszerek fejlesztési irányzatainál az IP alapú kommunikációt.
Bár egy mindenre alkalmas általános megoldást nem jelent, de az IP alapú kommunikáció valóban egy jól alkalmazható új terület az elektronikus vagyonvédelemben és az intelligens épület menedzsmentben.

Egyik szemléletes példa erre a 24 órás videó rögzítés. A korábbi CCTV rendszerek döntő hányadát 24 órás rögzítéssel tervezték, mivel ez volt az egyetlen lehetőség, hogy egy eseménnyel kapcsolatos minden fontos információról felvétel készüljön. Nagyon ritkán alkalmaztak eseményvezérelt rendszereket, mivel ezeknél a telepítők nem tudták garantálni minden lényeges mozzanat rögzítését.
Egy behatoló például néhány másodperc alatt átjut egy kerítésen. Mire egy érzékelő jelzésére a videó rögzítő elkezdi felvenni a helyszíni kamera képét, a behatoló legtöbbször már túljut a megfigyelt zónán. A digitális videó rögzítők megjelenéséig nem volt más megoldás, mint a folyamatos felvétel. A digitális videó felvevők, a „pre-alarm" tárolók megjelenésével azonban lehetőség nyílt a riasztás előtti események rögzítésére és ezzel reális alternatíva adódott a folyamatos rögzítés felváltására.

A hagyományos dedikált rendszereket alkalmazó megoldások sok hátrányt jelenthetnek a végfelhasználónak, legtöbbször annak tudta nélkül. Ezek a hátrányok egy a régitől gyökeresen eltérő biztonságtechnikai filozófiával kiküszöbölhetők.

Adatgyűjtés, többcélú adatfeldolgozás

Nézzük meg, mit jelenthet az adatgyűjtés és a többcélú adatfeldolgozás. Vegyünk egy épületet, ahol behatolás jelző rendszert, zártláncú TV rendszert és beléptető rendszert kell telepíteni.

A hagyományos behatolás jelző rendszer funkciója, hogy élesített állapotban (amikor az épületet bezárják) mozgás érzékelésekor riasztást generáljon. Ezen a funkcióján túl mást nem tesz. Nem élesített állapotban az érzékelők továbbra is jelzik a mozgásokat, de a behatolás jelző központ nem dolgozza fel a jelzéseket. Lényeges, a területen személyek jelenlétét vagy jelen nem létét jelző információk, adatok így nem kerülnek felhasználásra. Holott a mozgás hiányát jelző információ jelezheti, hogy az adott zónában nem tartózkodik senki és ezt más rendszerek (világítás, fűtés, szellőztetés) egyes funkciói (indítás, leállítás, szabályozás) bemenő adatként használhatják.

Integrált rendszer alkalmazásával egy egyszerű behatolás jelző rendszert más szerepkörben is használva például jelentős energia és költség megtakarítást érhetünk el.

Sok objektumban jelentős összegeket költenek **zártláncú TV rendszer** kiépítésére, vagyonvédelmi céllal. Legtöbb helyen a videó információk őrző-védő szolgálatok által felügyelt ügyeleti helyiségekben kerülnek megjelenítésre, rögzítésre. Biztonságtechnikai esemény bekövetkezésekor az ügyeletesek az eseménynek megfelelően intézkednek. A közbenső időben, amikor nem történik biztonságtechnikai szempontból fontos esemény, a videó információkat többnyire semmire sem használják.

IP alapú integrált technológia alkalmazásával a videó adatok bárki által, bárhonnét elérhetők, akinek szüksége és jogosultsága van a hozzáférésre, egyes kamerák képének megtekintésétől akár a teljes rendszer vezérléséig. Egy áruházi alkalmazásnál például ellenőrizhető a gondolák, áruk megfelelő elhelyezése, a beszállítók érkezése, távozása Irodai alkalmazásoknál ellenőrizhető a személyzet mozgása, a munkatársak hivatalos szüneteken túli kinn tartózkodása.

A **beléptető rendszerek** már ma is sokkal inkább kapcsolódnak más, például munkaidő nyilvántartó rendszerekhez, mint más biztonságtechnikai rendszerek. Az IP alapú technológia alkalmazásával a beléptető rendszerek adatainak felhasználása még szélesebb körűvé tehető.

A felhasználási lehetőségek korlátlanok, csak a tervező/telepítő és a felhasználók képzelete szab határt. Az IP alapú integrált rendszer minden számítógépes munkaállomásról elérhető és igény szerinti, dinamikusan változtatható rendszerek alakíthatók ki.

AZ IP ALAPÚ RENDSZEREK ALKALMAZÁSÁNAK ELŐNYEI

Működési, funkcionális előnyök.

Lehetővé válik a rendszerek táv-elérése és távvezérlése és ez által a helyi rendszerek korlátainak kitágítása. Ehhez kapcsolódóan a rendszerek adatai, legyenek akár CCTV, beléptető rendszer, vagy integrált rendszer adatbázisai, tetszőlegesen szétoszthatók az egyes felhasználók között.

Telepítési előnyök.

A beruházók számára a beruházási költségeknél jelentkező előnyöket kell megvilágítani. Például, hogy a beruházási költség egy már meglévő kábelrendszer használatával óriási mértékben csökkenthető. Vagy, hogy még egyedi, dedikált kábelezés kiépítésénél is nagymértékű megtakarítás érhető el a hálózati technológia alkalmazásával. Egy rendszernél például, ahol több videó kamerát, vagy beléptető terminált olvasókkal kell az objektum egy távolabbi részén telepíteni, a felügyeleti központból mindkettőhöz külön kábelezést kellene kiépíteni. Még ha analóg kamerákat alkalmazunk is, azokat egy helyi videó szerverhez csatlakoztatva, vagy IP kamerákat és IP olvasókat egy modulra kötve, egyetlen kábellel csatlakozhatunk a felügyeleti központhoz, vagy a hálózathoz.

3.3. INTEGRÁLT VAGYONVÉDELMI RENDSZEREK TERVEZÉSI FOLYAMATA

A BIZTONSÁGVÉDELMI PROGRAM

Egy létesítmény vagyonvédelmi rendszerének megtervezéséhez szükséges a létesítmény biztonságvédelmi programjának a kidolgozása. A program több összetevőt tartalmaz:

- A fizikai védelem: a mechanikai és elektronikai védelem.
- Az információ-védelem: azonosítás, hitelesítés, hozzáférés-szabályozás.
- Az emberi tényező: az alkalmazottak, a biztonsági személyzet és a vezetők.
- A védelmi politika: előírások, szabályzatok, intézkedési tervek, jogosultságok, felelősségek.

A program alapjául az adott cég védelmi filozófiája, „küldetés-nyilatkozata" szolgál.[32]

A VÉDELMI FILOZÓFIA

A „Da Vinci kód" című könyv elején szó esik a Louvre behatolás jelző rendszerének működéséről. A képtár védelmi koncepciójának alap-filozófiája nem a tolvajok kizárása, távoltartása, hanem azok megfogása, a képek „benntartása" az épületben. [30]

A múzeumok, képtárak behatolás jelző rendszereinek tervezésénél fontos szempont a magas szintű védelemnek a látogatók zavarása nélkül történő biztosítása, a „láthatatlan biztonság" („Invisible Security") megvalósítása. [31]
A védelmet rejtett vagy miniatűr érzékelők biztosítják, látható korlátok, sorompók nélkül. A képek, faliszőnyegek mögé szerelt közelítés-érzékelők, súlyérzékelők, rejtett kamerák nem zavarják a látogatókat, nem közvetítenek feléjük állandó fenyegetettség-érzetet.

[32] Példaképp egy cég küldetés-nyilatkozata: „A Cég biztonságvédelmi programja minden alkalmazottjának, ügyfelének és látogatójának nyitott és biztonságos környezetet garantál, ami elősegíti a kreatív, innovatív munkát. Az integrált vagyonvédelmi rendszer és menedzsment biztosítja a Cég tárgyi és szellemi tulajdonának védelmét, az információtechnológia- és az üzleti hírszerzés területén is."

Az elegáns, exkluzív üzletek vásárlói sem veszik jó néven, ha potenciális tolvajként kezelik őket. Emiatt a biztonsági rendszer elemeit, az érzékelőket, áruvédelmi kapukat itt is rejtve kell elhelyezni.

A másik megközelítés, védelmi filozófia az elriasztás, elrettentés a betörések, lopások megelőzése érdekében.

A komplex vagyonvédelem összetevői (megelőző intézkedések, mechanikai védelem, elektronikus jelzőrendszer, élőerős védelem, biztosítás, saját kockázat) közül a mechanikai védelem, az elektronikus jelzőrendszer és az élőerős védelem kialakításánál is szempont lehet az elriasztó funkció kiemelése. Erős, magas kerítés, vasrács az ablakokon, jól látható kültéri szirénák, kamerák, fegyveres biztonsági őrök a bejáratoknál, mind azt szolgálják, hogy ne ide törjenek be, ne itt raboljanak.

Ez a fajta védelmi filozófia azonban nemcsak az alkalmi bűnözők esetleges elriasztását segítheti, hanem állandó fenyegetettség-érzetet alakít ki a tulajdonosokban, felhasználókban, az egész társadalomban.

Az Európa Tanács Információs Társadalom Technológiák Tanácsadói Testülete 2000-ben indított, 2010-ig tervezett „Intelligens környezet” („Ambient Intelligence”) projektjében az átlagemberek környezetének intelligenssé tételét célozta meg.
Az információs és kommunikációs technológiák fejlődésével lehetővé válik felhasználóbarát, ember-központú, az emberi tevékenységeket, interakciókat támogató, kiszolgáló környezet kialakítása. Az embert körülvevő objektumokba beépülő („embedded”) intelligens, intuitív interfészek segítségével a környezet képes érzékelni és felismerni a különböző emberek jelenlétét, szándékaikat, igényeiket és reagálni azokra. Mindezt nem feltűnő, többnyire láthatatlan eszközökkel valósítjuk meg. [32]

Az intelligens környezet koncepció az intelligens épületek által nyújtott előnyöknek (kényelem, biztonság, hatékonyság, gazdaságosság) a kiterjesztése az ember környezetének legkülönbözőbb régióira.

Fejlettebb régiókban ma már az építészek, épületgépészek, villamos- és biztonságtechnikai tervezők közös feladata a legjobb biztonságtechnikai megoldások kialakítása az épületekben úgy, hogy azok ne zavarják a látványt, a „feeling”-et, ugyanakkor hatékonyan szolgálják az élet- és vagyonvédelmet. Az eredmény egy újfajta épülettípus, amely hatékony, de láthatatlan biztonságot nyújt. [33]

A hollandiai Twente Egyetemen az intelligens környezet témán belül 2003-2007. között a „Biometriai azonosítás a láthatatlan biztonság támogatására” kutatási projektben az alábbiakkal foglalkoztak [34]:

- Transzparens biometriai azonosítás (felhasználói közreműködés nélkül)
- Anonim biometriai azonosítás (személyi adatok tárolása nélkül)
- Biometriai azonosítás a lakáson belül

A fenti területek fejlődése már a közeljövőben lehetővé teszi, hogy biometriai azonosító eszközöket is felhasználhassunk a „láthatatlan biztonság” megvalósítására.

KOCKÁZATELEMZÉS

A tervezési folyamat során sok tényezőt kell figyelembe venni, a vonatkozó életvédelmi és vagyonvédelmi jogszabályoktól a rendszert kezelő biztonsági személyzet tagjainak képzettségén át a beruházási és üzemeltetési költségekig. A vagyonvédelmi rendszer tervezése során az első feladat a kockázatelemzés (Risk Analysis) elvégzése.

A kockázatelemzés célja az adott létesítménnyel, üzemeltetésével és a benne folyó tevékenységekkel kapcsolatban esetleg előforduló lehetséges kockázatok azonosítása, csoportosítása és értékelése. Az elemzés során a kockázatok bekövetkezési valószínűségét, okozott hatását, illetve a kockázat bekövetkeztének elkerülését, illetve hatásának csökkentését lehetővé tevő intézkedéseket vizsgáljuk. Az egyes kockázatcsökkentő intézkedések költségeit és várható hatásait figyelembe véve alternatív megoldásokat, javaslatokat dolgozhatunk ki.

Az elemzés során többek között az alábbi tényezőket kell figyelembe venni:

- A létesítmény környezeti adottságai, a környék bűnözési statisztikája.
- A létesítmény építészeti, energetikai, elektronikai, informatikai alrendszerei.
- A létesítmény üzemeltetési rendszerei, szabályzatok, hatósági előírások.
- A létesítmény alapfunkciói, időszakos, kiegészítő funkciók.
- A létesítményben dolgozó, oda látogató személyek összetétele.
- Biztosítási szerződések, feltételek.

A javaslatok közül kiválasztott kockázatcsökkentő intézkedések figyelembevételével készíthető el a védelmi koncepció, majd a rendszerterv.

VÉDELMI KONCEPCIÓ, RENDSZERTERV

A védelmi koncepció a vagyonvédelmi rendszer egyes összetevőinek funkcióit, kapcsolatát, működési módját írja le. Meghatározza a szükséges mechanikai, elektronikai, információ-technológiai alrendszerek, eszközök főbb paramétereit, egymásra-épülésüket, funkcionális jellemzőiket, kezelésük, karbantartásuk módját.

A rendszerterv a rendszer struktúráját, az egyes alrendszerek berendezéseinek, eszközeinek kapcsolatát írja le. A részletes tervezés ennek alapján történhet.

KIVITELI TERV

A kiviteli terv részletes, mindenre kiterjedő tervdokumentáció, amelynek alapján a megfelelő szakképzettségű telepítők megvalósítják a rendszert. A kiviteli terv több részből áll.

A leíró részek többek között tartalmazzák:

- A vonatkozó jogszabályok, előírások, szabványok felsorolását.
- A rendszer és a rendszerelemek működési leírását.
- Az alkalmazott eszközök kiválasztási szempontjait.

- Az alkalmazott eszközök működésének, telepítési előírásainak ismertetését, adatlapjait, megfelelőségi tanúsítványait.
- A felhasznált eszközök táblázatos felsorolását, a telepítési hely és a beállítási paraméterek megadásával.
- A tápegységek, akkumulátor-kapacitások és kábelkeresztmetszetek számításait.
- CCTV rendszereknél az eszközválasztásokat megalapozó megvilágítás, fókusztávolság, felbontás, kábeltípus/kábelhossz, átviteli- és rögzítési-kapacitás számításokat.
- Kábel-listákat, jelöléseket, bekötési listákat.
- A központok és más programozható berendezések programlistáit.
- A telepítési, átadás-átvételi, üzemeltetési és karbantartási utasításokat.
- A szükséges hatósági nyilatkozatokat, engedélyeket.
- A tervezői és munkavédelmi nyilatkozatokat.

A kiviteli terv rajz-dokumentációi közé tartoznak:

- A rendszer blokkvázlatok.
- Eszköz elhelyezési, elrendezési rajzok.
- Szerelési és bekötési rajzok.
- Csövezési és kábel nyomvonal rajzok.
- Tápellátás áramút tervei.
- Jelmagyarázatok.

ENGEDÉLYEZÉSI, MEGVALÓSULÁSI TERV

Hatósági engedélyhez kötött rendszerek (például tűzjelző rendszer) esetén engedélyezési tervet kell benyújtani az engedélyező hatósághoz. Az engedélyezési eljárás során az engedélyező hatóság azt vizsgálja, hogy a kérelemben, a tervben és a mellékletekben foglaltak megfelelnek-e a jogszabályokban, szabványokban előírt szakmai, műszaki és tartami követelményeknek. Az engedélyezési terv tulajdonképpen a majdani kiviteli terv.

A vagyonvédelmi rendszer kivitelezése, telepítése során a kivitelezési tervtől való eltéréseket egyeztetni kell a tervezővel és rá kell vezetni a tervekre. Bonyolultabb, új, korábban még nem alkalmazott eszközöket, megoldásokat tartalmazó terveknél szerencsés, ha a tervező legalább eseti művezetési tevékenységet is végez.

A beruházás befejezésekor a kivitelezés során a kiviteli tervektől történt eltérések, módosítások miatt a kiviteli terv aktualizálásával **megvalósulási tervet** kell készíteni.

A korrekt megvalósulási terv az alapja a hatékony üzemeltetésnek, karbantartásnak, esetleges későbbi átalakításoknak.

3.4. BIZTONSÁGTECHNIKAI ALRENDSZEREK INTEGRÁCIÓJÁNAK KLASSZIFIKÁCIÓJA

Ebben az alfejezetben megvizsgálom és osztályozom a diszjunkt biztonságtechnikai alrendszerek más (biztonságtechnikai és egyéb) alrendszerekkel történő integrálásának lehetséges típusait, formáit és az integrálás általános követelményeit. Az integrált vagyonvédelmi rendszerekkel foglalkozó szabványtervezet[33] struktúráját követve a lehetséges integrációs típusokat két osztályba sorolom, az egyes osztályokon belül további alosztályokat is megadva. Definiálok egy harmadik, általam virtuálisnak nevezett integrációs osztályt is.

1. típusú integrációs osztály

Az 1. integrációs osztály diszjunkt alrendszerei az adott alrendszerek funkcióinak ellátását biztosító saját dedikált eszközöket és központi egységeket tartalmaznak. Az integráció addicionális elemek (kommunikációs hálózat, felügyeleti központ) alkalmazásával valósul meg.[34] Az 1. típusú integrációs osztályba tartozó megoldások nem alkalmaznak az egyes alrendszerek által közösen használt eszközöket, központokat. Ennél az integrációs típusnál az egyes dedikált funkciókat teljesítő diszjunkt alrendszerek semmilyen funkcióját nem befolyásolhatja sem másik, dedikált funkciókat ellátó alrendszer, sem bármelyik addicionális elem.

Az 1. integrációs osztályon belül további alosztályokat is megkülönböztetek.

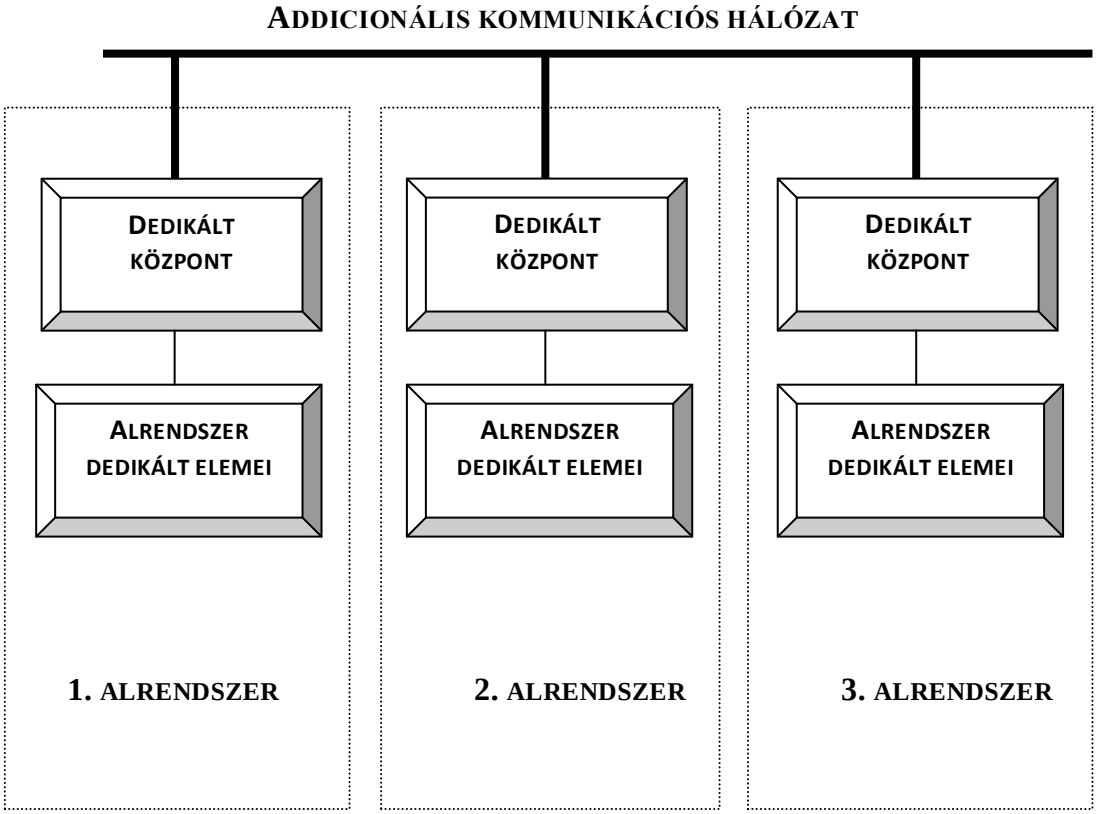
- Az 1A típusú integrációnál addicionális elemként csak a diszjunkt alrendszerek által közösen használható kommunikációs hálózatot alkalmazunk.
- Az 1B típusú integrációnál addicionális elemként helyi felügyeleti központot alkalmazunk az alrendszerek monitorozására, eseményeik naplózására.
- Az 1C típusú integrációnál az egyik diszjunkt alrendszer meglévő központját használhatjuk más diszjunkt alrendszerek monitorozására, eseményeik naplózására.

[33] A vizsgálatokhoz felhasználtam a riasztórendszerek integrálásával foglalkozó CLC/FprTS 50398 szabványtervezetet. [35]

[34] Az alkalmazott addicionális felügyeleti központ általában egy az alrendszerek monitorozására, eseményeik naplózására használt számítógép.

„1A” TÍPUSÚ INTEGRÁCIÓ

Ennél az integrációs típusnál az egyes dedikált, különálló funkciókat ellátó diszjunkt biztonságtechnikai (és esetleg egyéb, például épületgépészeti) alrendszerek közös kommunikációs hálózatot használnak távfelügyeleti központok vagy más rendszerek eléréséhez. Az ilyen típusú megoldásnál az egyes alrendszerek nincsenek hatással egymásra, a közös kommunikációs hálózat addicionális, később is kialakítható.

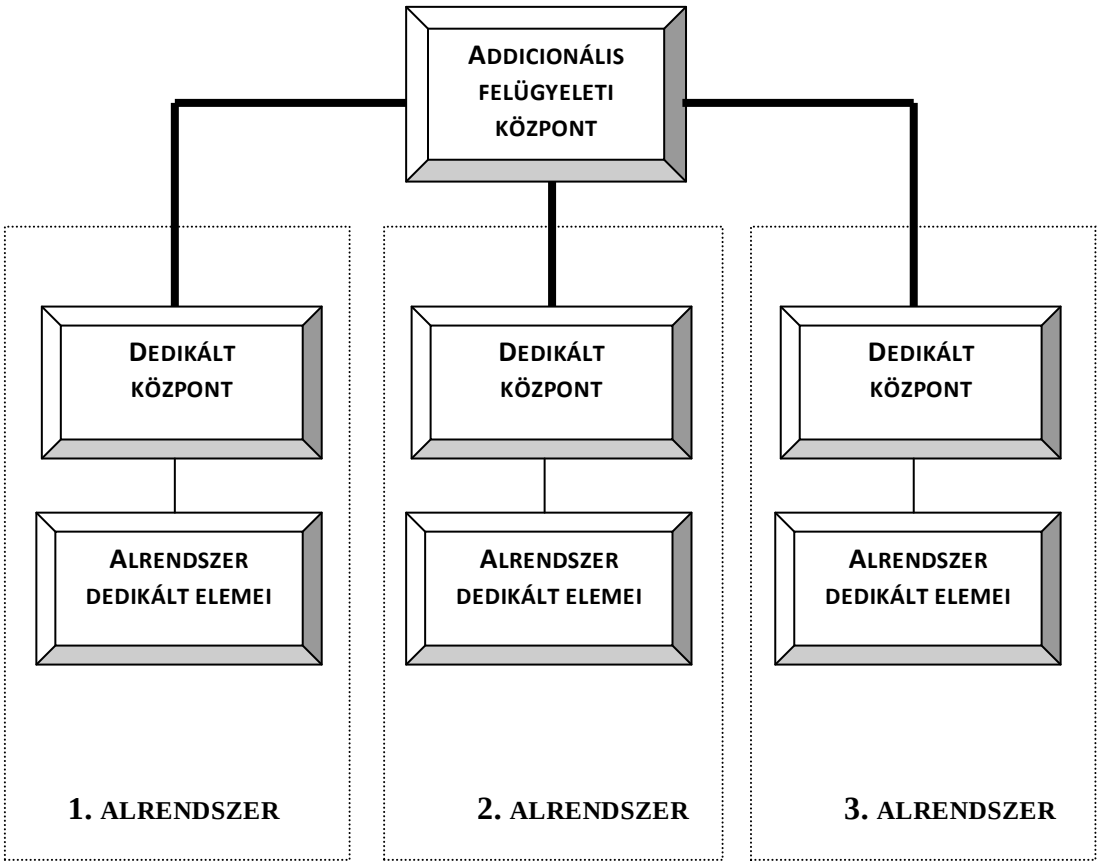


3.1. ábra. „A” típusú integráció

Tipikus alkalmazási példa az „1A” típusú integrációs formára a TCP/IP protokollt alkalmazó helyi LAN hálózat közös használata, amikor például a behatolás jelző alrendszer a távfelügyeleti központ elérésére, a videomegfigyelő rendszer az IP kamerák képeinek távoli elérésére, az épületgépészeti alrendszer pedig távdiagnosztikai célokra ugyanazt a kommunikációs hálózatot használja.

„1B” TÍPUSÚ INTEGRÁCIÓ

Ennél az integrációs formánál az egyes dedikált, különálló funkciókat ellátó diszjunkt alrendszerek által addicionális kommunikációs hálózaton keresztül elérhető felügyeleti központot alkalmazunk az alrendszerek monitorozására, eseményeik naplózására. Az egyes alrendszerek nincsenek hatással egymásra és az addicionális felügyeleti központ sem befolyásolja az alrendszerek funkcióit.

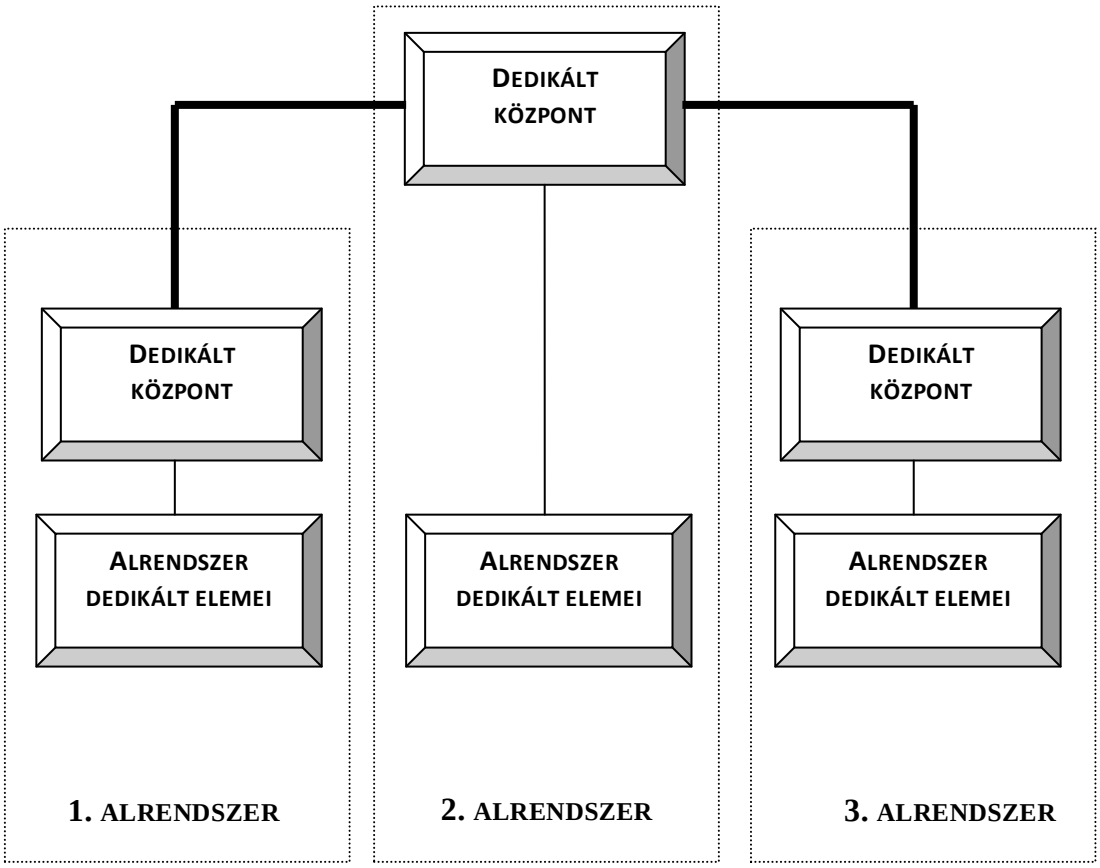


3.2. ábra. „1B” típusú integráció

Tipikus alkalmazási példa az „1B” típusú integrációs formára a behatolás jelző alrendszer állapotainak grafikus megjelenítését és eseményeinek naplózását; a tűzjelző alrendszer állapotainak grafikus megjelenítését és eseményeinek naplózását, valamint a videófelügyeleti rendszer képeinek megjelenítését ugyanazon a felügyeleti számítógépen, de külön felhasználói programokkal ellátó megoldás.

„1C” TÍPUSÚ INTEGRÁCIÓ

Ennél az integrációs formánál az egyik dedikált diszjunkt alrendszer központját alkalmazzuk más alrendszerek monitorozására, eseményeik naplózására is. Az egyes alrendszerek nincsenek hatással egymásra és a monitorozására, események naplózására közösen használt dedikált központ sem befolyásolja a többi alrendszer funkcióit.



3.3. ábra. „1C” típusú integráció

Tipikus alkalmazási példa az „1C” típusú integrációs formára az épületautomatizálási felügyeleti központok alkalmazása, ahol az épületautomatikai alrendszer központja elvégzi a behatolás jelző alrendszer és a tűzjelző alrendszer állapotainak grafikus megjelenítését és eseményeinek naplózását is, de nincs visszahatással azokra.

2. típusú integrációs osztály

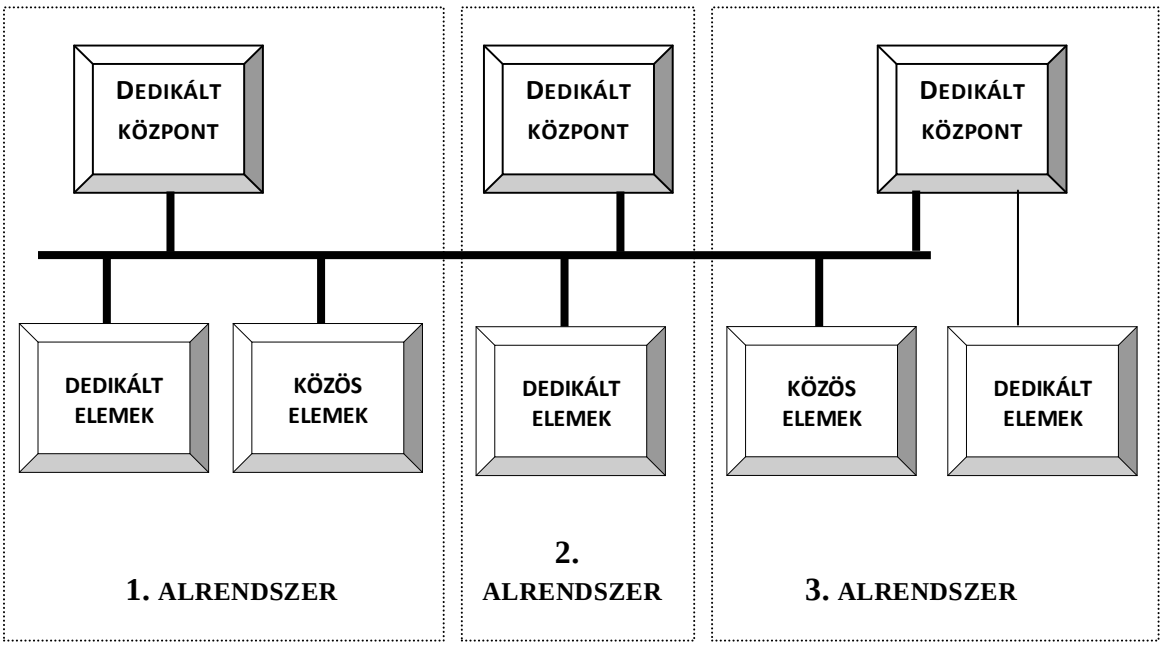
A 2. integrációs osztály alrendszerei az adott alrendszerek funkcióinak ellátására a saját, csak az alrendszerhez tartozó dedikált eszközök mellett más alrendszerekkel közösen használt eszközöket is alkalmazhatnak. Az adott alrendszer dedikált központi egysége mellett vagy helyett más alrendszerekkel közös központi egységek is alkalmazhatók. Az integrációt közösen használt kommunikációs hálózat is segítheti.

Ennél az integrációs típusnál az egyes dedikált funkciókat teljesítő alrendszerek funkcióit más alrendszerek eseményei is befolyásolhatják.

A 2. integrációs osztályon belül is megkülönböztetek további alosztályokat.

„2A" TÍPUSÚ INTEGRÁCIÓ

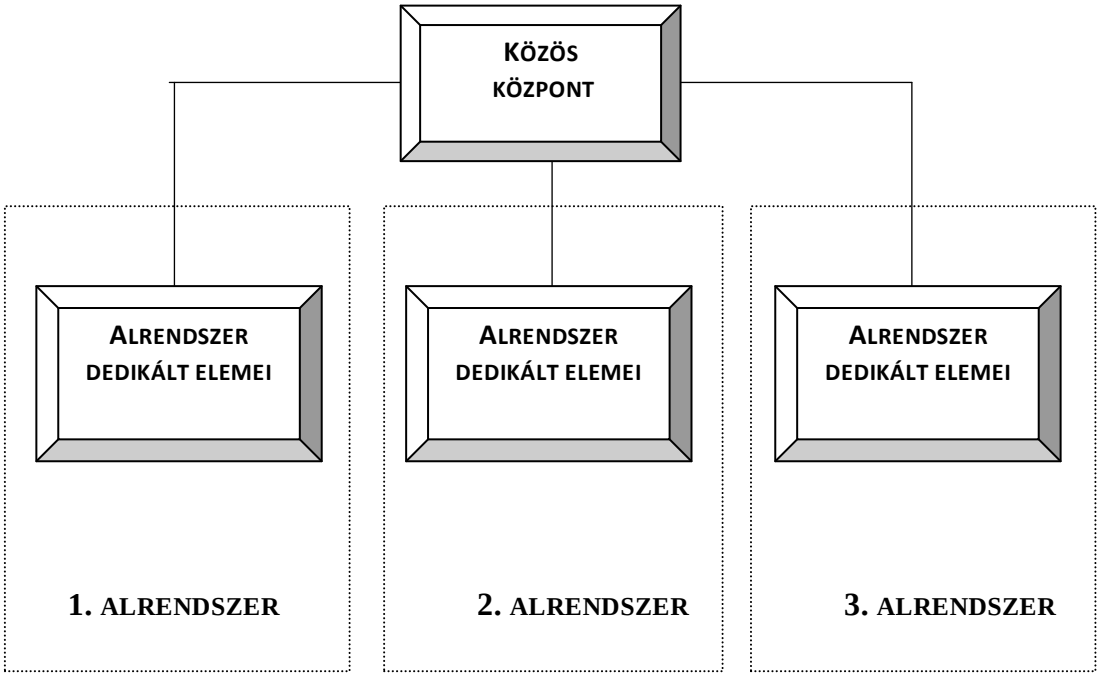
A 2A típusú integrációnál az alrendszerek saját, dedikált központokat és a csak hozzájuk tartozó, dedikált eszközök mellett más alrendszerekkel közösen használt eszközöket alkalmaznak. A közösen használt eszközök eléréséhez a dedikált központok közös kommunikációs hálózatot alkalmaznak.



3.4. ábra. „2A" típusú integráció

„2B” TÍPUSÚ INTEGRÁCIÓ

A 2B típusú integrációnál az alrendszerek saját, dedikált eszközöket, de más alrendszerekkel közös központot alkalmaznak. Az egyes alrendszerek dedikált elemei elkülönült kommunikációs hálózattal kapcsolódnak a közös központhoz

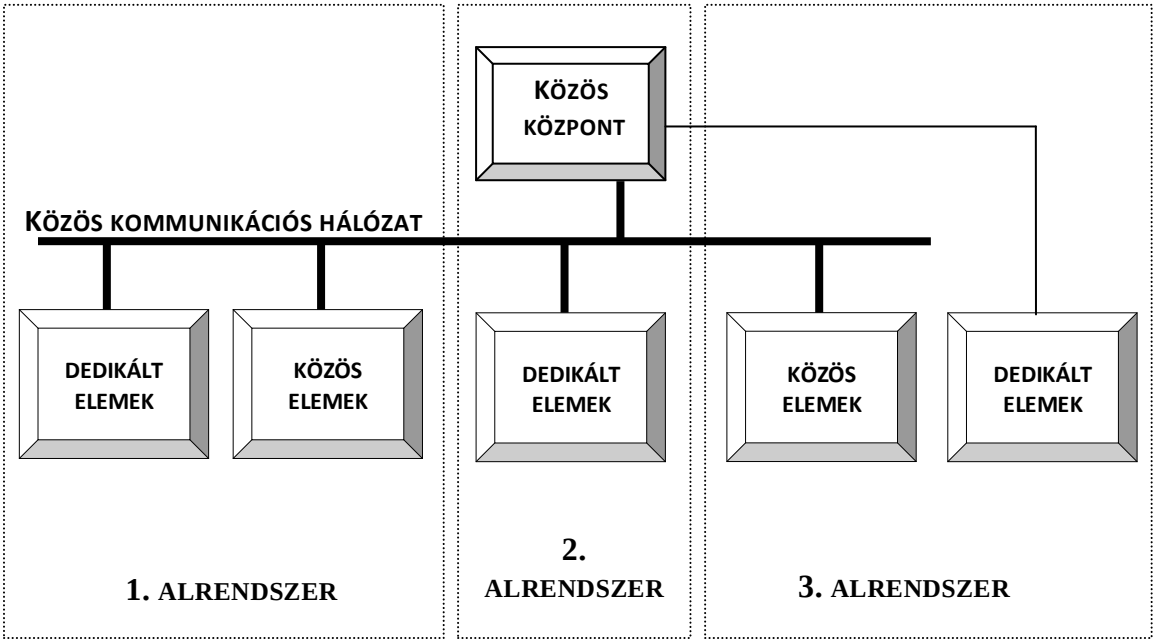


3.5. ábra. „2B” típusú integráció

Tipikus alkalmazási példa a „2B” típusú integrációs formára egy behatolás jelző alrendszer funkcióinak, egy beléptető alrendszer funkcióinak és egyes épületautomatizálási funkcióknak egy közös (behatolás-jelző) központtal történő megvalósítása, integrálása. [36]

„2C” TÍPUSÚ INTEGRÁCIÓ

A 2C típusú integrációnál az alrendszerek más alrendszerekkel közös központot, és a csak hozzájuk tartozó, dedikált eszközök mellett más alrendszerekkel közösen használt eszközöket alkalmaznak. A központ a közösen használt és esetenként a dedikált eszközök eléréséhez is közös kommunikációs hálózatot alkalmaz.



3.6. ábra. „2C” típusú integráció

Virtuális (3. típusú) integrációs osztály[35]

A 3. típusú virtuális integrációs osztály egyetlen integrált rendszer, ahol a rendszer valamennyi eleme közös, a rendszer központjának virtuális processzorai adott alrendszerek funkcióit virtuális alrendszerekként valósítják meg, a 3.1. alfejezet befejező gondolatának megfelelően.[36]

[35] Általam definiált külön osztály. A hivatkozott [35] szabványtervezet csak az 1. és 2. osztályt definiálja.

[36] Ilyen virtuális integrált rendszerek a biztonságtechnikában ma még nem működnek, de csírái a videófelügyeleti rendszereknél már megtalálhatók. Ilyenek például a rendszám-azonosító funkció (beléptető alrendszer), vagy a videó-mozgásérzékelés (behatolás jelző alrendszer). A videórendszerek intelligens funkcióinak további fejlődése is ebbe az irányba mutat.

Az egyes integrációs alosztályok diszjunkt alrendszereinek jellemzőit (dedikált és közös elemek, kommunikációs hálózatok használata) a 3.2. táblázatban foglalom össze.

3.2. táblázat. INTEGRÁCIÓS OSZTÁLYOK DISZJUNKT ALRENDSZEREINEK JELLEMZŐI

Integrációs osztályok	**1.**			**2.**			**3.**
Integrációs alosztályok	**A**	**B**	**C**	**A**	**B**	**C**	
DISZJUNKT ALRENDSZEREK JELLEMZŐI							
Dedikált központ	X	X	X	X	-	-	-
Dedikált elemek	X	X	X	X	X	X	-
Dedikált kommunikációs hálózat	X	X	X	X	X	X	-
Addicionális központ	-	X	-	-	-	-	-
Addicionális kommunikációs hálózat	X	X	X	-	-	-	-
Csatlakozás más alrendszer dedikált központjához	-	-	X	-	-	-	-
Csatlakozás közös kommunikációs hálózathoz	-	-	-	X	-	X	X
Közös elemek más alrendszerekkel	-	-	-	X	-	X	X
Közös központ más alrendszerekkel	-	-	-	-	X	X	X
Virtuális alközpontok	-	-	-	-	-	-	X

RÉSZKÖVETKEZTETÉSEK

A biztonságtechnikai alrendszerek integrálási lehetőségeinek, trendjeinek, tervezési folyamatának leírása, az integrálás előnyeinek, esetleges hátrányainak felmérése is szükséges az integrált rendszerek komplexitásának, integráltsági fokának számításához.

A fejezet elején elemeztem a hagyományos vagyonvédelmi rendszerek lehetőségeit, az egyes alrendszerek diszjunkt voltából adódó hátrányokat, majd funkcióik szerint osztályoztam az épületek gyengeáramú alrendszereit.
Ezt követően az alrendszerek integrálási kényszereinek, lehetőségeinek szempontjából megvizsgáltam az alrendszerek kötelező és lehetséges hatásait más alrendszerekre. Az egyes alrendszerek más alrendszerekre történő hatását interdependencia táblázatban foglaltam össze.

Elemeztem a vagyonvédelmi rendszerek integrációjának tendenciáit, megállapítva az elektronikus vagyonvédelem és az információ-technológia gyorsuló konvergenciáját, majd megvizsgáltam az IP alapú integráció lehetőségeit és előnyeit a hagyományos diszjunkt biztonságtechnikai alrendszerekkel megvalósított vagyonvédelmi rendszerekkel szemben.

Az integrált vagyonvédelmi rendszerek tervezési folyamatának vizsgálatánál elemeztem az objektumok védelmi koncepciójának alapjául szolgáló védelmi filozófiákat, összehasonlítva két, a „láthatatlan biztonság” és az”elriasztás, elrettentés” alapú megközelítést. Megállapítottam, hogy az Európai Unió és más fejlett régiók törekvései a „láthatatlan biztonság” koncepcióval esnek egybe.
A tervezési folyamat fázisainak (kockázatelemzés, védelmi koncepció, rendszerterv kialakítása) bemutatása után részletes felsorolását adtam a kiviteli terv leíró jellegű és rajz dokumentációinak, külön kiemelve a megvalósulási dokumentáció fontosságát.

A következő részben megvizsgáltam és osztályoztam a diszjunkt biztonságtechnikai alrendszerek más (biztonságtechnikai és egyéb) alrendszerekkel történő integrálásának lehetséges típusait, formáit és az integrálás általános követelményeit. Az integrált vagyonvédelmi rendszerekkel foglalkozó szabványtervezet struktúráját követve a

lehetséges integrációs típusokat két osztályba soroltam, az egyes osztályokon belül további alosztályokat is megadva. Definiáltam egy harmadik, általam virtuálisnak nevezett integrációs osztályt is.
Az egyes integrációs alosztályok diszjunkt alrendszereinek jellemzőit (dedikált és közös elemek, kommunikációs hálózatok használata) táblázatban foglaltam össze.

Ezeknek a területeknek a feldolgozása, feltárása is elősegítette a felsőfokú MSc szintű biztonságtechnikai képzésben általam oktatott szakmai tárgyak tananyagának kialakítását. (Szakmai gyakorlat I.-II., Intelligens épületek, Biztonságtechnikai rendszerek tervezése I.-II., A személy és vagyonvédelem rendszertana, Személy és vagyonvédelmi rendszerek kialakításának módszerei, Személy és vagyonvédelmi rendszerek üzemeltetése, üzemfenntartása I.-II.)

Ebben a fejezetben feltártam és leírtam a biztonságtechnikai alrendszerek integrációs trendjeit, lehetőségeit és az integrált biztonságtechnikai rendszerek tervezési folyamatát, klasszifikáltam a biztonságtechnikai alrendszerek integrációjának lehetséges típusait, lehetővé téve nemcsak az egyes alrendszerek, hanem az integrált rendszerek komplexitásának, és az integrált rendszerek integráltsági fokának modellezését is.

Ezzel teljesítettem a kutatási célkitűzések 2. pontját, a „Biztonságtechnikai rendszerek integrálási lehetőségeinek, tervezési folyamatának leírása, a rendszerek integrációs típusainak osztályozása” részt.

4. RENDSZEREK KOMPLEXITÁSA

A komplex villamos rendszerek integráltsági fokának becsléséhez szükség van az adott rendszerek komplexitásának előzetes meghatározására. Általánosságban elmondható, hogy minél nagyobb egy rendszer komplexitása, annál költségesebb a tervezése, kiépítése és üzemeltetése. A rendszer komplexitásának meghatározásával és a komplexitás csökkentésével csökkenthetők lesznek a tervezési, kiépítési és üzemeltetési költségek is. **A komplexitás csökkentésének egyik lehetséges módja a rendszerintegráció.**

Egy adott rendszer komplexitásának meghatározása a rendszer architektúra-modelljének segítségével lehetséges. Egyes források szerint a rendszer-architektúra modell kialakítására, tervezésére általában az összköltségek kevesebb, mint egy százalékát fordítják, holott a rendszer-architektúra kialakítása hatással van az összköltségek több, mint 80 százalékára. Emiatt a kivitelezés közben történő architektúra módosítás igen költséges. [37]

Az integrált vagyonvédelmi rendszerekkel olcsóbban, hatékonyabban és egyszerűbben lehet garantálni a biztonságot és emellett több járulékos előnyük is van.[37]

4.1. DEFINÍCIÓK

RENDSZER

A rendszer olyan elemek együttese, amelyek egymással kapcsolatban, kölcsönhatásban állnak. Másképp: rendszernek nevezzük az egymással strukturális kapcsolatban álló, egymásra kölcsönösen ható rendszerelemek és alrendszerek együttesét.
A rendszer valamely objektuma lehet alrendszer és ugyanaz az objektum egyszerre több rendszernek is lehet az eleme. A rendszerek alrendszerekből, ezek pedig elemekből állhatnak.

[37] A korábban már hivatkozott Jay Hendrix: Top 10 Reasons for Integrating Your Building Systems [2] irodalom meggyőző érveket sorakoztat fel az integráció mellett.

A rendszer **architektúrája**, struktúrája a rendszerelemek halmazát és az elemek kapcsolatát adja meg, ezen keresztül befolyásolhatjuk a rendszer viselkedését. A rendszer-architektúrának sokféle definíciója létezik a definiálás céljától függően. Az egyik, általam is használt definíció szerint: egy rendszer architektúrája a rendszerkoncepció megvalósulása, a fizikai/informatikai funkcióknak a rendszer elemeihez rendelésével és az elemek közötti és a környezethez kapcsolódó interfészek definiálásával. [38]
A struktúrán kívül a rendszerre jellemző még a célja, működési szabályainak összessége, valamint elemeinek tulajdonságai. [39]

MODELL

Bonyolult rendszerek egyszerűsített, minden részletében áttekinthető, gyakorlatilag megvalósított vagy szemléletesen elképzelt, arányosan lekicsinyített vagy felnagyított, matematikailag szabatosan leírható, idealizált mása, amely többé-kevésbé helyesen szemlélteti a vizsgált rendszer vagy folyamat geometriai, kinetikai, dinamikai vagy más fizikai, illetve sztochasztikus sajátosságait. A modell nem azonos a vizsgált rendszerrel vagy folyamattal és nem tükrözi maradéktalanul összes tulajdonságait. A helyesen alkotott modell magán viseli az objektív anyagi világban meglevő rendszer vagy lejátszódó folyamat fontos ismérveit és így alkalmas a döntő törvényszerűségek feltárására és szemléltetésére.

KOMPLEXITÁS

A komplexitás az összetettséggel szinonim kifejezés. Egy olyan aspektusát jelöli a dolgoknak, mely alapján meg tudjuk ítélni, az adott dolog elemi építőelem, vagy egy elemi építőelemekből álló összetett egység, esetleg önmagában álló rendszer. A komplex rendszerben a rendszer elemeiből egy új egység jön létre, azok mintegy önálló struktúrát alkotnak. A komplex (azaz összetett) kifejezést gyakran keverik össze a bonyolult kifejezéssel. A két kifejezés közötti különbséget azok eredetével lehet a legjobban megvilágítani.[38]

[38] A bonyolult, vagy komplikált kifejezés a latin *-plic* végződésből származik, amelynek jelentése összehajtani, hajtogatni; míg a komplex a *plex* kifejezésből, amelynek magyar megfelelője a szőni, fonni. A bonyolult rendszer, tehát egy olyan egység, amelynek egyfajta összetevője van, de amelynek részletei rejtettek maradnak a szemlélő számára; ezért látja bonyolultnak.

A komplexitással kapcsolatban beszélhetünk a redukcióról is, hiszen a redukció egyik jelentése az összetettség, komplexitás csökkentése.

A komplex rendszerek egyik fontos jellemzője a hozzájuk rendelhető hálózat. Abban az esetben, amikor nagyszámú, specifikusan kölcsönható részből áll a rendszer, az egyik legegyszerűbb megközelítés a gráfelméleti leírás. Ahelyett, hogy a teljes dinamikát írnánk le, első közelítésben csak feltérképezzük a kölcsönhatások hálózatát. Már ennek a statikus hálózatnak, gráfnak a topológiája is rejt néhány nem-triviális, újszerű érdekességet a gyakorlati rendszerekre vonatkozóan. Az ilyen gráfoknak sztochasztikus, de korrelált mátrixok felelnek meg, hasonlóan ahhoz, ahogy számos fizikai (például kvantummechanikai, magfizikai) rendszer képezhető le véletlen mátrixokra. [40]

4.2. KOMPLEXITÁS SZÁMÍTÁSI MODELLEK

A rendszer-architektúra modellek komplexitásának mérésére az informatikai rendszerekben sokféle módszert alkalmaznak. Ezek közül néhány a komplex villamos rendszerek komplexitásának meghatározásánál is alkalmazható.

A legtöbb módszer alapgondolata, hogy minél komplexebb egy rendszermodell, annál több információt tartalmaz, illetve annál több információ szükséges a leírásához:

$$\mathbf{I(M) > I(N) \rightarrow K(M) > K(N)} \qquad \mathbf{(4.1)}$$

ahol M és N a rendszermodellek, I(M) és I(N) a rendszermodellek információtartalma, K(M) és K(N) pedig a rendszerek komplexitása. [41]

A különböző komplexitás-meghatározó módszerek a modellek információtartalmának mérésében különböznek.

AZ ALGORITMIKUS KOMPLEXITÁS-ELMÉLET

Az alapötlet egy adott sztring előállításához egy adott gépen (általában Turing gépen) szükséges program hosszának a mérésére visszavezetni a komplexitás mérését.[39]

Ha adott egy Turing gép (T) és egy bináris sztring (s), akkor az s sztring komplexitását a T gépen az s sztring előállításához szükséges legrövidebb program (p) hosszával definiáljuk,

$$\mathbf{K_T(s) = min\{l(p): T(p) = s\}} \qquad \mathbf{(4.2)}$$

ahol $K_T(s)$ az s sztring Turing gépen értelmezett algoritmikus komplexitása, l(p) pedig a p program hossza.

A fenti definíció felhasználható adott rendszermodell komplexitásának definiálására is.

Adott egy S rendszer és a rendszer modelljének leírására (kódolására) használt L leíró nyelv (c: S -> L). Nevezzük az S rendszer L nyelven leírt (kódolt) modelljét $c_L(S)$ – nek.

Ekkor az adott rendszermodell Turing gépen értelmezett algoritmikus komplexitása

$$\mathbf{K_T(c_L(S)) = min\{l(p): T(p) = c_L(S)\}} \qquad \mathbf{(4.3)}$$

A definíció alkalmazásával összehasonlíthatóvá válik tetszőleges rendszermodellek komplexitása, feltéve, hogy azonos leíró nyelvet és azonos Turing gépet használunk.

A definíció nem magának a modellezett rendszernek, hanem a rendszert leíró modellnek a komplexitására vonatkozik. Feltételezzük viszont, hogy a modell komplexitása korrelál az adott rendszer komplexitásával.

A rendszerek és modellek komplexitásának összehasonlításához meg kell határozni az egyezés kritériumait. Kétféle egyezést vizsgálhatunk, belsőt és külsőt.

[39] Először A.N. Kolgomorov publikálta 1965-ben.: Andrei N. Kolmogorov. Three approaches for defining the concept of information qantity. Problems of Information Transmission, 1965.

Két rendszer külsőleg akkor egyező, ha azonos bemeneti változásokra azonos kimeneti reakciókkal válaszolnak. Vagyis, ha kívülről nézve nem lehet őket megkülönböztetni. (A belső azonosság azonos belső struktúrát tételez fel.)

A rendszerek modellezésénél minél részletesebb a leírás, annál komplexebb lesz a modell.
Az összehasonlíthatóság érdekében az egyes rendszereket azonos részletességgel kell modellezni.

(Ez azt is jelentheti, hogy két rendszert azonos részletességgel leírt elemekkel modellezünk és a különbség esetleg csak az egyes elemek kapcsolatában, azaz az interfészekben található.)

A komplexitás (és a későbbiekben az integráltság) meghatározásánál az alkalmazott módszernek teljesítenie kell a következő kritériumokat: [42]

1. Ha egy M és egy N rendszermodellre K(M) >< K(N), akkor a mérési módszernek is különböző komplexitás értékeket kell adnia.
2. Minden M és N rendszermodellre K(M) < K(MuN) és K(N) < K(MuN), azaz, egy rendszer komplexebb, mint az alrendszerei.
3. Létezhet olyan M, N és O rendszermodell, amelyekre K(M) = K(N) és K(MuO)>< K(NuO), azaz az M és O közötti interfészek különböznek az N és O közötti interfészektől.
4. Létezhet olyan M és N rendszermodell, amelyeknél N az M rendszerelemeinek a permutációja és K(M) >< K(N), azaz az elemek interfészeinek megváltozása megváltoztatja a komplexitás mértékét.
5. Létezhet olyan M és N rendszermodell, amelyeknél K(M) + K(N) kisebb, mint K(MuN), azaz a rendszerek egyesítése új interfészeket hoz létre.

Ezek a kritériumok a komplex villamos rendszerek komplexitásának meghatározásánál is fontosak. Az alábbiakban a komplex villamos rendszereknél (az integráltság meghatározására is) alkalmazható módszereket tekintem át.

MEYER MÓDSZERE

Meyer a komplexitási tényezőt az alábbi módon számolja:

$$\mathbf{K(M) = (N_{Mp} \times N_{Mt} \times N_{Mi})^{1/3}} \qquad \mathbf{(4.4)}$$

ahol K(M) a komplexitási tényező értéke, N_{Mp} az elemek száma, N_{Mt} az elemtípusok száma, N_{Mi} pedig az interfészek száma. [43]

A módszer egyszerű, de csak a nagyon részletes, a rendszerelemeket részletesen leíró rendszer modelleknél ad szignifikánsan eltérő értékeket.

CRAWLEY KOMPLEXITÁS DEFINÍCIÓI

Crawley szerint a komplexitás a rendszerek abszolút, meghatározható tulajdonsága.

Három, a rendszerek komplexitását befolyásoló tényezőt definiál: A kapcsolódások számát és típusát, a kapcsolatok bonyolultságát és a kapcsolatok érzékenységét, vagy tűrőképességét. Fontosnak tartja az interfészek milyenségét, minthogy egyik interfész komplexebb lehet, mint egy másik.

Definiálja az elemi szintű *részt*, a komplexitás mérésének elemi, tovább nem bontható egységét. A *modul* nála részek csoportja.

A *részek kapcsolata* négyféle lehet: logikai, topológiai, alkalmazási és műveleti kapcsolat.

Háromféle komplexitást definiál:

1. A *„lényegi komplexitás*” az a minimális komplexitás, amely még lehetővé teszi a szükséges funkciók megvalósítását.

2. Az *„észlelt komplexitás*” a megfigyelő által a különböző részletességű modelleken tapasztalt komplexitás.
3. A *„valódi komplexitás*” a valódi rendszer tényleges komplexitása.

Crawley szerint az *észlelt komplexitást* a megfigyelő (tervező, kivitelező, karbantartó) által még felfogható, megérthető komplexitási szint alatt kell tartani, mert különben a rendszer tervezése, kivitelezése, üzemeltetése, szervízelése drága és hiba-érzékeny lesz.

A *„valódi komplexitás*” soha sem lehet kisebb, mint a *„lényegi komplexitás*”, máskülönben sérülnek a rendszer funkciói. Egy rendszer megvalósítása során, az absztrakciós szint elmélyítésével (a rendszer részletesebb leírásával) a komplexitás nő. [44]

Crawley *„lényegi komplexitás*” definíciójának felhasználásával a komplex villamos rendszerek biztonságtechnikai alrendszereinek összehasonlító elemzésénél egy adott alrendszerrel szemben támasztott funkcionális követelmények alapján meghatározható az adott alrendszer adott részletességű modelljének *lényegi komplexitása.* Az alrendszer terveinek hasonló részletességű modellezésével kimutathatóvá válik, hogy az adott terv alapján megvalósítandó biztonságtechnikai alrendszer teljesítheti-e a vele szemben támasztott funkcionális követelményeket. Ezzel lehetővé válik például tendertervek objektív értékelésének támogatása.

KINNUNEN INTERFÉSZ KOMPLEXITÁS SZORZÓJA

Crawley felvetése alapján Kinnunen kidolgozta az interfészek komplexitásának figyelembevételét lehetővé tevő *interfész komplexitás szorzó* fogalmát, amely a rendszermodellek komplexitásának pontosabb mérését teszi lehetővé.
(Ezt a későbbiekben adott biztonságtechnikai alrendszerek komplexitásának meghatározásánál én is alkalmazom.)

Bár Kinnunen az interfész fogalmat általános értelemben használja, amely anyag, energia és információ csere céljára szolgálhat, a továbbiakban csak az információcsere céljára szolgáló interfészeket vizsgálom.

Az interfész komplexitás szorzó meghatározásakor az adott interfész alábbi jellemzőit lehet figyelembe venni:

- *Távolság* – Minél nagyobb az áthidalandó távolság, annál több információ szükséges az interfész specifikálásához.

- *Átvitt információ mennyisége* – A nagyobb tömegű információ átvitelére alkalmas interfész specifikálásához több információ szükséges.

- *Minőségi követelmények* – Például a kisebb hibaarányt biztosító interfész specifikálásához több információ szükséges.

- *Megbízhatósági követelmények* – A nagyobb megbízhatóság specifikálásához több információ szükséges.

- *Tűrések* – Például nagyobb feszültség, frekvencia, idő tűrési tartományok megvalósításának specifikálásához több információ szükséges.

- *Környezeti feltételek* – Egy nagyobb környezeti hőmérséklettartományban, zajos környezetben is működő interfész specifikálásához több információ szükséges.

- *Általános használat, szabványosítás* – Egy általánosan használt, ismert, vagy szabványos interfész specifikálásához kevesebb információ szükséges, mint egy egyedi, vagy újdonságnak számító interfészéhez.

Az interfész komplexitás szorzó alapértéke 1. A fenti jellemzők figyelembevételével ezt többszörözhetjük. Ezzel azt a tényt vesszük figyelembe, hogy az adott modell absztrakciós szintjén a komplexebb interfészek részletei rejtve maradnak, ezt kompenzáljuk a szorzó megemelt értékével. A gyakorlatban a szorzó értéke maximum 10 lehet. Ha ennél komplexebb interfészt kell kezelnünk, akkor érdemes a modellben az adott interfész dekompozíciójával az interfészt több részre bontani. [45]

Ha egy adott modellről egy részletesebb modellre térünk át, ahol az előző modell egy interfészét például két részre bontva modellezzük, akkor az előző modell interfészének komplexitás szorzóját a részletesebb modell két interfésze megosztva kapja. (Például egy hatos interfész komplexitás szorzójú modul dekompozíciójával kapott két rész között az interfész komplexitás szorzó 3 + 3 vagy 2 + 4 arányban kerülhet megosztásra).

4.3. RENDSZER MODELLEK KOMPLEXITÁS JELLEMZŐI

A rendszer-architektúra modellek sok információt tartalmaznak a rendszer összetevőiről, objektumokról, folyamatokról, kapcsolat-típusokról, rendszer-állapotokról és interfészekről (objektum-folyamat párokról).
Ahhoz, hogy egyetlen számmal jellemezhessük egy rendszer komplexitását, egyszerűsített modellre van szükség.
Egyes szerzők önkényesen választanak ki néhány összetevőt, jellemzőt és abból próbálják valamilyen egyszerűbb (például a Meyer-féle háromelemű) módszerrel kiszámítani egy adott rendszermodell komplexitását. Még tovább egyszerűsítve, akár két rendszer-jellemző adatból (például a részek és az interfészek számából) négyzetátlagot számítva is lehet összehasonlítani rendszereket.

Akár ilyen redukált, vagy más, kombinált eljárásokat alkalmazunk, először ki kell választanunk a modellből meghatározható jellemzőket.

A komplexitás meghatározásánál számba vehető jellemzők:

1. ***Elemtípusok száma*** – Minél többféle típusú elemből áll, annál komplexebb a modell.

2. ***Egy adott típushoz tartozó elemek száma*** – Minél több elem tartozik egy adott típushoz, annál több információ kell a modell leírásához. (A leíráshoz szükséges információ-mennyiség azonban nem feltétlenül lineárisan függ az elemek számától.)

3. ***Egy adott objektumra hatással lévő folyamatok száma*** – Minél több folyamat befolyásol egy adott objektumot, annál több információ szükséges a modell leírásához. Hasznos lehet számolni a minimális, maximális és átlagos számával is az adott objektumra hatással lévő folyamatoknak. Amennyiben a minimum nulla, akkor az adott objektum egy passzív, vagy a rendszer-modelltől elkülönülve létező objektum.

4. ***Egy folyamat által befolyásolt objektumok száma*** - Minél több objektumot befolyásol egy adott folyamat, annál több információ szükséges a modell leírásához. Kezelése hasonló lehet az előző jellemzőéhez.

5. ***Folyamatonkénti operandusok száma*** – Ennél a jellemzőnél is érdemes számolni az operandusok minimális, maximális és átlagos számával. A magas átlag vagy maximum nagy komplexitású rendszerre utal.

6. ***Az interfészek száma*** – Minél több interfészt tartalmaz egy modell, annál komplexebb. Az egyes interfészek komplexitásának eltérését az ***interfész komplexitás szorzóval*** lehet kompenzálni.

A fenti jellemzők alkalmazásával összehasonlítható az egyes rendszermodellek komplexitása.

A jelen dolgozat keretei között a biztonságtechnikai alrendszerek makro-szintű vizsgálatához a gyakorlatban is alkalmazható jellemzők az architektúra modellből adódó 1., 2., és 6. jellemző.

A folyamatokhoz kapcsolódó 3., 4., 5. jellemző nagyobb rendszerek mikro-szintű komplexitás-számítási modelljeinél jöhetnek számításba, de ehhez szükséges a rendszermodulok szoftverének, programjának részletes ismerete is.

4.4. DISZJUNKT BIZTONSÁGTECHNIKAI ALRENDSZEREK KOMPLEXITÁS JELLEMZŐI

BEHATOLÁS JELZŐ RENDSZEREK KOMPLEXITÁSA

A behatolás jelző rendszerek komplexitás számítási modelljénél a rendszerjellemzők közül az alábbiakat veszem figyelembe:

1. ***Elemtípusok száma***
   Központ, érzékelők, jelzésadók, kezelők, bővítő modulok, tápegységek (Minél többféle típusú elemből áll, annál komplexebb a modell.)

2. ***Egy adott típushoz tartozó elemek száma***
   Központ, adott típusú érzékelők, jelzésadók száma.(Minél több elem tartozik egy adott típushoz, annál több információ kell a modell leírásához.)

3. ***Az interfészek száma***
   A központ és az érzékelők, jelzésadók, kezelők, bővítő modulok, tápegységek közötti, valamint a bővítő modulok és az érzékelők, jelzésadók közötti interfészek száma. (Minél több interfészt tartalmaz, annál komplexebb egy modell.)

   Első közelítésben nem teszek különbséget az interfészek között, majd megvizsgálom, hogy az eltérő komplexitású interfészek komplexitásának figyelembevételével milyen változás adódik a rendszer-komplexitás értékében.

A folyamatokhoz kapcsolódó, a behatolás jelző központ programjától függő paramétereket (egy adott objektumra hatással lévő folyamatok száma, egy folyamat által befolyásolt objektumok száma, folyamatonkénti operandusok száma) ennél a modellnél nem alkalmazom. Nagyobb rendszerek mikro-szintű komplexitás-számítási modelljeinél ezek is használhatóak, de ehhez szükséges a központ programjának részletes ismerete is.

A vezetékes rendszerek érzékelői a behatolás jelző központ szempontjából digitális bemeneti adatpontok, általában két feszültségmentes relé kontaktussal adják a riasztás- és a szabotázs-jelzést. A rádiós rendszereknél digitális „táviratok” továbbítják az

érzékelők jelzéseit, a riasztás- és a szabotázs-jelzés mellett alacsony telepfeszültség- és „életjel” jelzéseket is. Az adatátvitel nem szabványosított, gyártó-specifikus, egyedi protokollokkal történik. [46]

Egyes rendszereknél címezhető érzékelők is alkalmazhatóak, amelyek a kezelőegységek, vagy a bővítő egységek adatbuszára csatlakoznak. Az adatátvitel ezeknél is gyártó-specifikus, nem szabványosított, egyedi protokollokkal történik.

Az egyes interfészek komplexitásának eltérését az interfész komplexitás szorzóval veszem figyelembe.

Az interfész komplexitás szorzó számítása

A Kinnunen által az interfész komplexitás szorzó megállapításánál figyelembe venni javasolt interfészjellemzők közül az alábbiakat alkalmazom:

1. ***Adatátviteli távolság*** az egyes eszközök és a központ vagy más modul (például zónabővítő modul) között.

2. ***Átvitt információ mennyisége*** (egy üzenetben vagy a másodpercenként).

3. ***Környezeti feltételek*** a „Riasztórendszerek. 5. rész: Környezetállósági vizsgálati módszerek”, MSZ EN 50130-5:2000 szabvány környezetállósági osztályai (Beltéri I., Beltéri II., Kültéri I., Kültéri II.) szerint. [11]

4. ***Szabványosítás***, az egyes interfészek kommunikációs protokolljainak szabványos vagy egyedi volta alapján.

A többi Kinnunen által említett jellemzőkben a biztonságtechnikai alrendszerek eszközei között nincs szignifikáns különbség, ezért azokat nem alkalmazom az interfész komplexitás szorzó számításánál.

A fenti interfész jellemzőket az alábbi szabályok alapján veszem figyelembe az interfészek interfész komplexitás szorzójának számításánál:

1. A vezetékes, rövid adatátviteli távolságot ($L \leq 50m$) áthidaló, 1 bit/üzenet átvitt információmennyiséget tartalmazó üzenetekkel kommunikáló, a Beltéri I. és a Beltéri II. környezetállósági osztályba tartozó, szabványos protokollú interfészek interfész komplexitás szorzóját 1-nek veszem.

2. A nagyobb adatátviteli távolságot ($L > 50m$) áthidaló interfészeknél +1 értékkel növelem az interfész komplexitás szorzó értékét.

3. Ugyancsak +1 értékkel növelem az interfész komplexitás szorzó értékét a Kültéri I. és a Kültéri II. környezetállósági osztályba tartozó eszközök esetében.

4. A nem szabványos protokollal kommunikáló eszközök interfész komplexitás szorzó értékétét is növelem +1 értékkel.

5. A 2 bit/üzenet átvitt információmennyiséget tartalmazó üzenetekkel kommunikáló eszközök interfész komplexitás szorzó értékétét is növelem +1 értékkel.

6. A 3 bit/üzenet vagy annál nagyobb átvitt információmennyiséget tartalmazó üzenetekkel kommunikáló eszközök interfész komplexitás szorzó értékétét +2 értékkel növelem.

7. A folyamatos vagy kvázi-folyamatos kommunikációt folytató 9.6kbit/s átviteli sebességű modulok interfész komplexitás szorzó értékétét +4 értékkel növelem.

8. A 20kbit/s vagy annál nagyobb átviteli sebességű modulok interfész komplexitás szorzó értékétét +5 értékkel növelem.

9. A speciális, önálló alrendszerként kezelhető modulok (radar, videó kamera) interfész komplexitás szorzóit 10-es értékkel veszem figyelembe.

A behatolás jelző alrendszereknél az érzékelők és egyéb eszközök, modulok táblázatos klasszifikációját a tárgyalt rendszermodellek interfész-specifikus paraméterezési igényeinek figyelembevételével hajtottam végre, és az előzőekben leírt algoritmussal elvégeztem az egyes eszközök interfész komplexitás szorzó értékének meghatározását.

Az eredményeket a 4.1. – 4.8. táblázatokban foglalom össze.

4.1. táblázat. BEHATOLÁS-JELZŐ RENDSZER KÜLTÉRI ÉRZÉKELŐINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG[40]	ÁTVITT[41] INFORMÁCIÓ	KÖRNYEZETI[42] FELTÉTELEK	SZABVÁNYOS[43] PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Passzív infravörös mozgásérzékelő	150m	2 bit	Kültéri II.	Igen	**4**
2.	Passzív infrav. mozgásérzékelő (rádiós)	150m	20 bit	Kültéri II.	Nem	**7**
3.	Mikrohullámú mozgásérzékelő	150m	2 bit	Kültéri II.	Igen	**4**
4.	Mikrohullámú mozgásérzékelő (rádiós)	150m	20 bit	Kültéri II.	Nem	**6**
5.	Kombinált mozgásérzékelő	150m	3 bit	Kültéri II.	Igen	**5**
6.	Kombinált mozgásérzékelő (rádiós)	150m	20 bit	Kültéri II.	Nem	**6**
7.	Infravörös fénysorompó	150m	2 bit	Kültéri II.	Igen	**4**
8.	Mikrohullámú sorompó	150m	2 bit	Kültéri II.	Igen	**4**
9.	Kerítés rezgésérzékelő	150m	2 bit	Kültéri II.	Igen	**4**
10.	Pneumatikus lépésérzékelő	150m	2 bit	Kültéri II.	Igen	**4**
11.	Hidraulikus lépésérzékelő	150m	2 bit	Kültéri II.	Igen	**4**
12.	„Szivárgó-kábeles” lépésérzékelő	150m	2 bit	Kültéri II.	Igen	**4**
13.	Optikai kábeles lépésérzékelő	150m	2 bit	Kültéri II.	Igen	**4**
14.	Szeizmikus lépésérzékelő	150m	2 bit	Kültéri II.	Igen	**4**
15.	Lézer-szkenner, radar	500m	1200 bit/s	Kültéri II.	Nem	**10**
16.	Videó kamera, termo kamera	300m	9600 bit/s	Kültéri II.	Igen	**10**
17.	IP videó kamera	-	100Kbit/s	Kültéri II.	Igen	**10**

[40] A Kinnunen által az interfész komplexitás szorzó megállapításánál figyelembe venni javasolt interfészjellemzők közül az egyes eszközök és a központ vagy más modul (például zónabővítő modul) közötti ***adatátviteli távolságot***,

[41] az egy üzenetben vagy a másodpercenként átvitt ***információ mennyiségét***,

[42] a [11] Riasztórendszerek. 5. rész: Környezetállósági vizsgálati módszerek, MSZ EN 50130-5:2000 szabvány ***környezetállósági osztályba sorolási követelményeit***

[43] és az egyes interfészek kommunikációs ***protokolljainak szabványos vagy egyedi voltát*** vettem figyelembe.

4.2. táblázat. BEHATOLÁS-JELZŐ RENDSZER HÉJVÉDELMI ÉRZÉKELŐINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Mechanikus nyitásérzékelő (2 vezetékes)	20m	1 bit	Beltéri I.	Igen	**1**
2.	Mechanikus nyitásérzékelő (4 vezetékes)	20m	2 bit	Beltéri I.	Igen	**2**
3.	Mechanikus nyitásérzékelő (rádiós)	50m	20 bit	Beltéri I.	Nem	**4**
4.	Reed relés nyitásérzékelő (2 vezetékes)	20m	1 bit	Beltéri I.	Igen	**1**
5.	Reed relés nyitásérzékelő (4 vezetékes)	20m	2 bit	Beltéri I.	Igen	**2**
6.	Reed relés nyitásérzékelő (rádiós)	50m	20 bit	Beltéri I.	Nem	**4**
7.	Kontakt üvegtörés érzékelő	20m	2 bit	Beltéri I.	Igen	**2**
8.	Akusztikus üvegtörés érzékelő	20m	2 bit	Beltéri I.	Igen	**2**
9.	Akusztikus üvegtörés érzékelő (rádiós)	50m	20 bit	Beltéri I.	Nem	**4**
10.	Falbontás érzékelő	20m	2 bit	Beltéri I.	Igen	**2**
11.	Háló-tapéta	20m	1 bit	Beltéri I.	Igen	**1**
12.	Címezhető vezetékes érzékelő	100m	20bit	Beltéri I.	Nem	**5**

4.3. táblázat. BEHATOLÁS-JELZŐ RENDSZER TÉRVÉDELMI ÉRZÉKELŐINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Passzív infravörös mozgásérzékelő (PIR)	20m	2 bit	Beltéri I.	Igen	**2**
2.	Passzív infravörös mozgásérzékelő (rádiós)	50m	20 bit	Beltéri I.	Nem	**4**
3.	Mikrohullámú mozgásérzékelő (MH)	20m	2 bit	Beltéri I.	Igen	**2**
4.	Ultrahangos mozgásérzékelő (UH)	20m	2 bit	Beltéri I.	Igen	**2**
5.	Kombinált (PIR + MH) mozgásérzékelő	20m	3 bit	Beltéri I.	Igen	**3**
6.	Kombinált (PIR + MH) m.érz. (rádiós)	50m	20 bit	Beltéri I.	Nem	**4**
7.	Kombinált (PIR + UH) mozgásérzékelő	20m	3 bit	Beltéri I.	Igen	**3**
8.	Címezhető vezetékes érzékelő	100m	20bit	Beltéri I.	Nem	**5**

4.4. táblázat. BEHATOLÁS-JELZŐ RENDSZER TÁRGYVÉDELMI ÉRZÉKELŐINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Kapacitív közelítés érzékelő	20m	2 bit	Beltéri I.	Igen	**2**
2.	Reflexiós infravörös közelítés érzékelő	20m	2 bit	Beltéri I.	Igen	**2**
3.	Infravörös fénysorompó	20m	2 bit	Beltéri I.	Igen	**2**
4.	Taposószőnyeg	20m	1 bit	Beltéri I.	Igen	**1**
5.	Súlyérzékelő/képakasztó	20m	2 bit	Beltéri I.	Igen	**2**
6.	Kontakt pénzjegycsapda	20m	1 bit	Beltéri I.	Igen	**1**
7.	Reflexiós pénzjegycsapda	20m	2 bit	Beltéri I.	Igen	**2**
8.	Rezgés/fúrás érzékelő	20m	2 bit	Beltéri I.	Igen	**2**
9.	Ultrahangos „vitrin” érzékelő	20m	2 bit	Beltéri I.	Igen	**2**
10.	Infrahangos „vitrin” érzékelő	20m	2 bit	Beltéri I.	Igen	**2**
11.	Címezhető vezetékes érzékelő	100m	20bit	Beltéri I.	Igen	**5**

4.5. táblázat. BEHATOLÁS-JELZŐ RENDSZER SZEMÉLYVÉDELMI ESZKÖZEINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Támadásjelző pedál, taposósín	20m	1 bit	Beltéri I.	Igen	**1**
2.	Taposó (kontakt) szőnyeg.	20m	1 bit	Beltéri I.	Igen	**1**
3.	Térdkapcsoló	20m	1 bit	Beltéri I.	Igen	**1**
4.	Támadásjelző gomb	20m	1 bit	Beltéri I.	Igen	**1**
5.	„Lehajtható fedelű” támadásjelző	20m	1 bit	Beltéri I.	Igen	**1**
6.	Rádiós támadásjelző	50m	20 bit	Beltéri II.	Nem	**4**
7.	Dőlés érzékelő rádiós jelző	50m	20 bit	Beltéri II.	Nem	**4**

4.6. táblázat. BEHATOLÁS-JELZŐ RENDSZER HELYI JELZÉSADÓINAK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Beltéri hangjelző („sziréna”)	20m	1 bit	Beltéri I.	Igen	**1**
2.	Beltéri fényjelző („villogó”)	20m	1 bit	Beltéri I.	Igen	**1**
3.	Beltéri kombinált hang- és fényjelző	20m	2 bit	Beltéri I.	Igen	**2**
4.	Beltéri hang- és fényjelző (akkumulátoros)	20m	4 bit	Beltéri I.	Igen	**3**
5.	Beltéri hang- és fényjelző (rádiós)	50m	20 bit	Beltéri I.	Nem	**4**
6.	Kültéri hangjelző („sziréna”)	50m	1bit	Kültéri I.	Igen	**2**
7.	Kültéri fényjelző („villogó”)	50m	1 bit	Kültéri I.	Igen	**2**
8.	Kültéri hang- és fényjelző (akkumulátoros)	50m	6 bit	Kültéri I.	Igen	**4**
9.	Kültéri hang- és fényjelző (rádiós)	100m	20 bit	Kültéri I.	Nem	**6**

4.7. táblázat. BEHATOLÁS-JELZŐ RENDSZER KEZELŐEGYSÉGEINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	LED kezelőegység	50m	9600 bit/s	Beltéri I.	Nem	**6**
2.	LCD kezelőegység	50m	9600 bit/s	Beltéri I.	Nem	**6**
3.	LCD kezelőegység (grafikus)	50m	9600 bit/s	Beltéri I.	Nem	**6**
4.	LCD kezelőegység (rádiós)	50m	9600 bit/s	Beltéri I.	Nem	**6**

4.8. táblázat. BEHATOLÁS-JELZŐ RENDSZER KIEGÉSZÍTŐ/BŐVÍTŐ MODULJAINAK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Zónabővítő modul	100m	9600 bit/s	Beltéri I.	Nem	**7**
2.	Kimeneti bővítő modul	100m	9600 bit/s	Beltéri I.	Nem	**7**
3.	Segédtáp modul	100m	9600 bit/s	Beltéri I.	Nem	**7**
4.	Rádiófrekvenciás zónabővítő modul	50m	9600 bit/s	Beltéri I.	Nem	**6**
5.	Rádiófrekvenciás kimeneti modul	50m	9600 bit/s	Beltéri I.	Nem	**6**
6.	Kommunikátor modul (GSM, IP)	500m	100Kbit/s	Beltéri I.	Igen	**7**
7.	Hangmodul	1m	20Kbit/s	Beltéri I.	Nem	**6**
8.	X10 épületautomatikai modul	100m	20 bit/s	Beltéri I.	Igen	**7**

A beléptető rendszerek komplexitás számítási modelljénél a rendszerjellemzők közül a behatolás jelző rendszerekhez hasonlóan az alábbiakat veszem figyelembe:

1. ***Elemtípusok száma***
   Vezérlő egység, áthaladás-gátló, nyitottság/zártság érzékelők, rácsukás érzékelők, áthaladás érzékelők, speciális érzékelők, vésznyitók, visszajelző eszközök, olvasók, tápegységek (Minél többféle típusú elemből áll, annál komplexebb a modell.)

2. ***Egy adott típushoz tartozó elemek száma***
   Vezérlő egység, adott típusú érzékelők, jelzésadók száma.(Minél több elem tartozik egy adott típushoz, annál több információ kell a modell leírásához.)

3. ***Az interfészek száma***
   A vezérlő egység és az érzékelők, jelzésadók, olvasók, tápegységek közötti, valamint az on-line rendszereknél a vezérlőegységek és a beléptető központ közötti interfészek száma. (Minél több interfészt tartalmaz, annál komplexebb egy modell.)

   Első közelítésben itt sem teszek különbséget az interfészek között, majd megvizsgálom, hogy az eltérő komplexitású interfészek komplexitásának figyelembevételével milyen változás adódik a rendszer-komplexitás értékében.

   Az egyes interfészek komplexitásának eltérését itt is az interfész komplexitás szorzóval veszem figyelembe.
   A behatolás jelző rendszerhez hasonlóan egy egy-bites digitális adatpontként kezelt eszköz (például egy nyitásérzékelő) interfészének komplexitás szorzója 1, a két-bites, digitális adatpontként kezelhető eszközök (például szabotázskapcsolót is tartalmazó passzív infravörös áthaladás érzékelő) interfészének komplexitás szorzója 2, míg a komplexebb, busz-interfészű eszközök (például olvasók, on-line vezérlő modulok) interfészének

komplexitás szorzója 8 lesz. (A gyakorlatban a szorzó értékét 10 fölé itt sem érdemes emelni. Ha ennél komplexebb interfészt kell kezelni, akkor érdemes a modellben az adott interfész dekompozíciójával az interfészt több részre bontani.)

A folyamatokhoz kapcsolódó, a belépési pont, vagy a beléptető központ programjától függő paramétereket (egy adott objektumra hatással lévő folyamatok száma, egy folyamat által befolyásolt objektumok száma, folyamatonkénti operandusok száma) ennél a modellnél sem alkalmazom. Nagyobb rendszerek komplexitás-számítási modelljeinél ezek is használhatóak, de ehhez itt is szükség van a programok részletes dokumentációjára.

A belépési pont elemeinek, érzékelőknek, olvasóknak és egyéb eszközöknek a táblázatos klasszifikációját itt is a tárgyalt rendszermodellek interfész-specifikus paraméterezési igényeinek figyelembevételével hajtottam végre, és az előzőekben leírt algoritmussal végeztem el az egyes eszközök interfész komplexitás szorzó értékének meghatározását.

Az eredményeket a 4.9. – 4.13. táblázatok tartalmazzák.

4.9. táblázat. BELÉPTETŐ RENDSZER ÉRZÉKELŐINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Mechanikus nyitásérzékelő (2 vezetékes)	20m	1 bit	Beltéri I.	Igen	**1**
2.	Mechanikus nyitásérzékelő (4 vezetékes)	20m	2 bit	Beltéri I.	Igen	**2**
3.	Reed relés nyitásérzékelő (2 vezetékes)	20m	1 bit	Beltéri I.	Igen	**1**
4.	Reed relés nyitásérzékelő (4 vezetékes)	20m	2 bit	Beltéri I.	Igen	**2**
5.	Mechanikus rácsukás érzékelő (2 vezetékes)	20m	1 bit	Beltéri I.	Igen	**1**
6.	Pneumatikus rácsukás érzékelő (2 vezetékes)	20m	1 bit	Beltéri I.	Igen	**1**
7.	Mechanikus zártság érzékelő (2 vezetékes)	20m	1 bit	Beltéri I.	Igen	**1**
8.	Passzív infravörös áthaladás érzékelő	20m	3 bit	Beltéri I.	Igen	**3**
9.	Infravörös fénysorompó	20m	2 bit	Beltéri I.	Igen	**2**
10.	Speciális érzékelők (fémdetektor)	20m	2 bit	Beltéri I.	Igen	**2**

4.10. táblázat. BELÉPTETŐ RENDSZER KIMENETI ESZKÖZEINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ESZKÖZÖK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Vésznyitó gomb (elektronikus)	20m	2 bit	Beltéri I.	Igen	**2**
2.	Áthaladás-gátló engedélyező kimeneti eszköz	20m	1 bit	Beltéri I.	Igen	**1**
3.	Hangvisszajelző eszköz („zümmer”)	20m	2 bit	Beltéri I.	Igen	**2**
4.	Fényvisszajelző eszköz (LED)	20m	2 bit	Beltéri I.	Igen	**2**
5.	LCD visszajelző modul	20m	9600 bit/s	Beltéri I.	Nem	**6**
6.	Hangmodul	2m	20Kbit/s	Beltéri I.	Nem	**7**

4.11. táblázat. BELÉPTETŐ RENDSZER OLVASÓ EGYSÉGEINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Kódbillentyűzet	20m	9600 bit/s	Beltéri I.	Nem	**6**
2.	Vonalkód olvasó	20m	9600 bit/s	Beltéri I.	Nem	**6**
3.	Vonalkód olvasó (Wiegand protokollal)[44]	20m	9600 bit/s	Beltéri I.	Igen	**5**
4.	Mágnes-csíkos kártya olvasó	20m	9600 bit/s	Beltéri I.	Nem	**6**
5.	Mágnes-csíkos kártya (Wiegand protokollal)	20m	9600 bit/s	Beltéri I.	Igen	**5**
6.	Proximity kártya olvasó	20m	9600 bit/s	Beltéri I.	Nem	**6**
7.	Proximity kártya olvasó (Wiegand prot.)	20m	9600 bit/s	Beltéri I.	Igen	**5**
8.	Mikrohullámú kártya olvasó	20m	9600 bit/s	Beltéri I.	Nem	**6**
9.	Mikrohullámú kártya olvasó (Wiegand prot.)	20m	9600 bit/s	Beltéri I.	Igen	**5**
10.	Intelligens kártya olvasó	20m	9600 bit/s	Beltéri I.	Nem	**6**
11.	Intelligens kártya olvasó (Wiegand prot.)	20m	9600 bit/s	Beltéri I.	Igen	**5**
12.	Dallas gombos olvasó	20m	9600 bit/s	Beltéri I.	Nem	**6**
13.	Dallas gombos olvasó (Wiegand prot.)	20m	9600 bit/s	Beltéri I.	Igen	**5**

[44] A beléptető rendszereknél szabványosított adatátviteli protokoll.

4.12. táblázat. BELÉPTETŐ RENDSZER BIOMETRIAI OLVASÓ EGYSÉGEINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Ujjlenyomat olvasó	20m	9600 bit/s	Beltéri I.	Nem	**6**
2.	Kézgeometria azonosító	20m	9600 bit/s	Beltéri I.	Nem	**6**
3.	Írisz szkenner	20m	9600 bit/s	Beltéri I.	Nem	**6**
4.	Retina szkenner	20m	9600 bit/s	Beltéri I.	Nem	**6**
5.	Arc felismerő modul	20m	9600 bit/s	Beltéri I.	Nem	**6**
6.	Arc hő-térkép azonosító modul	20m	9600 bit/s	Beltéri I.	Nem	**6**
7.	Hangminta azonosító modul	20m	9600 bit/s	Beltéri I.	Nem	**6**
8.	Kézírás azonosító modul	20m	9600 bit/s	Beltéri I.	Nem	**6**
9.	Gépírás azonosító modul	20m	9600 bit/s	Beltéri I.	Nem	**6**

4.13. táblázat. BELÉPTETŐ RENDSZER EGYÉB ESZKÖZEINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Szünetmentes tápegység	20m	2 bit	Beltéri I.	Igen	**2**
2.	IP videó kamera	-	100Kbit/s	Beltéri I.	Igen	**6**

ŐRJÁRAT ELLENŐRZŐ RENDSZEREK KOMPLEXITÁSA

Az őrjárat ellenőrző rendszerek célja, funkciója az élőerős védelmet a helyszínen ellátó őrjáratozó személyek tevékenységének ellenőrzése. Segítségükkel ellenőrizhető, hogy a járőrök a járőrútvonal minden előzetesen kijelölt állomását, ellenőrzési pontját bejárták-e, ezt mennyi időközönként tették meg és mennyi idő alatt értek egyik helyről a másikra.

Az őrjárat ellenőrző rendszerek komplexitás számításának modellezésénél az on-line ellenőrző rendszereket vizsgálom. Ezeknél a rendszereknél a járőr útvonala folyamatosan nyomon követhető, az eredeti járőr-útvonal tervtől való eltérés azonnal jelezhető.

A diszjunkt, önálló on-line őrjárat ellenőrző rendszereknél a járőrözési útvonalon ellenőrzési pontokat telepítünk, amelyek vezetékes vagy rádiós kapcsolatban vannak az őrjárat ellenőrző rendszer központjával. Az ellenőrzési pontokon olvasó terminálokat helyezünk el, amelyek az őrjárat azonosító eszközeinek kódját leolvasva beküldik azokat a központba. Kiegészítő elemként szabotázs-érzékelő dobozfedél kapcsolókat, áthaladás érzékelőket is alkalmazhatnak

A rendszerjellemzők közül a beléptető rendszerekhez hasonlóan az alábbiakat veszem figyelembe:

1. ***Elemtípusok száma***

   Központi egység, olvasók, áthaladás érzékelők, szabotázs-érzékelők, visszajelző eszközök, tápegységek (Minél többféle típusú elemből áll, annál komplexebb a modell.)

2. ***Egy adott típushoz tartozó elemek száma***

   Olvasók, visszajelző eszközök száma.(Minél több elem tartozik egy adott típushoz, annál több információ kell a modell leírásához.)

3. ***Az interfészek száma***

   A központi egység és az olvasó terminálok közötti interfészek száma. (Minél több interfészt tartalmaz, annál komplexebb egy modell.)

   Első közelítésben itt sem teszek különbséget az interfészek között, majd megvizsgálom, hogy az eltérő komplexitású interfészek komplexitásának figyelembevételével milyen változás adódik a rendszer-komplexitás értékében.

   Az egyes interfészek komplexitásának eltérését itt is az interfész komplexitás szorzóval veszem figyelembe.
   A beléptető rendszerhez hasonlóan egy egy-bites digitális adatpontként kezelt eszköz (például egy nyitásérzékelő) interfészének komplexitás szorzója 1, a két-bites, digitális adatpontként kezelhető eszközök (például szabotázskapcsolót is tartalmazó passzív infravörös áthaladás érzékelő) interfészének komplexitás szorzója 2, míg a komplexebb, busz-interfészű eszközök (például olvasók, on-line vezérlő modulok) interfészének komplexitás szorzója 8 lesz.

A folyamatokhoz kapcsolódó, az ellenőrzési pont, vagy az őrjárat ellenőrző központ programjától függő paramétereket (egy adott objektumra hatással lévő folyamatok száma, egy folyamat által befolyásolt objektumok száma, folyamatonkénti operandusok száma) ennél a modellnél sem alkalmazom.

Az őrjárat ellenőrző rendszer elemeinek, érzékelőknek, olvasóknak és egyéb eszközöknek a táblázatos klasszifikációját itt is a tárgyalt rendszermodellek interfész-specifikus paraméterezési igényeinek figyelembevételével hajtottam végre.

Az előzőekben leírt algoritmussal elvégeztem az egyes eszközök interfész komplexitás szorzó értékének meghatározását is.

Az eredményeket a 4.14. – 4.15. táblázatokban foglalom össze.

4.14. táblázat. ŐRJÁRAT ELLENŐRZŐ RENDSZER OLVASÓ TERMINÁLJAINAK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI[45]

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Kódbillentyűzetes terminál (beltéri)	200m	9600 bit/s	Beltéri I.	Nem	**6**
2.	Kódbillentyűzetes terminál (kültéri)	1000m	9600 bit/s	Kültéri II.	Nem	**8**
3.	Vonalkódos terminál (beltéri)	200m	9600 bit/s	Beltéri I.	Nem	**6**
4.	Vonalkódos terminál (kültéri)	1000m	9600 bit/s	Kültéri II.	Nem	**8**
5.	Mágnes-csíkos terminál (beltéri)	200m	9600 bit/s	Beltéri I.	Nem	**6**
6.	Mágnes-csíkos terminál (kültéri)	1000m	9600 bit/s	Kültéri II.	Nem	**8**
7.	Proximity kártya terminál (beltéri)	200m	9600 bit/s	Beltéri I.	Nem	**6**
8.	Proximity kártya terminál (kültéri)	1000m	9600 bit/s	Kültéri II.	Nem	**8**
9.	Dallas gombos terminál (beltéri)	200m	9600 bit/s	Beltéri I.	Nem	**6**
10.	Dallas gombos terminál (kültéri)	1000m	9600 bit/s	Kültéri II.	Nem	**8**

4.15. táblázat. ŐRJÁRAT ELLENŐRZŐ RENDSZER EGYÉB ESZKÖZEINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Szünetmentes tápegység	20m	2 bit	Beltéri I.	Igen	**2**
2.	Szabotázsérzékelő kapcsoló (2 vezetékes)	20m	1 bit	Beltéri I.	Igen	**1**
3.	Passzív infravörös áthaladás érzékelő	20m	3 bit	Beltéri I.	Igen	**3**
4.	Passzív infravörös áthaladás érzékelő	20m	3 bit	Kültéri I.	Igen	**4**

[45] Az olvasó terminálok vezetékes vagy rádiós átvitelt alkalmazhatnak a központ eléréséhez. Az interfész szorzónál alapvető különbség nincs a két típus között.

RÉSZKÖVETKEZTETÉSEK

A komplex villamos rendszereknél az integrált vagyonvédelmi rendszerek integráltsági fokának becsléséhez szükség van az adott alrendszerek komplexitásának előzetes meghatározására. Egy adott rendszer komplexitásának meghatározása a rendszer architektúra-modelljének segítségével lehetséges.

A fejezet elején megadtam a rendszer, a modell és a komplexitás általam használt definícióját.

Ismertettem és elemeztem a rendszer-architektúra modellek komplexitásának mérésére az informatikai rendszerekben alkalmazott algoritmikus komplexitás elméletet és a komplexitás meghatározásánál az alkalmazandó módszer által (biztonságtechnikai alrendszerek modellezésénél is) teljesítendő kritériumokat.

Megvizsgáltam a rendszerek komplexitását leíró modelleket, Meyer komplexitási tényező számítási módszerét, Crawley komplexitás definícióit és Kinnunen interfész komplexitás szorzó fogalmát.

Megállapítottam, hogy Crawley „lényegi komplexitás” definíciójának felhasználásával a komplex villamos rendszerek biztonságtechnikai alrendszereinek összehasonlító elemzésénél egy adott alrendszerrel szemben támasztott funkcionális követelmények alapján meghatározható az adott alrendszer adott részletességű modelljének lényegi komplexitása, amivel lehetővé válik tendertervek objektív értékelésének támogatása.

Meghatároztam a Meyer féle komplexitás modell Kinnunen interfész komplexitás szorzóival módosított változatánál számba vehető jellemzőket, és kiválasztottam a biztonságtechnikai alrendszerek makro-szintű vizsgálatánál a gyakorlatban is alkalmazható paramétereket.

Szabálysorozatot állítottam fel a biztonságtechnikai alrendszerek eszközei interfész komplexitás szorzójának megállapításához, majd ezek alkalmazásával végrehajtottam a

behatolás jelző alrendszereknél az érzékelők és egyéb eszközök, modulok táblázatos klasszifikációját és az egyes eszközök interfész komplexitás szorzó értékének meghatározását.

Ugyancsak végrehajtottam a beléptető rendszerek komplexitás modelljének meghatározását és belépési pont elemeinek, érzékelőknek, olvasóknak és egyéb eszközöknek a táblázatos klasszifikációját, valamint az egyes eszközök interfész komplexitás szorzó értékének meghatározását.

Az őrjárat ellenőrző rendszerek komplexitás modelljének kialakítását, a rendszerek eszközeinek táblázatos klasszifikációját és az egyes eszközök interfész komplexitás szorzó értékének meghatározását is elvégeztem.

Ebben a fejezetben elemeztem a komplex villamos rendszerek integráltsági fokának becsléséhez szükséges rendszer-komplexitás leíró modelleket, meghatároztam a biztonságtechnikai alrendszerek komplexitásának becsléséhez alkalmazható módszereket, paramétereket és klasszifikációs táblázatokba rendeztem az egyes alrendszerek eszközeit, meghatározva az egyes eszközök interfész komplexitás szorzóit.

Ezzel teljesítettem a kutatási célkitűzések 3. pontját a „Matematikai modell kidolgozása a biztonságtechnikai alrendszerek komplexitásának meghatározására, és a biztonságtechnikai alrendszer-modellekben szereplő eszközök kvantitatív és kvalitatív jellemzőinek definiálása, gyakorlati értékeik meghatározása” célt.

Igazoltam a kutatási hipotézisek 2. pontjában megfogalmazott „A biztonságtechnikai alrendszer-architektúrák kezelésére meghatározhatók olyan specifikus (kvantitatív és kvalitatív) mutatók, amelyek figyelembevételével az alrendszerek komplexitása számolható” hipotézist.

5. BIZTONSÁGTECHNIKAI RENDSZEREK MODELLEZÉSE

5.1. AZ INTEGRÁLTSÁGI FOK DEFINÍCIÓJA

Bármely rendszer integráltsági szintjét az alábbi jellemzők befolyásolják:

1. Kapcsolatok (kapcsolódási pontok) száma az alrendszerek között.
2. Az alrendszerek által közösen használt I/O elemek (adatpontok) száma/aránya.
3. Az alrendszerek által közösen használt adatelemek (adatbázis mezők) száma/aránya.
4. Az alrendszerek által más alrendszerekben kiváltott/letiltott műveletek, funkciók száma/aránya.

Sem a biztonságtechnikai alrendszerek, sem az integrált vagyonvédelmi rendszerek, mint komplex villamos rendszerek integráltsági szintjének, fokának mutatója nincs definiálva sem a polgári, sem a katonai szakirodalomban. Ebből adódóan nincs sem számítási, sem becslési modell az integráltsági fok számítására.

A rendszerek integráltsági szintjének vizsgálatát a rendszerek modellezésének több szintjén végezhetjük.
A dolgozatban alkalmazott makro-szintű modellezéshez elegendő az 1. és 2. pont szerinti jellemzők, paraméterek alkalmazása.
A mikro-szintű modellezésnél az 1. és 2. pont szerinti jellemzők, paraméterek mellett szükség lehet a 3. és 4. pont szerinti jellemzők, paraméterek alkalmazására is, ehhez viszont szükséges az alrendszerek szoftver moduljainak részletes elemzése is. A biztonságtechnikai alrendszerek mikro-szintű modellezése nem tartozik jelen dolgozat tárgyához.

A 4. fejezetben vizsgált komplexitás-tényező makro-szintű számítási modelljeinél hasonló alapvetéseket tettem. Az ott kapott eredményeket használom fel az integráltsági

fok definiálásánál is. Az egyes biztonságtechnikai alrendszerek komplexitásának meghatározása az előzőekben kidolgozott modellekkel a gyakorlatban is elvégezhető.

Hogy a gyakorlatban is jól használható modellt adjak az integrált biztonságtechnikai rendszerek integráltsági szintjének meghatározására, **az integráltsági fokot az alábbiak szerint definiálom:**

Egy $S_1, S_2, ...S_N$ alrendszereket tartalmazó, azok integrálásával létrehozott, integrált M biztonságtechnikai rendszer IS(M) integráltsági foka a rendszert alkotó $S_1, S_2, ...S_N$ alrendszerek integráció nélküli $K(S_1)$, $K(S_2)$, … $K(S_N)$ komplexitás-értékeinek összege, osztva az M integrált rendszer komplexitás-értékével.

A definíció alapján az integrált biztonságtechnikai rendszer integráltsági foka az

$$\mathbf{IS(M) = (K(S_1) + K(S_2) + \ldots + K(S_N)\ ) / K(M)} \qquad \mathbf{(5.1)}$$

képlettel számítható, ahol

- IS(M) az M integrált rendszer integráltsági foka,
- $K(S_1)$, $K(S_2)$, … $K(S_N)$ az M rendszert alkotó $S_1, S_2, ... S_N$ alrendszerek integrálás előtti komplexitás-értékei,
- K(M) az M integrált rendszer komplexitás-értéke.

Röviden megfogalmazva: ***Egy integrált rendszer integráltsági szintje az integrált rendszer funkcióival azonos funkciókat ellátó, különálló részrendszerek komplexitás-összegének és az integrált rendszer komplexitás-értékének hányadosával jellemezhető.***

Az integrált biztonságtechnikai rendszerek jellemzésére, az azonos funkciók ellátására tervezett biztonságtechnikai rendszerek kiviteli terveinek minősítésére jól használható módszer lehet az egyes rendszerek integráltsági fokának összehasonlítása.

A gyakorlatban a minősítendő integrált biztonságtechnikai rendszer és az azonos funkciókat integráció nélkül ellátó biztonságtechnikai alrendszerek kiviteli tervei alapján először ki kell számolni az adott alrendszerek komplexitási tényezőjét.

A biztonságtechnikai alrendszerek funkcióinak, az egyes eszközök, modulok jellemzőinek kezeléséhez jól használható az alrendszerek rendszerezett leírása a 2. fejezetben.

A számításokhoz a 4.4. alfejezetben leírt rendszerjellemzők és az egyes modulok klasszifikációs táblázataiban megadott interfész komplexitás szorzók alkalmazhatók.

5.2. BEHATOLÁS-JELZŐ ÉS BELÉPTETŐ RENDSZER INTEGRÁCIÓJA

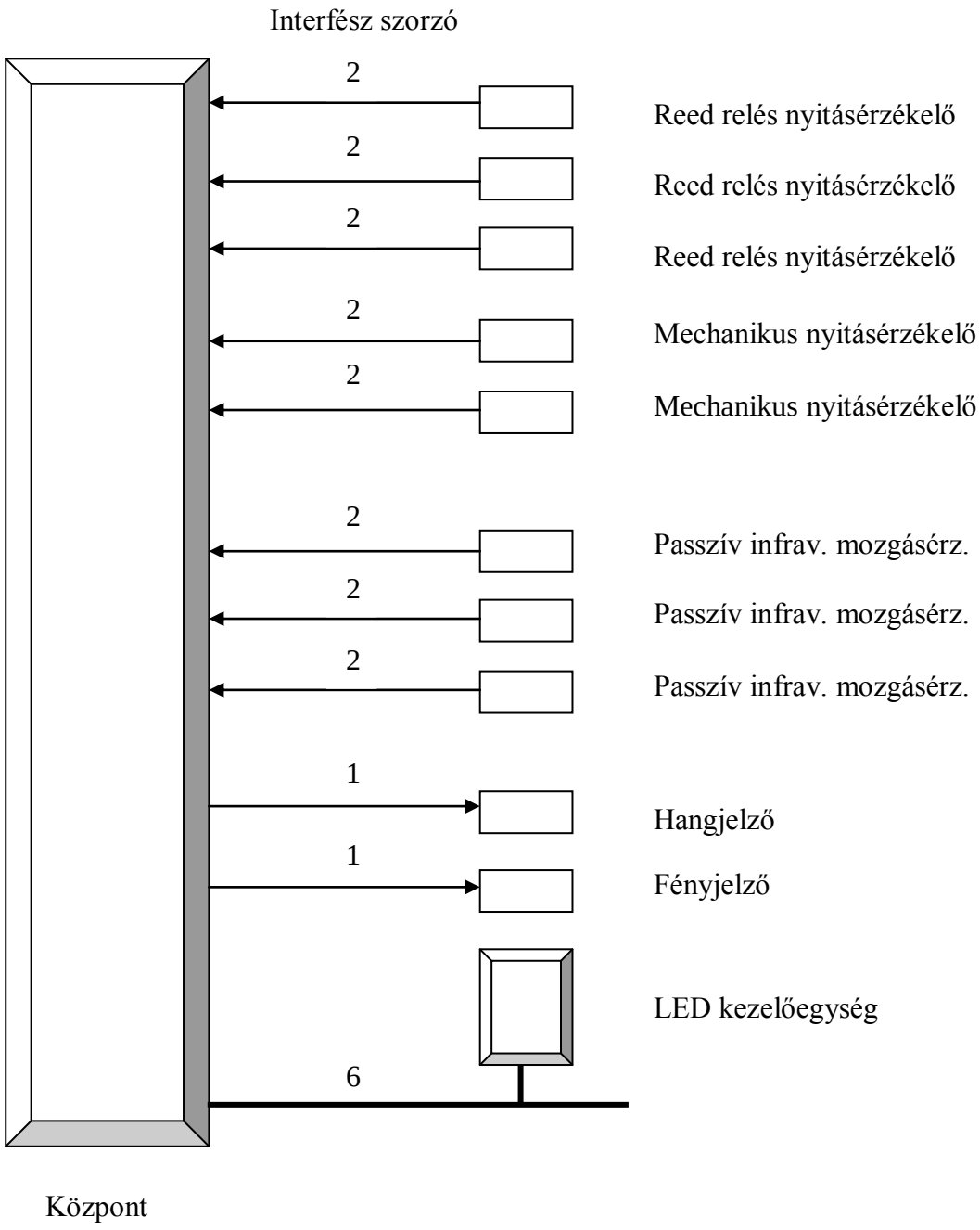
A biztonságtechnikai, vagyonvédelmi rendszerek közül legnagyobb számban a behatolás jelző rendszerek és a beléptető rendszerek vannak telepítve. Ma még legtöbbször külön rendszerekként, általában külön gyártók rendszerei kerülnek alkalmazásra.

Ezeknek a rendszereknek az integrálását megkönnyíti, hogy ma már sok behatolás jelző központ beléptető funkciókkal is rendelkezik, a kezelői buszra beléptető rendszer olvasói is csatlakoztathatók.

Ebben az alfejezetben megvizsgálom egy-egy különálló behatolás jelző rendszer és beléptető rendszer komplexitását, majd a két rendszer integrációjával megvalósítható rendszer komplexitását és az integrált rendszer integráltsági fokát.

A BEHATOLÁS JELZŐ RENDSZER KOMPLEXITÁSA

A behatolás jelző rendszerek közül egy egyszerű topológiájú, kis zónaszámú, vezetékes, kompakt központot tartalmazó rendszer vizsgálatát végzem el.



5.1. ábra. Behatolás jelző rendszer blokkvázlata

Egy ilyen rendszer egy központi panelt, a központhoz a zónabemeneteken csillag topológiával kapcsolódó, digitális bemeneti adatpontként viselkedő érzékelőket, néhány, ugyancsak csillag topológiával kapcsolódó, digitális kimeneti adatpontként viselkedő jelzésadót (hangjelző, fényjelző, egyéb programozható kimenet – PGM) és néhány busz topológiájú interfészre kapcsolódó kezelőt tartalmaz.

Egy három-helyiséges katonai ügyeleti objektumot feltételezve, a kialakítandó behatolás jelző rendszer az alábbi elemeket tartalmazza:

1 db Behatolás jelző központ (8 zónás, 2 partíciós, vezetékes).
3 db Reed relés (mágneses) nyitásérzékelő.
2 db Mechanikus nyitásérzékelő (iratszekrény- és központ fedél-kapcsoló) .
3 db Passzív infravörös mozgásérzékelő.
1 db Beltéri hangjelző.
1 db Beltéri fényjelző.
1 db LED-es kezelőegység.

A behatolás jelző rendszer blokkvázlata az 5.1. ábrán látható

Meyer képletét (4.4) a behatolás jelző rendszerre alkalmazva a komplexitási tényező az alábbi módon számolható:

$$\mathbf{K_{BH}(M) = (N_{BHMp} \times N_{BHMt} \times N_{BHMi})^{1/3}}$$

ahol

$K_{BH}(M)$ a behatolás jelző rendszer komplexitás értéke,
N_{BHMp} a behatolás jelző rendszernél az elemek száma,
N_{BHMt} a behatolás jelző rendszernél az elemtípusok száma,
N_{BHMi} pedig a behatolás jelző rendszernél az interfészek száma.

A vizsgált esetben

$$\mathbf{N_{BHMp}} = 1+3+2+3+1+1+1 = 12$$
$$\mathbf{N_{BHMt}} = 1+1+1+1+1+1+1 = 7$$
$$\mathbf{N_{BHMi}} = (3+2+3) + (1+1) + 1 = 11$$

Ezekkel az értékekkel az adott behatolás jelző rendszer komplexitás értéke

$$\mathbf{K_{BH}(M) = (12 \times 7 \times 11)^{1/3} = 9.74} \qquad \mathbf{(5.2)}$$

A vizsgálatnál nem vettem figyelembe az egyszerű, csillag topológiájú digitális bemeneti és kimeneti interfészek és a bonyolult, busz-topológiájú kezelő interfész közötti különbséget.

Kinnunen interfész komplexitás szorzó elméletét alkalmazva, az interfész komplexitás tényezőket a 4.4. fejezetben általam létrehozott táblázatokból véve, a rendszer elemeinek interfész-komplexitás szorzóit az 5.1. táblázatban adom meg.

Az interfész komplexitás szorzókkal súlyozott interfész szám

$$\mathbf{N_{BHSMi}} = (3+2)\times 2 + 3\times 2 + (1+1)\times 1 + 1\times 6 = 24$$

Ezzel a súlyozott interfész értékekkel az adott behatolás jelző rendszer komplexitás értéke

$$\mathbf{K_{BHS}(M) = (12 \times 7 \times 24)^{1/3} = 12.63} \qquad \mathbf{(5.3)}$$

Látható, hogy az (5.2) nem súlyozott interfészekkel számolt értékhez képest szignifikáns eltérés adódott.

Ez az érték önmagában nem sokat mond, más diszjunktív, vagy integrált rendszerekkel történő összehasonlításnál lesz hasznos szerepe.

5.1. táblázat. KATONAI ÜGYELETI OBJEKTUM BEHATOLÁS JELZŐ RENDSZERE ESZKÖZEINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

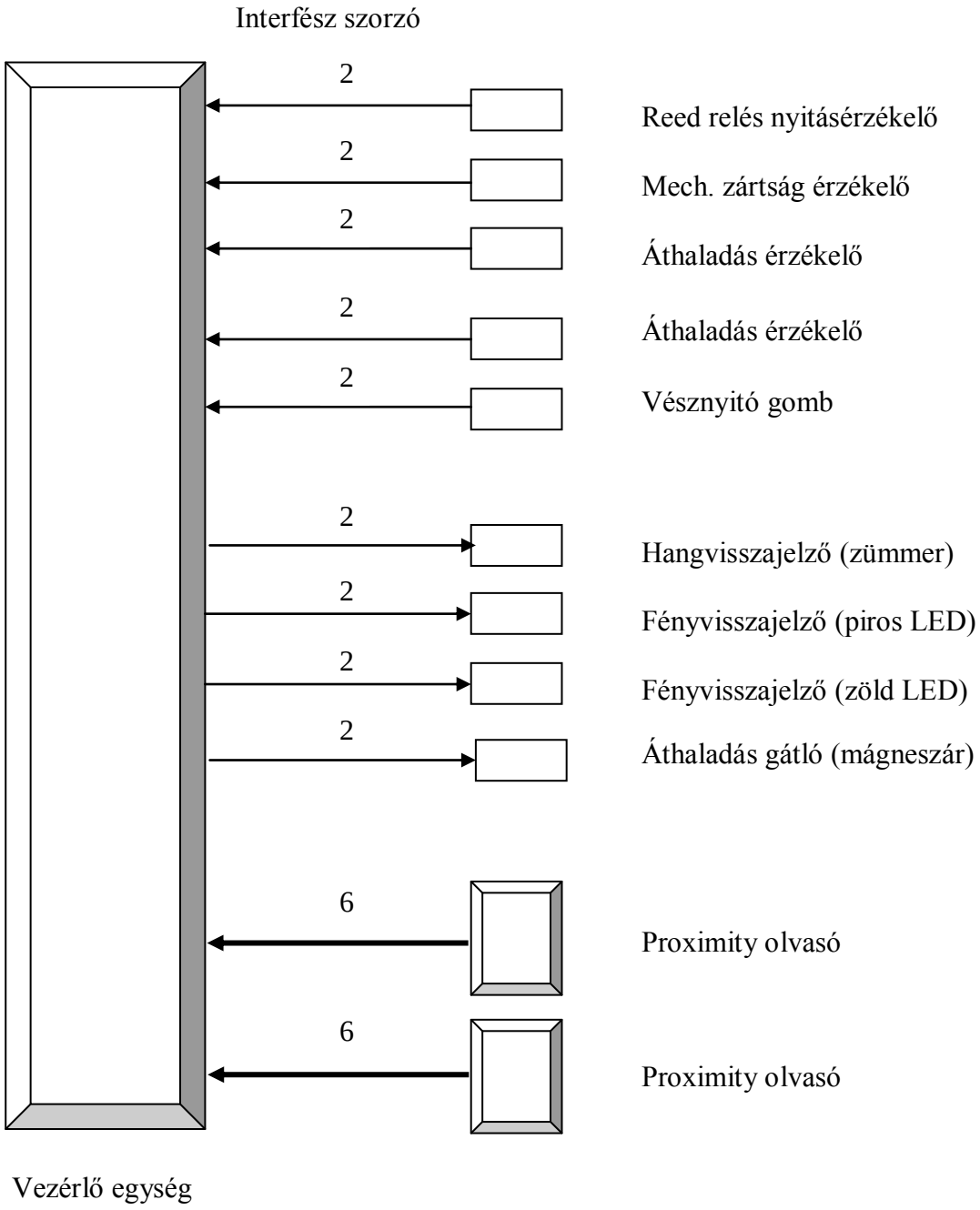
SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Reed relés nyitásérzékelő (4 vezetékes)	20m	2 bit	Beltéri I.	Igen	**2**
2.	Mechanikus nyitásérzékelő (4 vezetékes)	20m	2 bit	Beltéri I.	Igen	**2**
3.	Passzív infravörös mozgásérzékelő (PIR)	20m	2 bit	Beltéri I.	Igen	**2**
4.	Beltéri hangjelző („sziréna”)	20m	1 bit	Beltéri I.	Igen	**1**
5.	Beltéri fényjelző („villogó”)	20m	1 bit	Beltéri I.	Igen	**1**
6.	LED kezelőegység	50m	9600 bit/s	Beltéri I.	Nem	**6**

5.2. táblázat. KATONAI ÜGYELETI OBJEKTUM BELÉPTETŐ RENDSZERE ESZKÖZEINEK INTERFÉSZ KOMPLEXITÁS JELLEMZŐI

SOR-SZÁM	ÉRZÉKELŐK MEGNEVEZÉSE	TÁVOLSÁG	ÁTVITT INFORMÁCIÓ	KÖRNYEZETI FELTÉTELEK	SZABVÁNYOS PROTOKOLL	INTERFÉSZ SZORZÓ
1.	Reed relés nyitásérzékelő (4 vezetékes)	20m	2 bit	Beltéri I.	Igen	**2**
2.	Mechanikus zártságérzékelő (4 vezetékes)	20m	2 bit	Beltéri I.	Igen	**2**
3.	Infravörös fénysorompó	20m	2 bit	Beltéri I.	Igen	**2**
4.	Vésznyitó gomb (elektronikus)	20m	2 bit	Beltéri I.	Igen	**2**
5.	Hangvisszajelző eszköz („zümmer”)	20m	2 bit	Beltéri I.	Igen	**2**
6.	Fényvisszajelző eszköz (LED)	20m	2 bit	Beltéri I.	Igen	**2**
7.	Áthaladás-gátló engedélyező kimeneti eszköz	20m	1 bit	Beltéri I.	Igen	**1**
8.	Proximity kártya olvasó	20m	9600 bit/s	Beltéri I.	Nem	**6**

A BELÉPTETŐ RENDSZER KOMPLEXITÁSA

A beléptető rendszerek közül egy egyszerű topológiájú, egy belépési pontból álló, off-line rendszert vizsgálok.



5.2. ábra. Beléptető rendszer blokkvázlata

Egy ilyen rendszer egy vezérlő egységet, a vezérlő egységhez csillag topológiával kapcsolódó, digitális bemeneti adatpontként viselkedő nyitottság/zártság érzékelőket, áthaladás érzékelőket, vésznyitót, ugyancsak csillag topológiával kapcsolódó, digitális kimeneti adatpontként viselkedő visszajelző kimeneteket (hangjelző, fényjelző), mágneszár-vezérlő jelet és két, több-vezetékes interfészre kapcsolódó olvasót tartalmaz.

Az előzőekben tárgyalt három-helyiséges katonai ügyeleti objektumot feltételezve, a kialakítandó beléptető rendszer az alábbi elemeket tartalmazza:

1 db Vezérlő egység.
1 db Reed relés (mágneses) nyitásérzékelő.
1 db Mechanikus zártság-érzékelő.
2 db Áthaladás érzékelő (infravörös fénysorompó).
1 db Vésznyitó gomb.
1 db Hangvisszajelző (zümmer).
2 db Fényvisszajelző (LED piros/zöld).
1 db Áthaladás-gátló (mágneszár).
2 db Proximity olvasó.

Itt is Meyer képletét (4.4) a beléptető rendszerre alkalmazva az egyes tényezők:[46]

$\mathbf{N_{BLMp}} = 1+1+1+2+1+1+2+1+2 = 12$

$\mathbf{N_{BLMt}} = 1+1+1+1+1+1+1+1+1 = 9$

$\mathbf{N_{BLMi}} = (1+1+2+1) + (1+2+1) + 2 = 11$

Ezekkel az értékekkel az adott beléptető rendszer komplexitás értéke

$$\mathbf{K_{BL}(M) = (12 \times 9 \times 11)^{1/3} = 10.59} \qquad \mathbf{(5.4)}$$

[46] N_{BLMp} az elemek száma, N_{BLMt} az elemtípusok száma, N_{BLMi} pedig az interfészek száma.

A vizsgálatnál nem vettem figyelembe az egyszerű digitális bemeneti és kimeneti interfészek és a bonyolultabb olvasó interfészek közötti különbséget.

Kinnunen interfész komplexitás szorzó elméletét alkalmazva, az interfész komplexitás tényezőket a 4.4. fejezetben létrehozott táblázatokból véve az alábbi a rendszer elemeinek interfész-komplexitás szorzóit az 5.2. táblázatban adom meg.

Az interfész-komplexitás szorzókkal súlyozott interfész szám

$$\mathbf{N_{BLSMi}} = (1+1+2+1)\times 2 + (1+2+1)\times 2 + 2\times 6 = 30$$

Ezzel a súlyozott interfész értékekkel az adott beléptető rendszer komplexitás értéke

$$\mathbf{K_{BLS}(M) = (12 \times 9 \times 30)^{1/3} = 14.79} \qquad \mathbf{(5.5)}$$

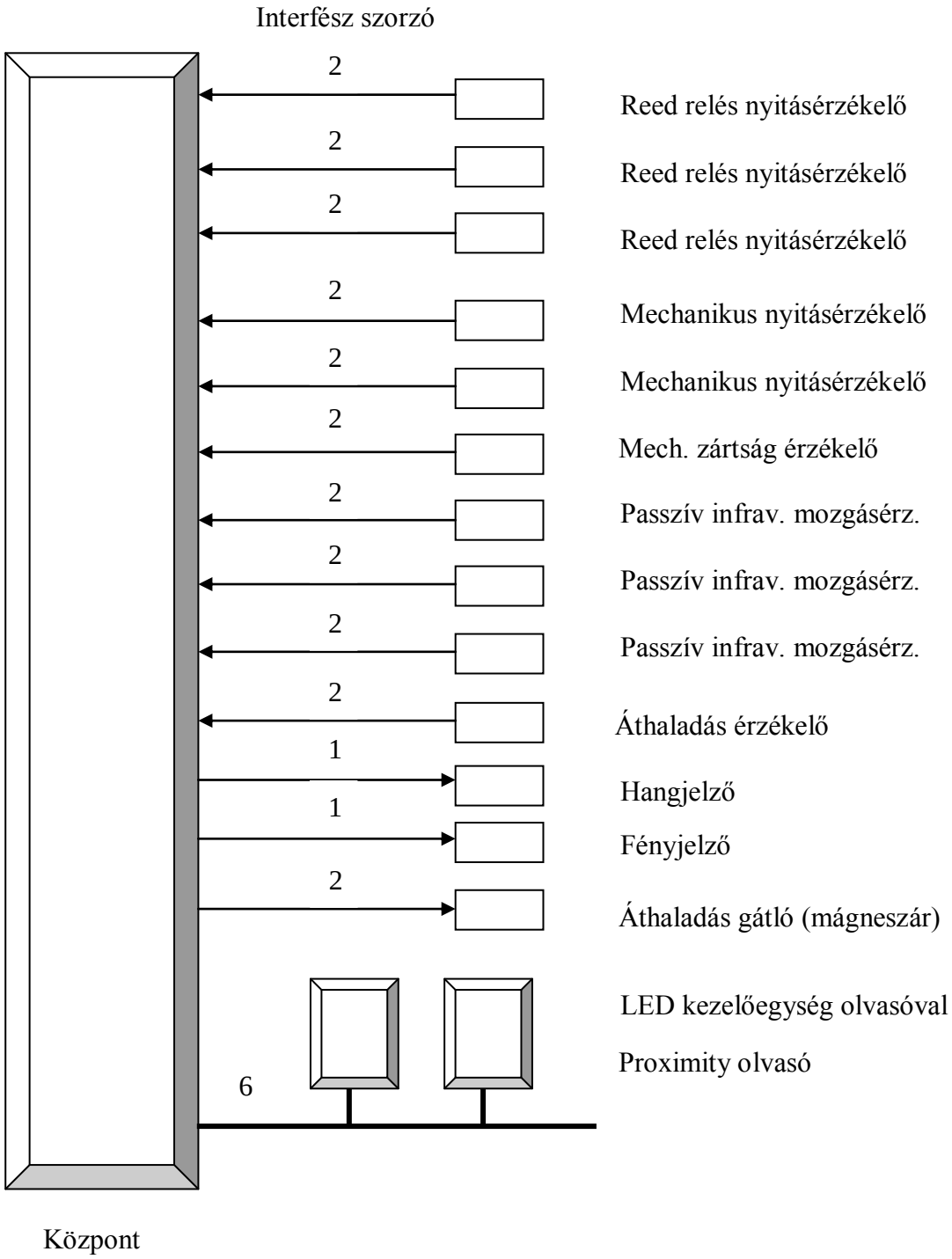
Látható, hogy az (5.4) nem súlyozott interfészekkel számolt értékhez képest itt is szignifikáns eltérés adódott.

AZ INTEGRÁLT RENDSZER KOMPLEXITÁSA

Az előző részekben tárgyalt három-helyiséges katonai ügyeleti objektum behatolás-jelző- és beléptető rendszerek komplexitására nagyságrendileg hasonló értékeket kaptam.

A behatolás jelző rendszer komplexitás értéke **9.74**, súlyozott interfész értékekkel számolt komplexitása **12.63**.
A beléptető rendszerének komplexitás értéke **10.59**, súlyozott interfész értékekkel számolt komplexitása **14.79**.
A két rendszer komplexitásának összege **20.33**, illetve súlyozott interfész értékekkel számolva **27.42**.

Vizsgáljuk meg, hogy a két rendszer integrálásával hogyan változik a teljes rendszer komplexitása!



5.3. ábra. Az integrált rendszer blokkvázlata

A két alrendszer integrálásával létrejövő rendszer az alábbi elemekből áll:

1 db Központ (behatolás- és beléptető funkciókkal).
3 db Mágneses nyitásérzékelő (az egyiket a beléptetőnél is felhasználjuk).
2 db Mechanikus nyitásérzékelő (iratszekrény- és központ fedél-kapcsoló).
1 db Mechanikus zártság-érzékelő.
3 db PIR mozgásérzékelő (az egyiket áthaladás-érzékelésre is használjuk).
1 db Áthaladás érzékelő (a másik helyett az egyik PIR-t alkalmazzuk).
1 db Beltéri hangjelző.
1 db Beltéri fényjelző.
1 db Mágneszár kimenet.
1 db LED-es kezelőegység (a beléptető rendszer LED-jeit is tartalmazza).
1 db Olvasó (a másik helyett a LED-es kezelőegységet alkalmazzuk).

Meyer képletét (4.4) az integrált rendszerre alkalmazva az egyes tényezők:

$$\mathbf{N_{IMp}} = 1+3+2+1+3+1+1+1+1+1+1 = 16$$

$$\mathbf{N_{IMt}} = 1+1+1+1+1+1+1+1+1+1+1 = 11$$

$$\mathbf{N_{IMi}} = (3+2+1) + (3+1) + (1+1+1) +1 = 14$$

Ezekkel az értékekkel az integrált rendszer komplexitás értéke

$$\mathbf{K_I(M) = (16 \times 11 \times 14)^{1/3} = 13.50} \qquad \mathbf{(5.6)}$$

Kinnunen interfész komplexitás szorzó elméletét alkalmazva, az interfész komplexitás tényezőket a 4.4. fejezetben általam létrehozott táblázatokból véve, a rendszer elemeinek interfész-komplexitás szorzóit az 5.1. és 5.2. táblázatban adtam meg.

Az interfész komplexitás szorzókkal súlyozott interfész szám:

$$\mathbf{N_{ISMi}} = (3+2+1)\times 2 + (3+1+1)\times 2 + (1+1)\times 1 + 1\times 6 = 30$$

Ezzel a súlyozott interfész értékekkel az adott behatolás jelző rendszer komplexitás értéke

$$\mathbf{K_{IS}(M) = (16 \times 11 \times 30)^{1/3} = 17.41} \qquad \mathbf{(5.7)}$$

AZ INTEGRÁLTSÁG VIZSGÁLATA

Az előzőekben kiszámoltam egy három-helyiséges katonai ügyeleti objektum különálló behatolás jelző rendszerének és beléptető rendszerének komplexitását, majd a két rendszer integrációjával megvalósítható rendszer komplexitását. A számításokat a Meyer féle modell (4.4) alkalmazásával kétféle modellen végeztem el.

1. Először a Mayer által javasolt egyszerű, csak az interfészek számát tartalmazó modellel állapítottam meg az egyes vizsgált alrendszerek és az integrált rendszer komplexitását. Ezt a modellt alkalmazva az alábbi értékek adódtak.

A különálló behatolás jelző rendszer komplexitás értéke (5.2): $\mathbf{K_{BH}(M) = 9.74}$

A különálló beléptető rendszer komplexitás értéke (5.4) pedig: $\mathbf{K_{BL}(M) = 10.59}$

A két különálló alrendszer komplexitásának összege: $\mathbf{K_{BH}(M) + K_{BL}(M) = 20.33}$

Az integrált rendszer komplexitás értéke (5.6): $\mathbf{K_I(M) = 13.50}$

Ezekkel az értékekkel számolva, az általam adott (5.1) modellt alkalmazva a két alrendszer integrálásával létrehozott integrált rendszer integráltsági foka:

$$\mathbf{IS(M) = (K_{BH}(M) + K_{BL}(M)) / K_I(M) = 20.33 / 13.50 = \underline{1.50}}$$

2. Másodszor a Meyer módszerét és a Kinnunen-féle interfész-komplexitás szorzó általam generált értékeit együtt alkalmazó modellel állapítottam meg az egyes vizsgált alrendszerek és az integrált rendszer komplexitását. Ezt a modellt alkalmazva az alábbi értékek adódtak.

A különálló behatolás jelző rendszer komplexitás értéke (5.3): $\mathbf{K_{BHS}(M) = 12.63}$

A különálló beléptető rendszer komplexitás értéke (5.5) pedig: $\mathbf{K_{BLS}(M) = 14.79}$

A két különálló alrendszer komplexitásának összege: $\mathbf{K_{BHS}(M) + K_{BLS}(M) = 27.42}$

Az integrált rendszer komplexitás értéke (5.7): $\mathbf{K_{IS}(M) = 17.41}$

Ezekkel az értékekkel számolva, az általam adott (5.1) modellt alkalmazva a két alrendszer integrálásával létrehozott integrált rendszer integráltsági foka:

$$\mathbf{IS_S(M) = (K_{BHS}(M) + K_{BLS}(M)) / K_{IS}(M) = 27.42 / 17.41 = \underline{1.57}}$$

A fenti eredményeket az 5.3. táblázatban foglaltam össze.

5.3. táblázat. KOMPLEXITÁSI ÉS INTEGRÁLTSÁGI JELLEMZŐK SZÁMÍTOTT ÉRTÉKEI

VIZSGÁLT RENDSZER	K(M)	$K_S(M)$	$K_S(M)/K(M)$
Diszjunkt behatolás jelző alrendszer	**9.74**	**12.63**	**1.29**
Diszjunkt beléptető alrendszer	**10.59**	**14.79**	**1.39**
Diszjunkt behatolás jelző + beléptető alrendszer	**20.33**	**27.42**	**1.34**
Integrált (behatolás jelző + beléptető) rendszer	**13.50**	**17.41**	**1.32**
INTEGRÁLTSÁGI FOK ÉRTÉKE (IS(M) ÉS $IS_S(M)$)	**1.50**	**1.57**	**1.04**

K(M) – az egységnyi interfész komplexitás értékkel számolt komplexitás érték.
$K_S(M)$ – súlyozott interfész komplexitás értékekkel számolt komplexitás érték.
$K_S(M)/K(M)$ – a súlyozott és a súlyozatlan modellekkel számolt értékek aránya.

RÉSZKÖVETKEZTETÉSEK

A rendszerek integráltsági szintjének vizsgálatát a rendszerek modellezésének több szintjén végezhetjük. A dolgozatban alkalmazott makro-szintű modellezésnél a gyakorlatban is jól használható modell kialakítása volt a cél.

A fejezet elején a 4. fejezetben leírt komplexitás-tényező modellek felhasználásával megadtam az integrált biztonságtechnikai rendszerek integráltsági fokának definícióját, és az integráltsági fok számszerűsítésére alkalmas matematikai modellt. Eszerint egy integrált biztonságtechnikai rendszer integráltsági szintje az integrált rendszer funkcióival azonos funkciókat ellátó, különálló részrendszerek komplexitás-összegének és az integrált rendszer komplexitás-értékének hányadosával jellemezhető.

Egy katonai ügyeleti objektum behatolás-jelző- és beléptető rendszerének példáján bemutattam a komplexitás-mutatók és az integráltsági fok meghatározásának menetét.

Az objektum diszjunkt behatolás jelző rendszerének rendszerterve alapján az interfész komplexitás szorzók nélküli Meyer féle modellel, majd a modell finomításával, Kinnunen interfész komplexitás szorzó elméletét alkalmazva, az interfész komplexitás tényezőket a 4.4. fejezetben általam létrehozott táblázatokból véve is meghatároztam a behatolás jelző rendszer komplexitás értékét.

Hasonló metódussal az ügyeleti objektum diszjunkt beléptető rendszerének rendszerterve alapján előbb az interfész komplexitás szorzók nélküli Meyer féle modellel, majd a Kinnunen interfész komplexitás szorzó elméletét alkalmazó modellel a behatolás jelző rendszer komplexitás értékét is meghatároztam.

Ezután az adott objektum integrált behatolás-jelző- és beléptető rendszerének terve alapján kiszámoltam az integrált rendszer egyszerű (Meyer féle) komplexitás mutatóját, majd az interfész komplexitás szorzókat is tartalmazó komplexitás értéket.

A kapott komplexitás értékekből kiszámoltam az integrált behatolás-jelző- és beléptető rendszer integráltsági fokát.

Ezzel teljesítettem a kutatási célkitűzések 4. pontját, a „Definíció adása és matematikai modell kidolgozása az integrált biztonságtechnikai rendszerek integráltsági jellemzőjének (fokának) meghatározására” célt.

Ugyancsak teljesítettem a kutatási célkitűzések 5. pontját, a „Próbaszámítások végzése katonai és polgári objektumok biztonságtechnikai alrendszereinek és integrált rendszereinek komplexitás-meghatározására valamint az integrált rendszer integráltsági fokának kiszámítására” feladatot.

Igazoltam a kutatási hipotézisek 3. pontjában megfogalmazott „Az integrált biztonság-technikai rendszereknél az integráltság foka meghatározható, számszerűsíthető” hipotézist.

Az integrált behatolás-jelző- és beléptető rendszer integráltsági fokára kapott 1.50 és 1.57 integráltsági fok értéke alapján megállapítható, hogy az alrendszerek integrálásával a teljes rendszer komplexitása mintegy 2/3-ára csökkent.

Ezzel igazoltam a kutatási hipotézisek 4. pontjában megfogalmazott „Adott katonai és polgári objektumok biztonságtechnikai rendszereinél az alrendszerek integrálásával a rendszer komplexitása csökkenthető” hipotézist.

Az 5.3. táblázat elemzésekor kitűnik, hogy a kétféle modellel számolt komplexitás értékek aránya 1.29 és 1.39 közé esik, viszont a kétféle modellel számolt integráltsági fokok értéke közel azonos (1.51 és 1.57), arányuk mindössze 1.04.

A vizsgálthoz hasonló kis rendszerek ($Z < 16$) integráltsági mutatójának makro-szintű vizsgálatánál nem adódik jelentős eltérés a kétféle modellel kapott értékek között. A közepes és nagy rendszerek vizsgálatánál azonban már szignifikáns eltérés lehet a kétféle modell alkalmazásával kapott értékek között.

6. ÖSSZEFOGLALÁS

A kutatómunka a diszjunkt és az integrált biztonságtechnikai rendszereknek, mint a komplex villamos rendszerek összetevőinek modellezési kérdéseire irányult.

A nemzetközi irodalomban is hézagpótló, az integrált vagyonvédelmi rendszerek integráltsági fokának definiálását és számszerűsítését célzó kutatómunka az integrált rendszerek integrációs fokának definiálásával, a komplexitás-számítási és az integráltsági fok számítási modell kidolgozásával elérte célját.

A tevékenység során végzett - a végső cél eléréséhez alapvetően szükséges - a tématerület felmérését, rendszerezett leírását is adó munka az MSc szintű biztonságtechnikai oktatás egyes területeinek tudományos igényű megalapozását is elősegítette.

A komplex villamos rendszerek biztonságtechnikai összetevőinek, alrendszereinek felmérése, rendszerezett összefoglalása elengedhetetlen volt az egyes alrendszerek, valamint az integrált rendszerek komplexitásának, majd integráltsági fokának megállapításához.
A 2. fejezetben rendszerezett leírását adtam a vizsgált terület biztonságtechnikai összetevőinek, alrendszereinek, ami megalapozta az egyes alrendszerek komplexitásának, integráltsági fokának modellezését, a későbbi fejezetek interfész táblázatainak kialakítását.

A biztonságtechnikai alrendszerek integrálási lehetőségeinek, trendjeinek, tervezési folyamatának leírása, az integrálás előnyeinek, esetleges hátrányainak felmérésére is szükség volt az integrált rendszerek komplexitásának, integráltsági fokának vizsgálatához.
A 3. fejezetben feltártam és leírtam a biztonságtechnikai alrendszerek integrációs trendjeit, lehetőségeit és az integrált biztonságtechnikai rendszerek tervezési folyamatát, klasszifikáltam a biztonságtechnikai alrendszerek integrációjának lehetséges típusait, lehetővé téve nemcsak az egyes alrendszerek, hanem az integrált rendszerek komplexitásának, és az integrált rendszerek integráltsági fokának modellezését is.

A komplex villamos rendszereknél az integrált vagyonvédelmi rendszerek integráltsági fokának becsléséhez szükség van az adott alrendszerek komplexitásának előzetes meghatározására. Egy adott rendszer komplexitásának meghatározása a rendszer architektúra-modelljének segítségével lehetséges.
A 4. fejezetben elemeztem a komplex villamos rendszerek integráltsági fokának becsléséhez szükséges rendszer-komplexitás leíró modelleket, meghatároztam a biztonságtechnikai alrendszerek komplexitásának becsléséhez alkalmazható módszereket, paramétereket és klasszifikációs táblázatokba rendeztem az egyes alrendszerek eszközeit, meghatározva az egyes eszközök interfész komplexitás szorzóit.

A rendszerek integráltsági szintjének vizsgálatát a rendszerek modellezésének több szintjén végezhetjük. A dolgozatban alkalmazott makro-szintű modellezésnél a gyakorlatban is jól használható modell kialakítása volt a cél.
Az 5. fejezetben ismertettem az integrált biztonságtechnikai rendszerek integráltsági fokának általam adott, a fenti követelményt teljesítő definícióját, számítási modelljét, majd egy katonai ügyeleti objektum behatolás-jelző- és beléptető rendszerének példáján kétféle modellt is alkalmazva bemutattam a komplexitás-mutatók és integráltsági fok meghatározásának menetét.
Kimutattam, hogy kis rendszerek ($Z < 16$) integráltsági mutatójának makro-szintű vizsgálatánál a két modell között nincs jelentős eltérés, a komplexitás értékekre viszont a Kinnunen-féle interfész komplexitás szorzók figyelembevétele szignifikáns eltérést eredményez.

6.1. ÚJ TUDOMÁNYOS EREDMÉNYEK

1. A tématerület tudományos igényű feldolgozásával, a diszjunkt és integrált biztonságtechnikai rendszerek többszintű taxonómiai klasszifikációjával megalapoztam a katonai műszaki felsőoktatás fontos területén, az MSc szintű biztonságtechnikai képzésben általam is oktatott szakmai tárgyak egyes tématerületeinek színvonalas kialakítását.[47]

2. Elemeztem az integrált biztonságtechnikai rendszerek integráltsági fokának becsléséhez szükséges rendszer-komplexitás leíró modelleket, meghatároztam a biztonságtechnikai alrendszerek komplexitásának becsléséhez alkalmazható módszereket, paramétereket.

3. Megállapítottam, hogy egyes, a komplexitás meghatározásánál alkalmazott modellek bizonyos feltételekkel az integráltság meghatározásánál is használhatók és meghatároztam a leggyakrabban alkalmazott biztonságtechnikai rendszerek (a behatolás jelző rendszerek, a beléptető rendszerek és az őrjárat ellenőrző rendszerek) komplexitásának modellezéséhez a gyakorlatban is alkalmazható paramétereket.

4. Megfogalmaztam az integrált biztonságtechnikai rendszerek integráltsági fokának definícióját, kialakítva az integráltsági fok számszerűsítésére alkalmas matematikai modellt és egy katonai ügyeleti objektum behatolás-jelző- és beléptető rendszerének példáján bemutattam a komplexitás-mutatók és az integráltsági fok meghatározásának menetét.

[47] Szakmai gyakorlat I.-II., Intelligens épületek, Biztonságtechnikai rendszerek tervezése I.-II., A személy és vagyonvédelem rendszertana, Személy és vagyonvédelmi rendszerek kialakításának módszerei, Személy és vagyonvédelmi rendszerek üzemeltetése, üzemfenntartása I.-II. [29]

6.2. A HIPOTÉZISEK IGAZOLÁSA

1. A 4. fejezetben elemeztem a komplex villamos rendszerek integráltsági fokának becsléséhez szükséges rendszer-komplexitás leíró modelleket, meghatároztam a biztonságtechnikai alrendszerek komplexitásának becsléséhez alkalmazható módszereket, paramétereket.

   Ezzel igazoltam az 1. hipotézist, miszerint „a komplex villamos rendszerek biztonságtechnikai alrendszereinek leírására, ezen belül a komplexitás számítására matematikai eljárások alkalmazhatók".

2. A 4. fejezetben klasszifikációs táblázatokba rendeztem az egyes alrendszerek eszközeit, meghatározva az egyes eszközök interfész komplexitás szorzóit.

   Az 5. fejezetben egy katonai ügyeleti objektum behatolás-jelző- és beléptető rendszerének példáján pedig bemutattam a komplexitás-mutató számításának menetét.

   Ezzel igazoltam a 2. hipotézist, miszerint „a biztonságtechnikai alrendszer-architektúrák kezelésére meghatározhatók olyan specifikus (kvantitatív és kvalitatív) mutatók, amelyek figyelembevételével az alrendszerek komplexitása számolható".

3. Az 5. fejezetben megadtam az integrált biztonságtechnikai rendszerek integráltsági fokának definícióját és az integráltsági fok számszerűsítésére alkalmas matematikai modellt, majd egy katonai ügyeleti objektum behatolás-jelző- és beléptető rendszerének példáján bemutattam a komplexitás-mutatók és az integráltsági fok meghatározásának menetét.

   Ezzel igazoltam a 3. hipotézist, miszerint „az integrált biztonságtechnikai rendszereknél az integráltság foka meghatározható, számszerűsíthető".

4. Az 5. fejezetben megmutattam, hogy egy katonai ügyeleti objektum nem integrált behatolás jelző rendszerének és beléptető rendszerének összegzett komplexitás-mutatói nagyobbak, mint az ugyanezen objektum integrált behatolás-jelző- és beléptető rendszerének komplexitás mutatója.

Ezzel igazoltam a 4. hipotézist, miszerint „adott katonai és polgári objektumok biztonságtechnikai rendszereinél az alrendszerek integrálásával a rendszer komplexitása csökkenthető”.

6.2. AJÁNLÁSOK, A KUTATÁSI EREDMÉNYEK HASZNOSÍTÁSA

A kutatási téma újszerűsége és összetettsége csak az alapok lefektetését tette lehetővé. Az elért eredmények lehetővé teszik, hogy a kutatások több irányban is folytatódjanak:

1. A komplex villamos rendszerek biztonságtechnikai alrendszerei közül további alrendszerekre is ki kell próbálni a komplexitás és integráltsági fok meghatározására kidolgozott modelleket.

2. A rendszertechnikailag nagy eltérést mutató rendszermodelleknél (például a videó-megfigyelő rendszereknél) egyéb paraméterek alkalmazását is meg kell vizsgálni és szükség esetén módosítani lehet a matematikai modelleket.

3. A biztonságtechnikai alrendszerek mellett más, például az épületgépészeti automatika rendszerekre (fűtés, hűtés, szellőztetés, világításvezérlés), vagy az erősáramú automatika rendszerekre is alkalmazni kell és szükség esetén módosítani a matematikai modelleket.

4. A már önmagukban is nagy integráltsági fokú alrendszerekre (például IP alapú hálózati alrendszerekre) új, a folyamat-paramétereket is figyelembe vevő matematikai modelleket kell kidolgozni.

5. A rendszerek komplexitása, integráltsági foka és a rendszerek megbízhatósága, tervezési, beruházási, üzemeltetési költségei közötti összefüggések matematikai modellezése is további kutatások témája lehet.

6. Egyik legfontosabb irány lehet a komplexitás számítás és integráltsági fok számítás alkalmazási lehetőségeinek kutatása katonai alkalmazásoknál.

7. A komplex vagyonvédelem felépítését, összetevőit és rendszerezett összefoglalását, valamint a komplex villamos rendszerek biztonságtechnikai alrendszereinek integrálási lehetőségeit és az integrált biztonságtechnikai rendszerek tervezési folyamatát leíró fejezetek további oktatási anyagok kidolgozásához adhatnak tudományos alapot a katonai műszaki felsőoktatás fontos területén, az MSc szintű biztonságtechnikai képzésben.

A TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓIM

LEKTORÁLT- ÉS SZAK-FOLYÓIRATBAN MEGJELENT CIKKEK

1. Utassy Sándor: Integráció és védelem – Komplex villamos rendszerek biztonságtechnikai kérdései (Biztonság, 2008/2. különszám, 22.-28. oldal, ISSN 0864 9189)
2. Utassy Sándor: Integrált vagyonvédelem (ÁRGUS, VII. évf. 4. szám, 2007. szeptember, 16.-18. oldal, ISSN 1586 5363)
3. Utassy Sándor: Vagyonvédelmi rendszerek tervezése, telepítése (Detektor Plusz, 14. évf. 8-9. szám 2007. aug.-szeptember, 18.-20. oldal, ISSN 1217 9175)
4. Utassy Sándor: Láthatatlan biztonság (BAUTREND, I. évf. 2. szám 40.-41. oldal 2007. május, ISSN 1788 8646)
5. Utassy Sándor: Behatolás-jelző rendszerek védelmi filozófiái (Detektor Plusz, 14. évf. 3-4. szám 2007. márc.-április, 17.-20. oldal, ISSN 1217 9175)
6. Utassy Sándor – Bárkányi Pál: IP alapú kommunikáció az elektronikus vagyonvédelmi rendszerekben. (Bolyai Szemle, 2006/2. szám, 64.-76. oldal, Budapest)
7. Utassy Sándor: Behatolás-jelző rendszerek tápellátási kérdései II. (Detektor Plusz, 2006/11. szám, 21.-24. oldal, ISSN 1217 9175)
8. Utassy Sándor: Felsőfokú (MSc) biztonságtechnikai tervező képzés. (Detektor Plusz, 2006/7. szám, 16.-17. oldal, ISSN 1217 9175)
9. Utassy Sándor – Rónai Gyula: A tűzjelző rendszerek tervezésének jogi szempontjai. (Flórián Pressz, 2006/1. szám, 32.-36. oldal,)
10. Utassy Sándor – Rónai Gyula: A tűzjelző rendszerek tervezésének néhány kérdése. (Detektor Plusz, 2006/1.-2. szám, 23.-26. oldal, ISSN 1217 9175)
11. Utassy Sándor: Lakóparkok biztonsága. (Biztonság, 2005/4. szám, 15.-18. oldal, ISSN 0864 9189)
12. Utassy Sándor: Tervezési szempontok. – A biztosítások feltételei. (Detektor Plusz, 2005/12. szám, 16.-19. oldal, ISSN 1217 9175)
13. Utassy Sándor: Tervezés – Típustervek; Rovatvezetői beköszöntő.

(Detektor Plusz, 2005/10.-11. szám, 16.-17. oldal, ISSN 1217 9175)

14. Utassy Sándor: Felügyeleti informatika – Integrált épületfelügyeleti rendszerek. III. (Tudományos megközelítés) (Áram és Technológia, 2004. III.évf. 10.szám, 21.-27. oldal, ISSN 1588 8694)
15. Utassy Sándor: Felügyeleti informatika – Integrált épületfelügyeleti rendszerek. II. (Társasházak épület-felügyeleti rendszerei) (Áram és Technológia, 2004. III.évf. 9.szám, 21.-25. oldal, ISSN 1588 8694)
16. Utassy Sándor: Felügyeleti informatika – Integrált épületfelügyeleti rendszerek. I. (Bevezetés) (Áram és Technológia, 2004. III.évf. 5-6.szám, 23.-27. oldal, ISSN 1588 8694)
17. Utassy Sándor: Felügyeleti informatika – Az IP alapú kommunikáció. IV. (Képtömörítési eljárások) (Áram és Technológia, 2004. III.évf. 3.szám, 21.-26. oldal, ISSN 1588 8694)
18. Utassy Sándor: Felügyeleti informatika – Az IP alapú kommunikáció. III. (Alkalmazás) (Áram és Technológia, 2004. III.évf. 2.szám, 22.-24. oldal, ISSN 1588 8694)
19. Utassy Sándor: Felügyeleti informatika – Az IP alapú kommunikáció. II. (Glossary). (Áram és Technológia, 2004. III.évf. 1.szám, 20.-23. oldal, ISSN 1588 8694)
20. Utassy Sándor: Felügyeleti informatika – Az IP alapú kommunikáció. (Alapok) (Áram és Technológia, 2003. II.évf. 10.szám, 21.-23. oldal, ISSN 1588 8694)

IDEGEN NYELVŰ KIADVÁNYBAN MEGJELENT CIKKEK

1. Prof. Dr. Gyula Zsigmond – Sándor Utassy: High harmonic currents' problems in the complex electric systems. **(**"MTA Review" Bucharest, 2006./2. p.33.-38., Military Technical Academy in, Romania)

2. Prof. Dr. Gyula Zsigmond – Sándor Utassy: On Realibility of the Complex Electric Systems. (Bolyai Szemle, cikk, 2006/2. szám, p.77.-82., Budapest)

KONFERENCIA KIADVÁNYBAN MEGJELENT ELŐADÁS

1. Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései – Néhány gondolat a komplexitás meghatározására. (XXIV. Nemzetközi Kandó Konferencia, BMF_KVK, 2008.11.6., előadás, Budapest)
2. Utassy Sándor: Integrált felügyeleti rendszerek a vagyonvédelemben. (II. tudományos szimpózium, BMF_KVK, 2007. 11.29., előadás, Budapest)
3. Utassy Sándor: Vagyonvédelmi rendszerek tervezési folyamata. (Nemzetközi Gépész és Biztonságtechnikai szimpózium, BMF _ BGK 2007. 11.14., előadás, Budapest)
4. Utassy Sándor: Rádiós rendszerek térhódítása a biztonságtechnikában. (Biztonságtechnikai szimpózium, BMF _ BGK 2006. 11.10., előadás, Budapest)
5. Utassy Sándor – Dr. Zsigmond Gyula: A biztonságtechnikai tervezés jogi, etikai, szakmai problémái, kockázatai. (XXIIIth Kandó Conference 2006, előadás, Budapest)
6. Utassy Sándor – Dr. Horváth Elek: The Evolution of the Integrated Security Systems. (XXIIIth Kandó Conference 2006, **angol nyelvű előadás,** Budapest)
7. Utassy Sándor – Rónai Gyula: Distributed fire alarm systems and panels. (XXIIIth Kandó Conference 2006, **angol nyelvű előadás,** Budapest)
8. Utassy Sándor – Rónai Gyula: Tűzjelző rendszerek tervezése a XXI. században.
   (XXIIIth Kandó Conference 2006, előadás, Budapest)
9. Utassy Sándor: An Approach of the Risk Analysis of Integrated Security Systems. (XXII. Internationale Konferenz „Science in Practice“, Schweinfurt 2005., Fachhochschule Würzburg-Schweinfurt, University of Applied Sciences, 18. – 20. Mai 2005., **angol nyelvű előadás**)
10. Utassy Sándor, Szalay János, Dr. Zsigmond Gyula**:**Üzemen kívül helyezett katonai objektumok környezetbiztonsági kockázatainak csökkentése integrált épületfelügyeleti rendszerek kialakításával. (Havaria-esetek és kezelésük 2005. konferencia, ZMNE, előadás, 2005. március 22.)
11. Utassy Sándor, Dr. Kovács Károly, Tárnok Tamás: Intelligens ház és a biztonság. (II. Magyar Biztonságtechnika Szimpózium, előadás, 2003. Budapest)
12. Utassy Sándor: A betörésmegelőzés elektronikus módszerei.

(Épületvillamossági Szakmai Napok, Biztonságtechnika – tűzvédelem konferencia, előadás, 2003. Budapest)

13. Utassy Sándor: Felügyeleti informatika, behatolásvédelem, tűzjelzés. (Épület villamossági Szakmai Napok, Biztonságtechnika – tűzvédelem konferencia, előadás, 2003. Budapest)
14. Dr. Horváth Elek, Utassy Sándor: A Felügyeleti informatika és elektronikus vagyonvédelem modul oktatásának tapasztalatai. („Kandó Konferencia 2002" **előadás,** 2002. Budapest)
15. Utassy Sándor, Dr. Horváth Elek: Behatolás jelző központok fejlődési irányai. („Kandó Konferencia 2002" előadás, 2002. Budapest)
16. dr.Horváth Elek, Utassy Sándor: Felügyeleti informatikai és elektronikus vagyonvédelmi képzés a KKMF Műszertechnikai és Automatizálási Intézetében. (KKMF Tudományos Ülésszak előadás, 1998. Budapest)
17. Utassy Sándor, Dr. Horváth Elek: Integrált épületinformatikai rendszerek kialakítási szempontjai. (KKMF Tudományos Ülésszak előadás, 1998. Budapest)
18. Utassy Sándor: Integrált épületinformatikai rendszerek kórházi alkalmazása az egészségügyben. (III.Kórháztechnikai Konferencia, előadás, 1993.Szeged)
19. Utassy Sándor: Integrált épületinformatikai rendszerek.(III.Egészségügyi Konferencia, előadás, 1991.Szeged)

EGYÉB SZAKMAI ANYAGOK

1. Utassy Sándor: Áramszolgáltatói biztonságvédelmi modell javaslat (ELMŰ-ÉMÁSZ cégcsoport, Tanulmányterv, 2008. Budapes)
2. Utassy Sándor: Szakkönyv lektorálása: Farkas Cs.-Tóth A. Biztonságtechnika (RTF, 2007. Budapest)
3. Utassy Sándor: Tantárgytematikák a Biztonságtechnikai Mérnöki Mester (MSc) Szak létesítési kérelméhez. (ZMNE –BMF, 2005.07.20. Tananyag)

4. Utassy Sándor: Intelligens épületek funkcióinak, informatikai infrastruktúráinak és az Internet alkalmazási lehetőségeinek feltárása intelligens épületeknél. (Gábor Dénes Főiskola, előzetes kutatási jelentés, 2004.11.28.)
5. Utassy Sándor: Szakkönyv lektorálása: Tóth Levente, CCTV magyarul (BM Nyomda Kft.., 2004. Budapest)
6. Utassy Sándor: Az Ópusztaszeri Nemzeti Történelmi Emlékpark "Erdő" kiállítás-együttes pavilonjai tűz- és vagyonvédelmi rendszerének működéséről. (Szakvélemény, 1998. Budapest)
7. Utassy Sándor, Dr. Horváth Elek: A MATÁV országos ingatlan-felügyeleti rendszere. (Tanulmányterv, 1997. Budapest)
8. Utassy Sándor: Az Ópusztaszeri Nemzeti Történelmi Emlékpark Feszty Körkép épületében lévő régészeti kiállítás vagyonvédelmi és beléptető rendszere. (Tanulmányterv, 1995. Budapest)
9. Utassy Sándor, Kaló József: Az IBUSZ központi iroda vagyonvédelmi rendszere. (Szaktanulmány, 1992. Budapest)

Csak a témához kapcsolódó publikációkat soroltam föl fordított időrendi sorrendben mától 1991-ig. (Előtte más témákban végeztem kutató-fejlesztő munkát.)

HIVATKOZOTT IRODALMAK

[1] Dr. Zsigmond Gyula Komplex villamos rendszerek rendszerszemléletű vizsgálata. ZMNE Kutatási jelentés. 54 oldal, 2004.

[2] Jay Hendrix: Top 10 Reasons for Integrating Your Building Systems, Building Solutions Magazine, © 2004 Siemens Building Technologies, Inc.

[3] Edward Sullivan: System Integration, Building Operating Management August 2003.

[4] *Peter Piazza:* Integrated Cure, Security Management Online, September, 2001. http://www.securitymanagement.com

[5] Will Podgorski: The "Right Stuff": What it takes to become a true building system integrator in today's world, © 2004 Siemens Building Technologies, Inc., HVP Division, Staefa Control System

[6] TOTAL BUILDING COMMISSIONING GENERAL PRINCIPLES AND PROCEDURES, National Institute of BUILDING SCIENCES, http://edesign.state.fl.us/fdi/edesign/resource/totalbcx/guidemod/docs/01nov98.html#intro

[7] BuilDog - Integrált Intelligens Épület Menedzser, http://www.hp.hu/IBCC/magyar/BuilDog.php

[8] Magyar Biztosítók Szövetsége, Biztonságtechnikai útmutató a betöréses lopás-rablásbiztosítási kockázatok kezelésére. 2007.10.17. http://www.mabisz.hu/informacio/biztonsagtechnika/A1fejezetszefoglalodokumentum20071017.pdf

[9] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 1. rész: Rendszerkövetelmények, MSZ EN 50131-1:2007

[10] Dr. Lukács György szerkesztő: Új Vagyonvédelmi Nagykönyv, Cedit 2000 Kft, 2002. Budapest

[11] Riasztórendszerek. 5. rész: Környezetállósági vizsgálati módszerek, MSZ EN 50130-5:2000

[12] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 2-4. rész: Kombinált, passzív infravörös- és mikrohullámú érzékelők követelményei, MSZ EN 50131-2-4:2009

[13] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 2-6. rész: Nyitásérzékelők, MSZ EN 50131-2-6:2008, (angol nyelvű)

[14] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 2-7-1. rész: Üvegtörés érzékelők, MSZ EN 50131-2-7:2008, (angol nyelvű)

[15] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 4. rész: Figyelemfelhívó eszközök, MSZ EN 50131-4:2009, (angol nyelvű)

[16] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 3. rész: Vezérlő- és kijelző berendezés, MSZ EN 50131-3:2009, (angol nyelvű)

[17] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 6. rész: Tápegységek, MSZ EN 50131-6:2006

[18] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 7. rész: Alkalmazási irányelvek, MSZ CLC/TS 50131-7:2008

[19] Riasztórendszerek. Beléptető rendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: Rendszerkövetelmények, MSZ EN 50133-1:2006

[20] Riasztórendszerek. Beléptető rendszerek biztonságtechnikai alkalmazásokhoz. 2-1. rész: Részegységek általános követelményei, MSZ EN 50133-2-1:2001

[21] Riasztórendszerek. Beléptető rendszerek biztonságtechnikai alkalmazásokhoz. 7. rész: Alkalmazási irányelvek, MSZ EN 50133-7:2000

[22] Tóth Levente: CCTV magyarul, BM Nyomda, 2004. Budapest

[23] Riasztórendszerek. Zárt láncú televíziós megfigyelő rendszerek biztonság-technikai alkalmazásokhoz. 7. rész: Alkalmazási irányelvek, MSZ EN 50132-7:200x, (angol nyelvű, kidolgozás alatt)

[24] Riasztórendszerek. Zárt láncú televíziós megfigyelő rendszerek biztonság-technikai alkalmazásokhoz. 1. rész: Rendszerkövetelmények, MSZ EN 50132-1:200x, (angol nyelvű, kidolgozás alatt)

[25] Riasztórendszerek. Zárt láncú televíziós megfigyelő rendszerek biztonság-technikai alkalmazásokhoz. 5. rész: Videoátvitel, MSZ EN 50132-5:200x, (angol nyelvű, kidolgozás alatt)

[26] Utassy Sándor - Bárkányi Pál: IP alapú kommunikáció az elektronikus vagyonvédelmi rendszerekben, Bolyai Szemle, 2006/2. szám, Budapest

[27] Tűzjelző berendezés. 1. rész: Bevezetés, MSZ EN 54-1:2002

[28] Tűzjelző berendezés. 2. rész: Tűzjelző központ, MSZ EN 54-1:2002

[29] Prof. Dr. Óvári Gyula egyetemi tanár, szakfelelős: A Biztonságtechnikai mérnöki mesterképzési szak tanterve, ZMNE-BJKM, 2006.

[30] Dan Brown: The Da Vinci Code, ISBN 0-552-14951-9

[31] Invisible Security
(http://www.boschindia.com/content/language1/html/715_2842.htm)

[32] Scenarios for Ambient Intelligence in 2010
ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf

[33] Ann Longmore-Etheridge: Artful Integration, Security Management Online, September, 2001. http://www.securitymanagement.com

[34] www.ctit.utwente.nl/research/projects/national/iop-gencom/basis.doc/index.html

[35] Alarm Systems – Combined and integrated alarm systems – General requirements Final Draft CLC/FprTS 50398:2008

[36] Rita Premo: An Academic Approach, Security Management Online, September, 2001. http://www.securitymanagement.com

[37] *Michael A. Gips*: News and Trends_Integration or Dis-Integration, Security Management Online, September, 2004. http://www.securitymanagement.com

[38] Edward Crawley. System Architecture – curse notes. MIT, 2005.

[39] Pécsi Tudományegyetem Pollack Mihály Műszaki Főiskolai Kar Műszaki Informatika Tanszék http://e-oktat.pmmf.hu/04_bevezets Bodlaki Tamás: Bevezetés az operációs rendszerekbe

[40] Vicsek Tamás az MTA rendes tagja, tanszékvezető egyetemi tanár, ELTE TTK Fizika Tanszékcsoport, Biológiai FizikaTanszék; "Komplexitás elmélet" Magyar Tudomány**, 2003/3,** Egyszerű és bonyolult
http://www.matud.iif.hu/03mar/vicsek.htm

[41] Panu raatikainen: Complexity and information. Reports from the departement of Philosophy, 2, 1998.

[42] Mohsen N AlSharif. Assesing the complexity of software architecture. PhD thesis, Florida Institute of Technology, May 2005.

[43] Mark Meyer and Alvin Lehnerd. The Power of Product Platforms. Free Press, 1997.

[44] Edward Crawley. System architecture – course notes. MIT, 2005.

[45] Matti J Kinnunen. Complexity Measures for System Architecture Models. MIT, 2006.

[46] Riasztórendszerek. Behatolás-jelző rendszerek. 5.3. rész: Rádiófrekvenciás technikát alkalmazó, összeköttetést biztosító berendezések követelményei, MSZ EN 50131-5-3:2005

[47] Dr. Zsigmond Gyula-Dr. Sipos Jenő A ZMNE és a BMF által közösen indított b.t. mérnökképzés (MSc) villamos jellegű tantárgyainak oktatási tapasztalatairól. Elektrotechnika, 2009./01. 16.-17. oldal

KÖSZÖNETNYILVÁNÍTÁS

Köszönetet mondok

Prof. Dr. Zsigmond Gyula egyetemi tanár úrnak, témavezetőmnek sokirányú szakmai és emberi segítségéért,

Dr. Túrmezei Péter dékán úrnak a kezdeti és végső stádiumbeli segítségéért, ösztönzéséért,

Dr. Horváth Elek igazgató úrnak a nyugodt munkakörülmények biztosításáért és támogatásáért,

a Katonai Műszaki Doktori Iskola vezetőinek,

Prof. Dr. Solymosi József úrnak,
Prof. Dr. Halász László úrnak,
Dr. Haig Zsolt tudományszak-vezető úrnak,

és valamennyi kollégának, munkatársnak, akik segítették tudományos kutató munkámat.

2009. Budapest Utassy Sándor