HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Bunyitai Ákos
bunyitai.akos@gmail.com

A BELÉPTETŐ RENDSZEREK HELYE ÉS SZEREPE A VAGYONVÉDELEMBEN

Absztrakt

E rövid tudományos cikk célja a beléptető rendszerek vagyonvédelemben betöltött helyének és szerepének vizsgálata. Röviden összefoglalja az alapösszefüggéseket, definiálja a fogalmakat. Az elméleti tárgyaláson túl gyakorlati szempontból is megközelíti a tudományos problémát.

This short article is for investigate the access control system's functions in security. It gives a brief summary of the main definitions. Beyond the theoretical negotiation also includes practical support.

Kulcsszavak: *vagyonvédelem, beléptető rendszer ~ security, access control system*

BEVEZETÉS

A beléptető rendszerek elterjedtségéből adódóan szükségesnek véljük tudományos alapú vizsgálatukat, különös tekintettel a vagyonvédelemben betöltött helyükre, szerepükre, alkalmazási területükre vonatkozóan. A fentieken túl célszerűnek tartjuk a téma gyakorlatias megközelítését is, valamint a fejlődés irányának rövid bemutatását.

FOGALMAK, ALAPÖSSZEFÜGGÉSEK

Beléptető rendszer fogalma

„Komplex elektromechanikai-informatikai rendszer, amely telepített ellenőrző pontok segítségével lehetővé teszi objektumokban történő személy- és járműmozgások hely-, idő- és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését.” „A szerkezeti elemeken túl tartalmazza azokat az intézkedéseket és apparátusokat melyek az üzemeltetéshez és a beléptetés felügyeletéhez szükségesek!”[1][2]

A beléptető rendszer fő részei [1]

- *Olvasó(k)* feladata, hogy az azonosításra alkalmas adatokat szolgáltassa a rendszer felé.
- *Vezérlő(k)* feladata, hogy az olvasóról beérkező adatok alapján eldöntse, hogy az adott személy az adott időpontban adott irányban jogosult-e az áthaladásra, működtesse, felügyelje az APAS-t (ld. később), naplózás.
- *Felügyeleti rendszer (pl.: PC-n futó felügyeleti szoftver):* feladata a rendszer ellenőrzése, a vezérlő egységek felprogramozása és a jogosultságok eldöntése, események rögzítése, visszakeresése, listázása.
- *Áthaladást szabályzó eszközök és érzékelőik* (a szakirodalomban az *APAS* rövidítés használatos az angol *Access Point Actuators and Sensors* meghatározásból) feladata, hogy kizárólag az arra jogosultak belépését tegye lehetővé (jogosulatlan személy be/ki lépésének akadályozása mechanikus vagy elektromechanikus eszközökkel), szingularizáció (egy azonosítás, egy áthaladás) és a gátló-szerkezet állapotának (nyitott, zárt, stb.) megállapítása. Pl.: forgókereszt, forgóvilla, gyorskapu, mágneszár, stb. érzékelőik működését a továbbiakban nem vizsgáljuk.

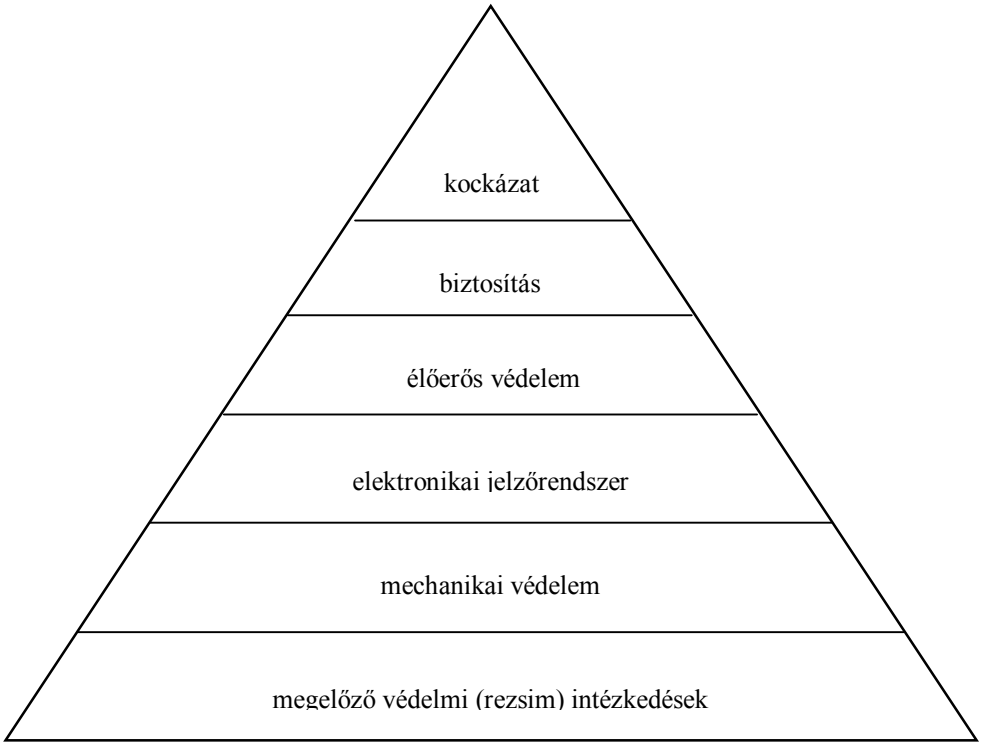
A *beléptetés folyamata:* azonosítás (személy, gépjármű, stb.), belépési jogosultság eldöntése, APAS működtetése, áthaladás, visszazárás. A beléptető további funkciói az események naplózása, rendszerfelügyelet, stb.[1]

A beléptető rendszer helye és szerepe a vagyonvédelemben

A beléptető rendszerek vagyonvédelemben betöltött szerepének vizsgálatához ismernünk kell a komplex vagyonvédelem megvalósításának elvi modelljét, vagyis a védelem megtervezésének lépcsőit és azok célszerűen alkalmazott arányait.

Az alábbiakban tekintsük a vagyonvédelem elvi felépítését ábrázoló vagyonvédelmi piramist!

A vagyonvédelmi piramis felépítése [3]:



1. ábra. A vagyonvédelmi piramis

- Megelező védelmi intézkedések célja olyan szabályok, szabályrendszerek bevezetése, betartása, betartatása, amelyek csökkentik a biztonsági kockázatot.
- Mechanikai védelem célja, hogy a védeni kívánt személytől, tárgytól, helyiségtől, információtól (információhordozótól) fizikailag távol tartsa a hozzáférési jogosultsággal nem rendelkező személyeket. Áthatolhatatlannak kell lennie a beavatkozó élőerő megérkezéséig.
- Elektronikai jelzőrendszer célja adott állapottól való eltérés (esemény) figyelése, rögzítése, továbbítása. Önmagában nem véd, csak jelez. Mind a mechanikai, mind az élőerős védelem támogatója lehet.
- Élőerős védelem célja, hogy nem kívánt folyamatokat megakadályozza. Az elsődleges beavatkozó megfelelő közelségben kell legyen, hogy időben történjen a beavatkozás.
- Biztosítás célja az eddigiekben tárgyalt eszközökkel gazdaságosan le nem fedhető kockázatok csökkentése.
- Kockázat azt jelenti, hogy mivel 100%-os biztonság nem létezik mindig számolni kell fennmaradó kockázattal.

A mai beléptető rendszerek a vagyonvédelem részét képzik, ellenőrzik, hogy a személy jogosult-e adott időpontban, adott irányban, adott átjárón való áthaladásra, vagyis a védett tértől távol tartható a belépésre jogosulatlan személy.

A beléptető rendszerek szűkebb értelemben az elektronikai jelzőrendszer részei. Tágabb értelemben azonban magukba foglalják (illetve szükséges kiegészítői): a rezsim intézkedéseket (pl.: kényszerített személyazonosítás), a mechanikai védelmet (pl.: forgóvilla) és az élőerős védelmet (pl.: vagyonőr, aki riasztás esetén beavatkozik) is. A fentiekből adódóan a beléptető rendszer egyéb rendszerekkel kiegészítve megvalósítja a komplex

vagyonvédelmet. Támogató rendszerekre az eltérő funkciókból adódóan van szükség. Hiszen a beléptető rendszer nem helyettesíti pl.: a kamerarendszert vagy a behatolásjelző rendszert.

Hol van szükség beléptető rendszerre? Hol, milyen rendszer javasolt?

Beléptető rendszerre szükség van minden olyan helyen, ahol a belépést felügyelni kell. Filkorn József – egy vezető beléptető rendszert fejlesztő, gyártó és forgalmazó cég műszaki igazgatója – szerint indokolt elektronikus beléptető rendszer létesítése, ha az alább felsorolt feltételekből bármelyik fennáll [4]:

- A védett terület biztonsága megköveteli
- Biztonságos (hamisíthatatlan) belépési kulcsra van szükség
- A belépőt azonosítani kell
- Tudni kell a védett területen tartózkodók számát
- Limitálni kell a védett területen tartózkodók számát
- Azonosítani kell a védett területen tartózkodókat
- Ki kell zárni a belépési jogosultság átruházásának lehetőségét
- Ki kell zárni, hogy jogosult beengedjen jogosulatlant
- Ki kell zárni a belépési kulcsok illetéktelenek általi felhasználását
- A belépést időben korlátozni kell
- Tudni kell, hogy az azonosított hol tartózkodik
- Tudni kell, hogy valaki mikor ment be, és mikor távozott
- Tudni kell, hogy egy adott területen ki, mennyi ideig tartózkodott
- Folyamatosan változik a belépésre jogosultak köre
- Egy átjáróhoz háromnál több kulcs kell
- Egy személynek háromnál több kulcsra van szüksége
- A belépésért díjat kell fizetni
- A védett területen való tartózkodásért (időarányos) díjat kell fizetni
- A védett területre való belépés különleges technológiai eljárást igényel

Jellemzően ilyen helyek az irodaházak, közép-és nagyvállalatok telephelyei, gyárak, uszodák, fürdők, szállodák, erőművek, katonai objektumok, stb.

A fentiekből következően valamely objektum beléptető rendszerének tervezésekor számos körülményt kell számításba venni, különösen a rendszerrel szemben támasztott követelményeinket illetően. Meg kell vizsgálni egyebek mellett az épület tereinek (zónáinak) sajátosságait, azokba a belépésre jogosultak körét, a bármely szempontból ellenőrzött terek veszélyforrásait. Bár a beléptető-rendszereknek a be-, és kiléptetés a primer funkciója, valamint az objektumon belüli mozgások különböző jogosultsági szintek szerinti szabályozása, napjainkban a jogosultság megállapíthatóságán kívül elvárható igény egyebek mellett a jogosultság időben és térben történő lehatárolhatósága és változtathatósága, így előre meg kell határozni a beléptető rendszertől megkívánt funkciókat.[5]

A téves következtetések elkerülése érdekében fontosnak tartjuk deklarálni az alábbiakat:

- Tökéletes, 100%-os biztonság nem létezik, minden rendszernek van gyenge pontja, minden rendszer kijátszható. A védelem szintje úgy értelmezhető, hogy milyen nehéz a komplex vagyonvédelmi rendszert megkerülni. Ennek megállapítására igen kevés objektív, mérésen alapuló eljárás ismeretes, a megfelelő rendszer tervezése mérnöki feladat. Köztudott, hogy egy lánc olyan erős, mint a leggyengébb láncszeme.
- A vagyonvédelem gyenge pontja nem csak a vagyonvédelmi piramis eleme lehet, hanem maga a felhasználó is. A mechanikai és elektronikai rendszerek szabotálása tervezhető. Az ember figyelmetlen, feledékeny, óvatlan, megzsarolható, megvesztegethető… vagyis megbízhatatlan. Vis maiorra nehéz tervezni.

- Mindhárom személyazonosítási módszernek (tudás, birtok, biometrikus tulajdonság alapú) vannak előnyei, hátrányai, javasolt és alkalmazott felhasználási területük eltér egymástól, ezért annak az esélye, hogy a közeljövőben valamelyik terület kiszorítja a másikat, minimális.
- Ma a tudás, a birtok és a biometria alapú beléptető rendszerek is kijátszhatók valamilyen módon. A tudás alapú az óvatlanságból, figyelmetlenségből, feledékenységből adódóan; a birtok alapú az átadhatóságból, másolhatóságból adódóan; a biometria alapú a minta másolhatóságából adódóan. A felhasználó kényszeríthető, hogy beüsse PIN kódját (erre az esetre használatos a duress, vagyis kényszerített kód), hogy átadja RF kártyáját vagy odatartsa ujját az olvasóhoz (ilyen esetre célszerű másik ujjat rögzíteni). Az előbbiek a mai közbiztonság mellett nem jellemzőek. Az ismert kijátszási módszerek ellehetetlenítésén fejlesztőmérnökök dolgoznak.
- A fentiekből nem következik, hogy egyik rendszer sem alkalmas feladatának ellátására. A biztonságtechnikai mérnök fő feladata az adott személy, tárgy, objektum, információ(hordozó) optimális védelmének tervezése. A kockázatok elemzése, a védett értéke, a lehetőségek, a kialakításra fordítható keretösszeg, a speciális igények figyelembevételével.
- A kockázatelemzést nem csak a rendszer tervezésekor, kivitelezésekor kell elvégezni, a körülmények üzemeltetés alatt is változhatnak!

Azokon a helyeken, ahol viszonylag nagyszámú felhasználót kell relatíve rövid idő alatt be-vagy kiléptetni, ott vonalkódos vagy rádió-frekvenciás azonosítás ajánlott. Vonalkódos azonosítás ott ajánlható, ahol a vagyonvédelem nem elsődleges (könnyedén reprodukálható), általában olcsón, nagy mennyiségű, egyszeri belépő kiadása indokolt (pl.: koncertjegy, parkolójegy, stb.). Kódos vagy biometrikus azonosítás nem ajánlott nagy forgalmú (nagy számú beléptetést igénylő) helyeken. Kódos azért nem, mert könnyen leleshető, elfelejthető. A kódok kiosztásánál ügyelni kell a kombinációk maximális számára és egyéb, a biztonságot befolyásoló tényezőkre (4 digites kód esetén maximum 10^4/2db kód osztható ki, ha van kényszerített kód, akkor maximum 10^4/4db, a kiosztásnál kerülni kell a 4 egyforma digitet „0000”, a számsorokat „1234” és két kód nem lehet egyforma). Biometrikus azért nem, mert kevésbé elfogadott és epidemiális kockázatok is jelentkezhetnek (kézgeometria azonosítás, tenyérerezet azonosítás, írisz-azonosítás, stb.). Ilyen, vagy kombinált személyazonosítású rendszerek kevesebb jogosult felhasználót érintő, fokozottabb biztonságot élvező helyiségbe jutáskor, a többkörös védelem részeként célszerű kialakítani, pl.: a vállalat szerverterme, TÜK-szoba, stb.

Mire jó még a beléptető rendszer?

A beléptető rendszerek – a fentieken túl – alkalmazhatók: jelenlét-figyelésre (ki, melyik helyiségben tartózkodik), munkaidő-nyilvántartásra, dolgozók adatainak nyilvántartására, programozott kimenetek vezérlésére, illetve integrált rendszer esetén minden gépészeti, tűz-és vagyonvédelmi feladat ellátására.

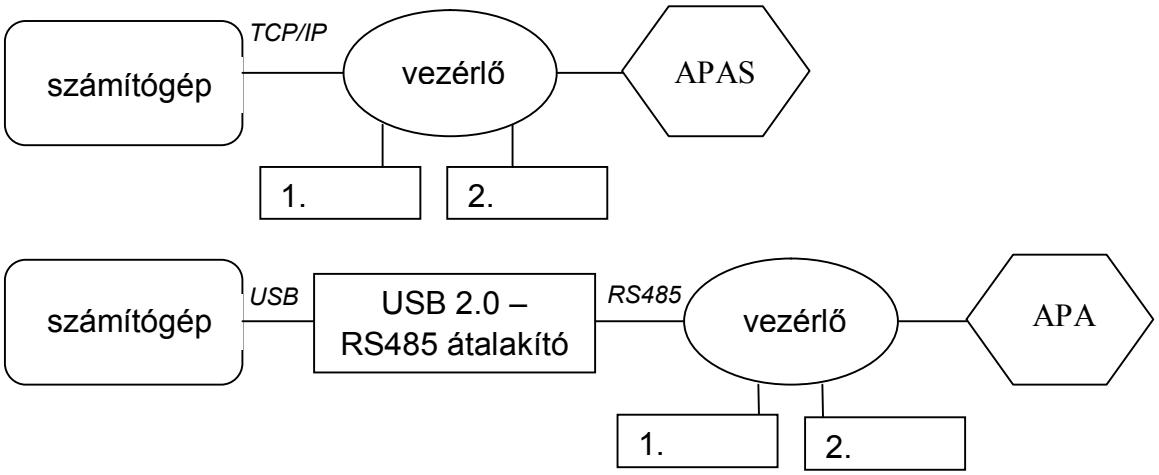
GYAKORLATI ISMERETEK

A beléptető rendszer felépítése, rendszertopológia

A továbbiakban tekintsük a fentiekben részletezett egységek egymáshoz kapcsolásának néhány lehetséges módját, vagyis hogyan lesz az alkatrészekből rendszer!

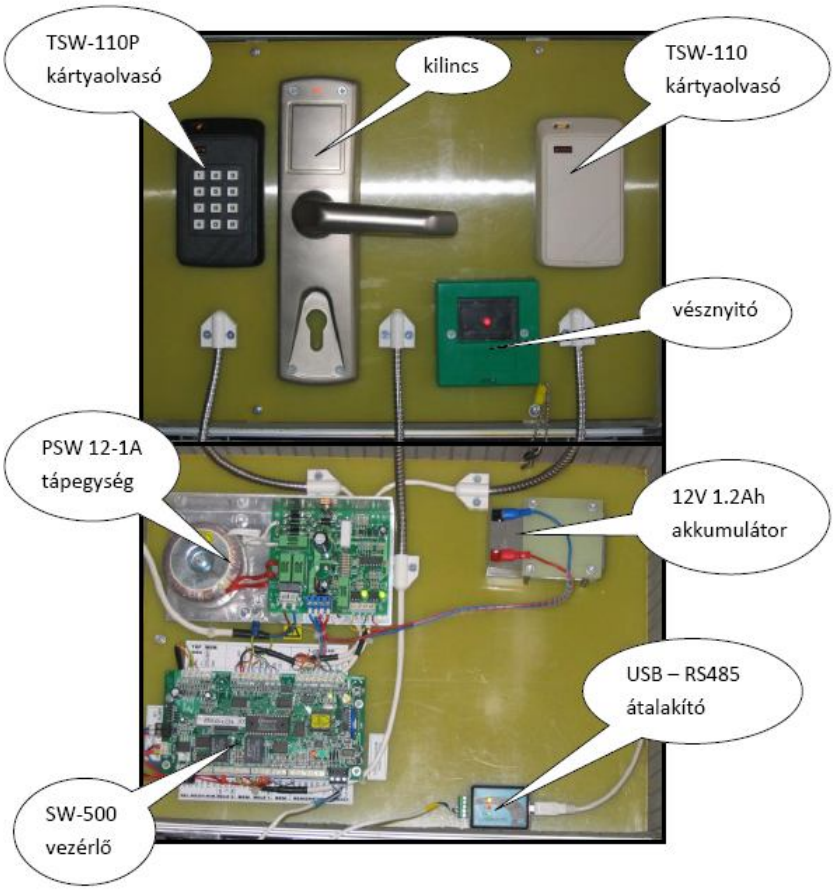
Az olvasó beolvassa az azonosításra alkalmas adatokat, majd ezeket továbbítja a vezérlő felé, ahol döntés születik az APAS vezérléséről. Mindenről esemény készül, ezt a vezérlő

tárolja és tovább is küldi a számítógép felé. Ld. 2/a. és 2/b. ábra, eltérés a vezérlő és a számítógép közti kommunikációs protokollban van. Ilyen rendszertopológia valósítható meg pl.: a Cryptex CR2001IP (2/a.ábra) és a Seawing SW-500 (2/b.ábra) vezérlőkkel.



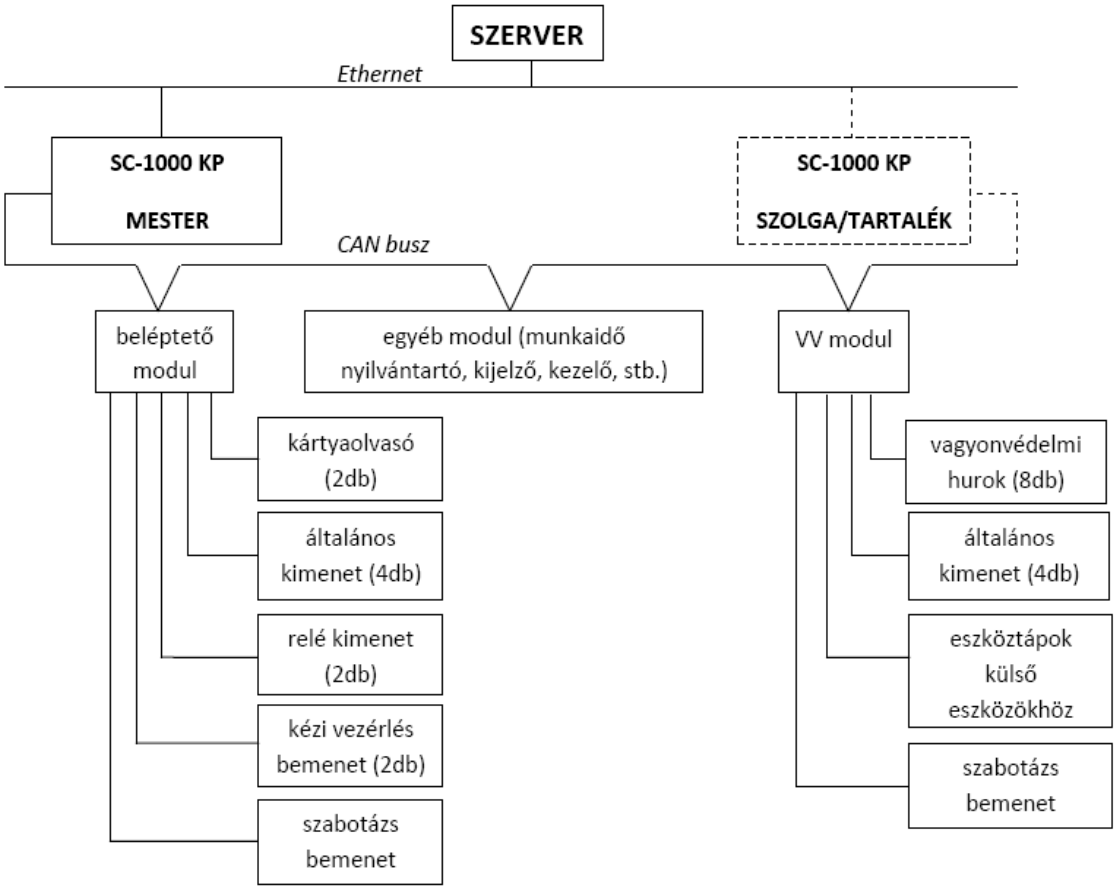
2/a-b ábra. Rendszertopológiai példák

Az alábbiakban – a könnyebb érthetőség kedvéért – a fenti (2/b.ábra) rendszertopológia megvalósítása kerül bemutatásra. Az alábbi ábrán (3. ábra) egy RFID beléptető rendszer látható, melynek elemei: SW-500 vezérlő, TSW-110 és TSW110P olvasók, PSW12-1A tápegység, akkumulátor, vésznyitó, elektronikusan reteszelhető kilincs, USB-RS485 átalakító. A tesztkészülékeket a kutatásokhoz a Seawing Kft. bocsátotta rendelkezésre.



3.ábra. A tesztbőrönd belseje

A továbbiakban röviden bemutatjuk a fejlesztések új irányának egyik képviselőjét, az SC-1000-res családot, mellyel integrált rendszer valósítható meg (4. ábra). A vezérlő CAN buszon kommunikál moduljaival, amelyeken keresztül csatolhatók a beléptető, vagyonvédelmi, munkaidő nyilvántartó, stb. eszközök, alrendszerek. A rendszertopológia és az eszközök nagy előnye az integrálhatóság, a széleskörű alkalmazhatóság, magas biztonsági szintű rendszer (Grade 4) valósítható meg velük, nagy kiterjedésű és/vagy több telephely integrált felügyelete lehetséges, RS485-höz képest gyorsabb adatforgalom. Az ikervezérlős kialakítás nagyobb megbízhatóságú rendszert eredményez, hiszen a vezérlő kiesésekor sem áll meg a rendszer, a felhasználókat nem érinti a jelenség.[6]



4. ábra. Az SC-1000 topológiája

Fontosnak tartjuk megjegyezni, hogy más gyártók szintén fejlesztenek hasonló termékeket, a fenti eszköz rövid leírásának célja nem a kiemelés, hanem a fejlesztés irányának bemutatása.

Mire kell ügyelni beléptető rendszer tervezésekor, kivitelezésekor?

- A tervezés első szakasza a kockázatelemzés és igényfelmérés
  - mit kell védeni
  - mitől kell védeni
  - mekkora a rendelkezésre álló keretösszeg
  - milyen speciális igények vannak
- A fentiekből el kell dönteni, hogy milyen védelmi szintű rendszer kerüljön kialakításra és milyen eszközökkel.
- Ügyelni kell a megkerülhetetlenségre és kijátszhatatlanságra
  - megkerülhetetlenség: a védendő tér összes belépési pontját védjük

    - kijátszhatatlanság: szingularizáció, megfelelő nyitvatartási idők és anti-passback beállítások
- Életvédelmi előírások betartása
    - menekülési útvonalak szabaddá tétele (vésznyitó vagy pánikkar felszerelése)
    - az áthaladást szabályzó eszközök átbocsátó képességének figyelembe vétele
    - zsilipben nem ragadhat benn senki
- Empátia
    - feleslegesen ne akadályozza a rendszer a védett objektum használóinak szabad mozgását
    - karbantartó, postás, szállító, vendég, stb. bejutását (kijutását) is meg kell oldani (jellemzően a recepcióhoz) pl.: kaputelefon és távnyitó alkalmazásával
- Dokumentáció a kivitelezéshez
- Telepítéskor
    - vezérlő csak a védett térrészben lehet
    - kábelezés csak a védett térben lehet, vagy ugyan olyan szintű védelemmel kell ellátni, mintha ott lenne, olvasók megfelelő magasságba telepítése, átolvasás tervezése
- Megvalósulási dokumentáció a karbantartáshoz, szervízeléshez

A (NEM TÚL TÁVOLI) JÖVŐ

A fejlődés iránya a különböző rendszerek integrálása felé vezet. Ma is számtalan termék létezik, mely egyszerre, integráltan képes kezelni az épületfelügyeleti (világítás, fűtés, melegvíz, árnyékolás, légkondicionáló, stb.), tűz (tűzjelző és tűzoltó) és vagyonvédelmi (behatolásjelző, beléptető, kamera, stb.) rendszert, egységes felületen megjelenítve. Ahhoz viszont, hogy ez a rendszerstruktúra széles körben megjelenjen és elterjedjen, mindenki számára elérhetővé váljon, el kell telnie néhány évnek. A későbbiekben elképzelhető, hogy minden épületben az ott lévő összes elektromos berendezés informatikai kapcsolatban lesz egymással. Ennek előnye lenne, hogy kényelmes, egy felületen könnyen és átláthatóan kezelhetővé válna minden, gazdaságos (pl. lekapcsolódik a villany, ha nem tartózkodik senki a helyiségben), illetve kitágulna az egyes eszközök funkciója (pl. a TV segítségével videó-telefonálhatnánk, a kamerarendszer segítségével videó-üzeneteket küldhetnénk) stb. Hátránya az elektromos áramtól való nagyobb mértékű függés.

Tekintsük példaként az alábbi szituációt: behatolás történik egy családi házba vagy lakásba éjszaka, amikor a tulajdonos otthon van. A rendszer értesíti a rendőrséget a kamerarendszer első képeivel és a GPS pozíció megjelölésével. Lezárja a helyiséget, amelyben a behatoló tartózkodik („nem büntethető, akinek a cselekménye a saját, illetőleg a mások személye, javai vagy közérdek ellen intézett, illetőleg ezeket közvetlenül fenyegető jogtalan támadás elhárításához szükséges” [7]) – vagy ahol a tulajdonos tartózkodik – a tulajdonos és családja, anyagi javai védelme és a hatóság munkájának segítése érdekében, blokkolja a helyiségben található összes konnektort.

Egy másik példa: tűz üt ki, a jelző-és oltórendszer aktivizálódik, értesíti a tűzoltóságot és felhívja a figyelmet az épületben tartózkodó személyekre. Megkezdődik a kiürítés, biztosítja a megfelelő tájékoztatást, a kiürítési utak nyílászáróit oldja, akár intelligensen a tüzet elkerülve vezeti a bent lévőket. A felvonókat az alsó szintre irányítja, esetleg plusz információkkal látja el a tűzoltóságot (elküldi az épület alaprajzát, a tűz lokalizálása, gócpontja, mi ég, milyen anyagok találhatók a közelben és milyen mennyiségben, mekkora a helyiség belső hőmérséklete és milyen gázok találhatók a légterében stb.). Lekapcsolnak a közművek, a tűzoltóság megérkezéséig kinyílnak a kapuk és ajtók a könnyebb megközelítés érdekében,

részükre megfelelő kommunikációs hálózatot biztosít. Értesíti a tulajdonost, a tűz lefeketítése után szellőztetés indul, a rendszer ön-kárfelmérést végez.

Feltételezzük hogy a fentiekhez hasonló rendszer hasznára válna a társadalomnak.

ÖSSZEGZÉS

A fentiekből látható – az alapfogalmakon és összefüggéseken túl – hogy mire alkalmas egy beléptető rendszer, hol milyen rendszer javasolt. Röviden bemutattuk a beléptető rendszerek felépítését, konkrét, széles körben alkalmazott eszközök rövid bemutatásán keresztül rendszertopológiai példákat hoztunk. Elképzeltünk egy mindenki számára elérhető integrált rendszert, mely segít az épületfelügyeleti, tűz és vagyonvédelmi rendszereket felügyelni, átlátni.

Felhasznált irodalom

[1] Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból, Hadmérnök, VI. Évfolyam 1. szám, 2011/1, ISSN1788-1919, http://hadmernok.hu/2011_1_bunyitai.pdf

[2] Filkorn József: Beléptető rendszerek c. előadás, Seawing Kft, Székesfehérvár, 2009.

[3] Dr. Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései c. PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2009.

[4] Interjú Filkorn Józseffel, Székesfehérvár, 2011.

[5] Dr. Berek Tamás: ABV (CBRN) analitikai laboratórium beléptetőrendszere a biztonságos üzemeltetés szolgálatában, Hadmérnök, VI. Évfolyam 2. szám, 2011/2, ISSN1788-1919, http://www.hadmernok.hu/2011_2_berek.pdf

[6] Seawing SC-1000 műszaki paraméterek, 2010.

[7] 1978. évi IV. törvény a Büntető Törvénykönyvről, A jogos védelem 29.§ 1)