IP a biztonságtechnika világában

Mindennapi életünknek a digitális világ, az Internet már meghatározó része. Elvárható tehát, hogy a biztonságtechnikai eszközök – lépést tartva a gyors technikai fejlődéssel – részesei legyenek ennek a digitális világnak, és felhasználják belőlük azokat a vívmányokat, melyek hatékonyabbá teszik működésüket. Az IP biztonságtechnikai alkalmazások gyors fejlődési trendet mutatnak. Ennek során egyre több eszköz jelenik meg a piacokon, amely használja e „digitális platformot".

Az ***IP – internet protokoll*** (angolul: Internet Protocol) a világ „talán" legelterjedtebb számítógép-hálózata az Internet (és Internet alapú) hálózat egyik alapvető szabványa (avagy protokollja). Ezen protokoll segítségével kommunikálnak egymással az internetre kötött csomópontok (számítógépek, hálózati eszközök, webkamerák stb.). A protokoll meghatározza az egymásnak küldhető üzenetek felépítését, sorrendjét stb.

Az internet mindennapos elérésével, a sávszélesség növekedésével, a szolgáltatások és az egyre költséghatékonyabb hálózati megoldások terjedésével indult el az IP infrastruktúrák alkalmazásának folyamata a biztonságtechnika világában. Az IP rendszerek azonos „nyelven" beszélnek, az információkat megosztják egymás között, ezáltal nagyobb intelligencia és automatizálás valósul meg. Kevesebb vezetékkel épülnek fel, így a kivitelezés költségei olcsóbbá válnak. Ez a technikai rendszer egy új lehetőséget biztosít azáltal, hogy az adatforgalmak mellett video-, audio- és más jelek átvitelét is garantálja. Az IP hálózatra már CCTV berendezéseket, beléptető és behatolásjelző rendszereket tudunk kapcsolni. Megszűnnek a szolgáltatási határok, bármely információ a világon bárhol megjeleníthető PC-n, mobil telefonon vagy PDA-n. Annak köszönhetően, hogy videót, hangot és adathálózatokat gyűjtünk össze egyetlen IP alapú hálózatra, csökkentjük az üzemeltetési, fenntartási és karbantartási költségeket. „E technikai világ azonban más szemléletet és gondolkodást kíván." Hallgassuk meg, mit mond egy olyan szakember, aki munkája során gyakran találkozik IP rendszerek alkalmazásával a biztonságtechnikában. ***Papp Péter*** biztonságtechnikai mérnököt kérdeztem szakmai tapasztalatairól.

P. P.: Az újabb műszaki megoldások segítségével bizonyos oldalon előnyhöz jutunk, de a másik oldalon újabb és újabb feltételeket kell teljesítenünk. Lássunk egy példát: amikor egy biztonságtechnikai rendszert távközlési vonalra kapcsolunk, az csak egy egyszerű telefonvonal bekötésével jár. Tudomásul vesszük, hogy a rendszer üzemszerű ellenőrzése naponta egyszer vagy kétszer történik meg, tesztjelentések formájában. Csak míg az analóg vonalon napi egy, esetleg kettő ellenőrző jelentést tudunk lefuttatni, addig az IP rendszer esetében gyakorlatilag ez korlátlan. Ezáltal rövid időn belül tudomásunkra jut a rendszer hibája. Természetesen minden egyes jelzésátvitel pénzbe is kerül a kapcsolt vonali alkalmazásoknál. Az IP alapú átvitelnél az egyes jelentések ingyenesek, de a szolgáltatásért alapösszeget kell fizetni. (A rendszerek szabotázs-védettek köszönhetően a szolgáltatók „magas szintű" műszaki megoldásainak).

Manapság nagyon sok felhasználó rendelkezik szélessávú eléréssel, ezért költségnövekedést nem okoz a jelátvitel, és mivel minimális adatmennyiség kerül átvitelre érdemben a hálózat forgalma sem nő.

Az IP alapú jelátvitel egyik gyenge pontja a tápellátás, hiszen a vagyonvédelmi rendszertől független egységek biztosítják a kapcsolatot a műszaki szolgáltatóval, és áramszünet esetén biztosítanunk kell ezen eszközök üzemszerű működését.

P. P.: A hagyományos telefonvonal alkalmazásánál (mely kisfeszültségű egyenárammal működik) nem volt szükség a jelátvitelhez külső tápfeszültségre. A biztonságtechnikai központok rendelkeztek segédtáplálással, így akár helyi, akár nagyméretű áramkimaradáskor is biztosított bármely információ átvitele a telefonvonalon keresztül. Az IP alapú megoldásoknál a modemek és egyéb hálózati elosztó berendezések folyamatos tápellátást igényelnek, ezért áramszünetkor szünetmentes tápegységgel kell biztosítanunk az üzemeltetéshez szükséges feszültséget. Látszólag egyszerű a probléma, valójában azonban a táplálás az egész integrált telekommunikáció egyik meghatározó kulcskérdése.

Napjainkban kevés olyan vagyonvédelmi rendszert találunk, melyekről elmondható, hogy önálló IP technológiával felszerelt központi egységgel rendelkezik. A régebbi fejlesztésű rendszerekhez a BUS-ra illesztett bővítő kártyákkal valósítják meg az Ethernet felőli csatlakozás lehetőségét. Ezek, általában a belső protokollhoz kapcsolódó egységek kevés többletfunkciót eredményeznek. Általánosságban elmondható, hogy lehetőséget biztosítanak a rendszer programjának feltöltéséhez, illetve saját felügyeleti szoftverek LAN hálózaton keresztüli eléréséhez.

P. P.: Eddig általános kommunikációs csatorna volt a soros port RS-232 protokollal. A nagy tudással rendelkező központi egységek adat le- és feltöltése soros porton keresztül sok időt vett igénybe a mozgatott adatmennyiségek miatt. Kritikus volt a modemmel felépített távprogramozás is. Az új technikai megoldásokkal ez leegyszerűsödött. A soros porton keresztül történő programozási lehetőség másik problémája a laptopokon lévő csatlakozók hiánya. Az új hordozható számítógépeken soros port csatlakozó felületek már nem ke-

rülnek elhelyezésre. Helyette az USB illetve a LAN (RJ45) csatlakozó került előtérbe. Az új fejlesztésű vagyonvédelmi központoknál már a központi panelba integrálják az RJ45 felülettel rendelkező LAN hálózati elérés lehetőségét. Ezeket a felületeket nem a bővítő modulok számára alakítják ki. A rendszerek programozása nagyrészt már webes felülettel, böngésző alkalmazásával érhető el.

Az IP hálózatot használó rendszerek alkalmazásánál egy nagyon fontos dolgot figyelembe kell venni. „Nevezetesen a telepített rendszerek által védett objektumok LAN-ra történő kapcsolásával a biztonsági szinteket előtérbe kell helyezni. Az általánosan használt titkosítások – amelyek általában igazak a beléptető és CCTV rendszerekre is – 128 bites AES titkosítással kerülnek megvalósításra." Az alkalmazott AES (Advanced Encryption Standard) titkosítási algoritmust a belga Vincent Rijmen dolgozta ki. „Az amerikai Nemzeti Szabványügyi és Technológiai Intézet (National Institute for Standards and Technology) több évig tartó elemzés után, 2001-ben választotta az Egyesült Államok új hivatalos titkosítási szabványául." (A 128 bites kulcs generálásakor 340-szer tíz a harminchatodikon számú lehetséges eredmény létezik.) A másik alkalmazott titkosítási algoritmus az IPSEC. „Ezt a protokollcsomagot az IETF (Internet Engineering Task Force) dolgozta ki, RFC-kben rögzítették az egyes protokollok definícióit. Az IPSEC hálózati szinten nyújt lehetőséget arra, hogy a kommunikációban résztvevők hitelesen azonosítsák egymást (authentication), és kódolják (encryption) az egymás közt zajló adatforgalmat."

IP CCTV TECHNIKA

Jelenleg a piacon lévő IP berendezések közül az IP CCTV technika fejlődik a legdinamikusabban. Naponta jelennek meg azok a berendezések és alkalmazások, amelyek alkalmasak a hálózati csatlakoztatásra. Cikkünkben az IP CCTV technikára terjedelmi korlátok miatt nem fordítunk figyelmet, hiszen az IP biztonságtechnika ezen ága a legelterjedtebb és a legbővebb dokumentációval rendelkezik.

IP ALAPÚ BEHATOLÁSJELZŐ RENDSZEREK

A piacon jelenleg kevés a forgalomban lévő, Magyarországon is beszerezhető IP alapú szolgáltatást biztosító riasztó panel. Ezek közül egy Magyarországon fejlesztett és gyártott – a Sky Laboratories Kft. GIO 300s v2 behatolásjelző központját vizsgáljuk meg a beállítási lehetőségek oldaláról.

P. P.: Az eszköz a működése szempontjából az általánosan használt alaplapokhoz hasonlítható. Az első szokatlan megoldás, hogy nem a központ saját programjával kell programozni, hanem bármely internet-böngésző alkalmas e feladatra. Hasonlít egy router programozásához. Az általánosan használt funkciókat, mint például a zónajellemzők, különböző időzítések, belépő kódok a megszokott módon bevihetőek a rendszerbe. Az alapok után jönnek az újdonságok – az Ethernet kapcsolathoz szükséges paraméterek beállítása. Természetesen a gyári beállítás segítségével rá tudtunk kapcsolódni, de most van rá lehetőség, hogy a mi általunk használt hálózati adatokat rögzítsük a rendszerben. A hálózati mód, az alhálózati maszk és egyéb beállítások után a rendszer alkalmas a kommunikációra. Beállíthatjuk a levelező szerverrel kapcsolatos információkat, hogy riasztás esetén levelet kaphassunk a bekövetkezett eseményekről. A kimeneti pontokat távolról, az internet segítségével is tudjuk vezérelni. A vizsgált berendezés nem csak az általa észlelt események jelentését tudja továbbítani, hanem más riasztóközpontok eseményeit is át tudja jelezni a LAN hálózaton keresztül. Ennek az eszköznek az előnye, hogy az Ethernet felület a panelra került integrálásra. Ilyen rendszerek összekapcsolásával több nyolcas blokkot alkotó egységekből nagy hálózatokat is tervezhetünk.

Hasonló termékek kezdenek megjelenni a külföldi piacon is. A lényeges különbség az elérhető zónaszámokban, illetve a kommunikációs csatornákban található. A nyugat-európai piacon megjelenő berendezéseknél a központi panelra integrálva, a LAN hálózati csatlakozó mellett a GPRS kommunikátor is megtalálható. Ezek a berendezések elő vannak készítve a 21. század ügyeleti szolgáltatásaira.

P. P.: Napjainkban általánosan használt ügyeleti szolgáltatások kapcsolt vonalon történnek. Az esemény bekövetkezte után a telefonvonal állapotától függően 10-15 mp eltelik, míg a jelzés beérkezik a diszpécser központba. E folyamatot tudjuk meggyorsítani az IP alapú technika segítségével. A jelzésátviteli idő a másodperces időkhöz képest nagyságrenddel lecsökken. Gyakorlatban 100 msec. A második fontos része a rendszer folyamatosabb tesztellenőrzése. A jelzések nem foglalják a telefonvonalat, és a jelentésküldési idők megengedik a sűrűbb teszteket. A harmadik, de talán legfontosabb része a költséghatékonyság. Az általánosan használt jelenlegi rendszerek a kapcsolt vonalú szolgáltatások percdíjait vonzzák maguk után. Az elküldött nyitás-zárás jelentések és tesztjelentések költséghatékonyabbá válnak, ha IP alapon kerülnek továbbításra. Ilyenkor nincs távközlési díj, általában az épülethez tartozó ADSL vagy más, szélessávú elérés segítségével történik az adattovábbítás. Az épület jellegéből adódó kockázati szinteknek megfelelően több szintű átviteli utat célszerű biztosítani. A tradicionálisan alkalmazott átjelzési útvonalak a GSM és a PSTN hálózatok helyett az IP alapú GPRS átjelzések is piacot hódítanak.

IP ALAPÚ BELÉPTETŐRENDSZEREK

Nagy különbségek vannak az eddig „hagyományosan" megszokott beléptetőrendszerek és az IP alapú technológián alapuló beléptetőrendszerek között. „Az IP bázisú beléptetőrendszerek lehetőséget nyújtanak a moduláris és gazdaságos rendszerbővítésre." A rendszerbe integrált eszközöket könnyen csatlakoztathatjuk a meglévő egységekhez a közös protokoll alkalmazásával. A gyártók is gondoskodnak arról, hogy az új termékek kapcsolódhassanak a régihez, egyszerű termékfrissítés segítségével. A szoftverek a ➲

IP a biztonságtechnika világában

megszokott RS-485 protokoll helyett IP alapon kommunikálnak. Az eddigi berendezések közötti összeköttetés más feltételekkel kell, hogy teljesüljön. Míg a régi rendszer akár 1 km távolságra is elvihető volt, most be kell tartani a LAN protokollok által előírt feltételeket. Támogatásra kerülnek a rendszerintegrációs folyamatok, biztosítják a legújabb frissítések alkalmazását a hardveres oldal módosítása nélkül is.

P. P.: Az IP alapú rendszer egy felhasználói interfészt jelent. Leegyszerűsíti az üzembe helyezés folyamatát, mivel ugyanazokat a feladatokat kell elvégezni és használni, mint bármely hálózatos eszköznél. Egyetlen felhasználói bejelentkezés egyszerű és biztos hozzáférést nyújt minden biztonsági funkcióhoz. A rendszerekhez a meglévő infrastruktúrákat is fel tudjuk használni. Az általánosan megszokott kábelezési metódusok átírásra kerülnek. Az üzembe helyezési és telepítési költségek is csökkenek. Egy vállalati struktúrában minden eszköz ugyanazt a platformot használja, a hálózatkezelési feladatok egyszerűsödnek. A rendszer másik előnye a központosított tápellátás. Ennek alapjait a PoE (Power Over Ethernet) eszközök segítségével érhetjük el. Több beléptetési ponttal rendelkező rendszert vizsgálva az IP technológia előnye a rendszerek önálló üzemmódjában van. Hagyományos rendszernél egy RS-485 hálózati eszköz meghibásodása az egész rendszerre kihatással lehet. A LAN alapú rendszerek több rétegű redundanciát alkalmaznak, egyik útvonal összeomlása esetén átirányítással új útvonal kerülhet meghatározásra. A mai vállalati környezetekben az informatikai hálózat több figyelmet kap, ezáltal a rendszerek üzembiztonságára fordított költségek és műszaki fejlesztések prioritásokat élveznek. Ha mégis a rendszerbe hibák generálódnak, a riasztási jelzések nagyon gyors idő alatt, általánosan 100 msec alatt jelentkeznek. Természetesen, ezt már felhasználói szinten is le kell tudni kezelni.

„Az IP beléptető rendszerek titkosítása az általánosan használt algoritmusokkal és metódusokkal valósul meg. Közös hálózati területeken VPN felület segítségével tudjuk biztosítani a rendszer ellenállóságát. Lehetőségünk van a vezérlők, kontrollerek olyan szintű szétválasztására, amely biztosíthatja az eszközök megfelelő védelmét. A hagyományos rendszereknél e két egység fizikai távolsága – az alkalmazott protokollok függvényének megfelelően – korlátozott távolságban nyert elhelyezést. Az IP alkalmazással megnövekedtek a távolsági korlátok, így az eszközök mechanikai védelme is könnyebbé vált. Védelmi szempontból még fontos tényező, hogy az IP alkalmazások védelmére számtalan szolgáltatói és értékesítői lehetőség áll előttünk. Felmérések szerint évente több milliárd euró áramlik a piac e szegmensébe."

P. P.: Az IP alapú beléptetőrendszerek sokkal több előnnyel és funkcionalitással rendelkeznek, mint a hagyományos rendszerek. A tradicionális és az IP alapú rendszerek is szervert alkalmaznak központi adat- és vezérlőegységként, és a felhasználó oldaláról is ugyanazok a funkciók állnak rendelkezésre, mégis a különbségek abban rejlenek, hogy a megszokott rendszerek általában egy ajtó figyelésénél nem használnak kétirányú kommunikációt, szemben az IP alapú rendszerekkel. Megjósolható a rendszerek fajlagos bekerülési költsége is. Míg egy általános, több belépési ponttal rendelkező beléptetőrendszernél a belépési pontok számának függvényében csökken az egy ajtóra jutó költség, addig az IP alapú rendszerek esetében egységesebbé tehető. A költségeket nem arányokban kell számolni, hanem egységekben. Ez az IP alapú beléptetőrendszerek piaci részesedésének növekedésével fog járni. A jövőben várhatóan olyan berendezések fognak előtérbe kerülni, amelyek ötvözik az információs biztonságot, a folyamatos üzleti fejlődés lehetőségét és az adattartalom feldolgozását. A beléptetőrendszerekről érkező adatok a hálózat segítségével könnyen elérhetővé válnak, hatékonyabbá és biztonságosabbá tudjuk tenni a rendszereket a felhasználók részére.

INTEGRÁLT FELÜGYELETI RENDSZEREK

Az integrált biztonsági (vagy vagyonvédelmi) rendszerek nagyon sok rendszer összességét jelentik. Ezalatt nem azt értjük, hogy a számos különálló rendszert egy központi számítógéppel felügyeljük, és kezeljük, hanem valódi integráltságot – kezdve a közösen használt vezetékektől az azonos protokoll-használatig, stb. – melynek eredményeképpen az objektumban előforduló összes berendezést egy rendszerként használhatjuk. Az épület-felügyeleti rendszerek, tűzjelző hálózat központja, klíma és gépészeti rendszerek és egyéb egységek is csatlakozhatnak az integrációhoz. A felügyeleti rendszerek információit általánosan számítógépen jelenítjük meg. Ez lehet egy videókép, belépések nyomon követése, vagy bármely eszköz hiba vagy riasztási jelzése. A kommunikációs csatorna természetesen IP alapú. Az általánosan használt protokollokat egy komplex felügyeleti szoftver dolgozza fel. A rendszerek lényege az összevont, egységesen automatizált és felügyelt világ.

MIRE FIGYEL TERVEZÉSKOR?

P. P.: IP alapú rendszerek tervezésénél első feladatunk annak megállapítása, hogy milyen berendezésekkel mire akarunk kapcsolódni. Külön kell választani az épületen belüli és a nagy távolságú /WAN- MAN/ hálózatokkal kapcsolatos feladatokat. Ha csak épületen belüli kommunikációra használjuk a LAN felületünket, akkor az informatikai hálózattal kapcsolatos útvonalakat kell pontosítani. A tervezési határok megállapítása fontos feltétele a jó tervek elkészítésének. Melyik eszköz, hol csatlakozik a hálózathoz, milyen sávszélességgel, van-e egyéb igénye. Nem mindegy, hogy egy kamerás rendszert akarunk üzemeltetni azon a számítógép-hálózaton, amely jelenleg is akadozva kommunikál, vagy csak időnként akarunk egy eseményt lehívni egy riasztóberendezésről. Szerencsés esetben közös kézben vannak a gyengeáramú rendszerek tervei. Ilyenkor tudunk figyelni a megfelelő átjárási pontok meglétére. Tervezéskor az informatikai kapcsolók szabad be-

menetét is meg kell határozni a dokumentációban. Az új technikai eszközök, mint például egy Power over Ethernet interface költsége utólagosan nem valószínű, hogy a megrendelői oldal felé pénzügyileg érvényesíthető lesz. Ha viszont kimarad, akkor az általunk elkészített rendszer üzemképtelen lesz. LAN rendszerek tervezésénél alapvető szabály a hálózati végpontok távolsága. Réz alapú összeköttetés esetén maximálisan 100 m lehet. Amennyiben nagyobb távolságban kell biztosítanunk az átvitelt, két lehetőségünk van. Első lépésként további repeatere-ket kapcsolhatunk a rendszerünkhöz, maximálisan négyet. Ha ez a távolság kevés, akkor az optikai kábellel és médiakonverterrel megvalósított hálózatot kell előtérbe helyezni. Előnye, hogy csak egy átjáró pontunk van, és stabil sebességet lehet elérni. Itt a távolság az optikai kábel típusától /multimódusú vagy monomódusú/ függően 100 métertől több kilométer is lehet. IP alapú átviteleknél a tápellátás tervezése is fontos feladat. Az aktív eszközök működéséhez szükséges feszültségeket a teljes készenléti időre kell méretezni. Fontos, hogy az átviteli kapukat biztosító eszközök olyan megtáplálást kapjanak, amelyek az épület hétköznapi áramtalanításakor is feszültség alatt maradnak. A rendszereink teljesítményfelvétele alapján meghatározott értékbiztonságot adjon eszközeink folyamatos üzemszerű működtetésére. Például egy 16 PoE porttal rendelkező switch teljesítményigénye közel 200 W. Ebből kiindulva kell meghatározni a szünetmentes tápforrás kapacitását, vagy a rendszerparamétereknél a készenléti időt.

Napjainkban az IP technológiát használó biztonságtechnikai eszközök egyre nagyobb piaci részesedésre tesznek szert. Egy olyan műszaki váltásnak lehetünk részesei, amelynél az eszközök eddigi megszokott, önálló élete összekapcsolódhat egy egységként, egy informatikai hálózatként. Azonban e rendszerek néhány fontos kérdést vetnek fel:

Az IP eszközök telepítése a piaci szegmens melyik részéhez fog tartozni: a biztonságtechnikai szakmához, ahol ismerik az eszközökkel kapcsolatos tervezési, telepítési alapelveket, szakmai elvárásokat, vagy az informatika szakmához, ahol az IP címek, MAC címek és egyéb beállítások világában jártas szakemberek dolgoznak? Úgy gondolom, hogy napjaink biztonságtechnikai szakembereinek mélyreható módon meg kell ismerniük e technikai alapokat, és ezeket szakmai tudásuk lényeges elemeként kell kezelniük.

Köszönettel tartozom Papp Péter biztonságtechnikai mérnök Úrnak a cikk megírásához nyújtott temérdek szakmai tapasztalatáért, melyet megosztott velem.

Papp József

Budapesti Műszaki Főiskola,
Kandó Kálmán Villamosmérnöki Kar,
Műszertechnikai és Automatizálási Intézet