ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Biztonságtechnika

Dr. Berek Lajos

Nemzeti Közszolgálati Egyetem

Budapest, 2014

Tartalomjegyzék

Bevezetés

A biztonságtechnika valójában egyidős az emberiséggel. Az ember védelme érdekében eszközöket készített és alkalmazott. A biztonságtechnika, mint kifejezés nem oly régi. A múlt század elején kiadott Révai Nagy Lexikona, de még az 1960-ban kiadott Új Magyar Lexikon sem tesz említést a biztonságtechnikáról. A Britannica Hungarica és a Magyar Nagylexikon1995. évi kiadásai már tartalmaznak biztonságtechnika szócikket. Mindkét lexikon a biztonságtechnikán még csak a baleset, egészségkárosodás, anyagi kár, üzemzavar, katasztrófa megelőzését illetve kiterjedésének, hatásának korlátozását szolgáló ismeretek, eszközök és rendszabályok összességét érti A Britannica Hungarica a következőképen definiálja a biztonságtechnikát: „biztonságtechnika a halálos, vagy sérüléses balesetek okainak és megelőzésének tanulmányozása és gyakorlata.”

A vagyonvédelmet és az információvédelmet még meg sem említik. Azóta nem telt el még 20 év sem és napjainkra a biztonságtechnika tartalma jelentősen kiszélesedett. Megnövekedett a vagyon és az információ védelmének a jelentősége. Óriási lökést adott általában a biztonságtechnikának az elektronikai és az informatikai lehetőségek jelentős növekedése.

A biztonság érdekében védelmi erőforrásokat alkalmazunk. Ezek a védelmi erőforrások lehetnek technikai jellegűek és lehet élőerősek. A technikaiak lehetnek mechanikaiak, elektronikaiak és a személyek által alkalmazott eszközök. Az élőerő természetesen nem technika, azonban a védelem komplexitása megköveteli, hogy a védelmi technikát szoros egységben tárgyaljuk az azt alkalmazó és felügyelő élőerővel. A biztonságtechnika körébe tartoznak mindazon mechanikai, gépészeti, elektronikai és elektro-mechanikai eszközök, műszaki-technikai megoldások, technológiák rendszabályok, valamint az ezeket felügyelő élőerő, amelyek célja az eredményes személy- és vagyonbiztonság.

A biztonságtechnikát lehet szűken és tágan értelmezni. A szűk értelmezés szerint csupán a vagyonvédelmet és a testőri tevékenységet biztosító technikát, technológiát és eljárásokat foglalja magába. Tágabb értelmezésben minden, ami a személy- és vagyonbiztonsághoz, a munkavédelemhez, a tűzvédelemhez, az információvédelemhez, a gépjármű-biztonsághoz, a repülésbiztonsághoz, a katasztrófabiztonsághoz stb. tartozik. Mindezek alapján a biztonságtechnikának igen erős kötődése van egy sor, elsősorban műszaki tudományhoz, mint az építőmérnöki, a gépészmérnöki, a villamosmérnöki, a vegyészmérnöki,

a műszaki informatikai, a katonai műszaki tudományokhoz. De szoros a kapcsolat rendészettudománnyal, az állam- és jogtudományokkal és más társadalomtudományokkal.

1. Biztonság, őrzés és védelem, az őrzés és védelem komplexitása, az integrált vagyonvédelem

Mintegy a téma bevezetéseként tisztáznunk kell a fejezet címében közölt kategóriákat. A szakirodalom nem mindig határozza meg ezeket egyértelműen. A tudomány egyik nagyon fontos alapelve, hogy a tudomány tárgyával kapcsolatos fogalmakkal rendelkezzen, azok, valamint a téma kutatásához, oktatásához és közléséhez szükséges szakmai nyelv és terminológia legyen logikus, tiszta és egyértelmű.

1.1 A biztonság értelmezése, a személy- és vagyonvédelem dinamikus fogalma

A biztonság a biztonságtudomány meghatározó, alapvető kategóriája. A biztonságot nap, mint nap használjuk például: biztonságpolitika, létbiztonság, közbiztonság stb. A biztonság csak valamilyen veszélyeztető tényezővel összhangban értelmezhető. Egy ország biztonsága a szomszédokkal való viszony által meghatározott. Egy család biztonsága, az apa, vagy az anya munkájától, illetve havi jövedelmétől függ. A biztonság tehát valakinek, vagy valaminek a veszélymentes állapota. Természetesen veszélymentes állapot nem létezik. Vagy úgy is megfogalmazhatjuk, hogy a biztonság valamilyen lét, vagy tevékenység és az azt veszélyeztető tényezők együtthatása.

A biztonság tehát csak valami veszélyeztető tényezővel együtt értelmezhető. A biztonság és a veszély olyan kategória páros, mint a világosság és a sötétség, a hideg és a meleg. Van valaki, vagy valami. A valakinek van léte, egészsége, a valaminek van rendeltetésszerű működése, ha ezeket semmi sem veszélyezteti semmi, akkor értelmezhetetlen a biztonság. Abban a pillanatban, ha megjelenik egy aprócska veszélyeztető tényező már értelmét nyeri a biztonság kifejezés. Minél nagyobb mérvű, vagy több a létet, vagy a rendeltetésszerű működést veszélyeztető tényező annál kisebb, annál alacsonyabb szintű a biztonság.

A biztonság nagyon leegyszerűsítve egy veszélymentes állapot. Ez a pár szó a lényeg, de nekünk egy kissé konkrétabban kell a biztonságot megfogalmazni. Van valaki, vagy valami. Ezeknek van egy rendeltetésszerű állapota. Ezt az állapotot pedig veszélyezteti valami. Tehát a biztonság valakinek a léte, vagy valaminek a működése és az azt veszélyeztető tényezők együtthatása. Ez egy nagyon általános és statikusságot és passzivitást

feltételező fogalom. A biztonságtudomány szempontjából a személy léte és a szervezetek rendeltetésszerű működése a veszélyeztetett, és ami veszélyezteti az a szándékos jogellenes magatartás, cselekmény. Így a biztonságtudomány szempontjából a biztonság valakinek a léte, vagy valaminek a rendeltetésszerű működése és az azt veszélyeztető szándékos jogellenes magatartások együtthatása

A személy- és vagyonvédelem szempontjából még mindig nem teljes a definíció. Ugyanis nem passzívan, ölbe tett kézzel, sorsunkba beletörődve várjuk a betörést, rablást, lopást és más szándékos jogellenes cselekményt, hanem teszünk a megelőzése, megakadályozása, elhárítása érdekében. Védelmi erőforrásokat alkalmazunk. Kerítést építünk, biztonsági zárat szerelünk fel, riasztó berendezést telepítünk, testőrt, biztonsági őrt alkalmazunk stb. Tehát a személy- és vagyonvédelem egy változó dinamikus állapot, melyet közvetlenül két tényező befolyásol. Az egyik a veszélyeztetés, a másik pedig az alkalmazott védelmi erőforrások. A két tényező egymással szemben hat, a veszélyeztetés növekedése csökkenti, az alkalmazott védelmi erőforrások szinten tartják, vagy növelik a biztonságot.

Tehát személy- és vagyonvédelmi szempontból a biztonság valakinek a létét, vagy valaminek a rendeltetésszerű működését veszélyeztető szándékos jogellenes magatartás és az azokkal szemben alkalmazott védelmi erőforrások együtthatása. Nagyon lényeges kiemelnünk a szándékosság meglétének fontosságát, valamint azt hogy jelen esetben jogellenes cselekményről beszélünk. Ebben a szűkebb értelmezésben kizárjuk az emberi figyelmetlenséget, gondatlanságot, a katasztrófákat stb., mint veszélyeztető tényezőket. Természetesen a vagyonvédelem tágabb értelmezése esetén ezeket is figyelembe kell vennünk, mint veszélyforrásokat.

A biztonságot, ahogy már jeleztük közvetlenül befolyásolja veszélyeztetés és az alkalmazott védelem. Ezeken kívül egy sor tényező befolyásolja a biztonságot. Ezek közül talán a legmeghatározóbbak a jogi környezet, a biztonsági menedzsment működése, a gazdasági tényezők, a biztosítási intézményrendszer működése, a közbiztonság állapota, a munkanélküliség és a korrupció mértéke stb.

1.2 Őrzés és védelem

Az őrzés-védelem, vagy őrzés és védelem helye és szerepe, kapcsolata meghatározó problémája a személy- és vagyonvédelemnek. Ezért tisztáznunk kell az őrzés-védelemmel, illetve az őrzéssel és védelemmel kapcsolatos néhány kérdést. Az egyik meghatározó probléma az őrzés és a védelem közötti viszony, kapcsolat. Az őrzés és a védelem egymást

követő, egymást feltételező, vagy netán egymástól független egymás mellett létező két kategória? Az őrzés egy előre jelzett, nagy valószínűséggel bekövetkezhető számunkra nem kedvező, illetve szükséges tevékenység megelőzését, megakadályozását célzó ellentevékenység. Megelőző ellentevékenység? Bármennyire is furcsának, szokatlannak tűnik ez így van. Ugyanis az őrzés megtervezésekor és megszervezésekor a biztonsági főnök a szándékos jogellenes magatartást várhatóan elkövetni szándékozók fejével gondolkodva, a lehetőségeiket alaposan áttanulmányozza. Valóságban a jogellenes magatartásról szinte semmit sem tudunk. Nem tudjuk mikor, hol, milyen konkrét céllal, szándékkal, kik, hányan, milyen körülmények között stb. fogják a nem kívánt tevékenységet elkövetni.

Az őrzés tehát alapvetően egy feladattal, paranccsal, intézkedéssel szigorúan leszabályozott biztosítás, amely eleve feltételezi azt, hogy valaki, vagy valakik az őrzött dolog vagy személy ellen véteni akarnak. Ugyanakkor az őrzésnek demonstráló, visszatartó szerepe is van, megmutatja a vétkezni szándékozónak, hogy vigyázz, mert itt vagyok, figyelek, és ha kell, megakadályozom azt, amit tenni akarsz.

A védelem egy bekövetkező, vagy folyamatban lévő szándékos jogellenes magatartással szembeni ellentevékenység. Tehát az az esemény, amelyre az őrzéskor feltételezve készültünk az most valósággá vált. Ez az ellentevékenység alapjaiban más, mint az őrzés, hiszen itt minden konkréttá vált. Tudjuk hányan, hol, milyen módszerrel, mit akarnak elkövetni. Ezáltal az ellentevékenység kellő mértékű és hatékonyságú lehet.

A védelem pedig az őrzést esetlegesen követő olyan tevékenység, mely során ezt a jogellenes tevékenységet hárítják el, illetve csökkentik annak következményét a minimálisra.

Az őrzés tehát egy hipotetikus, feltételezett tevékenységhez kötődő biztosítási, a védelem pedig az elkezdődött, illetve bekövetkezett eseménnyel kapcsolatos elhárítási feladat. Az őrzésnél az esemény időpontja, az elkövetők száma, ereje, szándéka, célja stb. csupán feltételezés, a védelemnél pedig konkrét adatokkal jellemzett.

Az őrzést az éppen szolgálatban lévő személy, a telepített és aktivizált technikai eszközökkel, valamint őrkutyákkal látja el. Ezzel szemben a védelemhez az összes rendelkezésre álló és bevonható erőt és eszközt mozgósítják (pihenőben és készültségben lévő őrszemélyzetet, újabb technikai eszközt, rendőrséget stb.)

Összefoglalva az őrzés és védelem nem egymásnak a szinonimája, nem egymást helyettesítő kategória, de egymással szoros kapcsolatban lévő tevékenység. Ezért helyesebb, ha nem az őrzés-védelem, hanem őrzés és védelem írásmódot használjuk.

1.3 A komplex vagyonvédelem fogalma, felépítése, összetevői, kapcsolatuk

Az őrzés és védelem komplexitása egyik meghatározó problémája a vagyonvédelemnek. Mit jelent az a komplex védelem? Ha egyszerűen és röviden akarjuk megfogalmazni a választ, akkor a komplex vagyonvédelem az őrzésre és védelemre rendelkezésre álló erők és eszközök összehangolása. Ez a vállalkozás keretében végzett vagyonvédelem őskorában legtöbb esetben valóban így is volt. Napjainkra azonban jelentősen megváltozott a helyzet. Az esetek döntő többségében nem a meglévő erőket és eszközöket hangoljuk össze, hanem a kockázatelemzés és a kockázatértékelés elvégzését követően határozzuk meg, hogy a kívánt védelmi szint eléréséhez milyen mechanikai védelmi eszközöket, elektronikai jelző berendezéseket kell alkalmazni és ezek felügyeletére milyen élőerőt kell alkalmazni.

A három védelmi forma egymásra épülése, egymás kiegészítése adja a komplexitást. A jogellenes cselekményt elkövetni szándékozó rendszerint először valamilyen fizikai akadályt képező mechanikai eszközzel találja magát szemben. Egy kaput, kerítést, rácsot, ajtót, ablakot, zárat stb. kell roncsolni, és ez által kerülhet cselekményének célja közelébe. Ezeket a mechanikai védelmi eszközök védelmére, megfigyelésére különböző elektromos érzékelő berendezéseket alkalmazunk, melyek pedig valamilyen módon adják a jelzést hang, fény és/vagy kép formájában az élőerős védelemnek. Mindezek alapján a biztonsági őr meg tudja tervezni az ellenlépést, dönthet újabb erők és eszközök aktiválásáról, gyakorlatilag reagál és elhárítja a támadást.

A komplex vagyonvédelemmel szemben jogosan elvárható igény, hogy az legyen hatékony. Jelen esetben mit is jelent ez a hatékonyság? Egyfelől azt, hogy vagyonvédelem tárgyának értékével, annak veszélyeztetettségével legyen összhangban a védelmi ráfordítás. Egy egyszerű példával szemléltetve. Ha egy bekerített területen lévő raktárban 40 kg-os zsákokban útszóró sót tárolunk, melyhez kialakítunk egy komplex vagyonvédelmet, akkor ez a védelem lehet hatékony, de ha ugyanott szórakoztató elektronikai eszközöket tárolnánk, az adott védelem már nem lenne hatékony. A kétféle vagyontárgynak nagyságrenddel különbözik a veszélyeztetettsége. Kijelenthetjük, hogy a védelemmel szemben megfogalmazott követelmény kettős, egyfelől elvárás, hogy a védelem csökkentse a vagyon elleni szándékos jogellenes cselekmény elkövetésének valószínűségét a minimálisra, másfelől a cselekmény bekövetkezte esetén az elkövető kockázatát pedig növelje a maximálisra. Természetesen mind a nem kívánt vagyon elleni cselekmény bekövetkeztének valószínűségére soha sem mondhatjuk, hogy az 100 %-os, ugyanúgy az elkövető kockázatára

sem. Mindez az optimális komplex vagyonvédelem kialakításával valósítható meg. Ha pedig a különböző vagyonvédelmi eszközök alkalmazásának aránya optimális, akkor a vagyonvédelem hatékony.

Komplex a vagyonvédelem tehát, ha a vagyonvédelmi feladathoz a mechanikai védelmi és az elektronikai jelző eszközök, valamint az élőerős állomány alkalmazása megfelelően arányos. A vagyonvédelem komplexitásához hozzá tartoznak a meghatározott védelmi rendszabályok és az egész rendszer működtetéséhez szükséges info-kommunikációs hálózat.

1.4 Az integrált vagyonvédelem

Többféle hardver és szoftver egymásra épüléséből kialakított rendszer az integrált felügyeleti rendszer. Feladatai a jelzésadó központok jelzéseinek vétele, értelmezése, mentése, nyomtatása, és nyugtázása. Az első ilyen rendszerek a hatvanas évek kezdtek működni az Egyesült Államokban. Ezek nagyon kezdetleges próbálkozások voltak. Meghatározó volt azonban, hogy a biztonsági szakma rájött arra, hogy az erőket és eszközöket a vagyonvédelem érdekében integrálni kell. Ahhoz, hogy ez a valóságban is létrejöhessen még vagy harminc évet kellett várni. Ugyanis ehhez az integrációhoz az asztali számítógépek megjelenésére, elterjedésére és fejlődésére volt szükség. Gyakorlatilag az ezredforduló körül érték el ezek a számítógépek azt a gyorsaságot és memória kapacitást, melyek a hozzájuk készített programok segítségével képessé váltak ezen integráló feladat elvégzéséhez. Az informatikai lehetőségek bővülése beláthatatlan lehetőséget biztosítanak nemcsak a nagy vállalkozások, hanem a háztartásoknak és a kisvállalkozásoknak is hogy vagyonvédelmüket integrálhassák.

Ahogy már jeleztem az integrált vagyonvédelemnek két alapvető feltétele van a hardver és a megfelelő szoftver. Technikai megvalósítás szempontjából két lehetőség van a számítógépbe helyezhető kártyás megoldás, vagy kifejezetten csak erre a célra önálló házba épített felügyeleti központok.

A PC kártya jellegű felügyeleti központok esetében egy szabvány PCI slot-ba illeszkedik a PC-s kártya, amelyen integrálva megtalálható minden szükséges be- és kimeneti csatlakozó. Általában 1-2 telefonvonal csatlakoztatható a kártyához. A tápellátást a személyi számítógép tápegysége biztosítja. Előnye, hogy jelentősen olcsóbb az előállítása a külső felügyeleti egységekénél. Hátránya, hogy csak addig működik ameddig a PC és az azon futó szoftver.

Az önállóan is működőképes felügyeleti központ igen sokféle létezik. Rendelkezik saját tápegységgel, telefon, vagy más adatátviteli csatlakozási lehetőségekkel, akkumulátorral, órával, memóriával, esetleg LCD képernyővel, nyomtatóval, vagy nyomtató porttal és számítógép csatlakozási lehetőséggel. Hátránya az igen magas ár, előnye a nagyobb megbízhatóság és a bővíthetőség.

Szoftver tekintetében már nehezebb a helyzet. Minden hardverhez készül egy szoftver, de hozzá lehet jutni több általános szoftverhez. Általában nagyobb felügyeleti központok az általuk használt szoftverhez szerzik be az olyan hardvert, amelyen képes futni az adott program.

2. A mechanikai védelem

A mechanikai védelem a technikai védelem része az egyik legrégebben alkalmazott területe a vagyonvédelemnek. Primer védelem, ugyanis a szándékos jogellenes cselekmény elkövetésekor először ezt kell leküzdeni. A mechanikai védelem a komplex személy- és vagyonbiztonság egyik meghatározó eleme, mindazon építészeti és gépészeti eljárások, eszközök és technológiák összessége, amelyek a személy vagy a vagyon létét, vagy a rendeltetésszerű működését veszélyeztető szándékos jogellenes cselekményt késlelteti, akadályozza, esetleg megakadályozza.

A mechanikai védelem fő területei:

- A kültéri védelem (kapuk, kerítések, sáncok, árkok, akasztók stb.);
- Építményvédelem (falazat, födém, padozat, tetőzet, ajtók, ablakok, rácsok, redőnyök, fóliák stb.);
- Mechanikai tárgyvédelem (lemez- és páncélszekrények, széfek, trezorok, zárható bútorok és ládák stb.). Mindhárom terület meghatározó elemei a különböző zárak, lakatok és reteszek.

A mechanikai védelem alkalmazásának elsődleges célja, hogy hatékony fizikai ellenállást tanúsítson az objektumokba való illetéktelen bejutási kísérletekkel szemben, ezért gyakran a mechanikai védelmet mechanikai-fizikai védelemnek is nevezik.

2.1 A kültéri mechanikai védelem

A mechanikai védelem már az objektum előterében, az előterében megkezdődik. A kültéri vagyonvédelmi megoldások és eszközök késleltetik, illetve akadályozzák az illetéktelen behatolót az őrzött területre, valamint objektumba való bejutásban. Ezek közül a leglényegesebbek az árkok, töltések, kerítések, kapuk, sorompók, tüskés drótok és lemezek, forgókeresztek. A kerítésekkel kapcsolatos követelmény, hogy beton alappal rendelkezzen és a magassága 1,8-2,8 m legyen, szerkezetének anyaga lehet beton vagy beton elem, tégla, kő, vas, tüskésdrót, tüskéslemez, vas- vagy drótháló. A meglévő kerítés magasságának és megbízhatóságának növelésére hatékonyan alkalmazható a sorokban kifeszített, vagy a tekercs spirál alakban széthúzott és rögzített tüskés drót, vagy tüskés lemez. A kapuszélességét a gépjárműforgalom jellege, az út szélessége határozza meg, legalább 2,5 m szélesre és 2,8 m magasra kell készíteni.

A sorompók a járművek folyamatos mozgását akadályozzák, illetve teszik szakaszossá. Anyaga, mozgatása sokféle lehet, könnyű szimbolikus, vagy erős megállító, kézi vagy elektro-mechanikus mozgatású. Igen gyakran a járművek megállítása a feladata ellenőrzés céljából. Telepítése történhet ellenőrző ponton, vagy a gépkocsi bejáratnál.

Töltések és az árkok egymással kombinálhatóak. Az árokból kitermelt anyagból töltés készíthető. Árkot és töltést általában bekerítetlen veszélyeztetett objektumnál alkalmazunk, de előfordul külterületen lévő bekerített szomszéddal nem rendelkező objektumnál is. Méreteikre nincs előírás, sőt még ajánlás sem, azt a veszélyeztetés határozza meg. Rendeltetése hogy megakadályozza az adott irányból a betekintést illetve a járművek behajtását.

2.2 Az építmény mechanikai védelme

Az építményvédelmet esetenként héjvédelemnek is nevezik. Főleg városokban, ott is elsősorban a központi részeken, a belvárosban találhatóak olyan épületek, amelyeknek nincs előkertjük, nincs kerítésük. A falazat közvetlenül az úttest mellett kezdődik.

Az építményekbe a behatolás elsősorban az ajtók és az ablakok roncsolásával történik (feszítés, törés stb.) A falakon, födémeken keresztül, építésük módjától függően falbontással, vagy robbantással történhet az átjutás. Mindkét esetben, de főleg a robbantáskor jelentős, távolabbról is jól érzékelhető zajjal jár. A falak anyagát és építési módját figyelembe kell venni a vagyonvédelem tervezésekor. Nem mindegy hogy egy beton, tégla, fa, vályog vagy könnyű szerkezetes építmény védelmét kell biztosítani. Általában biztonságosnak tekinthető egy 38 cm vastag H-50-es minőségű habarccsal készített, vagy azzal egyenszilárdságú fal.

Az ablakok és ajtók ráccsal történő megerősítése nagyban növeli azok betörésállóságát. Alkalmazásuk nem túl népszerű. Belülről bezártság érzetét keltik, kívülről pedig ridegek. Természetesen sok olyan példa található, amikor az építmény jellegéhez igazodó művészi tervezésű és kivitelezésű rácsot alkalmaznak.

A rácsok anyagával, méretével és szerelésével kapcsolatosan a Magyar Biztosítók Szövetsége (MABISZ) ajánlásokat fogalmaz meg. A MABISZ szabályzata a mechanikai védelem tekintetében három fokozatot különböztet meg, teljes körű, részleges és minimális mechanikai védelmet.

A MABISZ szerint három méternél alacsonyabban lévő ajtókat és az ablakokat ajánlatos acélráccsal ellátni. Amely az előírás szerint akkor tekinthető biztonságosnak, ha anyaga legalább 12 mm átmérőjű köracél, vagy ennek megfelelő szilárdságú más profilú acél,

pénzintézeteknél ez a méret 16 mm. A rácsszerkezeti nyílások nem lehetnek 100x300 mm-nél nagyobbak. A rácsokat 300 mm-enként a rács rudak keresztmetszeti tényezőjének megfelelő falazó körmökkel kell a falba legalább 150 mm mélyen rögzíteni. A rácsok anyagával kapcsolatban csupán annyit közöl az ajánlás, hogy acélból készüljön, de hogy szénacélból, vagy valamilyen más ötvözetből arra nincs még utalás sem. A rácsot oldalanként legalább négy helyen kell rögzíteni. A rácsot az ablak tokjához is lehet rögzíteni, de úgy hogy az kívülről ne legyen megbontható. Az ablakoknál bizonyos védelmet nyújtanak a redőnyök, valamint az ablaküvegre ragasztott törés gátló műanyag fóliák.

A külső ajtók szerkezetével és építésével kapcsolatos alapkövetelmény, hogy rendelkezzen legalább olyan szilárdsággal, mint a környező fal. Biztonságos az ajtó, ha anyaga 40 mm vastag tömör fa, biztonsági zárral van ellátva, az ajtótok pedig minden oldalon legalább három helyen falazó körömmel rögzítenek a falazathoz. Az ajtó biztonságát növeli, ha keményfából vagy fémből készül, illetve ha vaslemezzel, vasráccsal, vagy több ponton rögzítő zárral, például heveder zárral van ellátva. A lakat nem minősül biztonsági zárnak! Követelmény, hogy a zár nyelve legalább 20 mm-re hatoljon be a tokba.

Az épületek leggyakoribb behatolási pontjai az ajtók és az ablakok, melyek részben, vagy egészben üvegezettek. Ezen üvegfelületek védelmére sikeresen alkalmazhatóak a biztonsági fóliák. Melyek olyan többrétegű, laminált, műanyag alapú védőelemek, amelyeket az üvegfelületre utólag felerősítve (kasírozva, ragasztva, applikálva stb.) megakadályozzák annak támadás esetén történő azonnali összeesését. Az üvegfelületet egyben tartva, késleltetik a behatoláshoz szükséges nyílás kivágását, és a támadó számára a szilánkképződéssel nagymértékű balesetveszélyt okoznak. A biztonsági fóliák csökkentik az ultraviola sugárzást, színező réteggel is bevonható.

A biztonsági fóliák kombinálhatók fémszálakkal is. Ezek a riasztórendszerbe bekötve támadás esetén riasztó jelzést generálnak.

2.3 Mechanikai tárgyvédelem

Az épületen belül szükség lehet beépített, mozdítható esetleg hordozható olyan mechanikai tárgyvédelmi eszközre, melyekbe a különösen értékes tárgyakat, elsősorban pénzt, nemesfémeket, részvényeket, kötvényeket stb. lehet elzárni. Így abban az estben, ha betörő bejut az épületbe nem jut közvetlenül a legértékesebb tárgyakhoz. A tárgyvédelemhez létesíthető trezor, alkalmazható páncél-, vagy lemezszekrény, falba, vagy bútorba épített értékkazetta, vagy speciális értékszállító táska.

Ezekkel az eszközökkel szemben követelmény a táska kivételével a rögzítettség, furás- és vágásállóság, valamint a speciális biztonsági zár. Természetesen ezen eszközökkel kapcsolatos az az alapgondolat, hogy nincs olyan zár, amelyet nem lehet kinyitni, vagy amit nem lehetne feltörni. Minden csupán idő kérdése. És ez a lényeg, hogy minél több időt kell a betörőnek a feltörésre fordítani, annál nagyobb lehet az esélye az élőerős szolgálatnak a sikeres védelemre.

3. Az elektronikus vagyonvédelem területei

A szakmai terminológia elektronikai, elektronikus védelem, vagyonvédelem kifejezést alkalmazza. Valójában itt nem védelemről beszélhetünk, hanem jelzésről. A vagyonvédelmet az elektronikai jelzőrendszer teszi komplexszé. A mechanikai védelmi rendszer feltartóztatja, akadályozza a jogellenes cselekményt. Ezzel összehangolva a elektronikai vagyonvédelem érzékel és jelez az élőerős védelemnek. Ahhoz, hogy ez a komplex vagyonvédelem hatékonyan működjön, úgy kell a védelem alkotóelemeit összehangolni, hogy a mechanikai eszközök legalább addig akadályozzák meg a behatolást, ameddig az elektronikai jelzőrendszer riasztására az élőerő kivonul a veszélyeztetés területére és megfelelően reagál, mely eredménye a vagyon elleni támadás elhárítása.

Az elektronikai eszközök fejlődése jelentősen segítette és támogatja a komplex vagyonvédelem megvalósítását. Az elektronikai jelzőrendszerek, és így a vagyonvédelem tekintetében is az informatika térnyerése szinte korlátlan lehetőségeket biztosít már napjainkban is, a jövőt pedig szinte elképzelni sem lehet.

Az elektronikus vagyonvédelem főbb területei:

- Elektronikus kültéri védelem.
- Behatolás-jelző rendszerek.
- Beléptető rendszerek.
- Távfelügyeleti rendszerek.
- CCTV rendszerek.
- Elektronikus áruvédelmi rendszerek. (Az elektronikus vagyonvédelem e lényeges területével itt csak a megemlítés szintjén foglalkozunk.)

3.1 Elektronikus kültéri védelem és a behatolás-jelző rendszerek felépítése

Az elektronikus kültéri védelem és a behatolás-jelző rendszerek talán a leginkább egymáshoz kapcsolódó területe az elektronikai jelző-rendszernek, ezért egy fejezetben tárgyaljuk.

A kültéri védelmi és a behatolás-jelző rendszerek feladata a biztosított területre történő jogtalan behatolás érzékelése és jelzése. A behatolás-jelző rendszer felépítése: érzékelők,

központ, kezelő, jelző és kiegészítő eszközök. A behatolás-jelző elemei vagy vezetékkel hálózatba, vagy vezeték nélküli kapcsolatban vannak.

Korszerű, vezeték nélküli rendszer esetén az érzékelő, mint rádióadó, a központ vevőként üzemel, és nincs összekötő vezeték. A riasztást végző egység lehet riasztócsengő, sziréna és tér megvilágító lámpa. A nagy fényerejű lámpák hirtelen bekapcsolása, villogása hasonló hatást vált ki, mint a sziréna bekapcsolása. Magánházaknál egyre több helyen alkalmaznak automatikusan segélyhívást tárcsázó, telefonos behatolás-jelző rendszert vagy rádiókapcsolatot létesítő riasztást.

A behatolás-jelző rendszer agya a behatolás-jelző központ. A riasztóközpont tartalmazza a zónabemeneteket, vezérlőkimeneteket, telefonkommunikátort és egy akkumulátoros tápegységet. Ehhez kapcsolódik a kezelőegység, a különböző érzékelők, a hang- és fényjelző egységek, valamint az adatátviteli eszközök. A behatolás-jelző rendszerek a legmodernebb technikával készülnek, hogy korszerű, biztonságos védelmet nyújtsanak felhasználóinak. A rendszert gyakran kiegészítik videó megfigyelő rendszerek, melyek kombinált alkalmazása nyújtja a legoptimálisabb védelmet az esetleges behatolók ellen. A kezelőegység segítségével lehet a behatolás-jelző rendszert élesíteni és hatástalanítani, el tudjuk végezni, a rendszer programozását is.

A behatolás érzékelését a védendő objektum szélén el kell kezdeni és a behatoló tevékenységét folyamatosan figyelemmel kell kísérni. Ennek érdekében védelmi köröket kell létrehozni.

- A védendő épületen kívül található a *kültéri védelem*. A kültéri védelemben alkalmazhatóak kerületvédelmi fix telepítésű eszközök, valamint kerítésvédelmi eszközök. A leggyakoribb kerületvédelmi fix telepítésű eszközök: a hidraulikus lépésjelzők, a mágneses térérzékelők, infra sugaras eszközök, mikrohullámú eszközök, valamint kültéri passzív infra érzékelők. A kerítésvédelem eszközei: az érzékelő kábeles rendszerek, az optikai szálas rendszerek és a vibrációs érzékelők.

- A védett épület külső felületén, annak falazatán, padozatán, mennyezetén, ajtóin, ablakain helyezkednek el a *felületvédelem,* vagy a *héjvédelem* érzékelői. A felületvédelem alapvető eszközei: a nyitásérzékelők, az üvegtörés-érzékelők, a falbontás-érzékelők és az infrasorompók.

- Az épületen belül helyezkednek el a *térvédelem* eszközei, melyek a mikrohullámú passzívinfra mozgásérzékelők.

- Az értékes tárgyakat *tárgyvédelem*mel biztosítjuk. Eszközei a közelítésérzékelők, a rezgésérzékelők, a fémhang-érzékelők, a feszítés érzékelők és az elmozdítás érzékelők.

3.1.1 A kültéri védelem érzékelői

A kültéri érzékelőknek két nagy csoportja van, a kerületvédelmi, fix telepítésű és a kerületvédelmi eszközök.

Kerületvédelmi, fix telepítésű eszközök a hidraulikus lépésjelzők, a mágneses térérzékelők, az infrasugaras eszközök, a mikrohullámú és a kültéri passzív érzékelők.

A *hidraulikus lépésjelzőt* a föld felszíne alá telepítik, mely egy fagyálló folyadékkal töltött műanyag tömlő, melyben egy érzékelő egységet helyeznek el. A lényege, hogy a tömlőre lépve a folyadék nyomása megemelkedik, mely következtében az érzékelő elektromos jelet bocsájt ki.

A *mágneses térérzékelőket* szintén a földfelszín alá telepítik. Az érzékelő felett áthaladó személy, illetve tárgy megváltoztatja az elektromágneses teret, mely jelzést ad a központ felé.

Az *infrasugaras érzékelő* két szembenálló egységből áll az adóból és egy érzékelőből. Az adó impulzusmodulált infravörös sugarat bocsájt ki, mely a vevőegységbe jut. Ha ezt a sugárnyalábot megszakítják a vevő egység jelez a központ felé.

A *mikrohullámú behatolás jelző* szintén adó és vevő egységből áll. Az adó irányított mikrohullámú jelet bocsájt ki, melyet az antenna érzékel, továbbít és egy állandó jelzést ad. Ezt a sugarat a behatoló megszakítja a testével, melyet a vevőegység érzékel és riaszt.

A *kültéri passzív érzékelők* az emberi test hőmérsékletét érzékeli, mely eltér a környezeti hőmérséklettől és ez az eltérés ad jelzést a központ felé.

A legismertebb *kerítésvédelmi eszközök* az érzékelő kábeles, az optikai szálas és a vibrációs berendezések.

Az *érzékelő kábeles berendezés* érzékelő eleme egy speciális árnyékolt maximálisan 300 méteres kábel, mely érzékeli a kerítésen a behatolást és jelt ad.

Az *optikai szálas berendezés* a fény hullámterjedésén alapuló érzékelő. A kerítésen optikai szálat vezetnek végig, melyben fényt vezetnek állandó intenzitással. Amennyiben behatolási kísérlet történik, akkor a fény intenzitása megváltozik. Ez érzékelhető és riaszt.

A *vibrációs berendezés* elektromechanikus, vagy piezo elektromos elven működik. Ezek az érzékelők a kerítésfonat vibrációs mozgása esetén továbbítanak egy kis elektromos jelet a jelfeldolgozó egységnek, mely a központi egység felé továbbítja a riasztás jelzést.

3.1.2 Az épület felületvédelmi érzékelői

Az épület ablakain, ajtóin, falazatán, födémén és padlózatán helyezkednek el a felületvédelem érzékelői. Leggyakoribb érzékelők a nyitás-, az üvegtörés-, a falbontás-érzékelők, valamint az infra sorompók.

A *nyitásérzékelők* az ajtókra és az ablakokra szerelt mechanikus kapcsolók vagy reed relés érzékelők, amelyek élesítés esetén az ajtó, illetve ablak nyitása esetén riasztó jelzést ad. A mechanikus kapcsoló egy rugós és érintkezős, viszonylag könnyen meghibásodó egység. Lehet nyomó- vagy billenő kapcsolós. Nyitás esetén zárja az áramkört, mely riaszt. A reed relés érzékelő két részből áll a mágnesből és a reléből. A mágnest a nyitható elembe, vagy elemre, a relét a tokba, vagy a tokra építik. Élesítés esetén nyitás után a mágnes elmozdul a relében az érintkezők zárják az áramkört és riaszt.

Az *üvegtörés érzékelők* lehetnek az üvegre ragasztottak (higanykapcsolós, piezo elven működő), optikaiak, vagy akusztikusak. A higanykapcsolós érzékelőben a törés esetén keletkező rezgés hatására a két érzékelő között elmozduló higany csepp megszakítja az érintkezést és riaszt. A piezo kristály a törés esetén elektromos jelet bocsájt ki a riasztáshoz. Az optikai érzékelő az üvegfelületre bocsájtott és visszavert infra sugarak megváltozása esetén, az akusztikus pedig a töréshang észlelése esetén jelez.

A *falbontás érzékelő* lehet fémhálós, testhang érzékelős, vagy érzékelő kábeles. A fémhálót a falba építik annak szakadása esetén riasztójelet továbbít. A testhang érzékelők a piezo technológiát használják az érzékelésre és a riasztásra. Az érzékelő kábeles a kerítésvédelemnél alkalmazott elven működő eszköz.

Az *infra sorompó* egy adó és egy vevő egységből áll. A behatoló megszakítja a két egység között lévő infravörös sugarat és ezáltal riaszt.

3.1.3 A belső térvédelmi érzékelők

Ezek az eszközök a mozgást érzékelik. Lehetnek mikrohullámú és passzívinfra mozgásérzékelők.

A *mikrohullámú mozgásérzékelők* a Doppler elv alapján működnek. Az adóból kibocsátott 2,5; 6, vagy 10 GHz-es környezetről visszavert jelet veszi az antenna és továbbítja a vevőhöz. Ha a térben mozgás történik, akkor megváltozik a visszavert jel és riaszt.

A *passzívinfra mozgásérzékelő* az ember hőkibocsájtását érzékeli, és mivel az eltér a környezet által kibocsájtott hőmennyiségtől riaszt.

3.1.4 A tárgyvédelem eszközei

A leggyakrabban alkalmazott tárgyvédelmi eszközök a közelítésérzékelők, a rezgésérzékelők, a fémhang-érzékelők, a feszítés érzékelők és az elmozdulás érzékelők.

3.2 Beléptető rendszerek

A beléptető rendszerek az elektronikai védelem egyik meghatározó területe. Rendeltetése, hogy az adott területre csak engedéllyel rendelkező személy lépjen be és tartózkodjon. Objektumokon belül különböző részekre, területekre történő belépés is külön korlátozható.

Tehát a beléptető rendszer alapvetően szabályoz, azonban az objektum tulajdonosának, üzemeltetőjének van lehetősége a rendszer más szolgáltatásait is igénybe vennie munkaidő nyilvántartás, rendszámfelismerés stb. Alapvetően a beléptető rendszernek három fő funkciója van. A belépési jogosultság megállapítása, a belépő azonosítása és az áthaladás szabályozása.

A beléptető rendszer fő egységei: a központi egység, az olvasó terminálok és a vezérlő egységek. Az olvasó terminál fő feladata érzékelni és továbbítani a vezérlő egység felé a belépő személyazonosítási jellemzőit. A vezérlő egység ezen adatok alapján azonosítja a belépőt, megállapítja a jogosultságát, vagy annak hiányát, és ezek függvényében vezérli a bejárat mechanikai, vagy elektromechanikai elven működő szerkezetét, mely lehet ajtó, sorompó, forgóvilla, forgókereszt, vagy gyorskapu.

3.2.1 Személyazonosítási alapmódszerek

A személyazonosítást aktív és passzív módszerekre bonthatjuk attól függően, hogy szükség van-e az azonosítandó személy közreműködésére. Az azonosításra használt információ alapján a személyek azonosítására három alapvető módszer létezik. A *tudás alapú azonosítás* esetén a személy olyan információ tudatában van, amit az azonosítási eljárás során ellenőrizni lehet. Ilyen információ lehet például egy jelszó, vagy a PIN kód is. *Birtok alapú azonosítás* esetén már az azonosítás egy olyan eszközzel történik, amely a személy birtokában van, például egy kulcs, vonalkód, mágneskártya, chipkártya vagy smartcard. A harmadik

lehetőség pedig a *biometria alkalmazása*, amikor a személy valamilyen fizikai vagy biológiai jellemzőjét felhasználva történik az ellenőrzés.

Mivel mindhárom módszernek vannak kiküszöbölhetetlen hátrányai is, egymagában alkalmazva egyik sem nyújt kellő mértékű védelmet. Éppen ezért a szakirodalom ajánlása szerint célszerű a három eltérő elven alapuló módszerből legalább kettőt együttesen, de egymástól függetlenül alkalmazni a megfelelő védelem elérése érdekében. A függetlenség ebben az esetben nagyon fontos kritérium, mert ennek hiányában a két különböző módszer együttes alkalmazása nemcsak hogy nem erősíti egymást, de összességében még egy jóval gyengébb védelmet is okozhat. Ez történik például akkor, ha egy védelem alapját mágneskártya (birtok) és PIN kód (tudás) együttese képezi oly módon, hogy a PIN kódot a mágneskártyán tárolják. Ebben az esetben, ha a mágneskártya illetéktelen kézbe kerül, annak birtokában már a PIN kód sem titkos többé. Látható hogy az ilyen módon megvalósított védelem semmivel sem erősebb mintha csak a kártyás azonosítást használtuk volna, sőt a kártyát megszerezve az illetéktelen személy esetleg egy olyan kódhoz juthat hozzá, amelyet felhasználója más rendszerekben is használ.

Tudás alapú azonosítás

A tudás alapú azonosító módszerek családját olyan megoldások alkotják, melyek a felhasználókat az általuk birtokolt egyedi tudás alapján azonosítják. Ezek közül a legismertebbek a jelszó alapú azonosítás és ennek egy speciális esete a PIN (Personal Identity Number) alapján történő azonosítás. A továbbiakban jelölje a „jelszó” elnevezés ezt az egyedi tudást.

A jelszó alapú azonosítás folyamata egy egyszerű sémán alapul:

- a felhasználó egy arra alkalmas billentyűzet segítségével megadja a jelszavát (általában egy felhasználói névvel együtt),

- a megadott jelszó összehasonlításra kerül egy (esetleg) több tárolt jelszóval, és egyezőség esetén lesz pozitív eredménye az eljárásnak.

Abban az esetben, ha a felhasználó csak a jelszavát adja meg (felhasználó felismerés), azt minden tárolt jelszóval össze kell vetni, ami a keresési teret jelentős mértékben megnövelheti, ezáltal az azonosítási eljárás hatékonyságának komoly gátja lehet. De ez a probléma könnyen megoldható felhasználói nevek használatával, esetleg más azonosítási módszerek a jelszóval együttes használatával.

A jelszavak – megfelelő alkalmazás esetén – igen megbízható azonosítási megoldást jelenthetnek, bár a felhasználók többsége túl rövid, túl egyszerű vagy más okok miatt egyszerűen megfejthető jelszavakat használ (például valamilyen a személyéhez kötődő információ), ami ezt a biztonságot gyengíti. A jelszavak előnye, hogy bár kognitív terhelést jelent azok megjegyzése, mégis mindig kéznél vannak, nem kell semmilyen tárgyra sem ügyelnünk (ld. birtok alapú azonosítás). Másik előnyös tulajdonságuk, hogy szinte korlátlanok a lehetőségek a jelszavak megválasztásánál (kivételt képeznek egyes speciális esetek, például PIN). Ezáltal a jelszavak egyszerű próbálgatással történő kitalálásának valószínűsége nagyon alacsony értékre szorítható.

A tudás alapú azonosítás hátrányos tulajdonságai többnyire a helytelen jelszóválasztásból adódnak, aminek a jelszó könnyű kitalálásához vezethet. Ezen kívül az azonosítás folyamatában egy kritikus pont a jelszó megadása, amikor is illetéktelenek hozzáférhetnek jelszavunkhoz. Így elmondható a jelszavakról, hogy minden egyes használat után az általuk nyújtott biztonság mértéke csökken. Szintén hátrányt illetve biztonsági rést jelenthet az összehasonlításhoz használt jelszóminták nem megfelelő tárolása.

Jelszó megadáskor törekedni kell a következőkre:

- kis és nagybetűket, számot és lehetőleg szimbólumot is egyaránt tartalmazzon,
- ne a név, vagy születési adat, vagy annak egy része legyen a jelszó,
- lehetőleg négy vagy több karakterből álljon,
- ne tartalmazzon sorozatokat vagy ismétlődő karaktereket (123456, 22223333)
- semmiképp ne tartalmazza a jelszó a belépési nevet.

Lehetőség szerint időnként változtatni kell a jelszavakat.

Kulcs, avagy birtok alapú azonosítás

Egy másik jól ismert személyazonosítási módszer a birtok alapú azonosítás. Ebben az esetben az ellenőrzés egy olyan egyedi és mással össze nem téveszthető eszközön alapul, ami egyértelműen azonosít egy személyt azáltal, hogy annak mindig a jogosult személy birtokában kell lennie. Ilyen eszköz lehet például lyukkártyás, induktív kódolású, vonalkódos, Wiegand rendszerű, mágnes csíkos, érintés nélküli, memóriakártyás és optikai kártyás azonosító. A használata általában ennek a módszernek is egyszerű, a költségeket tekintve pedig léteznek olcsó, de egészen drága megoldások is. A módszer közismert hátránya, hogy amennyiben illetéktelen kezekbe kerül a kulcs, akkor jogosulatlan hozzáférés lehetséges. A

tudás alapú azonosítással szemben viszont ebben az esetben – már amennyiben nem másolható kulcsról van szó – az eltulajdonítás ténye érzékelhető, nem úgy, mint a jelszavak esetében. Így ez egyfajta utólagos védelmet nyújt azáltal, hogy az ellopott kulcs utólag letiltható. Éppen ezért itt az egyik legfontosabb követelmény a kulcsokkal szemben, hogy ne legyenek másolhatók. Másolhatóság szempontjából a birtok alapú azonosításhoz felhasznált kulcs eszközöket három nagy csoportra oszthatjuk.

Az elsőt a passzív eszközök jelentik, mint például a vonalkód, a csak adni tudó közelítéses kártyák vagy azok a mágneskártyák, amelyekről csak olvasnak az azonosítás során (a mágneskártya ugyanis egy írható-olvasható eszköz, de nagyon sok esetben az írási lehetőséget nem használják ki). A passzív eszközök széles körben elterjedtek főleg olcsóságuk és könnyű kezelhetőségük miatt. A második csoportot az írható-olvasható aktív eszközök jelentik, amelyek már bonyolultabb műveletek elvégzésére is képesek, és esetlegesen nehezebben is másolhatók, mint a passzív eszközök. Ide tartoznak azok a mágneskártyák, amelyeknél az azonosítás során az írhatóságot is kihasználják, valamint az úgynevezett ugrókódos rádiós kártyák, a memóriakártyák és a chip-kártyák.

Végül a harmadik csoportot azok az intelligens eszközök jelentik, amelyek már nyilvános kulcsú illetve többfaktoros kriptográfiai eljárásokat alkalmaznak az ellenőrzési folyamat során. Ide tartoznak például a smartcard-ok egyes típusai, vagy az idő alapú kétfaktoros azonosító kártyák is. Az eszközben egy titkos kulcs van tárolva, amelyet a kártya sohasem ad ki magából, csak rejtjelezéshez használja azt fel, így a felsorolt három típus közül ez jelenti a legjobb védelmet a másolhatatlanság szempontjából.

A leggyakrabban használt birtok alapú azonosítók esetében a birtoklás nem állapítható meg távolról. Vagy fizikai kontaktust igényelnek, mint például a kulcsok és a smart- és mágneskártyák, vagy csak közelről érzékelhetőek, mint a proximity kártyák.

Biometrikus azonosítás

A személyek azonosításának harmadik és egyben legmegbízhatóbb módszere a biometrikus azonosítás, amely az emberi test valamely, gépek által is könnyen kezelhető, fizikai vagy biológiai jellemzőjét használja fel az ellenőrzés során, mint például az ujjnyomat, a hang, a szem, a kéz vagy akár az arc jellegzetes vonásait. A tudás- illetve a birtok alapú azonosítással szemben itt már ténylegesen magát a személyt azonosítjuk, nem pedig valamilyen más, közvetett jellemzőt, mint a jelszó vagy a kulcs. Ezáltal az azonosítás alapját képező tulajdonság nem lopható el, megfelelő technológiai megvalósítással pedig az is

biztosítható, hogy a mintavételezés valós élő személytől származzon, jelentősen csökkentve ezzel a megtévesztés lehetőségét. Csendes riasztásra is lehetőség van, hiszen kényszerítés esetén megoldható például, hogy ujjnyomat ellenőrzésnél egy másik – riasztást kiváltó - ujjat használjon a kényszerített alany, illetve hang alapú azonosítás esetén másik jelszó használata váltsa ki a riasztást, miközben az azonosítás és a beengedés is megtörténik.

Természetesen a módszernek hátrányai is vannak. Az egyszerűbb megvalósítások viszonylag könnyen megtéveszthetők, a megbízhatóbb, komolyabb termékek viszont igen drágák. A biometrikus azonosítás ugyanis speciális hardware eszközöket igényel, amelyek ára a megbízhatóságuk növekedésével egyre magasabb. Ezen felül higiéniai szempontból is lehetnek problémák amennyiben az ellenőrzés folyamata fizikai kontaktust igényel, valamint egyes módszerek fogyatékos emberek esetében nem is alkalmazhatók. Tovább nehezíti a feladatot, hogy a biometrikus jellemzők nagy része az idő múlásával is változik, illetve különféle betegségek és sérülések is nagymértékben befolyásolhatják az azonosítás sikerességét. Bizonyos alkalmazások esetén adatvédelmi problémákkal is szembe kell nézni, mivel a biometrikus azonosítás módszere már a titkos megfigyelésre is lehetőséget teremt, hiszen technikailag a megfigyelésre sok esetben az adott személy tudta és beleegyezése nélkül is lehetőség van, ami jogi szempontból aggályos lehet.

Ugyanakkor a leolvasások eredménye az egyes azonosítási folyamatok során soha nem egyezik meg teljesen a korábbiakkal, így rendkívül fontos kérdés az adott rendszer hibatűrésének mértéke annak érdekében, hogy minél jobb eséllyel tudjon a rendszer egy személyt különböző körülmények között, más-más időpontokban is azonosítani úgy, hogy emellett a téves elfogadások illetve a téves visszautasítások aránya minél kisebb legyen. Végül pedig maga a leolvasó hardware eszköz – a bioszenzor – is támadás célpontjává válhat. Sajnos az ellenőrzést végző számítógép a legtöbb esetben nem képes a leolvasó eszköz megbízhatósága felől meggyőződni (ez azonban mindhárom azonosítási módszerre igaz). Mindezen hátrányok ellenére azonban léteznek széles körben elterjedt megoldások, és joggal tekinthetjük a biometrikus módszereket a személyazonosítás legmegbízhatóbb módjának. A biometrikus azonosítási módok közül személykövetésre a passzív módszerek a megfelelőek. Ilyenek a fül alapú, az arcfelismerésen, vagy a testalkat és járás alapú azonosítási technikák. Az írisz, ujjnyomat vagy tenyérnyomat alapú azonosításokat, vagyis amelyek aktív közreműködést igényelnek, várhatóan csak a beléptetés során lehet alkalmazni.

3.3 Távfelügyeleti rendszerek

A távfelügyeleti rendszer az élőerőt hatékonyan segítő elektronikai eszköz. A távfelügyeleti rendszer jelentősen lecsökkenti, optimalizálja az alkalmazott élőerő létszámát. Mindezek által növeli az őrzés és védelem hatékonyságát és csökkenti a költségeket. A távfelügyeleti rendszer lényege, hogy a rendszerben lévő riasztó központok egy beépített kommunikátor segítségével képesek kommunikálni a diszpécser központ számítógépével, illetve a távfelügyeletet ellátó személyzettel, akik a riasztásra megfelelően képesek reagálni.

A távfelügyeleti rendszerek lehetnek vezetékesek és vezeték nélküliek. A vezetékes kapcsolathoz felhasználhatóak a kapcsolt vonalas telefonhálózatok, vagy ugyanezen a hálózaton beszédsáv feletti jelátvitellel, közvetlen pont-pont közötti kapcsolat bérelt vonalon, kábel televíziós hálózatok és a távközlés-technika más lehetőségei.

Korszerűbbek a vezeték nélküli rendszerek, ehhez óriási lehetőséget biztosítanak a celluláris rádiótelefon hálózatok. A GSM hálózatok csak korlátozottan használhatók a biztonságtechnikában, a viszonylagos nyitottságuk, esetenkénti leterheltségük és főként a könnyű zavarhatóságuk miatt. A legbiztonságosabb az egyidejű vezetékes és vezeték nélküli rendszer alkalmazása. A kapcsolat lehet egyirányú vagy kétirányú. Legelőnyösebb, ha a kapcsolat egyidejűleg vezetékes és vezeték nélküli is, ugyanis a betörő az esetek döntő többségében először áramtalanítja az épületet és elvágja a telefonvezetéket. Így a kapcsolat még vezeték nélküli módon biztosított. A távbeszélő kapcsolat megszakadása és az áramellátás egyidejű megszűnése betörésre utaló jel. Így a diszpécser már akkor intézkedhet a járőr kiküldésére, amikor a betörő nem is jutott még be az épületbe. A távfelügyelet minden eszköze szünetmentes tápegységgel rendelkezik. A diszpécser központ számítógépe duplikálva van, tehát a számítógép meghibásodása esetén is a felügyelet folyamatos.

A diszpécser számítógépére befutó riasztás gyors pontosítása során a diszpécser megállapítja a riasztás valódiságát és riasztja a kivonuló járőrt, mely az adott objektumhoz megy és a szolgálati utasítása szerinti ellenőrzéseket és jelentéseket végrehajtja.

A diszpécserek a távfelügyeleti rendszer meghatározó személyei így azok kiválasztásuk és felkészítésük meghatározó fontosságú, munkájukat folyamatos felügyelet alatt végzik. A nagyteljesítményű és teljesen automatizált számító gépekkel felszerelt központok a beérkező jeleket gyorsan feldolgozza, archiválja és a kezelő monitorjára továbbítja. Mindezzel elősegíti az élőerő gyors reagálását.

3.4. Video felügyeleti (CCTV) rendszerek, felépítésük, eszközeik, alkalmazási területei, jogi hátterük

Az elektronikus vagyonvédelem a technikai színvonal szempontjából ellentmondásos fejlődő ága a zártláncú televíziós rendszer, a CCTV (Closed Circuit Television), abból a szempontból, hogy találhatunk olyan telepítéseket, ahol még 20-25 éves technológiai színvonalú eszközök működnek és olyanokat is, amelyek hihetetlen sebességgel modernizálódtak, modernizálódnak. A CCTV rendszer a televíziós technikából alakult ki, így nagyon sokáig fejlesztések főként e területen történtek és a videó megfigyelő rendszerek gyártói kis késéssel vették át az újdonságokat. Majd a 90-es évek közepétől a videós piac fokozatosan átalakult: a fejlett országokból egyre több önálló fejlesztésű termék kezdett beáramlani az európai országokba is. Mára az eszközválaszték már oly mértékben kibővült, hogy a rendszer elemek kiválasztása és igényekhez történő adaptálása jelentősen megnehezedett.

A zártláncú televízió rendszer elnevezés az alapvető működési elvet takarja, hiszen az analóg rendszereknél a kamera által felvett képet videó jellé alakítva, a jeltovábbítás zárt úton történik a monitorok és a rögzítők felé. Mindemellett fontos kitétele a CCTV rendszereknek, hogy mind az élő, mind a rögzített felvételeket csak az arra jogosult személyek nézhetik meg.

A technológia fejlődésével mára ez az elnevezés kissé elavulttá vált. Az IP rendszerek egyik legnagyobb előnye az, hogy a kamera képeit képesek vagyunk a helyi hálózat, vagy az internet segítségével távoli helyről is (gyakorlatilag bárhonnan) elérni. Ezekkel a fejlesztésekkel a CCTV rendszerek zártsága a hagyományos értelemben megszűnt, de ez nem jelenti azt, hogy bárki hozzáférhet ezekhez az adatokhoz.

Tehát összegezve azt lehet mondani, hogy: A videó megfigyelő rendszer egy olyan zárt televíziós rendszer, melyben a kamera, a képrögzítő és a képmegjelenítő eszköz közötti adatátvitel zárt vagy nyitott csatornán történik oly módon, hogy a közvetített képeket csak egy előre meghatározott célcsoport nézheti.

A CCTV rendszer célja egyrészt az, hogy a meglévő védelmet kiegészítve – azokkal kombinált módon – megfigyelje, dokumentálja (azaz rögzítse) a cselekményeket olyan formában, hogy azt a későbbiek során, ha kell, bizonyítási alapként is fel lehessen használni. Nagy alapterületű és nagy forgalmú létesítményekben (például bevásárlóközpont) alkalmaznak úgynevezett személykövető kamerarendszereket is, melyek segítségével a

gyanúsan viselkedő egyének mozgását a kezelőszemélyzet a kamerák kézi irányításával nyomon tudja követni megelőzve ezzel a lopásokat, rongálásokat.

A kamerarendszer telepítésének célja lehet statisztikai adatok gyűjtése például útszakaszok, kereszteződések esetében. Ezeket a statisztikai adatokat fel lehet használni az üzletpolitikában is, mondjuk egy-egy akció vagy kiárusítás mennyivel növeli meg a bevételt, mennyire volt sikeres egy ilyen megmozdulás és mit kell változtatni.

Automatizált gépsorok esetében nagyon sokat segíthet a dolgon, ha a meghibásodásokat, a nem üzemszerű működéseket azonnal jelezzük. Ezek a videó megfigyelő rendszerek alkalmasak az ipari és gyártási folyamatok ellenőrzésére, ki lehet szűrni a nem szokványos eseményeket, így megelőzve a nagyobb károk keletkezését.

Az utóbbi időben egyre elterjedtebbé és elfogadottabbá vált az úgynevezett térfigyelő kamera rendszer. Az ilyen rendszereket kezdetben csak a nagyobb városokba napjainkban viszont a kisebb városokban és néhol falvakban is megtalálhatók. Céljuk a közterületen elhelyezett műtárgyak, műemlékek és magántulajdon figyelése, a közbiztonság megőrzése, a közterületen elkövetett bűncselekmények visszaszorítása.

3.4.1 A kamerák

Ahhoz, hogy a megfigyelő terem monitorán képet, vagy képeket kapjunk, a megfigyelt helyszínről az élőképet vezetékes, vagy vezeték nélküli kapcsolaton szállítható elektronikus jellé kell átalakítani. Ezt az átalakítást végzik a videokamerák, amelyek szilícium alapú érzékelőjére a külvilág képét, egy összetett lencserendszerből álló optika vetíti. A szilícium alapon a fény elektromos töltésekké alakul, amelyet a kamera elektronikája kábelen vezethető videó jellé alakít. A megfigyelő teremben igény szerinti képátmérőjű videó monitor birtokában a videó jelet ismét optikai jellé átalakíthatjuk, vagy videó, illetve a digitalizált és tömörített jelet a PC alapú képrögzítővel archiválhatjuk.

Kialakításuk szerint vannak bel- és kültéri, a szolgáltatott kép alapján fekete-fehér és színes képet adó, mozgathatóságuk alapján fix és forgatható, illetve lineáris elmozdulásra képes és célkövető kamerák.

A biztonságtechnikában a helyzetnek és a feladatnak megfelelő típusú és műszaki paraméterekkel rendelkező kamerát kell alkalmazni. A leginkább elterjedt a hagyományos kialakítású boksz kamera, mely általában téglatest alakú. Ezeknél a kameráknál az objektív cserélhető, így rugalmasan alkalmazható. Ezt az eszközt elsősorban belső térben szoktak alkalmazni

Az utóbbi időben egyre inkább kedvelt az úgynevezett kompakt kivitelű kamera. Az ilyenekre jellemző az, hogy az optikát, magát a kamerát és esetleg az infra megvilágítást is gyárilag összeszerelve tartalmazza. Ennek egyérzelmű hátránya, hogy alkatrészeit cserélni nem lehet, így ha valami meghibásodik, akkor az egész kamera cserére szorul. Ezek a kamerák gyári összeillesztésnek köszönhetően igen magas az IP védettsége ezeknek a kameráknak (IP66, IP67), ráadásul gyakran fémből készülnek, így kiválóan alkalmazhatók kültéren. A hőmérsékleti szélsőségeknek is megfelelően ellenáll, és a gyári tartókonzol lehetővé teszi a rejtett kábelezést. Ezeknél a kompakt kiviteleknél igen gyakran alkalmaznak beépített infra LED-es megvilágítást, így éjszaka is jól használhatóak.

A másik igen kedvelt kialakítás, a dome kamera. Elnevezését a jellegzetes félgömb alakjáról kapta, mely kupolához (angolul: dome) hasonlít. Ezeket két kivitelben gyártják, az egyik a fix dome kamera, a másik ennek egy továbbfejlesztett változata a speed dome. Burkolata általában sötétített, így nem érzékelhető, hogy milyen irányba állították be. Készítenek beltéri, kültéri és vandál biztos kivitelt is melynél a búra ütésálló műanyag, a foglalat pedig valamilyen masszívabb fém. A speed dome kamerák hasonló felépítéssel rendelkeznek, mint a fix változatok, az alapvető különbség, hogy a bennük lévő kamera motorosan mozgatható. A speed dome kamerák a házon belül nagy sebességgel akár 360 fokban elfordíthatóak és függőlegesen 180-190 fokban. Lényegében a speed dome kamera tehát egy rejtett PTZ (PAN-TILT-ZOOM) kamera, pan-vízszintesen, tilt-függőlegesen elmozdítható. A másik forgathatósági lehetőség a forgózsámolyra épített kamera, mely lehet dome kamera is. Ebben az esetben a kamera lassú, pásztázó mozgást végez akár vízszintes, akár függőleges irányban. Ebben az esetben mindig látható a kamera állása.

Ezekkel a megoldásokkal képesek vagyunk egyetlen kamerával jelentősen nagyobb területeket megfigyelni. Ezek a kamerák képesek előre beprogramozott útvonalakat figyelni, ahol a sorrend és a pásztázási idő is beállítható. Kézi vezérlés esetén a nagyon alacsony mozgási sebességre is képesek, és elérhető akár a 40x-es zoom is. Elhelyezést tekintve lehetnek mennyezeti, oldalfalra, vagy oszlopra szerelhetőek. Az újabb fejlesztéseknek köszönhetően léteznek olyan intelligens speed dome kamerák, melyek képesek felismerni személyek, gépjárművek, vagy egyéb objektumok mozgását és követni azt. Behatolás jelző rendszerrel kombinálva is lehet használni, ugyanis a legtöbb ilyen kamerán van riasztás bemenet. Ha jelzést kap a kamera, akkor automatikusan az ilyen esetekre beprogramozott pozíciót veszi fel.

Speciális kamerák az úgynevezett csőkamerák (tube cameras), melyek egy mennyezetre szerelt csőszerkezetben lévő kötött sínpályán mozognak. Ezek általában valamilyen speed dome kamerát tartalmaznak, így meglehetősen nagy területet lehet pásztázni. Ezzel a konstrukcióval a holttér kiküszöbölhető például raktárakban, vagy hipermarketekben, és személykövetésre is alkalmas.

3.4.2 Képrögzítők, képmegjelenítők

A képek megjelenítésére általában valamilyen speciális CCTV monitort alkalmaznak. A CCTV monitorokat úgy alakították ki, hogy napi 24 órás használat mellett képesek huzamosabb ideig üzemelni, emellett olyan funkciókkal látták el, ami a biztonságtechnikai megfigyeléshez szükséges.

A monitoroknak három fő típusa van, a hagyományos katódsugárcsöves (CRT), a plazmakijelzős és a folyadékkristályos (LCD) monitort. Ezek közül a legrégebbi technológia a CRT monitor, melyet ma már nem is telepítenek azonban pár szót szükséges róla ejteni, hiszen régebbi rendszereknél még ma is használják. A monitor katódsugárcsövének belső falára egy olyan porréteget diffundálnak, mely nagy energiájú elektronok hatására fényt bocsájt ki magából. A katódsugárcső másik felében elhelyezett elektronágyú egy mágneses mezővel eltérített megfelelő intenzitású (a videojellel arányos) sugárral pásztázza ezt a por réteget, ami az intenzitásnak megfelelő erősségű fényt fog kibocsátani magából. Színes CRT monitorok esetén a három elektronágyú pásztázza az alapszínnek megfelelő pontokat és additív színkeverés szerint ad színes képet.

A plazmaeffektust alkalmazó monitorok lényege a gázkisülés elve. Két egymástó 0,1-0,15 mm távolságra lévő üveglemez között a fénycsöveknél is alkalmazott xenon és neon nemesgáz töltet található. A frontüvegen vékony elektródák találhatók. Ezek alatt helyezkednek el a három alapszínnek megfelelő lumineszkáló anyagot tartalmazó mikroszkopikus méretű cellacsoportok. A cellák alatt közvetlenül, a hátsó üvegen szintén elektródák találhatóak, melyek külön-külön vezérelhetők. Az elektródákra adott vezérlőfeszültség hatására elektromos erőtér jön létre, ami gerjeszti a nemesgáz keveréket. A gerjesztés hatására a gáz fényt bocsát ki az ultraviola (UV) tartományban. Az UV fény behatol a cellákban lévő luminofor rétegbe, és másodlagos gerjesztéssel látható, színes fény jön létre. Additív színkeveréssel jön létre a megfelelő kevert szín.

Az LCD (Liquid Crystal Display) - más néven folyadékkristályos kijelző - technikával a hétköznapjainkban is elég gyakran találkozunk. A működéshez szükséges anyagot Fridrich Reinitzer német biokémikus fedezte fel. Működési elve alapján két fajtát különböztetünk meg:

1. Dinamikus szóráson-,
2. Térvezérlésen alapulót.

A dinamikus szóráson alapulónál a kialakított karakterek vezérlés nélküli állapotban átlátszóak, vezérlés hatására pedig kifehérednek.

A térvezérlés esetében a folyadékkristály molekulákat fény polarizátorok közé helyezik, ezeknek a polarizációs síkjuk 90 fokot zár be. Így a polarizálódó belépő fény csak a terjedés következtében 90 fokkal elfordult állapotban képes áthaladni. A kijelzőt határoló két üveglemez belső felét egymásra merőlegesen, de párhuzamosan felrovátkolják. A folyadékkristály molekulái alapállapotban (feszültségmentes esetben) 90 fokos forgatást végeznek a beeső fény polarizációs síkján.

A képeket a legtöbb helyen rögzítik. Ez kezdetekben videomagnók segítségével történt, ilyen például a time-lapse videomagnó. Ennek segítségével a 180 perces kazettára, akár 24 óra videó anyagát is felvehettük, mert a rögzítő csak minden nyolcadik képet tárolta el. Az elektronika fejlődésével ezek a rendszerek eltűntek, és helyüket átvették a digitális rögzítők. Ezek feladata, hogy a beérkező analóg jelet digitalizálják, tömörítsék és tárolják. Legfőbb jellemzői, hogy mennyi kamera jelét tudja fogadni és hogy mekkora a tárolási kapacitása (gyakorlatilag mekkora winchester van benne). Megkülönböztetünk asztali és PC alapú rögzítőket. Asztali rögzítő esetén, az eszközön egy olyan célszoftver fut, amely csak a videó rögzítéshez és tároláshoz szükséges. Kezeli a ki és bemeneteket, a fő és mellékmonitorra képet ad ki, adathordozóra ki lehet írni a tárolt videókat, és ha szükséges visszajátssza azokat.

A PC alapú rögzítők annyiban különböznek asztali társaiktól, hogy itt egy számítógépre csatlakoztatjuk az eszközöket egy illesztőkártya segítségével, és az operációs rendszer a számítógép rendszere lesz (Windows, Linux). A digitalizálás ezen az illesztőmodulon történik, a tömörítés és egyéb eljárások pedig a számítógép erőforrásai által. Hátrányuk az általános operációs rendszerből adódik, instabilabb és könnyen támadható.

3.4.3 Nagyfelbontású IP rendszerek

3.4.3.1 Az IP kamerák kialakulása, szabványai, felépítése

A kilencvenes években elkezdődött az IP kamerák kifejlesztése, melyek sok lehetőséget kínáltak a vagyonvédelmi rendszerek tekintetében. Fejlesztésük terén az olcsóbb analóg rendszer minőségét (érzékenység és felbontás terén) valamikor 1996 után érték el. A fejlesztésben nagy előrelépést jelentett, hogy a 2000-es évek elején a nagyobb analóg CCTV gyártók is bekapcsolódtak ebbe, így már nem csak szoftveres előrelépések történtek, hanem megfelelő és cserélhető objektívekkel és jó minőségű CCD-vel látták el az eszközöket. 2005 környékére már elérték a 640x480-as felbontást és a 25 fps képfrissítést is, és már megjelent a váltott képsorost felváltó progresszív letapogatás is, így ténylegesen elérték az analóg rendszerek szintjét. Az igazi előnyét az elmúlt évek fejlesztései hozták meg az IP rendszereknek, ami nem más, mint a megapixeles felbontás. Ezeknél az érzékelés már CMOS szenzorokkal történik, melyeknél ma már általános az 1,3 és a 2 megapixel (Mp).

A hálózati videotechnikának a fejlődésében a 2008-as év egy újabb fordulópontot hozott. Egy olyan hiány pótlása történt meg több mint egy évtized elmúltával, ami a különböző gyártók termékei között kapcsolatot, kompatibilitást teremtett. Ez az IP CCTV irányelvek, szabványok létrehozása volt. A kezdetekben a gyártók rájuk jellemző specifikus protokollokat alakítottak ki, így az egyes termékeik kizárólag egymással voltak összepárosíthatóak. Egy adott rendszer bővítése, csak annak a típusnak a kameráival, rögzítőivel történhetett és csak az általuk tervezett szoftverekkel működtek. Természetesen a gyártó cégeknek a kezdetben ez még meg is érte, azonban az egyre szélesedő piaci igények nyomására engedtek ezekből. Két szabványrendszert alakítottak ki: az ONVIF és a PSIA.

Az ONVIF egy nyílt fórum, amit három nagy cég alapított, az Axis Communications, a Bosch Security Systems és a Sony Corporation. Célja az volt, hogy az IP alapú videó termékek hálózati paramétereit egységesítse, meghatározza az IETF és a Web Service szabványokat, valamint a biztonsági és az IP-konfigurációs követelményeket (eszköz- és eseménykezelés, valós idejű megtekintés, videó elemzés, stb.) Ez a szabvány biztosítja a hálózati eszközök közötti élő videó-, hang-, meta adat és vezérlő információk cseréjét, valamint azt, hogy az egyes eszközök automatikusan megkeressék a hálózatot és fel is csatlakozzanak rá. Ehhez a nyitott fórumhoz bárki csatlakozhat, gyártó, szoftverfejlesztő, végfelhasználó egyaránt. Az IP kameráknál ez a szabványhasonló, mint az analóg rendszerek

PAL szabványa, azonban az utóbbi használata kötelező azoknál az országoknál, akik ezt választották, míg az ONVIF csak egy javaslatcsomag a tagok számára.

A másik szabvány, a PSIA teljesen hasonló célokkal jött létre a piac alacsonyabb részesedésű cégei körében. Olyan neves gyártók is megtalálhatók benne, mint a Honeywell, a Cisco System vagy az IBM, és egy részük mindkét szervezetnek tagja.

Az IP kamerák felépítésüket tekintve annyiban különböznek az analóg kameráktól, hogy tartalmaznak egy képtömörítő, és egy hálózati egységet. Az előbbi hivatott arra, hogy a digitális jeleket olyan méretűre csökkentsék, melyet a hálózaton képesek legyünk közvetíteni, emellett csökkenti a videó fájlok méretét a tárolhatóság érdekében. Az újabb IP kamerák már sokszor tartalmaznak valamilyen tároló egységet is (ami lehet SD-kártya vagy winchester is), így olyan szituációkban, amikor a kommunikáció megszűnik a kamera képes eltárolni az adatokat. A hálózati illesztőkártyának köszönhetően lehet az internetre vagy helyi hálózatra kapcsolódva azonosítani az eszközt.

Az IP kamerák kivitelüket tekintve teljes mértékben megegyeznek az analóg rendszerekben megismertekkel. A kompakt kameráktól elkezdve egészen a speed dome kamerákig minden megtalálható a palettán. Felszerelhetők a mára már megszokottá vált infra LED-ekkel is az éjszakai megfigyeléshez, sőt létezik olyan kivitel, mely tartalmaz egy beépített mikrofont, így a kép mellé (megfelelően szinkronizálva) hangot is társíthatunk, mindezt ugyanazon a vezetéken.

3.4.3.2 Adatátvitel, webes felületek, tárolás

Az IP kamerák felbontásán kívül a legnagyobb különbséget a kommunikációban találjuk az analóg rendszerekhez képes. Mint a neve is mutatja, a számítógépek hálózati kommunikációjával megegyező módon működik. Maga az IP, azaz (Internet Protokoll) egyes eszközök, jelen esetben a kamerák hálózathoz (vagy internethez) való csatlakozása során, annak azonosítására szolgál. Azt hogy a hálózaton belül melyik eszköznek kell továbbítani az adatokat egy előre meghatározott irányítási rendszer szerint történik. Ez az úgynevezett TCP/IP20 Protokoll. A TCP feladata hogy az adatcsomagokat hibátlanul eljuttassa a fogadó számítógéphez, mely úgy történik, hogy az adatokat meghatározott csomagokra bontja, melyeket egyesével felcímkéz, a fogadó számítógépen pedig összerakja. Ezt a procedúrát lassítja, azonban üzembiztossá teszi, hogy minden egyes csomag átküldése után nyugtázást vár el a másik géptől, ha ezt nem kapja meg, akkor újraküldi. Az IP teszi lehetővé, hogy az

adatcsomag a megfelelő célba jusson el, valamint azonosítja a küldő és a fogadó számítógépet egyaránt.

Transmission Controll Protocol/Internet Protocol, azaz Átviteli Vezérlő Protokoll/Internet Protokoll

Az adatátvitel tömörített formában történik, mely nagyban befolyásolja az átvitel sebességét (ez főleg interneten keresztül érdekes). Az IP kamerák esetében alkalmazott első tömörítési forma az MJPEG volt, ami gyakorlatilag minden egyes képkockát JPEG eljárással tömörített be, majd ezeket egy video folyammá fűzte össze. Előnye, hogy nem túl nagy a hardverigénye, így gyengébb gépeken is alkalmazható, azonban nem tudunk vele elérni nagy tömörítési arányt. Manapság a legelterjedtebb az MPEG szabványcsalád tagjai, melyekre mind igaz, hogy olyan módon tömöríti a videót, hogy nagyjából 10-15 képkockás tartományra osztja, ahol az első képet teljes mértékben tömöríti (referencia képkocka), a többinél pedig csak a változásokat. Mivel ezek a változások egy megfigyelőrendszernél nem számottevőek, így elég nagy rátával tud tömöríteni. Ezzel az eljárással az MJPEG-hez képest mintegy 80%-kal jobb tömörítési aránnyal dolgozik. Ma ez a legelterjedtebb, nem csak az IP kameráknál, de a digitális rögzítőknél, és az interneten egyaránt. Ezzel dolgozik a Youtube, a Quick Time, a Blue-ray lemezek filmjei és így tovább.

Az hálózati videó megfigyelő rendszerek, amennyiben megfelelően vannak konfigurálva, akár a világ másik tájáról is elérhetőek. Ezt biztosítja az úgynevezett web szerver vagy más néven videó szerver, melyeket beleépítenek a kamerába. Ez rendelkezik egy honlappal, amelyet a hálózatra, vagy az internetre csatlakozott számítógépről, böngésző, vagy egy előre telepített szoftver segítségével el lehet érni, amennyiben birtokunkban van a megfelelő felhasználónév és jelszó. Az egyszerűbb kamerák esetében is mindkét megoldással nézhetjük élőben a történteket, illetve a szoftver segítségével rögzíthetjük is a képeket. Egy kamera élőképének nézése, illetve a rögzítés is történhet párhuzamosan több számítógépről.

Az IP rendszerek esetében az adatok tárolására több lehetőségünk is van. Hasonlóan, mint az analóg rendszereknél itt is van speciális rögzítő eszköz, az úgynevezett NVR (Network Video Recorder), azaz a hálózati videó rögzítő. Ez az eszköz teljes mértékben digitálisan működik, és mint a neve is mutatja, a hálózatról érkező videojelek rögzítése a feladata. Az ilyen eszközöknél nincsen meghatározva, hogy hány kamera képét képes fogadni, ennek megfelelően egy, esetleg két LAN csatlakozót találunk meg rajta. Mivel a legtöbb esetben a kamerák switchen keresztül csatlakoznak az NVR-hez, így ez a mennyiség elegendő. Az hogy egy IP rendszerbe mennyi ilyen rögzítőt kell alkalmazni, kizárólag attól

függ, hogy mekkora a tároló kapacitása az eszköznek (azaz mekkora és mennyi winchestert tartalmaz) és a képeket milyen minőségben kívánjuk rögzíteni. A rendszerbe való elhelyezésüket illetően nagyon nagy előnyt jelent, hogy nem feltétlenül kell a megfigyelő szobába, vagy a kamerák közelébe telepíteni, így az illetéktelen hozzáférés esélye jóval kisebb. Az egyedüli kitétel hogy a hálózati csatlakozás megfelelő sávszélességgel rendelkezzen. Egy hálózati CCTV rendszerben korlátlan mennyiségű NVR-t alkalmazhatunk, így a bővítés meglehetősen egyszerű, hiszen csak egy szabad csatlakozási pontra van szükségünk a hálózathoz.

3.4.3.3 A megapixeles és a HD IP kamerák

A megapixeles IP rendszer tulajdonképpen nem jelent mást, mint azokat az IP kamerákat melyek felbontása meghaladja az egy millió pixelszámot. Sokan gondolkodnak úgy, hogy ha IP kamera, akkor annak sokkal jobb képe lesz, mint egy régi analóg rendszernek, holott ez nem igaz.

Sokszor találkozni olyannal, hogy egy-egy ilyen nagyfelbontású kamerára az van ráírva hogy HD-IP. Természetesen nem hibás ennek a kifejezésnek a használata, azonban érdemes tudni, hogy van különbség a megapixeles és a HD kamerák között. A HD, azaz High Definition (nagy felbontás) tulajdonképpen egy jól körülhatárolt szabvány, amit a televíziózásban fejlesztettek ki. (1280x720 vagy 1920x1080), képaránnyal (16:9) és fps-el dolgozik. Ezzel ellentétben a megapixeles kamerák az ONVIF által meghatározott keretrendszerben, de mégsem kötelezően alkalmazva kerülnek a boltokba. A HD kamerák egy meglehetősen szűk réteget képviselnek a megapixeles rendszerekben, bár igen gyorsan fejlődnek. Egyetlen hátrányuk, ami a szabvány megkötéseinek köszönhető, hogy a maximális felbontásuk nem haladhatja meg a 2,1 MP-t

Nem szabad elfeledkezni egy nagyon fontos tényezőről, amennyiben nagy felbontást szeretnénk valahova alkalmazni, ahhoz megfelelő objektívet kell választani. Amennyiben nem megapixeles objektívet választunk, a drágán megvásárolt kamera semmivel nem fog többet nyújtani a kép minőségét tekintve, mint egy analóg rendszer. Amíg csak az élő képet kell megfigyelnünk, a különbség nem annyira szembetűnő, de ha a felvétel elemzésére kerül a sor, és bele kell nagyítani a képbe, részletszegény, elmosódott, homályos képet fogunk kapni. A megfelelő tulajdonságot mindig a lencsék tulajdonságaira vezethetők vissza, így a mérőszáma is innen van. Széles körben elfogadott mértékegység az lp/mm, ami annyit takar, hogy egy milliméteren hány képsort képes az objektív megkülönböztetni. Ez az úgynevezett térfrekvencia, ami a sötét és világos sávok hosszegységre eső számát fejezi ki. A korábbi

rendszereknél az objektív kiválasztásának a szempontjai kizárólag olyanokra koncentrálódtak, mint a fókusztávolság, vagy a day&night funkció, akkoriban viszont az objektíveknek elegendő volt 320 horizontális pixelszámot megkülönböztetni és erre majdnem mindegyik képes is volt. A nagyfelbontású rendszerekben ezzel ellentétben 200-700%-al megnőtt a pixelek száma (nem ritkaság a 2000 horizontális pixelszám sem például 3 Mp esetében).

3.4.3.4 A kamerarendszerek intelligenciája

A kamerarendszerek intelligenciája a gyakorlatban nem takar mást, mint egy összetett videó tartalomelemzést megfelelő algoritmusok alapján. Ezeknek a fejlesztéseknek a célja az volt, hogy a megfigyelő személyzetet segítsék, ugyanis felmérésekből kiderült, hogy egy megfigyelést végző személy 20 perc után a monitoron látható események akár 95%-át is figyelmen kívül hagyja. A fejlesztéseknek a veszélyeztetés, elsősorban a terrorfenyegetettség hatalmas lökést adott, az IP kamerák megjelenése pedig lehetőséget.

A képtartalom intelligens elemzésére alapvetően a mozgásérzékelés szolgál. A mozgásérzékelő algoritmus a videót, képkockákká, jelenetekké alakítja, elkülöníti az előteret és a hátteret, majd a kiválasztott objektumot képkockáról képkockára követi. Ezzel a módszerrel meg lehet állapítani az objektum helyét, sebességét, haladási irányát, majd egy újabb algoritmus alapján azonosítja és osztályozza azokat. Amennyiben úgy ítéli, rögzítésbe kezd és riasztást hoz létre. Egy háttérfelismerő algoritmus segítségével kiszűrhetőek a téves riasztások, hiszen képes alkalmazkodni olyan változásokhoz, mint a felhők, árnyékok, falevelek mozgása, de az időjárás változásokat (hó, eső, köd, stb.) is el tudja különíteni.

A képtartalmak elemzése alapvetően kétféleképpen történhet. Centralizált módon, ilyenkor az intelligencia a hálózati rögzítőkbe van beleépítve. Ebben az esetben a képek elemzése az NVR-ben történik, így bármilyen IP kamerával működik a rendszer, olcsóbbak és nem jogvédettek. Hátránya, hogy a sávszélesség igénye és hálózat leterheltsége jóval nagyobb, hiszen a teljes képanyagot át kell küldeni a rögzítőig, de tényleges rögzítés csak mozgás esetén történik. A másik módszer a decentralizált képtartalom elemzés. Ilyenkor a kamera tartalmazza az intelligens szoftvert és az elemzés még a képanyag továbbítása előtt megtörténik. Ennek köszönhetően kisebb a sávszélesség igénye, kevésbé van leterhelve a hálózat, és a szükséges tárhely is csökken, hiszen csak akkor küld adatokat, ha valamilyen esemény történik. Hátránya, hogy kiépítése drága, mivel speciális jogvédett kamerákat kell felszerelni.

Ezek az elemző szoftverek ma már nagyon sok mindent képesek érzékelni és olyan adatokat szolgáltatnak a kezelő és az üzemeltető számára, amiket nem csak biztonságtechnikai viszonylatban lehet felhasználni. A gyakorlati tapasztalatok alapján az intelligens rendszereket leginkább a következőkre szokták alkalmazni:

- Mozgásérzékelésre, ha valamilyen mozgást észlel a megfigyelt területen riasztást ad és rögzít.

- Alakfelismerésre, széles körben használt funkció. Képes megkülönböztetni, hogy a védett terület felé állat vagy ember közelít, így a téves riasztások kiküszöbölhetők. Jól hasznosítható a forgalomfigyelési statisztikák esetén, útterhelés számításnál, mivel meg tudja különböztetni a személy és tehergépjárművet.

- Objektumkövetésre, általában speed dome kamerák esetében célszerű alkalmazni. Könnyedén nyomon lehet követni gépjárművek és emberek mozgását a megfigyelt területen (például hipermarketek)

- Idegen/elhagyott tárgyak észlelésére, amennyiben a megfigyelt területen huzamosabb ideig felügyelet nélkül marad egy tárgy, a rendszer érzékeli és riasztást küld. Általában repülőterületeken, vasútállomásokon, vasúti kocsikban szokták alkalmazni a merényletek, elkerülése érdekében.

- Tárgyfigyelésre, ha a megfigyelt területen egy tárgynak fix helye van, annak elmozdítását képes érzékelni a kamera és erről riasztást is küld. Legtöbbször múzeumoknál, kiállításokon alkalmazzák ezt, hiszen nagy értékű műtárgyakról van szó. Ennek az érzékenysége széles skálán állítható, hiszen a látogatók kitakarhatják a képből a megfigyelt tárgyat téves riasztást generálva.

- Bóklászás detektálására, a szoftver segítségével könnyedén érzékelhető, ha egy adott személy cél nélkül bolyong, vagy ha rendszeresen és minden ok nélkül visszatér ugyanarra a pontra. Gyanús viselkedés esetén riasztást ad ki a rendszer.

- Zsúfoltságérzékelésre, a mozgásérzékelés továbbfejlesztett változata, ahol a közterületeken, vasútállomásokon, sportlétesítményeknél nagyobb tömeg összegyűlését lehet jelezni. Egy meghatározott szám után ad riasztást, így időben lehet cselekedni.

- Szabotázsérzékelésre, a kamera érzékeli a letakarást, a festékkel való lefújást, de azt is, ha elmozdítják, elfordítják vagy megrongálják

- Arcfelismerésre, egy előre létrehozott arcképes adatbázissal kombinálva ki lehet szűrni az illetéktelen személyek bejutását a védendő területre.

- Rendszámfelismerésre, a nagyfelbontású térfigyelő rendszerek alkalmasak erre a funkcióra. Alkalmazzák az autópályákon, bevásárlóközpontok parkolóiban, járművek keresésére stb.

Az intelligens kamerák alkalmazásával lecsökkenthetjük a megfigyelő személyzetet érő terhelést, és kevesebb alkalmazott elegendő nagyobb terület megfigyelésére. Az alkalmazás minden olyan esetben értesítést küld, amikor valami esemény történik. Ezen kívül a hálózati terhelés és a szükséges tárhely mérete is csökken, mivel rögzítés csak abban az esetben van, ha történik is valami. Az adott eseményeket el lehet látni címkékkel, így gyorsabb keresést hajthatunk végre a már rögzítésre került anyagban.

3.4.4 HDcctv rendszer

A HDcctv a filmiparban használt HD-SDI interfészt, és a HD műsorszórás elvét felhasználó olyan videó megfigyelő rendszer, mellyel nagy felbontású képeket tömörítetlenül lehet koaxiális kábelen továbbítani.

A HD-SDI technológiát a filmipar számára hozták létre, a filmstúdiókon belüli nagyfelbontású kép és hang veszteségmentes továbbítására. Az adatokat digitálisan továbbítja a rendszer 10-bites kódszavakban, mindezt igen nagy 1,485 Gbit/s adatátviteli sebességgel. Mivel ez gyakorlatilag veszteségmentes eljárás így tömörítés nélkül képes minderre akár fullHD minőségben. A hagyományos CCTV rendszereknél alkalmazott 75Ω-os koaxiális kábelek főbb típusai megfelelően alkalmazhatóak. A kábelek gyártójától és minőségétől függően az áthidalható távolság RG6 esetén 180-200m, a legáltalánosabban használt RG59 esetén pedig 100-170m, melyek 5x-ére növelhetők repeaterek (ismétlők) alkalmazásával. A HD-SDI

4. Tűzjelző rendszerek felépítése, funkciói, fajtái, a tűzjelző érzékelők

Az elektronikus tűzjelző rendszer a tágabb értelemben értelmezett elektronikus vagyonvédelem fontos területe. Az automatikus tűzjelző rendszer érzékel, jelez és riaszt még a tűz kifejlődésének kezdeti szakaszában. Így lehetőséget biztosít nagyobb károk megelőzésére még kezdődő tűz időbeni lokalizálására és eloltására.

Az önműködő tűzjelző rendszerek tartalmaznak: tűzjelző érzékelőket, tűzjelző központot, tápellátást és az egységeket összekapcsoló vezetékhálózatot. Ezeken kívül tartalmazhat: kézi jelzésadókat, riasztó egységet, vezérlő egységet, hibaátjelző egységet, riasztás fogadó központot, önműködő tűzvédelmi berendezést és hibajel fogadó ügyeletet.

4.1 Tűzjelző rendszerek

A tűzjelző rendszerek lehetnek:

- Hagyományos hurkos kialakításúak;
- Címzett hurkos kialakításúak;
- Analóg intelligensek;
- Interaktívak.

4.1.1 Hagyományos rendszer

Hagyományos rendszer esetén az automatikus érzékelők és a kézi jeladók egy hurkon helyezkednek el. A központ csak riasztó jelzést és hibajelzést tud észlelni és továbbjelezni. Ez a jelzés igazából egy hurokellenállás változás, hiszen a kialakítás olyan, hogy az érzékelő vonal végén egy ellenállás vagy egy kondenzátor van. Riasztás esetén pedig az eszközök raknak a jelzővonalra egy nagyobb ellenállást. Nyugalomban a központ általában 1 kΩ-os ellenállást érzékel, szakadás illetve rövidzár esetén 0 Ω-ot, riasztás esetén pedig 2 kΩ-os ellenállást.

Hagyományos kialakítás esetén, egy hurok az egy zónát jelent, melyre maximum 32 érzékelő rakható. „A tűzjelző berendezés áramköreit úgy kell kialakítani, hogy egy egyszeres vezetékszakadás vagy zárlat esetén legfeljebb 32 eszköz válhat működésképtelenné, és az eszközöknek azonos zónában, azonos funkciójúaknak kell lenniük.”

A működésből következik, hogy nyugalmi helyzetben a központ az érzékelőkről nem tudja, hogy működnek-e vagy sem. Azt tudja csak megállapítani, hogy a hurok sértetlen-e.

Jelzés esetén is csak a hurkot tudja azonosítani. Annak az azonosításában, hogy melyik érzékelő jelzett, a fejeken található LED-ek segítenek.

Egy másik probléma, hogy a kézi jelzésadókról érkező riasztási jelzést meg kell különbözetni a többi érzékelő jelétől. Ezt a kritériumot az OTSZ írja elő. Ez a probléma úgy oldható meg, hogy egy jelzőhurokra csak egyfajta érzékelőt teszünk. Az egyfajta itt azt jelenti, hogy vagy kézi, vagy automatikus kategóriába sorolt-e a készülék. Ennek a következtében kétszer annyi hurkos központot kell vásárolni, ahány zóna van. Azért kell a kétszeres szorzó, mert kell egy jelzővonal az automatikus érzékelőknek és a kézi jelzésadóknak is. Azt pedig nem lehet megtenni, hogy az összes kézi érzékelőt egy vonalra rakom, hiszen akkor nem teljesülne az **Hiba! A hivatkozási forrás nem található.** említett paragrafus sem, miszerint egyszeres vezetékhiba esetén a kieső eszközök egy zónában találhatók.

4.1.2 Címezett hurkos kialakítású rendszer

A 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 – 128 érzékelő telepíthető.

Mind a hagyományos, mind a címzett rendszereknél az érzékelők szintjén dől el a tűz-riasztás. Adott mértékű környezeti változás hatására az érzékelők generálják a riasztás-jelzést. A kialakításnak létezik monológ vissza tértő hurkos változata is. Monológ kialakítás esetén a hurokfelépítés hasonló a hagyományos rendszerekéhez. A hurok végén egy lezáró elem található. Különbözik azonban abban, hogy itt a címzés miatt egy vonalra kézi és automatikus érzékelők is tehetők. Visszatérő hurkos kialakítás esetén nincs lezáró elem, hiszen a vonal a központba tér vissza. Ez a kialakítás azért jobb a monológnál, mert így egyszeres vezetékszakadás esetén a központ a másik irányból is „le tudja kérdezni” az érzékelők állapotát.

4.1.3 Analóg intelligens rendszer

Ez a kialakítási mód fejlettebb az előzőektől. A központ itt már egy mikroprocesszoros számítógép. Az előző kialakításokhoz képest a három alapvető különbség állapítható meg. Az egyik, hogy itt már nem a fejek döntenek, hanem a központ. A másik, ami az előzőből következik, hogy itt fejek már nem kétállapotúak (riasztás, nyugalmi állapot), hanem analóg módon követik a tűzjellemzők mindenkori értékét és ezt az analóg jelből gyártott digitális

jelet küldik be a központba, hogy az tudjon dönteni. A harmadik különbség a „jelzővonalban van”. A hagyományos kialakításnál a jelzővonalon csak áram folyik, itt viszont a jelzővonalon digitális adatfolyam halad keresztül.

Az érzékelők ezen kialakításnál egyedileg címezhetők, így itt is lehetőség van a kézi és automatikus jelzésadók egy fizikai hurokra történő szerelésére. Itt azonban nem csak az érzékelők szerelhetők egy hurokra, hanem a vezérléseket végző ún. modulok is, sőt ezek címzése külön történik az érzékelőktől. Egy vezeték páron így összesen 99 érzékelő és 99 modul helyezhető el.

A központ a döntést a rajta futó szoftver segítségével hozza meg. A mért értékeket pedig ciklikusan kérdezi le az összes érzékelőtől. Riasztási szintnek akár minden érzékelőre különböző határértéket állíthatunk be. Ez a tulajdonság akkor jó, hogyha a rendszer több, különböző alapszennyezettségű helyiségen is áthalad. Hasonló beállítási lehetőség az ún. drift kompenzáció. Ha ez be van állítva, a központ automatikusan, feljebb állítja az alapszintet, így a riasztási szintet is. Ez persze csak egy darabig állítható, mert ha túl magas az alapszint az érzékelő hatékonysága is csökken. Ha ezt a bizonyos határt eléri a szennyezettség szintje, a központ jelzi a karbantartás igényét. További lehetőség, hogy be lehet állítani az előjelzési szintet. Ez azt jelenti, hogy ha valamelyik érzékelő eléri ezt a szintet, akkor a központ előjelzést ad. Ez a jelzés még nem tűzjelzés, tehát sem a vezérlések nem indulnak be, sem az átjelzés nem következik be. Lehetőség van a felderítésre a tűz esetleges gyors megfékezésére. Ha az érték tovább nő, a központ természetesen tűzjelzést ad.

4.1.4 Interaktív rendszerek

Az interaktív rendszereknél nem a központ végzi el a jelzés kiértékelését, hanem minden érzékelőbe letöltik a jelzési algoritmust. A tűzérzékelők döntenek a tűzjelzésről, ezáltal gyorsabb a tűzjelzés. Ennek a rendszernek az előnye még, hogy „alkalmazkodik” a környezeti jellemzőkhöz és csak akkor ad jelzést, ha hirtelen változnak meg azok.

4.2 Tűzjelző központ feladatai, jellemzői

- Ellátja energiával a rendszer többi részét.
- Fogadja és feldolgozza a hozzá kapcsolt érzékelőktől (jeladóktól) érkező jeleket.
- Meghatározza, hogy a jelek tűzriasztás állapotnak felelnek-e meg.
- Jelzi a tűzriasztás állapotot (láthatóan és) hallhatóan.

- Azonosítja és jelzi tűz helyét.
- Regisztrálja a tűzriasztási és egyéb információkat.
- Ellenőrzi a rendszer üzemszerű működését.
- Továbbítja a riasztást.
- Vezérli a tűzvédelmi berendezéseket (hő és füst elvezetés, oltórendszerek, ajtók)
- Üzemzavart figyelmeztető hanggal és fénnyel jelzi

4.3 Érzékelők csoportosítása

Az érzékelők sokféleképen csoportosíthatóak. Az érzékelő feldolgozási módja alapján lehetnek:

- küszöb (vagy határérték)
- különbség
- és változási sebesség érzékelők.

A térbeli elhelyezkedés alapján megkülönböztetünk:

- pontszerű
- vagy vonali érzékelőket.

Az érzékelő visszaállási (újraélesítési módja) szerint vannak:

- önműködő visszaálló
- valamilyen módon visszaállítható
- és nem visszaállítható érzékelők.

Az észlelt tűzjellemző alapján vannak:

- füstérzékelők,
- hőérzékelők,
- gázérzékelő,
- hangérzékelők,
- lángérzékelők és ezek kombinációi.

4.3.1 Füstérzékelők

A füstérzékelők, ahogy a nevükből is adódik, a tűzet kísérő füstjelenséget érzékelik. Ezen füstrészecskéket három módon tudjuk érzékelni: ionizáció, fényelnyelés- és fényszóródás elvén működő eszközök segítségével.

Az *ionizációs füstérzékelő* működési elve: az érzékelőben lévő radioaktív anyag ionizálja a referencia kamra levegőjét, ezáltal U_1 feszültség ébred és az ún. nyugalmi kamraáram kezd folyni. Az érzékelő kamrában is ugyanezen áram folyik nyugalmi állapot esetén. Amennyiben azonban füstszemcsék kerülnek az érzékelő kamrába, úgy az ionizált levegőmolekulák megtapadnak a füstszemcsék felületén, így az átfolyó áram lecsökken. Ezt az áramkülönbséget érzékei a különbségképző elem. Az érzékelés hatására az érzékelő ráteszi az ellenállását a hurokra. Az érzékelő nem alkalmas alkoholtüzek, kültéri tüzek és kezdődő nagyszemcsés tüzek érzékelésére és érzékeny a légáramra, mert az is lecsökkenti a kamraáramot.

A *fényelnyelés alapján működő füstérzékelők* két különálló egységből egy infra adóból és egy infra vevőből állnak. Az adó és vevő közötti távolság a 10 m-től a 100 m-ig terjedhet, de a két egységnek látni kell egymást. A működési elve egyszerű, ha látja egymást a két egység, akkor nincs tűz, ha nem látja egymást, mert füst került közéjük, akkor tűz van.

Alkalmazható:

- hosszú magas belső terek, osztott mennyezetek,
- tágas csarnokok átriumok,
- műemlékek, szerelhetetlen mennyezetek,
- korrozív karbantarthatatlan akadályokkal teli ipari épületek védelmére, valamint
- látható füstképződés (PVC, gumi, olaj, fa, szénhidrogének, folyadéktüzek) érzékelésére

Nem alkalmas:

- alkohol tüzek észlelésére,
- Külső terek,
- poros, füstös terek

- nem látható füstök észlelésére,
- magas páratartalmú vagy
- magas környezeti hőmérsékletű helyek védelmére illetve
- közvetlen meleg levegő befújásánál (megváltozó törésmutató).

A fényszóródás elvén működő optikai érzékelők a legáltalánosabban elterjedt érzékelő fajta. A legjobb ár érték aránnyal ez az érzékelő fajta rendelkezik. Az érzékelő a pontszerű kategóriába sorolható, hiszen egy egységből áll. Ez az egység foglalja magában a fényérzékelő elemet, a fénykibocsátó elemet és az optikai sötétkamrát, ami azonban nem zárt, hogy a füstrészecskék tudjanak behatolni. Nyugalmi állapotban az infra LED által kibocsátott fényt nem érzékeli a fotocella. Amennyiben füst kerül a kamrába a fény megtörik a füstrészecskéken és az érzékelőre fény kerül. Amit ezt érzékeli a fotocella, máris jelet ad a központnak (ellenállás rákapcsolás, mért érték változtatás). Az infra LED helyett használható lézerfény is, vagy kék fény. Ezen megoldások sokkal érzékenyebbek kis szemcseméret esetén, de mivel nagyon drágák, így még nem elterjedtek.

Alkalmazható:

- parázsló tüzek,
- jól látható füstképződés,
- Irodaszerű terek,
- menekülési utak védelmére,
- légcsatorna érzékelőként,
- nagyobb légáramlású terekben, és
- nagy értékek védelmére

Nem alkalmas:

- alkohol tüzek észlelésére,
- poros korrozív környezet esetén,
- kis szemcséjű, nem látható füst illetve
- fekete, abszorbitív füstök esetén, valamint
- magas páratartalom

- magas környezeti hőmérséklet
- hő párnák (nagy belmagasság)
- nagy frekvenciás tér jelenléte esetén.

Az aspirációs érzékelő nagyon speciális érzékelő. Speciális, mert itt nem a védett térben történik a levegő vizsgálata, hanem egy nagy érzékenységű központi egységben. A rendszerhez a központi részen kívül csak egy csőhálózat csatlakozik. A központi rész a csőhálózaton keresztül szívja a levegőt a védett térből és a benne található érzékelőn keresztül megvizsgálja. A kialakítás természetesen nem ilyen egyszerű. El kell érni, hogy minden lyukon, amik a csöveken találhatók, egyforma legyen a szívóhatás. A legtávolabbi elszívó pont maximum 100 m-re lehet a központtól és a minta utazási ideje nem haladhatja meg a 30 másodpercet. A csőhálózat hossza pedig maximum 200 m lehet. Ezen problémákból következik, hogy ezeket a berendezéseket nem olyan egyszerű telepíteni, hiszen mindent méretezni kell. A következő probléma, hogy a központi egységben lévő érzékelőnek is érzéketlennek kell lenni a légmozgásra. Ennek a kritériumnak legjobban a fényszóródás elvén működő optikai érzékelők felelnek meg, azon belül pedig általában lézer diódás érzékelőt alkalmaznak. A kialakításból következik, hogy a tűz korai szakaszában képesek jelezni, de a védett részen belül nem tudja megkülönböztetni a füstforrás helyét.

Alkalmas:

- adatfeldolgozó-, számítógép- és telefonközpontok,
- magas és bonyolult belső terek,
- állványos magas raktárak közbenső szintekre kiterjedő,
- ipari „tiszta terek”,
- közmű alagutak
- tokozott (szekrényekbe zárt) villamos berendezések védelmére.
- Ott ahol az induló tüzek korai felismerése szükséges valamint
- hűtőházakban és
- műemlékekben illetve
- ahol fontos, hogy rejtve maradjon a csőhálózat.

Alkalmatlan:

- alkohol tüzek észlelésére,
- külterek,
- üzemszerűen poros, füstös, párás környezet védelmére.

4.3.2 Hőérzékelők

A *hőérzékelők* a tűz során keletkező meleg levegőt észlelik különböző fizikai törvények segítségével. Kettő nagy csoportja van:

- Hőmaximum érzékelő: A rendelkezésre álló fizikai elvek (forráspont, hő tágulás, ellenállás változás, olvadáspont) szerint hőmérsékletet mérünk. Ha eléri ezt az előre rögzített hőmérsékletet, akkor jelzést ad, kivéve az analóg intelligens, hiszen az folyamatosan mér. A maximál hőérzékelőket oda lehet telepíteni, ahol a hőmérséklet viszonylag állandó, bizonyos értéket csak tőz esetén halad meg.
- Hősebesség érzékelő: A hőmérséklet változásának sebességét mérjük. Általában egy külső és egy szigetelt belső részben a hő tágulások különbsége alapján. 3/5/8/10/12°C/perc hőmérsékletváltozásra jeleznek. Nagy belmagasság vagy gyakori hőmérséklet ingadozás esetén célszerű telepíteni.

Az érzékelők fajtái:

- Bimetálos
- Olvadó (wood) fémes
- Membrános táguló légkamra
- Elektronikus
- Hőérzékelő kábelek

Hőérzékelők előnyei, hogy egyszerűek és olcsók, hátrányaik, hogy nagyobb a jelzési késedelem. Célszerű alkalmazás: Ha adott helyiségben a tűz nem jár füstképződéssel (vegyi raktár, alkohol tűz); vagy üzemszerűen előfordul a füst (garázs, dohányzó) Nem célszerű alkalmazni:

- rosszul égő, parázsló, kis hő növekedéssel járó ún. svéltüzek érzékelésére.

- menekülési utak,
- nagy belmagasságú terek és
- klimatizált terek védelmére.

A *bimetállos érzékelő* elem alakja hő hatására változik, ezzel elektromos kontaktust nyit vagy zár. Ennél előnyösebb az ún. gyorsműködésű korong termosztát (működési hőmérsékleten konvexből átpattan konkávba és működés után, ha a tűztől nem károsodott, önmagától visszaáll).

Az *olvadó (wood) kötés* számos formában alkalmazzák, nagy hátránya, hogy az egységet működés után cserélni kell.

A *törőüveg vagy kvarckörte* nem visszaállítható hőérzékelő, az üvegcsében meghatározott forráspontú, színezett folyadéktöltet van, ami megnövekvő gáznyomás hatására széttörik és így megnyitja a kifolyó nyílást (például sprinkler).

A *lég/folyadéktöltésű szelence* a folyadék forrponton megnövekvő gáz nyomására a rugalmas falú zárt szelence elmozdul. Kontaktot ad Lehet levegővel tölteni ezt a membrános szelencét, a működési elv azonos

A *hőérzékelő kábel* a gyakorlatban nem terjedt el, pedig egyszerű, olcsó, de működés után cserélni kell az adott vezetékszakaszt. Két összecsavart vezetékből áll, melyek meg vannak feszítve és köztük hőre lágyuló szigetelés van, mely magas hőmérsékleten kiolvad és zárlatot hoz létre. A hőérzékelő kábel másik fajtája a félvezetők tulajdonságait használja. Csak a drágább kábelek képesek a tűz pontos helyét jelezni, az egyszerű hőérzékelő kábel nem.

Az *elektromos érzékelő* más néven termo elektromos elven működű érzékelő. Ebben két egyforma termisztort helyeznek el hídkapcsolásban. Ezek korszerű érzékelők.

A *kombinált hőérzékelő* esetében a hősebesség érzékelőt kiegészítik küszöbhőmérséklet érzékelő betéttel, így kettős biztonság.

4.3.3 Lángérzékelők

Ezen érzékelők a látható láng infravörös és ultraibolya tartományát érzékelik. Ezeket manapság általában kombinálják, tehát mindkét érzékelési módot használják egyszerre. Ám én külön-külön elemzem őket. Fontos megjegyezni, hogy mivel magát a lángot érzékelik így minden esetben fontos a közvetlen rálátás.

Alkalmazásuk:

- gyors, lángfázissal kezdődő tüzek (folyadék tüzek, oldószeres technológiák, festő alagutak
- kültéri tüzek észlelése (farakatok, folyadék tartály tüzek)
- ahol a jelzési késedelem nem megengedhető (anyagszállító csatornák, hangárok, nagy csarnokok)

Nem alkalmazhatók:

- láng nélküli tüzek (például svéltűz) észlelésére,
- sűrű füstképződés (például PVC) esetén,
- hegesztés, szikra, villámlás esetén UV érzékelőnél,
- hősugárzó eszközökre irányítva IR érzékelőnél,
- korrozív környezet esetén,
- ha nagy páratartalom, gőz ez UV-nál okoz gondot illetve
- magas környezeti hőmérséklet esetén.

Az infra lángérzékelő érzékelő eleme félvezető. Általában két piroelemet tartalmaz. Egy a láng és egy a környezet infra sugárzását veszi. Ennek a segítségével kerül sor a környezeti zavarok kiküszöbölésére. Érzékeli a lobogás frekvenciáját (2-20 Hz), a téves riasztások kiküszöbölésére. A lángot késlekedés nélkül érzékeli, de a megtévesztő jelenségek kiszűrésére beépített kiegészítők miatt van 10-15 másodperces jelzési késedelem. Nem érzékeny a szennyeződésre, nedvességre, nagy az észlelési távolságuk. Előnye, hogy olaj, füstlerakódásra, porra nem érzékeny, párára kevéssé érzékeny.

Az *ultraibolya lángérzékelő.* A napfénynek az UV tartományát a légkör kiszűri, tehát nem kell zavaró hatásával számolni. Hidegkatódos gázkisüléses cső a működtető eleme (UV csövet egy halogéngázzal töltött üvegbúra alatt elektródapár alkotja). Ha az elektródára feszültséget kapcsolunk, akkor tűz hatására ionok keletkeznek. Előnyei, hogy napfény érzéketlen; gyors működésű; bel- és kültéren egyaránt. Működési korlátok a por, a nedvesség, az olajszennyezés, nagy relatív páratartalom és a gőz. Ezek UV nyelőek, tehát egyszerűen akadályozzák a rálátást. A szikra és villámérzékenység is fenn áll és a hegesztés is megzavarja.

4.4 Kézi jelzésadó

A kézi jelzésadó közvetlen, gyors, emberi tűzjelzés lehetőségét teremtik meg. Fontos elemei a rendszernek, hiszen az embernél gyorsabban egyik érzékelő sem képes pontosan felismerni a tüzet. Fontos a külön azonosíthatóság, így hagyományos rendszernél külön hurkon egyéb esetben címezve. alkalmazzuk.

Működési elv szerint a következő fajtákat különböztetjük meg:

- Törőüveges, kapcsoló nélküli. Az üveglapon van a vezető fém, ha betörik, megszakad
- Törőüveges nem visszaálló, itt egy mikrokapcsoló adja a kontaktot
- Műanyaglapos két lépcsős mikrokapcsolós. Ez visszaállítható.

Felhasznált irodalom

1. Dr. Lukács György- Gábor László (szerk.): Új Vagyonvédelmi Nagykönyv, CEDIT 2000 Kft. Budapest, 2002, ISBN 963 8180 39 0
2. Liszkayné Dr. Nagy Éva Katalin (szerk.): Biztonságtechnika, Rendőrtiszti Főiskola, Budapest, 2008.
3. Élesztős László (főszerk.): Magyar Nagylexikon 4. kötet, Akadémiai Kiadó, Budapest, 1995. ISBN 963 05 6928 0
4. Halász György (főszerk.): Britanica Hungarica III. kötet, Magyar Világ Kiadó, Budapest, 1995. ISBN 963 7815 83 X
5. Hűvös Lajos (szerk.): Őrzés-védelem, ProLex Kkt. Budapest, 1995.
6. Mabisz ajánlás, Betöréses lopás- és rablásbiztosítás technikai feltételei, www.pluto.hu
7. Vagyonvédelmi Nagykönyv, CEDIT Információtechnikai Kft, Budapest, 1996.

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.