



ÓBUDAI EGYETEM  
ÓBUDA UNIVERSITY

**DOKTORI (PHD) ÉRTEKEZÉS**

---

**JURÁS ZSOLT**

# Az elektronikus vagyonvédelmi eszközök aktivitás fokozásának lehetőségei

Témavezető: Prof. Em. Dr. Berek Lajos

---

**BIZTONSÁGTUDOMÁNYI  
DOKTORI ISKOLA**

Budapest, 2023.12.15.

**Szigorlati/komplex vizsga bizottság:**

Elnök:

Prof. Dr. Pokorádi László

Tagok:

Dr. habil. Kovács Tibor

Dr. habil. Berek Tamás

**Nyilvános védés teljes bizottsága:**

Elnök:

Prof. Dr. Pokorádi László

Titkár:

Dr. Pető Richárd

Tagok:

Dr. Békési Bertold

Dr. Fialka György

Dr. habil. Farkas Tibor

Bírálok:

Dr. Őszi Arnold

Dr. Szűcs Endre

**Nyilvános védés időpontja:**

2024.

D12) Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

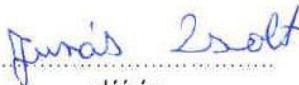
NYILATKOZAT

A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK MEGFELELŐ MÓDON TÖRTÉNT  
IDÉZÉSÉRŐL

Alulírott **Jurás Zsolt** kijelentem, hogy a **Tágabb értelemben vett elektronikai vagyónvédelmi eszközök aktivitás fokozásának lehetőségei**

című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2023.12.15.

  
aláírás

# TARTALOMJEGYZÉK

BEVEZETÉS .....	7
A tudományos probléma megfogalmazása .....	8
Célkitűzések.....	9
A téma kutatásának hipotézisei.....	10
Kutatási módszerek.....	11
Kutatás lehatárolása .....	11
1 OBJEKTUMVÉDELEM .....	13
1.1 Objektumok csoportosítása.....	13
1.1.1 Funkció szerinti csoportosítás .....	13
1.1.2 Objektumbiztonságot jelentősen befolyásoló tényezők szerinti csoportosítás .....	14
1.2 Az objektumvédelmében alkalmazott védelmi formák .....	15
1.2.1 Mechanikai védelmi alrendszer .....	15
1.2.2 Elektronikus védelmi alrendszer.....	21
1.2.3 Élőerős védelmi alrendszer.....	30
2 OBJEKTUMVÉDELEM KOMPLEXITÁSA .....	38
2.1 A védelem komplexitásának értelmezése lakóingatlanoknál .....	38
2.2 Energiatermelő nukleáris létesítmény objektumvédelme.....	42
2.2.1 Kritikus infrastruktúra az atomerőmű?.....	43
2.2.2 Nukleáris létesítmények veszélyeztettségének megállapítása .....	47
2.2.3 Atomerőművek őrzésének és védelmének fő feladatai .....	49
2.2.4 Nukleáris energiatermelő objektum komplex védelme .....	51
3 ÉLŐERŐ HATÉKONYSÁGÁT BEFOLYÁSOLÓ HUMÁN TÉNYEZŐK VIZSGÁLATA .....	55
3.1 A tervezési fázisból származtatható élőerős védelmi rendszer hatékonyságát befolyásoló tényezők .....	55

3.2	Az üzemeltetési fázisból származtatható előerős védelmi rendszer hatékonyságát befolyásoló tényezők .....	57
3.3	A humán kockázati tényezők komplex vizsgálata gyakorlati megközelítésben .....	60
3.3.1	Energiatermelő atomerőmű ellen elkövetett szabotázs elemzése .....	61
3.3.2	A világ legnagyobb gyémántbányájában elkövetett lopássorozat elemzése .....	62
3.4	Részkövetkeztetések .....	63
4	A TECHNOLÓGIA FEJLŐDÉSÉBŐL SZÁRMAZÓ BIZTONSÁGI KOCKÁZATOK, KIHÍVÁSOK .....	65
4.1	A dróntechnológia elterjedéséből jelentkező új kockázatok azonosítása és elemzése nukleáris létesítmények vonatkozásában .....	66
4.1.1	Kockázatok vizsgálata hipotetikus légi szcenáriók mentén .....	69
4.2	Az IoT technológia elterjedéséből jelentkező új kockázatok azonosítása és elemzése nukleáris létesítmények vonatkozásában .....	72
4.2.1	Okostelefon funkciói és kockázatai .....	73
4.2.2	Egy hipotetikus atomerőmű fokozottan őrzött üzemi területének IT eszközei .....	73
4.2.3	Kockázatok vizsgálata hipotetikus szcenáriók mentén .....	74
4.3	Részkövetkeztetések .....	77
5	AUTONOM MŰKÖDÉSŰ AKTÍV BEAVATKOZÁSRA IS KÉPES ELEKTRONIKUS VAGYONVÉDELMI RENDSZEREK .....	78
5.1	Autonóm elektronikai védelmi rendszer eszközeinek meghatározása .....	79
5.1.1	Nemhalálos fegyverek .....	80
5.1.2	Intelligens video analitika és video megfigyelési eszközök .....	82
5.1.3	Dróndetektáló, elhárító eszközök és a drón .....	84
5.1.4	A vagyonvédelemben alkalmazott eszközök továbbfejlesztési lehetőségei .....	89
5.2	Autonóm működésű aktív rendszerek kialakítási koncepciói .....	91

5.2.1	Belső elkövetők hatékony kiszűrése aktív védelmi rendszerekkel.....	91
5.2.2	Behatoló ártalmatlanítása aktív védelmi rendszerrel.....	94
5.2.3	Drónok az előerő szolgálatában.....	96
5.2.4	Drón detektálás és elhárítás .....	101
6	PRIMER KUTATÁS KÉRDŐÍVES ADATFELVÉTELI MÓDSZERREL.....	104
6.1	A primer kutatás módszertani leírása .....	104
6.2	A kutatásban résztvevő fegyveres biztonsági őrök eloszlása létesítményenként .....	105
6.3	A dróntechnológia ismertségére és a fegyveres erőknél szolgált időtartamra vonatkozó kérdések kiértékelése .....	105
6.4	A drónok védelmi rendszerbe integrálhatóságára irányuló kérdések kiértékelése .....	106
6.5	Gyakorlatok és képzések alkalmával készített drónos videófelvevételek jelentőségére irányuló kérdések kiértékelése .....	110
	ÖSSZEGZETT KÖVETKEZTETÉSEK.....	113
	Új tudományos eredmények .....	114
	Ajánlások .....	115
	IRODALOMJEGYZÉK .....	117
	RÖVIDÍTÉSJEGYZÉK.....	123
	TÁBLÁZATJEGYZÉK.....	124
	ÁBRAJEGYZÉK.....	125
	KÖSZÖNETNYILVÁNÍTÁS .....	126

## BEVEZETÉS

A XX. század utolsó évtizedének és napjaink informatikai, elektronikai és digitalizációs fejlődése rohamos léptéket öltött. Az életünk bármely területét nézve egyre több olyan elektronikus eszköz, megoldás jelenik meg, amely egyszerűbbé, hatékonyabbá és kényelmesebbé teszi a mindennapi életünket. Az ipari fejlődésben is kulcsfontosságú szerepet tölt be az elektronikai fejlődés, igazából nincs olyan szegmens, ahol a fejlődésnek ne az elektronikai ipar lenne a motorja. Új technológiák, iparágak jelentek meg, mint például a dróntechnológia, de az autóipar is nagy fejlődésen ment át. Megjelentek az elektromos hajtású autók, amik napjainkban már több mint 20 %-os piaci részesedéssel bírnak. Továbbá a gépjármű biztonság területén is számos új technológia vált alapfelszereltségé, mint a fékasszisztens, az adaptív tempómat vagy a sávtartó elektronika. Ezekről az autókról elmondható, hogy ha nem is teljes egészében, de bizonyos közlekedési helyzetekben a szenzorokra hagyatkozva működtetnek biztonsági berendezéseket, ezzel felülírva a gépjárművezetőt.

A nagyléptékű fejlődés megfigyelhető az elektronikus vagyónvédelmi rendszereknél is. Az analóg technológiák nem tették lehetővé a nagyszámú érzékelőt tartalmazó rendszerek alkalmazását, a többkamerás video megfigyelő rendszer képi tartalmának valós idejű rögzítését és korlátozott volt a távfelügyeleti állomáson megjelenített információk mennyisége. A digitalizáció megjelenésével és az informatika párhuzamos fejlődésével az analóg eszközök lassan kiszorultak a biztonságtechnika több területéről is. A technológia váltás eredményeként megjelentek a digitális és IP kamerák, a videóanalitikai alkalmazások, a biometrikus azonosítási eljárások a beléptető rendszerekben, a videó távfelügyeleti rendszerek és a rendszerek integrálhatóságának lehetősége. Sőt a videóanalitika területén megjelentek a gépi tanulási mechanizmusok alkalmazása is, ami lehetővé teszi a megfigyelt környezetben a deviáns emberi viselkedés érzékelését és azonosítását.

A biztonságtechnika és az autóipar is túlnyomó részt ugyanazon technikai vívmányokat alkalmazza a fejlesztések során, de a vagyónvédelmi rendszereknél mégse tapasztalható az olyan aktív beavatkozási képesség, mint az autóknál a ráfutás elleni védelem. A gépjármű orrába épített érzékelők alapján a túl kicsi követési távolság esetén figyelmeztet, majd a vezető reakciója hiányában helyzetfüggő fékezéssel lassítja, vagy veszély esetén meg is állítja az autót. Ezen felül még számos olyan funkciókkal

rendelkeznek a mai modern autók, amelyek aktívan beavatkozva felülbírálják a gépjárművezetőt, ezzel megalkotva a proaktív biztonsági funkciókat.

### **A tudományos probléma megfogalmazása**

Az autóipar és más iparágak dinamikusabban alkalmazzák az új technológiákat, míg a biztonságtechnika kisebb lépésekben halad. A gyakorlati alkalmazásoknál kibővült a kényelmi funkciók köre, de a komplex védelmi rendszerben még mindig jellemzően jelzési és riasztási funkciókat látnak el. Azokban az esetekben, amikor beavatkozó eszközöket alkalmaznak, azok funkciója a proaktív védelemre korlátozódik. Napjaink dinamikus fejlődésének velejárója, hogy az új kialakuló technológiák nem csak előnyöket jelentenek, hanem kockázatokat is hordoznak magukkal.

A legdinamikusabban fejlődő terület a dróntechnológia, aminek a használata már túlmutat a hobby jellegű felhasználáson. Sajnos a rosszindulatú felhasználásra is lehetőséget biztosít, aminek a számossága az elterjedés mértékével arányos. A rosszindulatú felhasználások elleni védekezés a nemzetállam számára kiemelten fontos létesítmények esetében elsődleges prioritásként kezelendő feladat.

A másik rohamosan fejlődő terület az infokommunikációs technológia (a továbbiakban: IKT) és a dolgok internete (Internet of Things: a továbbiakban IoT) technológia, ami külön-külön is új kockázatokat jelent az objektumok védelmében. Az IKT technológiák legelterjedtebb képviselői az okos eszközök (okos telefon, okos óra), amik az emberek mindennapi használati tárgyává váltak. Az iparban a termelékenység növelésének érdekében széleskörben alkalmazzák IoT technológiákat. A két technológia térben és időben egyszerre történő alkalmazása jelenti a felmerülő kockázatok alapját, amely már olyan mértékű, hogy az adminisztratív biztonsági intézkedéseken túlmutatnak. A gyakorlatban az adminisztratív intézkedések arra irányulnak, hogy a két technológia fizikailag el legyen választva. Legelterjedtebb megoldásként az okoseszközök bevitelét tiltják azon területekre, ahol ipari folyamatokat vezérlő IoT technológia található. A rezsimintézkedések betartásának ellenőrzését a biztonsági szolgálat végzi. Ennek a megoldásnak a hatékonysága sok esetben nem kielégítő.

A dróntechnológia szélkörű alkalmazhatóságának eredményeként, olyan fejlesztési irányok jelentek meg, amelyek alkalmassá teszik a biztonságtechnikai alkalmazásra, mint a védelmet segítő mobil eszközt.



Tudományos problémát jelent a fenti technológiák következtében megjelenő új kockázatok elleni hatékony és teljeskörű védelmi rendszerek hiánya az objektumvédelem területén. Továbbá az új technológiák biztonságtechnikai alkalmazásával olyan lehetőségek jelennek meg, amelyek lehetővé tennék az aktív beavatkozásra is képes elektronikus védelmi rendszerek kialakítását, de a biztonságtechnikai alkalmazásuk még mindig csak a jelzési, riasztási és elrettentési funkciókra terjednek ki.

### **Célkitűzések**

Az elektronikus vagyonvédelmi rendszerek széles körben alkalmazhatók, ami önmagában is további védelmi alterületekre osztható. A disszertációmban kizárólag az objektumvédelemhez közvetlenül kapcsolódó elektronikus védelmi eszközöket és rendszereket vizsgálom. Ezen belül is olyan területeket céloztam meg, ahol az aktív funkciók megvalósításának lehetősége valószínűsíthetőnek tűnik és hozzájárulhat a hatékonyabb komplex védelemi rendszer kialakíthatóságához.

Általános célul tűzöm ki, hogy áttekintsem a komplex objektumvédelemben alkalmazott védelmi alrendszereket és azok egymásra gyakorolt hatását. Valamint bemutassam különböző fenyegetettségű objektumok kockázatokkal arányos komplex védelmi rendszerét.

A kutatómunkám során célként fogalmazódott meg a napjainkban alkalmazott biztonságtechnikai eszköz és rendszerszintű vizsgálata, az aktív funkciókra való alkalmazhatóság tekintetében. Valamint a nem biztonságtechnikai elektronikus eszközök vizsgálata a vagyonvédelemi alkalmazhatóság szempontjából.

Célom a dróntechnológia biztonságtechnikai rendszerbe való integrálhatóságának vizsgálata.

Kutatási célom az élőerős védelmi alrendszer humánkockázati tényezőinek forrásoldali vizsgálata, valamint a dinamikus és statikus kockázati jelleg azonosítása.

Célom a technológiai fejlődésből származó objektumvédelmi kihívások és az új kockázatok jelenlétének igazolása.

Fő célom az aktív autonóm elektronikus vagyonvédelmi rendszerek koncepciójának és specifikációjának a meghatározása, valamint igazolni, hogy az autonóm rendszerek képesek a detektálási, a jelzési és riasztási funkciókon kívül elhárítási funkciókra is.

További célom, hogy az élőrös személyzet véleményét felmérjem az objektumvédelmi rendszerbe integrált aktív beavatkozásra is képes drón elfogadottságáról és alkalmazhatóságáról.

Célom felmérni az élőrös személyzet véleményét a madártávlati videofelvétel gyakorlati képzési célok hatékonyság növelési alkalmazhatóságáról és hasznosságáról.

## **A téma kutatásának hipotézisei**

### **Hipotézis 1**

Feltételezem, hogy napjainkban még mindig jelen vannak a komplex védelmi rendszerekben olyan élőrő hatékonyságát befolyásoló humán tényezők, amelyek számottevő kockázatokat jelentenek a védelmi rendszer egészére.

### **Hipotézis 2**

Feltételezem, hogy az elektronikai, az IT eszközök fejlődésével, valamint a világ nagyléptékű digitalizációjával új jelentős mértékű kockázatok jelennek meg az objektumvédelem vonatkozásában, amelyek csökkentésére még nincsenek műszaki védelmi intézkedések bevezetve.

### **Hipotézis 3**

Feltételezem, hogy kialakíthatók, olyan aktív autonóm elektronikus vagyónvédelmi rendszerek, amelyek alkalmasak a humán és a technikai fejlődésből származó kockázatok megszüntetésére vagy csökkentésére, valamint a komplex védelmi rendszer hatékonyságának növelésére.

### **Hipotézis 4**

Feltételezem, hogy a fizikai védelmi rendszer támogatására bevezethető új rendszerelemként integrált aktív autonóm drón a komplex védelmi rendszerben pozitív megítélésű az élőrös személyzet részéről.

### **Hipotézis 5**

Feltételezem, hogy a drónnal támogatott gyakorlati képzések végrehajtása nyomán az élőrő hatékonyabban képezhető, ezáltal a képzettségi szintje növelhető.

## **Kutatási módszerek**

Kutatásom módszertani alapját az irodalomkutatás, az adatelemzés és értékelés, valamint a szakmai tapasztalataimból származó kutatási eredmények alkotják.

Értekezésem elkészítése során elsősorban a komplex védelmi rendszerek témakörben született műszaki kutatási eredmények tanulmányozását, feldolgozását és elemzését végeztem el. Az értekezésemben a már létező és publikált tudományos eredményekre alapozva végeztem a szekunder kutatásaimat, amely fő irányvonala az objektumvédelem komplexitásának részletes bemutatása a primer kutatási fázis megalapozása céljából. Az indukción és a dedukción módszerét váltakozva alkalmaztam a kutatásaim során a komplex összefüggések megállapításához és a célként definiált következtetések meghatározásához. Az indukción módszerét alkalmaztam a komplex objektumvédelem feladatainak összegzése során,

A szekunder kutatási fázisban a gyakorlati tapasztaltok feldolgozását és értékelését végeztem el. Az empirikus kutatásnál a kvantitatív módszert alkalmaztam, azon belül az adatfelvételi eljárások közül a kérdőíves módszert választottam.

## **Kutatás lehatárolása**

Célom a disszertáció megírásával nem az volt, hogy mindegyik tudományterület legmélyebb ismereteit sajátítsam el, hanem ezen területek összefüggéseit, egymásra gyakorolt hatásukat, és a fejlődő technológiáknak köszönhetően az elektronikus vagyonvédelem aktivitás fokozásának lehetőségeit bemutassam.

A szekunder kutatási fázis során egyértelművé vált, hogy nem csak a technikai megoldások relevánsak a téma feldolgozása szempontjából és a felsorakoztatott „indító események” kiváltását generáló berendezések működési elvéből, elhelyezkedéséből és a védelmi rendszerben betöltött védelmi vonal mélységének szempontjából másodlagos jelentőségűek, mivel az összes eszköz egy indító jelet szolgáltató szenzorként értelmezhető. A kutatás szempontjából sokkal fontosabb területként azonosítottam a felhasználhatóság kérdéskörét és így a magánbiztonság területén belül a magánszemélyek tulajdonát képező objektumok további kutatását csak korlátozottan vettem figyelembe. Nagyobb hangsúlyt az ipari létesítmények védelmének a kiegészíthetőségére és optimalizálhatóságára fordítottam. Az ipari létesítmények közül is az olyan létfontosságú létesítményeket választottam, ahol 24 órás szolgálatban lévő Fegyveres Biztonsági Őrség

(a továbbiakban: FBŐ) látja el az előerős védelmi tevékenységet. A területen folytatott irodalomkutatás arra ösztökélt, hogy mélyebben vizsgáljam a drónok felhasználhatóságának, a védelmi rendszerbe integrálhatóságának, valamint az élőerő és a technikai rendszer kapcsolódásának lehetőségeit a komplex védelem funkciói mentén. A téma feldolgozásának első lépéseként a drónok alkalmazhatósági kérdéseit vizsgáltam a városok, illetve az okosvárosok vonatkozásában, a kritikus infrastruktúrák üzembiztonsági kérdései, valamint a hatékonyságnövelési lehetőségei tekintetében. Ezen kutatások és publikációk eredményei csak közvetetten jelennek meg a dolgozatomban.

A kutatásomhoz és disszertációmhoz nyílt forrásból származó információkat használtam fel. A kutatásaimat 2023. 06. 28-án fejeztem be, ekkor a felhasznált elektronikus irodalom elérhető volt.

# 1 OBJEKTUMVÉDELEM

Az elektronikus védelmi rendszerek legteljesebben az objektumok őrzése és védelme során jelentkeznek. Ezért mintegy a bevezetés folytatásaként szükségesnek tartom a téma vázlatos áttekintését. Az objektumok védelme vagy másnéven objektumbiztonság az egyik legnagyobb és egyben szétágazóbb területe a vagyonvédelemnek. Vagyonvédelmi szempontból az objektumok létesítmények, épületek, bekerített vagy bekerítettlen, de jól beazonosítható területek, amelyek valamilyen mértékű veszélyeztetésnek vannak kitéve és azokat biztosítani kell. Az objektumok védelme, akkor tekinthető megfelelőnek, illetve teljesnek, ha az őrzési és védelmi feladatok megvalósítása egy komplex védelmi rendszeren keresztül kerül kialakításra. A komplex védelem egy korábbi megfogalmazás szerint az őrzésre és védelemre rendelkezésre álló erők és eszközök összehangolását jelenti. Napjainkban azonban a védelmi rendszerek kialakításának az alapját a kockázatelemzés és kockázateértékelés adja. Ennek elvégzése után határozzuk meg, hogy milyen védelmi szintet kívánunk elérni és ehhez rendeljük hozzá a technikai és élőerős védelmet. A technikai védelem alatt a mechanikai és az elektronikus alrendszereket kell érteni. A három alrendszer megfelelő arányú használata adja a teljes rendszer komplexitását. [1]

Az objektum fogalmából kiindulva nagyon sokféle objektum típust lehet azonosítani ezért érdemes azokat jellemzőik alapján csoportosítani.

## 1.1 Objektumok csoportosítása

Az objektumvédelem tervezése, kialakítása során az egyik legfontosabb feladat, a biztonságra ható tulajdonságainak a feltérképezése. Meg kell vizsgálni az objektum biztonsági szempontú jellegzetességeit, működési sajátosságait, a benne zajló tevékenységet, ami egyben a létesítmény funkcióját is meghatározza. A vizsgálat lefolytatását követően az objektumokat több rendezőelv alapján lehet csoportosítani.

### 1.1.1 Funkció szerinti csoportosítás

Az objektumok funkció szerinti csoportosítása a biztonságot befolyásoló tényezők függvényében:

- **Középületek:** Ezen csoportosításba tartoznak a közhivatalok, az államigazgatási, a civil társadalmi szervezetek létesítményei, épületei. Jellemzőjük, hogy valamilyen nyitvatartási rend mentén dolgozók és ügyfelek (állampolgárok) személyi forgalma van jelen az objektumban.

- Civil, magánépületek: A hétköznapi élet szükségleteit kiszolgáló lakóépületek sorolhatóak ide, mint a tanyák, nyaralók, családi házak, sorházak és lakótelepi lakóépületek. Felhasználás szempontja szerint egy csoportba soroltam az ingatlanokat, de a biztonságot meghatározó jellemző paramétereik kisebb-nagyobb mértékben eltérőek lehetnek.
- Kommunális létesítmények: A közösségi élet folytatására alkalmas bármely olyan épületet ide lehet sorolni, amely valamilyen időintervallum erejéig teret és megfelelő feltételeket kínál az emberek számára az ott tartózkodáshoz. Ilyenek lehetnek a kulturális létesítmények, a mozik, az éttermek, a stadionok, a plázák és a színházak.
- Speciális objektumok: A vagyonvédelmi tevékenységek folytatása szempontjából az általános objektumvédelmi megoldásokon túl egyéb speciális csak, arra az objektum típusra jellemző biztonságtechnikai megoldásokat kell alkalmazni. Ide sorolhatóak a pénzintézetek, (bankok, takarékpénztárak és a pénzváltók) a kórházak és a szállodák.
- Ipari létesítmények: Túlnyomó részt valamilyen termelési folyamatot megvalósító gyáregységeket lehet ide sorolni, de ide tartoznak a raktárak, logisztikai központok és akár a veszélyeshulladék tárolók is.
- Kritikus infrastruktúrák: A technológiai fejlődés és a társadalmi ellátási lánc szoros kapcsolata következtében kialakultak olyan rendszerek, létesítmény csoportok, amelyek kiemelten fontos szerepet töltenek be a nemzeti stratégiai feladatok ellátásában. Nézzünk néhány létfontosságú létesítményt az objektumvédelem tekintetében: - villamos erőművek, - kőolajfinomítók, - gyógyszergyárak, - veszélyes hulladék tárolók, - vízművek stb.

### **1.1.2 Objektumbiztonságot jelentősen befolyásoló tényezők szerinti csoportosítás**

A létesítmények által ellátott funkciók alapvetően határozzák meg az objektumvédelem kialakítását, azonban ezen felül is vannak jelentős hatású sajátos jellemzői az építményeknek. A legmeghatározóbb jellemzők szerint az alábbi csoportokba sorolhatók:

- Objektumok elhelyezkedése szerin: A létesítmények elhelyezkedése alapján négy területet lehet megkülönböztetni, amelyek elsősorban a veszélyeztetettség mértékére vannak a legnagyobb hatással. Az ingatlanok lehetnek lakott területen kívül, közigazgatási területen belül, lakott területen és ezen belül még lehet város központi részen.

- Működési-és beléptetési rend alapján: A védelem tervezése szempontjából meghatározó szerepe van annak, hogy folyamatos vagy szakaszos működésű a védendő objektum. A beléptetés rendje pedig meghatározza azt is többek között, hogy szükséges-e, és milyen jellegű ellenőrző, áteresztő pontok kialakítása válik indokolttá. Ezek alapján a belépés lehet szabad, belépőjegyhez kötött, belépési engedély meglétéhez kötött és meghívásos alapú.
- Az élőerős védelmet végrehajtó személyzet alapján: Az élőerős védelmi feladatokat ellátó személyeket általánosságban biztonsági őrknek jelöli meg a szakirodalom. Annak függvényében, hogy milyen jellegű objektumvédelmi feladatot lát el, megkülönböztetünk vagyonőri, fegyveres vagyonőri és fegyveres biztonsági őri tevékenységeket. A megfelelő előre kiválasztását törvényi előírások határozzák meg. Továbbá az élőerő megvalósulhat a tulajdonos által, vállalkezési szerződés keretén belül, valamint rendvédelmi szervezetek bevonásával.

## **1.2 Az objektumvédelmében alkalmazott védelmi formák**

Az objektumvédelem során minden lehetséges kockázati tényezővel számolni kell, ezért javasolt a vagyonvédelemi alrendszerek tagozódás szerinti vizsgálatát elvégezni. Az elektronikus rendszerek integráltságának növelésével az objektumvédelem alapbiztonsági igényein túl egyéb szükségletek is kielégíthetőek, valamint megfelelő archiváltság mellett a későbbiek során visszakereshetőek adatok és információk. Az objektumvédelmi rendszer ilyen jellegű kialakításához a három vagyonvédelmi alrendszert és azok egymásra való hatását kell vizsgálni. [2]

### **1.2.1 Mechanikai védelemi alrendszer**

A mechanikai védelmi elemek alkalmazásával a vagyonvédelmi rendszerek tekintetében több alapfunkcióról beszélhetünk. A mechanikai védelem célja a behatolás késleltetése, (akadályozás, esetleg megakadályozás) az elektronikus védelem jelzőrendszerei által értesített élőerős védelem helyszínre érkezéséig, beavatkozásig. Másodlagos funkciója az elriasztás, elrettentés az alkalmi elkövetők szándékának befolyásolására. [3]

Mechanikai védelem fő területei:

- A kültéri védelem
- Építményvédelem
- Mechanikai tárgyvédelem [1]

### 1.2.1.1 Kültéri mechanikai védelem

A kültéri védelem tekintetében alapelv, hogy a zárt, bekerített jellegű objektumok esetében a védendő terület kerítéssel kell körül venni, ami egyben jelzi a terület határát is. A gyakorlatban és általánosságban is ez a mechanikai gát a leggyakrabban kiépített rendszer. A létesítmény jellegétől, kiterjedtségétől, illetve komplexitásától függően akár külső és belső kerítések alkalmazása is szükségessé válhat, így létrehozva több védelmi vonalat. A kerítések mellett a leglényegesebb passzív mechanikai gátak lehetnek az árkok, torlaszok, tüskés drótok és pengés drót, valamint a bóják. Az objektum védelmének érdekében az illetéktelen behatolás ellen kialakított passzív mechanikai akadályok mellett aktív mozgatható gátakat is kell alkalmazni az oda illetékes személyek, gépjárművek bejutása érdekében. Az aktív mechanikai gátak közé sorolom be a kapukat, sorompókat, mozgatható bójákat, aktív úttorlaszokat és forgókereszteket.

A kerítésekkel szemben támasztott követelmények több helyen is fellelhetők akár a Magyar Biztosítók Szövetsége (továbbiakban: MABISZ) ajánlások között, de az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló kormányrendeletben is. Mindkét helyen a védelmi képességeknek megfelelő követelményekhez mérten vannak meghatározva a kerítésekkel szembeni elvárások a leküzdési idő tekintetében. Továbbá védelmet kell biztosítani többféle támadási módszerrel szemben is. Ilyen támadási módszerek lehetnek az átmászás, az átvágás és a kerítés megemelésének segítségével az alatta való átbújás. A kerítésekkel szembeni követelmények, hogy beton alapja legyen, ami alacsonyabb védelmi szint esetén lehet pont alap, de magasabb védelem esetében minimum 50 cm mély vasbeton sávalap kell legyen. A magasságuk 1,8m és 2,8 m között van meghatározva, veszélyes ipari létesítmények esetében 3 m magasságig kiegészítve szöges vagy pengés dróttal, ami egyben az átmászás elleni védelmet is fokozza. Anyaga többféle is lehet preferálva a vasbetont vagy a fém kerítés elemeket, ugyanakkor nem kizárt a fa és a téglá anyagú kerítés sem. A lakóingatlanok telekhatárán épített utcafronti kerítések esetében a biztonsági funkció megtartása mellett szem előtt kell tartani az esztétikai jellemzőket is, amely egy példáját az 1. ábrán láthatjuk.





1. ábra - Lakossági utcafronti kerítés [4]

Az ipari létesítmények, kritikus infrastruktúrák kerítéseinek kialakításakor fontos a fixen telepített kerítéselemek és a kerítések részét képező kapuk, áteresztési pontok mechanikai védelmi egyenszilárdsága. A 2. ábrán látható kép jól bemutatja a gyalogos és gépjárműforgalom számára is kialakított beléptetési pontot. Véleményem szerint az ilyen jellegű kialakítás megfelel a mechanikai egyenszilárdság kritériumának.



2. ábra - személy-és gépjármű beléptetési pont [5]

A szakaszosan jelentkező nagy gépjárműforgalom lebonyolítására a legalkalmasabb megoldás a kapuk és a sorompók kombinációjával kialakított beléptetési, megállítási pontok alkalmazása. Ennek szemléltetése céljából egy távolabbi fotót készítettem, ami a 3. ábrán látható. A kapu becsukható az alacsony vagy forgalommentes állapotban, így biztosítva a terület zártságát, védettségét. Megemelkedett forgalom esetében a nyitott kapu mellett, akár zsiliprendszerként is működtethető sorompó páros a területre érkező gépjárművet megállásra készíti, ami lehetővé teszi a gépkocsi és a vezető személy

ellenőrzését. Magas veszélyeztetettségű létesítmények esetében lehet szükséges ez a megoldás.



3. ábra - Komplex ellenőrzési pont kapu és sorompó zsilip vegyes alkalmazásával  
A létesítményekhez vezető út jellegétől és a környezeti jellemzőktől függően szükségessé válhatnak további mechanikai védelmi gátak kialakítása. A belátás és a gépjárművel való kerítésen keresztüli behatolás elleni védelmi képesség fokozása céljából alkalmazhatóak árkor, természetes és mesterséges torlaszok. Valamint a gépjárműforgalmat lebonyolító ellenőrzési, áteresztési pontok ellenállóképességének fokozása is megvalósítható aktív úttorlasszal, ami különböző paraméterek mentén vezérelhető. Kialakítható olyan rendszer megfelelő elektronikai vezérléssel, hogy abban az esetben emelkedik ki az útburkolat síkjából az úttorlasz, amikor feltételezhetően a közeledő jármű ártó szándékkal megállás nélkül akar behajtani a védett területre. A nagy terhelhetőségű úttorlaszok tehergépjárművek feltartoztatására is alkalmasak.



4. ábra - Aktív és passzív úttorlasz [6]

### 1.2.1.2 Építmény mechanikai védelme

Az építmények közül a műtárgyak kivételével minden, olyan az ember által létrehozott épületet sorolok ide, amely emberek tartózkodására, rendeltetészerű azaz munkavégzés vagy tárolás céljából lett létrehozva. Az építmények védelme a héjszerkezetükre és az azokon található nyílászárókra lehet összpontosítani a mechanikai védelem vonatkozásában. Az épületek héjszerkezetének – falak, födém és aljzat – a mechanikai állóképességének a meghatározására szintén az áthaladásukhoz szükséges idővel lehet a legkönnyebben definiálni. A leggyakoribb áthatolási módszer a robbantás és a falbontás módszere. Az utóbbi módszer alkalmazása esetében speciális szerszámokra van szükség, amelyekkel szembeni állóképesség konkrétan meghatározható.[7] Több helyen is fellelhetőek a falazatokkal és födémekkel szembeni követelmények, de összerendezett adatokat, mint a falazatok anyaga, vastagsága és az áthatolási idő nem találtam, ezért azt az 1. számú táblázatba foglaltam össze. [8]

Ellenálló képesség	Behatóló	minimális kialakítás	Feltartoztatási idő	Alternatív kialakítás
nagyfokú mechanikai ellenálló képesség	speciális eszközökkel felszerelt	38 cm vastagságú tömör téglafal	minimum 15 perc	12 cm vastag, Ø8-10 mm es és 15 x 15 cm-es rácsosztású HD háló, C 12/15 minőségű beton
Jelentős mechanikai ellenálló képesség	speciális eszközökkel felszerelt	15 cm vastagságú tömör fal	minimum 10 perc	6 cm vastag, Ø6 mm es és 15 x 15 cm-es rácsosztású HD háló, C 12/15 minőségű beton
Mechanikai ellenálló képességgel rendelkezik	hagyományos kéziszközökkel felszerelt	6 cm vastagságú tömör téglafal	minimum 5 perc	Minimum 10 cm vastagságú speciális kétrétegű könnyűszerkezet, a rétegek között hőszigetelő, tűzálló vagy mechanikai ellenálló képességet biztosító egyéb anyaggal
Korlátozott mechanikai ellenálló képességgel rendelkezik	hagyományos kéziszközökkel felszerelt	nincs megadva anyagjellemző, akár könnyűszerkezetes építésű is lehet	minimum 3 perc	-----

1. táblázat - Mechanikai ellenálló képesség paraméterei összefoglalás

Az ablakok elsődleges funkciója, hogy kapcsolatot biztosítsanak a zárt belső tér és a külső környezet között úgy, hogy közben biztosítsák a külső környezeti hatások elleni védelmet, valamint nyitott állapotukban biztosítsák a megfelelő légcserét. Az ajtók méretbeli és mechanikai kialakítása minden esetben az áthaladó forgalom megfelelő

biztosításához mérten van kialakítva. [9] A lakóingatlanokkal szembeni jogtalan behatolásokat illetően a kriminalisztikai statisztikák alapján, nem meglepő módon a leggyakoribb elkövetési mód a nyílászárók roncsolásos felfeszítése, benyomása és betörése, valamint a zárok fúrása fészítése és törése. [10] Az elkövetési módok és a nyílászárók keresztüli behatolási gyakoriságból nem nehéz, arra a következtetésre jutni, hogy azoknak is minimum akkora feltartoztatási idővel kell rendelkeznie, mint az objektumok héjszerkezetének. Az ajtók esetében biztonságosnak tekinthető, ha minimum 40 milliméter vastagságú keményfából készült, biztonsági zárral van ellátva és oldalanként legalább három helyen a fal szerkezetébe 150 milliméter mélyen rögzítve van. Az üvegezett felületű ajtók, ablakok ellenálló képessége redőnyökkel, biztonsági fóliákkal, de leginkább rácsokkal növelhető meg. A kiválasztott megoldás szinte teljesen mindegy csak az fontos, hogy például egy ráccsal megerősített ablaknál elérjük a védelmi szintnek megfelelő késleltetési időt, ami a környezetében lévő fallal megegyező. Természetesen léteznek átdobást gátló üvegek, rácshelyettesítő és lövedékálló üvegek is, [7] de ezek bekerülési költsége olyan mértékben növelheti meg a védelemre fordított költségeket egy alacsony veszélyeztetettségű objektum esetén, hogy felborul az arányosság elve. A redőnyök alkalmazása csak akkor tekinthető biztonsági megoldásnak, ha azok visszatolás gátlóval is rendelkeznek. A külső ajtókat és kapukat leemeléssel ellen biztosítani kell. Az ajtók egyik legfontosabb biztonsági eleme a zár. A zár egy olyan általában mechanikai elven működő szerkezet, mely a hozzá tartozó kulcs segítségével rögzíti az ajtólapot a tokhoz. Kialakításuk szempontjából egybeépített és hengerzárbetétes zárszerkezeteket különböztetünk meg. Az egybeépített zárok közül csak azon egy vagy kéttollas zárat lehet biztonsági zárnak tekinteni, amelyek változó profilozásúak és a tollak egyszerre legalább öt vagy több lamellát mozgatnak. [1] Több különböző épületet magába foglaló létesítményeknél jellemző a vezérkulcsos vagy a főkulcsos zárrendszer alkalmazása. A főkulcsos zárrendszereknél egy kulcs nyitja az összes zárszerkezetet míg a többi kulcs, csak egy bizonyos zárat. A vezér vagy másnéven királykulcsos zárrendszereknél felépíthető például a szervezeti struktúrához is illeszthető hierarchikus rendszer.



5. ábra - Egybeépített biztonsági zár és biztonsági zárbetét [11] [12]

### 1.2.1.3 Mechanikai tárgyvédelem

Az objektumok mechanikai védelmének harmadik vonalát képezhetik a tárgyvédelemre kifejlesztett speciális értéktároló eszközök. Értéktárolásra alkalmazhatóak a fixen telepített lemezszekrények, pánccs szekrények, értékmegőrző kazetták, valamint a hordozható értékszallító bőröndök. Mindegyik eszközre elmondható, hogy akkor van szükség az alkalmazásukra, ha kis sűrűségben nagy érték koncentrációról van szó. Jellemzően nagy mennyiségű készpénz, műtárgy, értékes nemesfém ill. ékszer, továbbá lehet még értékes információ és radioaktív sugárforrás is a védendő tárgy, eszköz. Az értékmegőrző berendezésekkel szemben követelmény a rögzítettség, vágás-és fűrészállóság és a biztonsági zárok alkalmazása. A késleltetés mértéke arányos a megóvni kívánt eszköz értékével. Az európai és a hazai szabványok, valamint a biztosítói ajánlások több kategóriába sorolja az értékmegőrzőket.

### 1.2.2 Elektronikus védelmi alrendszer

A szakirodalomban elektronikus védelmi rendszernek, elektronikus vagyonvédelmi rendszernek és elektronikus jelzőrendszernek is nevezik a vagyonvédelem ezen területét. A legjellemzőbb megnevezésnek én az elektronikus jelző-és riasztó rendszer elnevezést tartom, de a vagyonvédelem tagozódásának bemutatásakor a legelterjedtebb kifejezés az elektronikus védelmi alrendszer. A rendszer feladatát és funkcióját tekintve mindazon elektronikus működésű eszközöket kell ebbe a technikai alrendszerbe sorolni az objektumvédelem vonatkozásában, amelyek jelzik az objektum területére, azaz a védett területre való illetéktelen behatolást vagy annak kísérletét és a védett értékek eltulajdonítási kísérletét. [1]

Az elektronikai védelmi eszközökből felépített objektumvédelmi rendszerek már önmagukban is hatékony önálló alrendszereket alkotnak, úgymint:

- · behatolás jelző rendszerek
- · periméter védelemi rendszerek
- · beléptető rendszer
- · video megfigyelő rendszer

Az elektronikai rendszerek fejlődése azt hozta magával, hogy nem minden esetben elegendő a rendszereket önállóan telepíteni, hanem azokat rendszerintegrációs módszerek segítségével - akár eszköz, akár rendszer szinten – komplex elektronikai védelmi rendszert alkotva kell alkalmazni. Ennek megfelelően a következőkben először a rendszereket magukat majd a védelem horizontális síkján mozogva a védelmi vonalak mentén fogom a témakört körül járni. [2]

#### 1.2.2.1 Behatolás jelző rendszerek

A behatolás jelző rendszerek célja és feladata a behatolás detektálása és a helyi környezet, illetve a távfelügyelet számára történő jelzés generálása, oly módon, hogy a mechanikai gáta által biztosított késleltetés letelte előtt a helyszínre tudjon érkezni a reagáló erő. A jól megtervezett behatolás jelző rendszer képes az elrettentési, detektálási funkciók maradéktalan ellátására. Ezek a klasszikus vagyónvédelmi központokból, a bementi zónáira kötött érzékelőkből, a kezelő egységből, a kimentén található hang-fényjelző eszközökből és a kommunikációs egységekből összeállított rendszer. [13] A védelmi koncepció kialakításakor a védendő objektumhoz és az egyéb védelmet befolyásoló tényezőkhöz kell igazítani a behatolás jelző rendszert. A több építményt magába foglaló objektumok védelmének kialakításakor célszerű tagoltan, épületenként egy-egy behatolásjelző központot alkalmazni. A külön-külön kiépített alrendszereket egy jelhálózatba kell kialakítani, amelyre egyesével fel lehet csatlakoztatni a kiépítésre kerülő védelmi alrendszereket. A jelhálózatot és a rendszerek betáplálását szolgáló elektromos hálózati infrastruktúra szegmentált kialakítása szintén indokolt és emellett biztosítani kell a visszahatás mentességet is. Tekintsük át az alrendszer funkcionális főbb egységeit röviden.

Behatolásjelző (riasztó) rendszer főegységei:

- Központi egység:

A központi egység fogadja és feldolgozza a rákapcsolt érzékelők jelzéseit, a hálózati tápegységgel és akkumulátorral kialakított betápláláson keresztül

biztosítja a teljes rendszer részére az áramellátást, behatolás esetén vezérli a szirénát és biztosítja a felügyeleti központ felé az online átjelzést.

➤ Kezelő egység:

A riasztórendszert a hozzá csatlakoztatott kezelőegységgel tudjuk ki- és bekapcsolni számkódokkal. A be- és kikapcsoláson túl rendszerállapotról képezhet jelzéseket: például nyitva maradt egy ablak; áramszünet van; esetleg a telefonvonallal van probléma.

➤ Érzékelők:

A riasztórendszerek alapegységei a különféle érzékelők. Egy teljes biztonsági rendszert a mélységi védelem elvének megfelelően kell kialakítani, melynek szintjei kívülről befelé haladva a következők: kültéri eszközök, felületvédelmi eszközök, belső térvédelmi eszközök, tárgyvédelmi eszközök és személyvédelmi eszközök.

➤ Szirénák:

Kültéri és beltéri szirénákat különböztetünk meg. A kültéri sziréna a környezet felé jelzi az esetleges behatolást, és felhívja a figyelmet a normálállapottól való eltérésre. A beltéri sziréna közvetlenül a behatolóra hat. Hirtelen megszólaló éles hangjelzésével sokkhatást képes előidézni. A kültéri szirénákba beépített fényjelzés a riasztás helyére hívja fel a figyelmet. [2]

#### 1.2.2.2 Periméter védelmi rendszer

A periméter védelmi rendszerek kialakítására az objektumot körül határoló kerítés mechanikai szerkezetein kerülhet sor. A rendszer elsődleges feladata a kerítés, mint mechanikai gáton keresztüli behatolás detektálása pontos helymeghatározással és a lehető legkorábbi időpontban. A kerítések szabotálása igen sokféle módon történhet, amelyeknél a védelmi rendszernek az összes eshetőségre választ kell adnia. A rendszer kiépítésekor többszintű védelmi vonal alakítható ki. Lehet előjelző rendszert létesíteni, ami a kerítés megközelítésekor már jelzést ad. Az átmászás, mint elkövetői módszer elleni védelem kialakítására is számos műszaki megoldás kínálkozik. Továbbá a kerítés belső oldalára, illetve közvetlen közelében is többféle kültéri érzékelő alkalmazható. Tehát a periméter védelmi rendszer kialakításakor egy többretegű és egymásba ágyazódott rendszer kialakításában érdemes elgondolkodni, mivel a technikai eszközök nagyon sokféle lehetőséget nyújtanak, de egyben nagyon speciálisak és csak egy szűk keresztmetszetben

alkalmazhatóak. Az egyes rétegek akár az elektronikus vagyonvédelem egy komplett területét is jelentheti. Az angolszász nyelvterület biztonsági terminológiájából származó „5-D” szabály alkalmazásának fontosságára érdemes figyelni. A szabály az elrettentés, detektálás, megtagadás, késleltetés, védekezés angol szavak kezdőbetűit jelenti, amelyek gyakorlatilag nem mások, mint a fizikai védelmi funkciók. Vegyük sorra azokat a funkciókat, amelyek az elektronikus védelmi rendszerekkel valósíthatóak meg. [2]

### Elrettentés

A funkció megvalósítását tekintve, már maga a kerítés, mint mechanikai gát a robusztusságával is képes ellátni, de vannak elektronikus megoldások is. Amennyiben a jogtalanul behatolni szándékozó személy szembe találja magát a kerítés külső felén 1,5 méterre a kerítéstől egy akusztikus hangos figyelemfelhívással, akkor a behatolók egy csoportja biztosan elgondolkodik, hogy érdemes-e újra próbálkozni.

### Érzékelés

A detektálási funkció megvalósítása igen sokféle képen megvalósítható. A kerítésen kívüli területeken kialakítható egy megelőzési zóna az érzékelők diverz alkalmazásával. Érzékelőként alkalmazható, akár egy kamera megfelelő video analitikával. Minden esetben tanácsos lépcsőzetes érzékelési rendszert építeni, amely legalább két különböző technológiát használ, csökkentve a kényelmetlen zavaró riasztások számát.

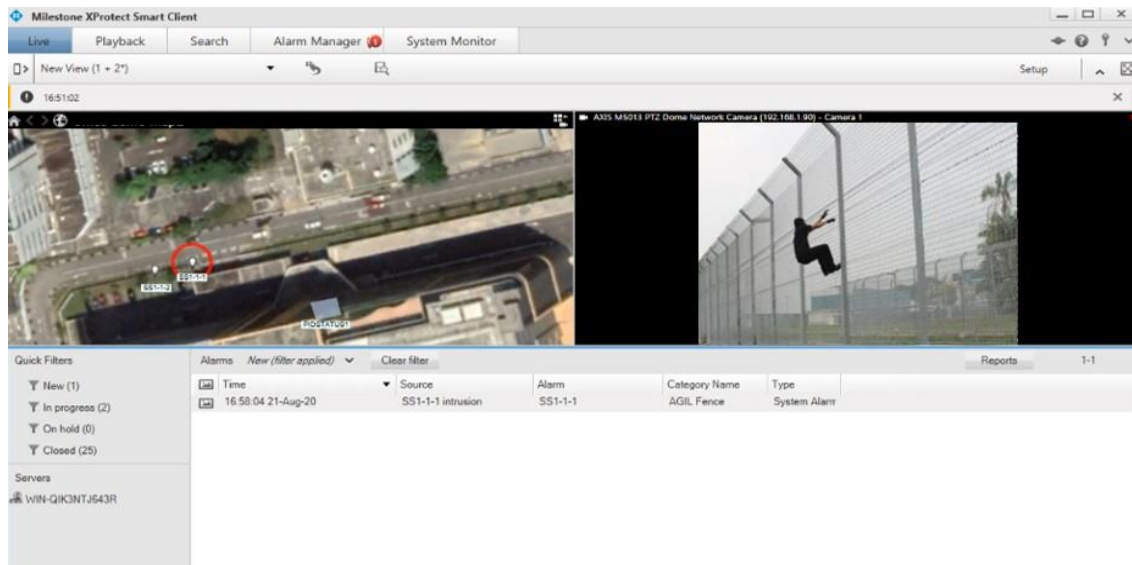
### Tiltás

Eddig a pillanatig a folyamatnak csak szemlélői voltunk, remélve, hogy az elrettentés elegendő lesz, de ha a detektáló rendszer jelez, akkor aktiválni kell a tiltási funkciót. A hatékonyan és gondosan megtervezett rendszerek nem csak a behatolási kísérleteket kell tudnia érzékelni, hanem segítségek kell nyújtsanak a behatolás természetének és szándékának a megállapításában. Amennyiben egy ilyen rendszerünk van kiépítve, akkor jobban meg tudjuk határozni a veszélyeztetettség mértékét is. A tiltás funkció szintén egy érzékelő és egy akusztikus átbeszélő segítségével könnyen megvalósítható. A különbség az elrettentéshez képest az akusztikus üzenet tartalmában van. Ebben az esetben már határozott és konkrét tiltások hangzanak el, ami felhívja a behatoló figyelmét arra, hogy az élőerős elhárítás fizikai kényszert fog alkalmazni.

A rendszer kiépítése az érzékelőtől egészen a megjelenítésig terjed a jelátviteli és átalakító hálózaton keresztül. Ne feledjük, hogy nagyobb kiterjedésű létesítmények



esetében a kerítések hossza több kilométer is lehet, ezért itt már csak digitális jelátvitellel valósítható meg a jelzés eljuttatása az élőerős személyzethez. A személyzet számára a megjelenítési módok közül a síktérképes szoftveres megoldás a legjellemzőbb.



6. ábra - Felügyeleti állomáson a periméter védelmi rendszer megjelenítése [14]

### 1.2.2.3 Beléptető rendszer

A beléptető rendszer célját és feladatát legjobban a fogalma tükrözi:

„Komplex elektromechanikai-informatikai rendszer, amely telepített ellenőrző pontok segítségével lehetővé teszi objektumokban történő személy-és járműmozgások hely -, idő-és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését. A szerkezeti elemeken túl tartalmazza azokat az intézkedéseket és apparátusokat melyek az üzemeltetéshez és a beléptetés felügyeletéhez szükségesek!” [15 p 18]

A beléptető rendszer fő részei:

- Olvasó
- Vezérlő
- Felügyeleti rendszer

A beléptetés folyamata: azonosítás, belépési jogosultság eldöntése, áteresztő pont nyitása, detektált áthaladás, visszazárás. Ezekon felül további feladat az eseménynaplózás és rendszerfelügyelet. [15] A belépési folyamatot alapul véve kijelenthető, hogy a beléptető rendszereknek három fő funkciója van. Az ellenőrző pontokon való áthaladás jogosultságának megállapítása, az áthaladó azonosítása és az áthaladás szabályozása. Az

objektumok beléptető rendszereinek kialakításakor a fő funkciókon kívül számos követelménynek kell megfelelnie. Az összetettebb nem csak egy beléptetési ponttal és több különböző védelmi zónával rendelkező objektumoknál a beléptető rendszertől elvárható a térben és időben lehatárolt jogosultság kezelése. Továbbá a csoportos zónakezelésen kívül az egyedi területi beállítások alkalmazása. Ipari környezetben nem ritka, hogy a gyártási folyamatok egy telephelyen belül, több üzemben valósul meg feladatszelektíven, így az egyik üzem munkavállalójának nincs szüksége a másik üzem területére történő belépésre és természetesen ez fordítva is igaz. A beléptető rendszer ilyen jellegű kialakítása teljes mértékben támogatja a szükséges és elégséges elvet, de vannak olyan egységek is, ahol ennél magasabb szintű védelmet az irányfigyeléssel valósítanak meg. Egyre több üzemi létesítménynél a magasszintű PR tevékenység következtében nagyszámú látogató jelenik meg az üzemi területen. A látogatók nyilvántartása, fogadása és az üzemi területre történő ki-és beléptetését is a beléptető rendszernek ideiglenes jogosultság formájában kezelnie kell.

#### 1.2.2.4 Video megfigyelő rendszer

A video megfigyelő rendszerek lehetővé teszik az objektumok területének vizuális megfigyelését, a cselekmények dokumentálását a kamerák által rendelkezésre bocsátott mozgóképek rögzítésével és tárolásával. A rögzített felvételek a későbbiekben akár bizonyítási eljárások alapját is képezhetik. [16] A video megfigyelő rendszer célja biztonságtechnikai szempontból megfogalmazva nem más, mint a megfigyelt terület képeinek megjelenítése és a felvételek rögzítése az élőerős szolgálatok számára, oly módon, hogy az illetéktelen személyek birtokába ne juthasson. A képtartalom megjelenítésének helyét alapvetően az objektumvédelmet ellátó élőerős védelmi tevékenység határozza meg. Tételezzük fel, hogy egy adott objektumnál a jellegéből adódóan elegendő a kivonuló szolgálat alkalmazása, akkor a képtartalom egy távfelügyeleti állomáson kerül megjelenítésre, míg egy helyszínen tartózkodó élőerő esetén az őrségközpontban lesz megjelenítve. Bármely élőerős védelmi forma alkalmazása esetén a video megfigyelő rendszer a meglévő rendszereket kiegészítve az őrszemélyzet munkáját segíti és nagymértékben növeli a hatékonyságát. Véleményem szerint nem túlzás, ha video megfigyelő rendszerrel kiegészített objektumvédelem hatékonyságát magasabb szintűnek tekintjük mint, az azt mellőző védelmi megoldást. Értelemszerűen a video megfigyelő rendszer akkor képes növelni a hatékonyságot, illetve hatásosan kiegészíteni és megkönnyíteni az élőerő munkáját, ha a rendszer magával az

objektum jellegével összhangban kerül kiépítésre. Ehhez pontosan ismernünk kell az objektumvédelmi feladatot, a felhasználás körülményeit (időjárási viszonyok, napszakok) és a video megfigyelő rendszerrel szembeni elvárásokat. [17] Továbbá a megfigyelő rendszert üzemeltetőknek is valamilyen alapszintű ismeretekkel rendelkeznie kell a hatékony üzemeltetéshez. A minimális tudás átadása az előerő számára a rendszer felépítésének és a rendszerelemek bemutatásának ismertetésével lehet a legegyszerűbben megvalósítani.

Az általános nyelvezetben elterjedt kamera, videokamera az alapfunkciójának tekintetében, nem más, mint egy fényt elektronikus analóg vagy digitális jellé átalakító eszköz. A külvilág felől érkező fény a kamera lencsén, objektívján keresztül a képérzékelőre (CCD vagy CMOS) kerül vetítésre, amelyet továbbítható elektronikus jellé alakítja át. A biztonságtechnikai kamera nagyban eltér a szórakoztató elektronikai kameráktól, mert az átalakított elektronikus jel nem kerül rögzítésre magában a kamerában, hanem a kimentén megjelenő elektronikus jelet továbbítani kell a video megfigyelő rendszer többi berendezései felé. A biztonságtechnikában használatos kamerákat jellemzően a felhasználási területük és a kiviteli formájuk szerint lehet csoportosítani. [18]

➤ Csőkamerák:

Nevét a jellegzetes cső kialakításából kapta. A méretéből adódóan a többi kameratípushoz képest viszonylag kisméretű úgynevezett tühegy optikával gyártják. Ebből adódóan a műszaki paraméterei nem kiemelkedőek. Bel-és kültéri objektumvédelmi feladatokra jól alkalmazható kisebb, max. 20 méteres tárgytávolságig, igaz csak megfelelő megvilágítás mellett.

➤ Kompakt kamerák:

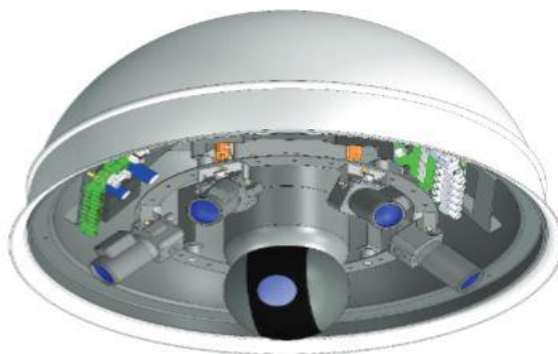
A nevéből egyértelműen adódik, hogy a kompakt kamera integráltan magánba foglalja minden alkatrészét, és elérhető variófokuszú kivitel is.

➤ Ipari kamerák:

Az ipari kamera a szakzsargonban box kamera néven vált ismerté. A box kamera a legelterjedtebben alkalmazott típus az objektumvédelmi feladatok ellátására a telepített video megfigyelő rendszereknél. A kompakt kamerákkal szemben egy kameratípussal és különböző objektívekkel felszerelve alkalmasak mozgás érzékelési, cselekmény megfigyelési és azonosítási feladatok ellátására egyaránt.[18]

➤ Dome kamerák:

A dome kamerák két féle változatban szerezhetőek be, az egyik változat a fix kivitelű a másik a mozgatható típus, ami speed dome kamera néven vált ismerté. A fix dome kamerák műszaki paramétereiben hasonlóak a kompakt kamerákhoz, gyakorlatilag a kupola alakú külsőmegjelenésében van csak szinte eltérés. A mozgatható dome kamerák a pan/tilt/zoom funkciójuknak köszönhetően, egy vezérlőegység segítségével 360 fokban körbe forgathatóak vízszintes irányban, függőlegesen 180 fokban vezérelhetőek és a zoommal nagyítható a megfigyelt terület. A mozgatható dome kamerák közé sorolható egy igen érdekes fejlesztés eredményeként megjelent scout automata térfigyelő kamera. A gyártó a központi speed dome kamera köré 4-8 darab fix referencia kamerát épített be. A referencia kamerák képtartalmának video analitikai elemzésével képes mozgó objektumokat detektálni és a speed dome kamerát a célra vezérelni. A referencia kamerák képtartalom elemzése és a dome kamera vezérlése folyamatos, ennek következtében egy automatikus mozgó tárgy vagy személy követési funkció valósul meg, egészen addig, amíg az a referencia kamerák látószögéből ki nem ér. Kijelenthető, hogy a kamera képes kezelő személyzet nélkül egy adott területen történő minden mozgást nyomon követni, ezzel kizárva az esetleges kezelői/emberi hibát. [19] A scout kamera 3D-s látványtervéen jól láthatóak a fix és a speed dome kamerák elhelyezkedése a gömbház belsejében (7. ábra)



7. ábra - Scout videokamera szerkezeti ábra [19]

➤ PTZ kamerák:

A PTZ elnevezés az angol PAN/TILT/ZOOM (függőleges, vízszintes, nagyítás) szavakból képzett mozaikszó. A PTZ kifejezés nem egy konkrét kameratípust jelent, hanem a mozgatható és zoomolható kamerák gyűjtőfogalma. Ezek közé

sorolható a speed dome kamera, a forgózsámolyra felszerelt boksz kamera és az olyan típusú kompakt kamera, amely a forgózsámolyt is magába foglalja.



8. ábra - PTZ kompakt kamera [20]

A képmegjelenítési folyamat fő egységei a monitorok és a videojel kapcsoló eszközök. A monitorok megjelenítő technológiák alapján három típusa van, ami a katódsugárcsőes, a folyadékkristályos és a plazmaképmegjelenítő. A biztonságtechnikai monitorok egyik fő paramétere a 7/24-es alkalmazhatósági képessége szemben a normál monitorokhoz képest. A megfigyelt területen alkalmazott kamerák számától függően lehet néhány monitorból álló megjelenítéstől a nagy kiterjedésű monitorfal kialakítással is találkozni. A monitorokon történő videojel megjelenítést, annak variálhatóságát és vezérlését a videojel kapcsoló eszközökkel lehet megvalósítani. Ezek az analóg eszközök lehetnek képléptetők, képosztók, video-multiplexerek és video-mátrixok, amelyek összefoglaló nevükön video központ néven is ismert. A digitalizáció fejlődésével megjelentek a digitális videó rögzítők és a számítástechnikai alapú hálózati rögzítők, amelyek elterjedésével az analóg technológia jelentősége teljesen visszaszorult.

A vezetékes jelátviteli megoldások közül kétfajta különböztethetünk meg, a rézalapú kábelekkel és az optikai kábelekkel kialakított átviteli rendszereket. A rézalapú kábelezés lehet koaxiális vagy csavart érpárú. Legfontosabb jellemzője a hullámimpedancia és a csillapítás. Az analóg rendszerekben kialakítására használt koax kábelek hullámimpedanciája 75 ohm, míg a csavart érpár kábeleké 100 ohm. A réz alapú kábelezéssel áthidalható jellemző távolság néhány 100 méter egyéb eszközök beépítése nélkül analóg videojel továbbítása esetén, de ez passzív, illetve aktív eszközökkel akár 1000-1500 méterig megnövelhető. Digitális, illetve IP alapú hálózatok esetében a TCP/IP technológia szabványaiban rögzített távolságok az irányadóak és az átviteli sávszélességgel fordítottan arányos. Egy 100Mbit/s sávszélességű hálózat esetén a csavart érpár maximális hossza 100 méter lehet. Nagy kiterjedésű és magas sávszélességű igény esetén az optikai kábelezés jelent megoldást. Az IP alapú videó megfigyelő

rendszereknél az IP kamerák UTP/FTP kábeleit switchekben gyűjtik össze, amelyeknek a gerincvezetékei már optikai kábellel van kialakítva. A switcheket jellemzően gyűrűs hálózati struktúrájúra alakítanak ki. Az optikai kábel mono vagy multimodusú lehet, amely meghatározza többek közt a maximális jelátviteli távolságot. Monomodusú kábellel több tíz kilométer is áthidalható egyéb eszköz beépítése nélkül, míg a multimodusnak maximum 1-2 kilométer. [21]

### **1.2.3 Élőerős védelmi alrendszer**

Az objektumvédelem területén a harmadik alrendszer az élőerős védelmi formában valósul meg. Az élőerős védelem esetében beszélhetünk először aktív védelmi funkció megvalósulásáról, mivel ezen alrendszer egyik kiemelt funkciója az elhárítási funkció, az objektum ellenében végrehajtott jogtalan cselekmények ellenében. Az élőerő képes a technikai rendszerek jelzéseinek kezelésére, azok valódiságának megállapítására és a veszélyhelyzet függvényében döntést hozni a reagálás szükségességéről és mértékéről. Mindezek alapján kijelenthető, hogy az élőerős védelemnek igen jelentős szerepe van az egymással szorosan összefüggő komplex vagyonsvédelmi rendszerben. A védelmi rendszer felépítésekor mindhárom alrendszer esetében kiemelt figyelemmel kerülnek kiválasztásra a rendszerbe integrált védelmi elemek. A mechanikai és az elektronikai technikai rendszerek minőségi megfelelőségüket elsősorban a vonatkozó szabványok és a feladat végrehajtásához megfelelően megtervezett rendszerek garantálják. Az élőerő jellegéből adódóan nem megvalósítható egy szabványosított személy-és vagyoniőr. A humán erőforrással szemben követelményeket, illetve követelmény rendszereket lehet támasztani, amik a jogszabályokban kerültek megfogalmazásra. Értelemszerűen a követelményrendszerben rögzített elvárások és feltételeken felül sok emberi tényező is jelen van, ami gyengítheti az élőerő hatékonyságát. Napjainkban egyre kevésbé jellemző, de az ember befolyásolható, korrumpálható, valamint a fegyelmezetlenségből következően képes szándékosan eltérni a szabályozott feladat végrehajtástól. Ezen felül jelentkezhetnek a monoton feladatvégrehajtásból származó nem szándékos hibás intézkedések is. Azonban a jól képzett és a biztonsági őri munka ellátásához szükséges humán paraméterekkel rendelkező őri képes rendkívüli helyzetekben is maximális hatékonyságú feladatvégrehajtásra.[1] A törvényi szabályozás a magánbiztonsági, vagyonsvédelmi előerős feladatok ellátására megkülönbözteti a személy-és vagyoniőr, valamint a fegyveres biztonsági őri tevékenységeket. Az objektumbiztonsági feladatok ellátásához a létesítmény jellegétől, a benne folytatott tevékenységtől, az ott jelenlévő

védendő javaktól és a fenyegetettségétől függően egyes esetekben vagyonőröket, máskor fegyveres biztonsági őreket, vagy mindkettőt egyidejűleg alkalmazzák. [22]

#### 1.2.3.1 Élőerős tevékenységek jogi szabályozási háttere

A személy-és vagyonőri munkavégzés feltételeit a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény és a törvényhez tartozó személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény végrehajtásáról szóló 22/2006 (IV.25.) BM rendelet szabályozza. A törvényi előírások rögzítik a személy-és vagyonvédelmi tevékenységet, a személy-és vagyonőri személyekkel szemben támasztott jogokat és kötelezettségeket, a tevékenységekhez tartozó szakképesítési követelményeket és a tevékenység folytatásának területi hatályát. A személy-és vagyonvédelmi tevékenység megkezdése és folytatása a rendőrség által a tevékenységet folytatni kívánó szervezet (egyéni vállalkozó vagy vállalkozás) kérelmére kiadott működési engedély alapján folytatható, amennyiben a kérelmező a rendőrség által kiadott személyre szóló igazolvány birtokában van. Az igazolvány kérelmezésének és kiadásának további feltételt szab a törvény a szakképesítés tekintetében. Személy-és vagyonvédelmi tevékenységet kizárólag az végezhet, aki biztonsági őr, testőr, vagyonőr vagy biztonságszervezői szakképesítés valamelyikével rendelkezik. Az igazolvány kérelmezői köréből a törvény kizárja a büntetett előéletű vagy bűncselekmény elkövetése miatt büntetőeljárás hatálya alatt álló személyeket, tehát az igazolvány igénylésének a büntetlen előélet a feltétele. Ennek igazolására a hatósági erkölcsi bizonyítvány szolgál. Természetesen ez csak az olyan kiállított bizonyítvánnyal lehetséges, amelyben a büntetlen előélet szerepel.

A vagyonvédelmi törvény szabályozása alapján a vagyonőr jogosult a megbízó közterületnek nem minősülő létesítményének őrzése során az alábbiakra:

- az őrzött objektumba a belépő személyt személyazonosságának igazolására felhívni
- a belépés céljának közlésére és a belépés jogosultságának igazolására felhívni
- az őrzött objektumba a belépő vagy onnan kilépő személyt csomag, illetve menet-szállítási okmány bemutatására felhívni
- az őrzött objektum területén tartózkodó vagy onnan kilépő személyt csomagja tartalmának, járművének, valamint a szállítmánynak bemutatására felhívni
- a jogsértő személyt magatartása abbahagyására felhívni

- elektronikus vagyonvédelmi rendszert alkalmazni
- az őrzött objektum területre belépők ellenőrzésére fegyver-, illetve robbanóanyag-kutató műszert alkalmazni és a közbiztonságra különösen veszélyes eszközök bevitelét megtiltani. [23 27§]

A fegyveres biztonsági őr munkavégzés feltételeit a fegyveres biztonsági őrsegről, a természetvédelmi és a mezei őrszolgálatról szóló 1997. évi CLIX. törvény és a törvényhez tartozó a fegyveres biztonsági őrseg Működési és Szolgálati Szabályzatának kiadásáról szóló 27/1998. (VI. 10.) BM rendelet szabályozza. Az fegyveres biztonsági őrsegről szóló törvény egyértelműen kimondja, hogy az állam illetőleg a lakosság ellátása szempontjából kiemelkedően fontos tevékenységet, létesítményt, szállítmányt, fegyveres biztonsági őrseggel kell védeni, amennyiben a védelemre az állami rendvédelmi szervek nem kötelezettek, de az őrzés a közbiztonság vagy a nemzeti vagyon védelme érdekében indokolt. Tehát a törvény fegyveres biztonsági őrseg alkalmazására kötelezi az alábbi tevékenységeket, illetve létesítményeket:

- „az állam biztonsága, illetve a honvédelem szempontjából fontos létesítményt
- a nemzetközi légiforgalomban működő repülőtereket
- olyan robbanásveszélyes, tűzveszélyes, mérgező, valamint az egészségre vagy a környezetre veszélyes anyag felhasználásával, gyártásával, tárolásával, forgalmazásával, szállításával összefüggő tevékenységet, amely katasztrófát okozhat
- nukleáris létesítményt, illetve radioaktív hulladék tárolókat.
- a lakosság alapvető szükségletét biztosító infrastruktúra és közműrendszer egyes elemeit
- a postai szolgáltató kiemelt létesítményét,
- a közszolgálati rádió és televízió, a távközlési rendszerek központi létesítményét.”

[24 1§(1)]

A törvényi előírások rögzítik a fegyveres biztonsági őr tevékenységet folytató személyek jogait és kötelezettségeit, a tevékenységekhez tartozó szakképesítési követelményeket és a tevékenység folytatásának területi hatályát. A fegyveres biztonsági őrseg létrehozásáról, működtetéséről és megszüntetéséről a rendőrség határozattal dönt. Az őrsemélyzettel szemben az erkölcsi megfelelés feltétele a büntetlen előélet, amely a hatósági erkölcsi bizonyítvánnyal igazolható. Szigorító szabályok vonatkoznak a nukleáris



létesítményekben szolgálatot teljesítő fegyveres biztonsági őrökkel szemben a 6. § (4a) bekezdés alapján, amely szerint nem elegendő a büntetlen előélet. A fegyveres biztonsági őr jogosultságait a következő fejezetben ismertetem a személy-és vagyonőri tevékenység jogosultságainak összehasonlításán keresztül.

#### 1.2.3.2 A fegyveres biztonsági őr és vagyonőr intézkedési jogainak összehasonlítása

A fegyveres biztonsági őrt az FBŐ törvény jóval szélesebb körű lehetőségekkel és eszköztárral ruházza fel, mint a személy-és vagyonőri törvény a személy- és vagyonőrt. Alapfeladatuk ellátása nagyban hasonló, de már a jogosultságok tekintetében is számottevő különbség figyelhető meg a jogi szabályozás következtében. A fegyveres biztonsági őr szolgálatának teljesítése során jogosult:

- az őrzött objektumba a belépő személyt személyazonosságának igazolására felhívni
- a belépés céljának közlésére és a belépés jogosultságának igazolására felhívni
- az őrzött objektumba a belépő vagy onnan kilépő személy csomagját, járművét, valamint a szállítmányát átvizsgálni
- belépő személy családi és utónevét, születési helyét és idejét, a személyazonosításhoz bemutatott okmány számát rögzíteni
- a belépésre használt jármű rendszámát és típusát rögzíteni
- a területre belépők ellenőrzésére fegyver-, illetve robbanóanyag-kutató műszert alkalmazni.

Amennyiben a belépni kívánó személy a fentieknek teljesítését megtagadja vagy vélelmezhető a közölt adatok valótlanága - a kötelezett, illetve a fegyveres biztonsági őrseget működtető szervezet vezetője eltérő rendelkezésének hiányában - a fegyveres biztonsági őr az alábbi intézkedések alkalmazására jogosult:

- a személy beléptetését megtagadhatja
- az őrzött objektum biztonságát veszélyeztető, továbbá a közbiztonságra különösen veszélyes eszközök bevitelét megtilthatja
- az objektumba belépő, illetve az objektumból kilépő személyt a csomagja tartalmának, járművének, valamint a szállítmányának bemutatásáig feltartóztathatja.
- a biztonságot sértő vagy veszélyeztető személyt tevékenysége abbahagyására felszólíthat és igazoltathat

- az intézkedésének tettelesen ellenszegülő vagy a bűncselekmény elkövetésén tetten ért személyt a rendőrség megérkezéséig visszatarthatja, vagy a rendőrségre előállíthatja. [24 9/B§]

az igazoltatott, visszatartott vagy előállított személytől a bűncselekményből származó, vagy annak elkövetéséhez használt dolgot, illetve támadásra alkalmas eszközt elveheti, ennek érdekében ruházatot, csomagot átvizsgálhat.

Továbbá a fegyveres biztonsági őr az FBŐ tv. 10. § (2) bekezdése szerint „A fegyveres biztonsági őr a biztonságot veszélyeztető tevékenység megszakítása érdekében, az azt elkövető személlyel szemben az arányosság követelményének betartásával:

- a) testi erővel cselekvésre vagy cselekvés abbahagyására kényszerítést, illetve pórázon vagy anélkül, szájkosárral ellátott szolgálati kutyát,
- b) a visszatartott személy szökésének, illetve személyőrzési vagy kísérési feladat végrehajtása során a személyes szabadságában korlátozott személy szökésének, önkárosításának megakadályozására bilincset,
- c) a támadás megakadályozására vagy az ellenszegülés megtörésére vegyi vagy elektromos sokkoló eszközt, rendőrbotot, illetve pórázon vezetett szájkosár nélküli szolgálati kutyát,
- d) az állam működése vagy a lakosság ellátása szempontjából kiemelkedően fontos tevékenység, létesítmény, szállítmány ellen fegyveresen vagy felfegyverkezve intézett támadás elhárítására szájkosár és póráz nélküli szolgálati kutyát vagy lőfegyvert alkalmazhat, illetve használhat.” [24 10 § (2)]

A különbségek egyszerű bemutatása miatt a személy- és vagyonőr, illetve a fegyveres biztonsági őr jogosultságait és kényszerítő eszköz használati jogosultságát a 2. táblázatban foglaltam össze.

	<b>jogosultág / kényszerítő eszközök</b>	<b>fegyveres biztonsági őr</b>	<b>személy-és vagyonőr</b>
1	testi kényszer	a biztonságot veszélyeztető tevékenység megszakítása érdekében, az azt elkövető személlyel szemben az arányosság követelményének betartásával testi erővel cselekvésre vagy cselekvés abbahagyására kényszerítést használhat, alkalmazhat	arányos mérvű kényszerítő testi erő alkalmazásával a védett létesítménybe, területre való jogosulatlan belépést megakadályozhatja, a jogosulatlanul bent tartózkodót onnan eltávolíthatja
2	bilincs	visszatartott személy szökésének, illetve személyőrzési vagy kísérési feladat végrehajtása során a személyes szabadságában korlátozott személy szökésének, önkárosításának megakadályozására bilincset használhat, alkalmazhat	bilincset nem használhat
3	vegyi eszköz	jogos védelmi helyzetben, végszükség esetén, illetve a támadás megakadályozására vagy az ellenszegülés megtörésére vegyi eszközt, használhat, alkalmazhat	jogos védelmi helyzetben, illetve végszükség esetén
4	elektromos sokkoló	jogos védelmi helyzetben, vég- szükség esetén a támadás megakadályozására vagy az ellenszegülés megtörésére elektromos sokkoló eszközt használhat, alkalmazhat	jogos védelmi helyzetben, illetve végszükség esetén
5	rendőrbot /gumibot	jogos védelmi helyzetben, vég- szükség esetén a támadás megakadályozására vagy az ellenszegülés megtörésére, rendőrbotot használhat, alkalmazhat	jogos védelmi helyzetben, illetve végszükség esetén
6	lőfegyver	jogos védelmi helyzetben, végszükség esetén, illetve az állam működése vagy a lakosság ellátása szempontjából kiemelkedően fontos tevékenység, létesítmény, szállítmány ellen fegyveresen vagy felfegyverkezve intézett támadás elhárítására lőfegyvert használhat	jogos védelmi helyzetben, illetve végszükség esetén
7	örkutya	A kényszerítőeszköz használatának fennálltakor az arányossági követelmények betartásával, szájkosárral, pórázzal, szájkosár nélkül, póráz nélkül, szolgálati kutyát alkalmazhat	jogos védelmi helyzetben, illetve végszükség esetén

	<b>jogosultág / kényszerítő eszközök</b>	<b>fegyveres biztonsági őr</b>	<b>személy-és vagyonőr</b>
8	intézkedési jogosultság	A fegyveres biztonsági őr szolgálatának jogszerű teljesítése során jogosult és köteles intézkedni. Intézkedései kikényszeríthetők.	Intézkedéseit a vagyonvédelmi törvényben meghatározottak szerint vagy az érintett személy önkéntes hozzájárulása alapján gyakorolja.
9	csomag átvizsgálás	A fegyveres biztonsági őr az őrzött objektumba történő be- és kiléptetésre irányuló szolgálatának teljesítése során jogosult az őrzött objektumba a belépő vagy onnan kilépő személyt csomagja tartalmának, járművének, valamint a szállítmányának bemutatására felhívni az objektumba belépő, illetve az objektumból kilépő személyt a csomagja tartalmának, járművének, valamint a szállítmányának bemutatásáig feltartóztathatja, a területre belépők ellenőrzésére fegyver-, illetve robbanóanyag-kutató műszert alkalmaz	A vagyonőr a csomag tartalmának, jármű és szállítmány bemutatására a szerződésből fakadó kötelezettségei érvényesítése céljából, a tervezett intézkedése okának és céljának közlése mellett akkor hívhat fel, ha a) megalapozottan feltehető, hogy az érintett bűncselekményből vagy szabálysértésből származó olyan dolgot tart magánál, amelynek őrzése a vagyonőrnek szerződésből fakadó kötelezettsége; b) e dolgot a felszólítás ellenére sem adja át; és c) az intézkedés a jogsértő cselekmény megelőzése, megszakítása érdekében szükséges
10	ruházat átvizsgálás	igazoltatott, visszatartott vagy előállított személytől a bűncselekményből származó, vagy annak elkövetéséhez használt dolgot, illetve támadásra alkalmas eszközt elvenni, ennek érdekében ruházatát, csomagját átvizsgálni, a területre belépők ellenőrzésére fegyver-, illetve robbanóanyag-kutató műszert alkalmaz	ruházatot nem vizsgálhat át
11	gépjármű átvizsgálás	A fegyveres biztonsági őr az őrzött objektumba történő be- és kiléptetésre irányuló szolgálatának teljesítése során jogosult az őrzött objektumba a belépő vagy onnan kilépő személyt csomagja tartalmának, járművének, valamint a szállítmányának bemutatására felhívni az objektumba belépő, illetve az objektumból kilépő személyt a csomagja tartalmának, járművének, valamint a szállítmányának bemutatásáig feltartóztathatja, a területre belépők ellenőrzésére fegyver-, illetve robbanóanyag-kutató műszert alkalmaz	A vagyonőr a csomag tartalmának, jármű és szállítmány bemutatására a szerződésből fakadó kötelezettségei érvényesítése céljából, a tervezett intézkedése okának és céljának közlése mellett akkor hívhat fel, ha a) megalapozottan feltehető, hogy az érintett bűncselekményből vagy szabálysértésből származó olyan dolgot tart magánál, amelynek őrzése a vagyonőrnek szerződésből fakadó kötelezettsége; b) e dolgot a felszólítás ellenére sem adja át; és c) az intézkedés a jogsértő cselekmény megelőzése, megszakítása érdekében szükséges

	<b>jogosultság / kényszerítő eszközök</b>	<b>fegyveres biztonsági őr</b>	<b>személy-és vagyonőr</b>
12	igazoltatás	Szolgálatának teljesítése során jogosult az őrzött objektumba a belépő személyt kiléte igazolására, a belépés céljának közlésére, jogosultságának igazolására felhívni, a biztonságot sértő vagy veszélyeztető személyt tevékenysége abbahagyására felszólítani és igazoltatni	A személy- és vagyonőr tevékenysége gyakorlása során - e törvényben meghatározott feltételek fennállása esetén - jogosult az intézkedésében érintett személyt felhívni kilétének igazolására. Ha az általa erre felkért személy önként és hitelt érdemlően nem igazolja kilétét, a személyazonosság megállapítására - indokolt esetben - igazoltatásra jogosult hatósági személyt kérhet fel

2. táblázat - a fegyveres biztonsági őr és a személyi-és vagyonőr jogosultságainak összehasonlítása [23][24]

A jogosultságok és kényszerítő eszköz használati jogosultság összehasonlításából jól látszik, hogy a fegyveres biztonsági őr hasonló szituációkban nagyon jobbkörrel rendelkezik és jóval hatékonyabban tud intézkedni, mint a személy-és vagyonőr. Miből adódik ez a különbség? A személy-és vagyonvédelemi, magánbiztonsági szakterületek kialakulását a társadalom részéről támadt alapvető biztonsági igény hívta életre, amelybe bele tartozik a személy-és vagyonőri terület is. [25] Ebből következik, hogy az elsődleges feladata a személy-és vagyonőrnek az objektum vagyonának, javainak, valamint az ott dolgozó munkavállalók védelme. A fegyveres biztonsági őrrel védett létesítmények és tevékenységek esetében a vagyon védelmén túl az adott létesítményben alkalmazott ipari technológiát is védeni kell a szabotázsztól és az illetéktelen behatolók rosszindulatú cselekményei ellen. A jogszabályok meghatározásaiból következik a fegyveres biztonsági őrök nagyobb jogköre. Míg a személy-és vagyonőr az esetek többségében tolvajokkal, betörőkkel nagyon ritkán fegyveres elkövetőkkel szemben kell hatékonyan intézkedjen, addig az fegyveres biztonsági őr akár egy felfegyverzett terrorista csoport által végrehajtott támadást kell hatékonyan elhárítson. Egyre több szakirodalomban találkozhatunk a fizikai védelem kifejezéssel, ami nem összekeverendő a mechanikai védelemmel és az informatikában használt fizikai hozzáférés védelemmel. A fizikai védelemi tevékenység és a vagyonvédelmi tevékenység két teljesen más előerős védelmi feladat. [26]

## 2 OBJEKTUMVÉDELEM KOMPLEXITÁSA

Az előző fejezetben összefoglaltam a három védelmi forma lényegét, jelentőségét és alkalmazásukat. Az objektum őrzés és védelem lényege, hogy e három védelmi formát egymással összehangoltan a veszélyeztetés mértékét figyelembe véve, mint komplex vagyónvédelmi rendszert alkalmazzuk. Ebben a fejezetben az előzőre alapozva az objektumvédelem komplexitását fogom elemezni. Elsőként a veszélyeztetettség mértékének a skáláján egy alacsony és egy nagyon magas pontján elhelyezkedő két objektumot fogok vizsgálni, a komplexitás megvalósulásának bemutatására a gyakorlatban. A szakmai tapasztalataimra alapozva szükségesnek tartom ezt az elemzést, a disszertációmban megfogalmazott hipotézisek igazolásához és az általam elképzelt aktivitás fokozását megvalósító vagyónvédelmi megoldások hatékonyságának alátámasztásához. [27]

### 2.1 A védelem komplexitásának értelmezése lakóingatlanoknál

Az objektumvédelemben alkalmazott védelmi formák külön-külön alkalmazva is védelmet nyújthatnak, de hatékony őrzésvédelmi rendszert, csak mind a három védelmi alrendszer egyidejű, összehangolt alkalmazásával valósítható meg. A hatékonyság nem jelent mást, mint a veszélyeztetettséggel szembeni arányos védelmi erőforrások alkalmazása. A mechanikai védelmi rendszerből, az elektronikai védelmi rendszerből és az élőerős védelmi rendszerből kiépített komplex védelem nem valósítható meg belső szabályozási rendszer nélkül. [28] Berek Lajos megfogalmazása szerint komplex a vagyónvédelmi rendszer, ha a vagyónvédelmi feladathoz felhasznált védelmi formák összehangoltan és a veszélyeztetéssel arányosan vannak alkalmazva. [29] A komplex védelmi rendszer kialakításának igénye a nukleáris létesítmények őrzésének és védelmének megvalósításánál is jelentkezik, habár a nukleáris ipar terminológiájában a fogalmat fizikai védelmi rendszer néven azonosítják. Hazai jogi szabályozásban az atomtörvényben található meg, ami szintén Berek Lajos meghatározását igazolja: „*fizikai védelem: azon belső szabályozás, technikai eszköztár és élőerős elhárítás összessége, amely a nukleáris védettség részeként a nukleáris létesítményekkel, valamint nukleáris és más radioaktív anyagokkal szemben elkövetendő jogtalan eltulajdonítás és szabotázs elrettentésére, észlelésére, késleltetésére és elhárítására irányul.*” [30]

A fejezet bevezetésében meghatározásra került az objektumvédelem komplexitásának fogalma, amely gyakorlatilag szembe állítja a veszélyeztettséget és az azzal szemben

kialakított arányos, optimális védelmi képességek halmazát. A komplexitás kialakítása egy objektumvédelmi feladat megtervezésekor a vagyonsvédelem területén belül több különböző szakember szoros együttműködését igényli. Az objektumok funkció szerinti csoportosításánál a felhasználás szempontja alapján egy csoportba sorolt hétköznapi élet szükségleteit kielégítő lakó ingatlanoknál a biztonságot meghatározó jellemző paraméterek nagy mértékben eltérhetnek egymástól. Ebből kifolyólag két hasonló lakó ingatlan esetében más és mást jelent a komplexitás. Ennek szemléltetésére táblázatos formában mutatom be a komplexitás kritériumának teljesüléséhez szükséges védelmi feltételeket, több feltételezett, de a biztonságot meghatározó jellemzők egyértelmű definiálásával az ingatlanok vonatkozásában.

Az ingatlanok biztonságát meghatározó jellemzőik:

- A vizsgált objektumok mindegyikére jellemző, hogy az elhelyezkedésük következtében azonos mértékű a környék bűnügyi fertőzöttsége. A környék meghatározó bűnesetei a lopás, a betörés és kismértékben előforduló rablás, amelyek a veszélyeztetettség mértékének az egyik komponense.
- Hétfélig ház szőlős birtokon: Az ingatlan értéke 20 MFt, azonos településen található a tulajdonos lakó ingatlanával. A tulajdonos heti rendszerességgel tölt ott több kevesebb időt pihenés, illetve munkavégzés céljából. Az szőlős tanyában található gépek, eszközök és berendezések összértéke nem haladja meg az 1 MFt-ot. Jelölése=SZT
- Családi ház1: Értéke 80 MFt, az ingóságok összértéke 10 MFt, ami szórakoztató elektronikai eszközökből, nagyértékű bútorokból, néhány festményből és antik műkincsből áll össze. Lakói egy négytagú átlagos család. Jelölése=CSH1
- Családi ház2: Értéke 900 MFt, az ingóságok összértéke 400 MFt, ami szórakoztató elektronikai eszközökből, nagyértékű luxus kivitelű bútorokból, több nagyértékű műkincsből, (festmény, szobor, porcelán gyűjtemény stb.) több nagyértékű autóból és családi ékszerekből áll össze. Lakói egy négytagú család, amelyek egyik felnőtt tagja egy többmilliárdos üzleti vállalkozás tulajdonosa. Jelölése=CSH2

	Ingatlanok		
	SZT	CSH1	CSH2
Mechanikai védelem	minimális	részleges	teljeskörű
kültéri védelem	drótkerítés	2 méter magas tömör kerítés	2,5 méter tömör kerítés
kerítés	szükséges	szükséges	szükséges
építményvédelem			
épület szerkezet	minimális	részleges	teljeskörű
ajtók	bejárati ajtó	3 perces áthatolás elleni védelem	15 perces áthatolás elleni védelem
ablakok	bejárati ajtóval egyenértékű áthatolási ellenállás	biztonsági ajtóval egyenértékű áthatolási ellenállás	biztonsági ablak ajtóval egyenértékű áthatolási ellenállás
zárak	3 perces ellenállóképesség minden féle támadási mód ellen	3 perces ellenállóképesség minden féle támadási mód ellen	biztonsági zár/zárbetét
üvegek / fóliák	min 6 mm vastagságú	biztonsági üveg	biztonsági üveg biztonsági fóliával
rácsok/ redőnyök	10 x 30 cm rácsosztású 12 mm vastag köracél.	Alumínium redőny visszatolás gátlóval	Alumínium redőny visszatolás gátlóval
tárgyvédelem	nem szükséges	szükséges	biztonsági széf elektronikai védelemmel
Elektronikai védelem			
Kerítés védelem	nem szükséges	nem szükséges	szükséges



	Ingatlanok		
	SZT	CSH1	CSH2
videó megfigyelő rendszer	nem szükséges	nem szükséges	szükséges
beléptető	nem szükséges	nem szükséges	szükséges*
behatolás jelző rendszer	szükséges	részleges elektronika védelem	teljeskörű elektronikai védelem
távfelügyeleti átjelzés	nem szükséges	szükséges	szükséges
kültéri védelemi érzékelőkkel	nem szükséges	nem szükséges	szükséges
felület védelemi érzékelőkkel	nem szükséges	opcionális	szükséges
belső térvédelmi érzékelőkkel	szükséges	szükséges	szükséges
tárgyvédelem	nem szükséges	szükséges	szükséges
Előerős védelem			
kivonuló járőr	nem szükséges	szükséges	szükséges
porta szolgálat /helyi őrszemélyzet	nem szükséges	nem szükséges	szükséges

3. táblázat - A komplex védelem kialakításához szükséges védelmi formák különböző objektumok tekintetében [31] [32]

A táblázatban alkalmazott védelmi formák mindhárom ingatlannál jelentős eltérést mutatnak, mégis kimondható, hogy minden esetben megfelelnek a komplex védelmi rendszer követelményeinek. Valójában mik is ezek? Leegyszerűsítve a veszélyeztetettség mértékével szembeállított arányos vagyónvédelmi erőforrások összessége. A veszélyeztetettséget befolyásoló tényezők közül a két legfontosabbat emelném ki, a környezet bűnügyi fertőzöttségét és az ingatlanban található értéket képező vagyontárgyakat. A fentiekben leírt biztonságot meghatározó jellemzőknél rögzítésre kerültek, a lopás, a betörés és a rablás, mint jellemző bűnesetek. Tehát a példában szereplő bűnügyi adatokból kijelenthető, hogy az elkövetők tekintetében vannak olyanok, akiknek

az sem jelent problémát, ha az ingatlan tulajdonosai otthon tartózkodnak, bevállalva egy sokkal súlyosabb elbírálás alá eső bűncselekményt. [10] Az ingatlanban található értékek alapján a három ingatlannál teljesen különböző a veszélyeztetettség mértéke. A CSH2 jelölésű ingatlannál a hatalmas ingósági érték okán sokkal valószínűbb egy profi jól szervezett bűnbanda által végrehajtott betörés, mint a másik két ingatlan esetében. Az ingatlanok megfigyelésével és egyéb kiegészítő információszerzési technikákkal a bűnelkövetők fel tudják mérni a várható hasznot, valamint azt is, hogy nagyjából milyen jellegű védelemmel találják szembe magukat. Ebből következik, hogy a nagyobb értékhez összetettebb védelmi megoldás párosul, így a sikeresen végrehajtott betöréshez felkészültebb elkövetőt feltételez. Az arányosság megállapításához szembe kell állítani a védelemre költött összeget az ingóságok biztosítási értékével szemben. A példában szándékoltnak lettek meghatározva úgy az értékek, hogy számítások nélkül is érzékelhető legyen a vagyontárgyak értéke és a megóvására fordított védelmi ráfordítás mértéke. Az élőerő jelenti a legnagyobb ráfordítást, de a CSH2 ingatlannál a személyvédelemre is jelentős figyelmet kell fordítani, így már az állandó őrszemélyzet alkalmazása is szükséges a komplex védelem kialakításához.

## **2.2 Energiatermelő nukleáris létesítmény objektumvédelme**

Az ismert legsúlyosabb következményekkel járó civilizációs katasztrófák egyike a nukleáris katasztrófa, ahol a bekövetkezése esetén óriási természeti és civilizációs károkkal kell számolni. Ennek ellenére a békéscélú nukleáris energia alkalmazása szinte az egész világon jelen van és jelentős mértékben járul hozzá a villamosenergia termeléshez. A nemzetközi energiatrendek alapján az atomerőművek az energiatermelésben várhatóan még sokáig meghatározó szerepet fognak játszani, kiemeltképpen Magyarországon gondolva a Paksi erőmű bővítésére, amellyel átmenetileg megkétszereződik a nukleáris alapú energiatermelés mérete.

Az atomerőművek működése a technológiából adódóan veszélyesnek mondható, mert az energiatermelési folyamatot különböző sugárzások kísérik. A sugárzás élettani hatásai miatt, ezek kiküszöbölésére és a nukleáris kockázat csökkentésére különböző berendezések, rendszerek, eljárások kerültek beépítésre, alkalmazásra. Az atomerőmű biztonsága egy összetett, bonyolult folyamat eredménye, ami a tervezéstől az üzemeltetésig tart. A magas szinten tartott nukleáris biztonság egy hatékony és tiszta erőforrást végeredményez. További jellemzője, hogy egy telephelyen több

energiatermelő reaktort üzemeltetnek, a mi esetünkben 4·500MW beépített villamos teljesítményű blokkokról van szó, ami az ország pillanatnyi fogyasztásának az 50%-a is lehet. A XXI. század elején a nukleáris alapú energiatermelési szektorban nagy figyelmet kell fordítani a létesítmények őrzésére és védelmére, hogy a terrorcselekmények megnövekedett számának ellenére, hazánkban a kiemelten magas szinten tartott nukleáris biztonság és védettség folyamatosan biztosított, valamint az ország nukleáris veszélyeztetettsége alacsony szintű legyen. A terrorcselekményekkel kapcsolatban talán a 2016 tavaszán megrendezett Washingtoni nukleáris biztonsági csúcstalálkozón elhangzott brit miniszterelnöki (David Cameron) felszólalása hívja fel a figyelmet arra, hogy véleménye szerint a terroristák bármit alkalmaznak, amit csak meg tudnak szerezni. [27]

Cameron úgy fogalmazott: *„hihetetlenül fontos a nukleáris anyagok biztonsága mindazon országok számára, amelyeknél futnak atomprogramok, hogy biztosak lehessünk abban, hogy biztonságban vannak ezek az anyagok, nemcsak Nagy-Britanniában, hanem szerte a világon.*

*A brüsszeli támadások felerősítették a félelmeket, miután az öngyilkos merénylők megfigyelték egy belga nukleáris létesítmény egyik vezetőjének az otthonát. Brit kormányzati források ugyanakkor azt mondták, nincs tényszerű bizonyíték, hogy a terroristák brit célpontokra támadnának.”* [33]

Az ország nukleáris veszélyeztetettsége nagyon sok tényezőtől függ, még a szomszédos országokban elhelyezkedő nukleáris létesítmények (erőművek, tárolók, kutatóreaktorok stb.) számától is, de első sorban a hazai objektumok telephelyein lévő reaktorok számától és teljesítményétől, tárolók esetében a tárolt nukleáris anyag mennyiségétől. A két új paksi blokk megépítésével hazánk veszélyeztettségének mértéke mindenképpen megváltozik, valamint a terroristák számára is új célpont lehet, ezért érdemes a biztonság tudománnyal foglalkozó szakembereknek erre a területre vonatkozó objektumvédelmi és őrzési feladatok összefüggéseit, szabályozásait felülvizsgálni a kritikus infrastruktúrák középpontba állításával. [27]

### **2.2.1 Kritikus infrastruktúra az atomerőmű?**

A kritikus infrastruktúrák megfogalmazásánál minden esetben figyelembe kell venni az adott ország, illetve valamilyen szervezet, közösség szemszögéből létfontosságú infrastrukturális elemeket, ami így került megfogalmazásra Rácz László István

tudományos cikkében: „*A kritikus infrastruktúrák vonatkozásában meg kell határozni az infrastruktúrához igazodó vizsgálati módszert. Ennek segítségével fel kell tárni a kritikus infrastruktúra körébe tartozó rendszereket és elemeket. Ezeket prioritásuk, a gyakorolt hatásuk szerint be kell sorolni, el kell készíteni az üzemeltetői biztonsági tervet.*” [34] A 90-es évek második felétől generálódott a létfontosságú infrastruktúrák meghatározásának és védelmének igénye, koncepcionális kérdésként való meghatározása. Több szervezet is, de elsőként az USA foglalkozott a tématerülettel műszaki biztonsági aspektusból megközelítve, majd az amerikai 2001-es terrorcselekmények után biztonságpolitikai és védelmi szempontok mentén. A későbbi európai terror események után sorra az ENSZ, a NATO és végül az Európai Unió is fokozott figyelmet fordított a létfontosságú infrastruktúrák meghatározására és védelmére. A fent leírtak alapján lehetséges az, hogy nincs egy egzakt kifejezés, fogalom, illetve meghatározás a létfontosságú infrastruktúrák területén.

Néhány meghatározás:

- Az USA Kritikus Infrastruktúra Védelmi Elnöki Bizottsága a következőképpen fogalmazta meg: „*Ember alkotta rendszerek és eljárások hálózata, amelyek szinergikusan együttműködve arra törekszenek, hogy folyamatosan alapvető termékeket és szolgáltatásokat állítsanak elő és terjesszenek.*”
- A NATO Polgári Védelmi Bizottsága által az alábbiak szerint került meghatározásra a fogalom: „*Kritikus infrastruktúra azokat a létesítményeket és információs rendszereket jelenti, amelyek olyan létfontosságúak a nemzetek számára, hogy működésképtelenné válásuknak vagy megsemmisülésüknek gyengítő hatása lenne a nemzet biztonságára, a nemzetgazdaságra, a közegészségre, a közbiztonságra és a kormány hatékony működésére.*” [34]
- Hazai szabályozás szerinti megfogalmazás: „*Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.*” [35]

A nem teljesen egybevágó megközelítés, megfogalmazás ellenére a nemzetközi együttműködések és a hazai előkészítő munkák eredményeként megszülettek a hazai nemzeti szabályozások, amelyek rögzítik a Nemzeti Kritikus Infrastruktúrák Védelmére vonatkozó irányelveket. A szabályozások közül az elemzés szempontjából a két legfontosabbnak, illetve irányadónak a „2012. évi CLXVI. törvény A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről”, valamint a „65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról” szóló kormányrendelet tekinthető. Az itt megfogalmazott rendelkezések alapján a kritikus infrastruktúrákat ágazati csoportokba lehet sorolni:

- energiaipar;
- közműellátás nélkülözhetetlen szektorai;
- közlekedés, szállítás;
- távközlés;
- bankrendszer;
- élelmiszer alapellátás;
- egészségügyi ellátás;
- folyamatos kormányzás feltételrendszere;
- rendvédelmi szervek működésének feltételrendszere;
- tömegtartózkodási helyek.

Az ágazati besorolás mellett még további felosztása is lehetséges a horizontális kritériumok mentén:

- a veszteségek kritériuma
- gazdasági hatás kritériuma
- társadalmi hatás kritériuma
- politikai hatás kritériuma
- környezeti hatás kritériuma

A kritikus infrastruktúrák meghatározásánál az ágazati besorolás és a horizontális kritériumok alapján történő felosztás mellett fontos megemlíteni 5 alapvető tulajdonságot, ami a kritikus infrastruktúrát jellemezheti:

- interdependencia – rendszerek egymástól való függősége;
- informatikai biztonság – kiemelt terület, automatizált FIR-ek, munkafolyamatok;

- üzemeltetés – sajátosságok, egyedi jelleg;
- dominóelv – láncreakciószerű sérülés/károsodás;
- leggyengébb láncszem – összekapcsolódó hálózatok stabilitása a leggyengébb elem erősségétől függ.

A hazai szabályozások mentén az atomerőműveket az energia szektoron belül a villamosenergia-rendszer létesítményei közé kell sorolni, és vizsgálni a horizontális kritériumok mentén. Ennél a vizsgálatnál figyelembe kell venni az atomerőművek telepítési konfiguráció gyakorlati megvalósításának a sajátosságait, amit az egy telephelyen létesített energiatermelő blokkok nagysága, és száma, valamint az egy blokk/országos alapfogyasztás hányadosa erősen befolyásol. Ma Magyarországon egy atomerőműi blokk kb. az országos átlagfogyás 10%-át adja, amiből egyenesen következik, hogy egy blokk üzemzavara esetében is már érzékelhető hatást fejt ki a gazdaságra. Értelmezésem szerint a számítások részletezése nélkül a gazdasági hatás kritériuma az egy blokk 22,5 napos termelőkiesése vagy a 4 blokk egyidejű 6 napos termelőkiesése estén teljesül. További kritériumok teljesüléséhez már az egyszerű üzemzavaron túlmutató eseménynek kell bekövetkeznie, ami lehet nukleáris szennyezéssel együtt járó üzemzavar is. [27]

Két alapvető kritikus infrastruktúrára jellemző tulajdonságot ki kell emelni az atomerőművek vizsgálata szempontjából, ami az interdependencia és az üzemeltetési sajátosságok.

- Interdependencia: Az atomerőmű energiatermelésének kiesésekor a villamosenergiaellátó hálózati rendszerben, okozhat olyan mértékű teljesítménylengést, ami a hálózat összeomlásához, Black Out-hoz vezethet. A hálózat teljes összeomlása egy igen bonyolult összetett kérdés, több egyéb befolyásoló tényezőtől függ, amiről Dr. Prof. Berek Lajos és Vass Attila „Gázturbinás erőművi objektum védelme” című cikkükben olvashatunk.
- Üzemeltetés, sajátosságok, egyedi jelleg: Az atomerőmű a fizikai létezésével és üzemelésével eleve egyedinek tekinthető, az ott alkalmazott technológia és különféle tudományok alkalmazásának a sokszínűségével. Szintén a technológia sajátosságból adódik, hogy egy blokk energiatermelésének megkezdéséhez úgynevezett idegen gőzös indítására van szükség. Az első blokk létesítésekor ezt a feladatot egy indító kazánház látta el. A második és a többi blokk indításánál

már az üzemelő blokkok valamelyike vette át ezt a feladatot. Tehát a négyblokkos kiesés, leállás esetén újból szükség lenne az idegen gőzös indítására, aminek az előállítása jelentős időt igényel. Fontos megjegyezni, hogy az elmúlt 40 éves üzemidő alatt még soha nem fordult elő a blokkok egyidejű teljes leállítása.

Összegezve, több szemszögből is vizsgálva az atomerőműveket mindenképpen a kritikus infrastruktúrák közé sorolom. Ezt a megállapítást azért teszem, mert hazánkban is hosszabb folyamat eredményeként azonosításra, kijelölésre kerültek a létfontosságú rendszerek és létesítmények a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló jogszabályban. A törvény 1. számú melléklete szerint a rendelkezései alól kivételt képeznek az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek. [27]

### **2.2.2 Nukleáris létesítmények veszélyeztetettségének megállapítása**

Az atomerőművek, nukleáris létesítmények okozta katasztrófák általi veszélyeztetettség mértékének kutatásánál, a katasztrófát kiváltó okokat tekintve 3 fő veszélyeztető tényezőt vettem számításba:

- Természeti katasztrófa (katasztrófavédelem)
- Üzemzavarból származó ipari katasztrófa (nukleáris biztonság)
- Szándékos jogellenes cselekmények, terrorcselekmények (nukleáris védettség)

A különböző eredetű katasztrófák elleni védekezéshez más-más védelmi koncepció, akcióterv kidolgozására van szükség. A természeti katasztrófák okozta károk és az üzemeltetéssel összefüggésben (technológiai, emberi mulasztás) keletkező meghibásodásból származó károsodások kialakulásának megakadályozására, már a létesítmény tervezésekor nagy figyelmet kapott a biztonsági rendszerek kidolgozása. Az első energiatermelő reaktor üzembehelyezése több mint 60 éve történt és azóta összesen 2 darab nagy nukleáris szennyezéssel együtt járó természeti katasztrófa történt a Csernobili atomerőműben emberi mulasztás miatt, és a Fukusimai atomerőműben tervezési határon túli cunami következtében. Véleményem szerint az atomerőművek nukleáris biztonsági szempontból magas műszaki színvonalat képviselnek, amit rendszeresen hazai és nemzetközi atomenergiái szervezetek ellenőriznek. Napjainkban

nagyobb energiaráfordítást a szándékos cselekmények elleni védelem területén kell alkalmazni a megnövekedett terrorcselekmények száma miatt. [27]

A XXI. század első két évtizedében nagyságrendekkel megnövekedett a terrorcselekmények száma a világban, és a természeti katasztrófák száma, ha nem is nagymértékben, de azért valamelyest csökkent. [36] A terrorcselekmények változását nagyságrendekkel megnövekedett számszaki értelmezésekor fontos, figyelembe venni, hogy az adatok az összes terrorcselekményt tartalmazzák, és ennek csak nagyon kis hányada irányult nukleáris létesítmény ellen. Ezek közül én két tanulságos támadást emelek ki röviden összefoglalva:

- Behatolás az Oak Ridge-i urántárolóba 2012-ben, ahol fegyver minőségű uránt tárolnak, kezelnek és dolgoznak fel. A nukleáris létesítmény az Y-12-es katonai komplexum (Manhattan-projekt) területén épült 2001. szeptember 11. után. A támadást 3 behatoló hajtotta végre: Michael Walli (63); Megan Rice (84); Greg Boertje-Obed (57). Kerítések átvtágták, különböző akadályokon áthatoltak, a tároló falát kalapáccsal ütötték, vérrel lellocsolták és jelszavakat festettek rá. A támadás célja a nukleáris fegyverkezés elleni tiltakozás volt.[37]
- A másik eseményről kevesebb információ áll rendelkezésre, ami viszont már üzemelő atomerőmű elleni támadását célozta meg. Oroszországban 2005 októberében Csecsen lázadók öt alkalommal kíséreltek meg repülőgépet eltéríteni, melyek során különböző oroszországi célpontokat szándékoztak támadni, melyek között szerepelt egy erőműi reaktor is.

A két esemény elkövetésének az indítéka, célja teljesen különböző volt. „Az Oak Ridge-i Környezetvédelmi Békeszövetség elnevezésű szervezet közlése szerint a csoport célja nem az volt, hogy demonstrálja az objektum sebezhetőségét, hanem az, hogy az általuk háborús bűnnek minősített nukleárisfegyver-gyártás ellen tiltakozzanak.”[37] Az oroszországi tervezett cselekménynél viszont egyértelműsíthető a háborús helyzetben, belső zavargásokat gerjesztő Csecsen lázadók terroristatámadása volt, amivel nukleáris katasztrófát akartak előidézni. Számomra nagyon tanulságos az Oak Ridge-i behatolás, mert az aktivisták szándéka csak a tüntetés, tiltakozás volt, de magával a szabotázs végrehajtásával felhívhatták a figyelmét a nemzetközi terrorszervezeteknek arra, hogy egy fokozottan őrzött nukleáris objektum területére milyen egyszerűen be lehetett jutni. Fontos itt megjegyezni, hogy az incidens után az amerikai kongresszus és az energiaügyi



minisztérium vizsgálatot indított melynek eredményeként a biztonsági vezetőket és a biztonsági szolgálatot ellátó őrzés-védelmi céget leváltották. A két eseményt összegezve elmondható, hogy a tüntetéstől a terrorcselekményekig nagyon sokféle céllal hajthatnak végre nukleáris létesítmények ellen irányuló támadásokat, aminek a sokszínűségét az 1966 és 2007 közötti támadások felsorolása is megmutatja.

Nukleáris létesítmények ellen irányuló támadások 1966-tól 2007-ig:

- 1966 - 1977: Európa - 10 nukleáris létesítmény ellen elkövetett terrortámadás
- 1968 - 1974: USA - 32 károkozással járó cselekményt, ill. szabotázs gyanúját észlelték különböző nukleáris létesítményekben
- 1978: Spanyolország - bomba robbant a leonizi atomerőmű gőzfejlesztőjénél
- 1982: Franciaország – 4 páncéltörő rakétát lőttek ki a creys - malville-i nukleáris létesítményben elhelyezkedő Super Phénix kutatóreaktorra
- 1982: Dél-Afrikai Közt. - robbantásokat hajtottak végre az épülő koebergi atomerőműnél
- 1987: USA - bomba robbant a Sandia Nemzeti Laboratórium parkolójában
- 1992: Oroszország - 3 atomerőmű ellen irányuló fenyegetést regisztráltak
- 2004: Ausztrália - terrortámadást terveztek Sydney-ben a Lucas Heights kutatóreaktor ellen
- 2005: Lashkar - e - Toiba (Igazak Hadserege) terrorszervezet tagjai a kihallgatásuk során beismerték, hogy a célpontok között szerepelt az indiai Kaiga atomerőmű
- 2007: Dél-Afrikai Közt. - 4 felfegyverzett támadó behatolt a pelindabai fokozottan őrzött nukleáris létesítménybe [38]

### **2.2.3 Atomerőművek őrzésének és védelmének fő feladatai**

Az atomerőművek nukleáris védettségi rendszerének üzemeltetése összetett bonyolult feladat, mert a létesítmény működésének teljes időtartama alatt illeszkednie kell a társaság gazdasági céljaihoz, hazai jogszabályi előírásokhoz, a hatósági elvárásokhoz, útmutatókhoz és a nemzetközi követelményekhez. A nukleáris anyagok, nukleáris létesítmények, radioaktív sugárforrások és radioaktív hulladékok elleni terrorcselekmények vagy szabotázsok elkövetésének fenyegetésével szemben a fizikai védelemnek kell biztonságot nyújtani. A fizikai védelem – az atomenergiáról szóló 1996. évi CXVI. törvény 2. § 33. bekezdése alapján – „*azon belső szabályozás, technikai*

*eszköztár és előerős elhárítás összessége, amely a nukleáris védettség részeként a nukleáris létesítményekkel, valamint nukleáris és más radioaktív anyagokkal szemben elkövetendő jogtalan eltulajdonítás és szabotázs észlelésére, elrettentésére, késleltetésére és elhárítására irányul.” [30 2 § (33)]*

A nukleáris létesítmények, nukleáris és más radioaktív anyagok fizikai védelmével kapcsolatos előírásokat többek között az atomenergiáról szóló 1996. évi CXVI. törvény, az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló 190/2011. (IX. 19.) Korm. rendelet, valamint hatósági és nemzetközi útmutatók tartalmazzák. Hazánkban a nukleáris létesítmények fizikai védelmi rendszerének alkalmasnak kell lennie a tervezési alapfenyegetettség hatékony és időbeni észlelésére, késleltetésére és elhárítására. A tervezési alapfenyegetettség a fenyegetettség állam által meghatározott azon szintjét jelenti, amely ellen a hatékony fizikai védelmet az atomenergia alkalmazója biztosítja. A tervezési alapfenyegetettséget meghaladó mértékű fenyegetés esetén állami eszközökkel egészül ki a védelem [30]. A tervezési alapfenyegetettséggel szemben a hatékony fizikai védelmi rendszer tervezéséért, létrehozásáért és folyamatos működtetéséért az atomenergia alkalmazója a felelős.

Az atomerőművek fizikai védelmi rendszerével szemben támasztott törvényi követelményeket kielégítésére biztonságtechnikai eszközöket és technikákat kell alkalmazni. Az alapvető technikák alatt az előerős védelem, a mechanikai védelem és az elektronikai vagyonvédelmi rendszerek összességét értjük, amit más néven komplex védelmi rendszernek is hívhatunk. A továbbiakban felvázolt őrzési-védelmi feladatok megvalósítására készített javaslatom egy általános megoldási lehetőséget kínál az atomerőművek részére, nem a Paksi atomerőmű jelenlegi kialakítását tükrözi. A komplex védelmi technikákat a biztonságtechnikai alrendszerek mentén mutatom be:

Élőerős védelem alkalmazott erőforrásai:

- Fegyveres Biztonsági Őrség (FBŐ) 27/1998. (VI. 10.) BM rendelet alapján
- Őrszolgálat – a 2005. évi CXXXIII. törvény. a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól. szóló törvény alapján
- TEK Terror Elhárítási Központ a tervezési alapfenyegetettséget meghaladó cselekmények elhárítására

Mechanikai védelem:

- Kerítésvédelem (mechanikus védelem elektronikus fedővédelemmel)
- Beléptetési pontok és zónahatárok forgókapui, zsilipjei
- Rácsok, szögesdrótok
- Zárak

Elektronikus rendszerek:

- beléptetőrendszerek
- videó megfigyelő rendszerek (látható és infratartomány)
- fokozott védelmet igénylő helyiségek kiegészítő védelme
- kommunikációs hálózat (biztonságos kommunikáció, alternatív megoldások)
- monitorközpont (kijelzések, vezérlések, irányító központ)
- kültéri mozgásérzékelők
- beltéri mozgásérzékelők
- objektum felületvédelmi eszközei
- nyílászárók elektronikus védelme
- biometria azonosítók
- röntgengépek (csomag)
- fémdetektáló kapuk
- sugár kapuk
- robbanóanyag detektáló berendezések [27]

#### **2.2.4 Nukleáris energiatermelő objektum komplex védelme**

A komplex védelmi megoldásokon túl a nukleáris létesítmények védettségének kialakításához alkalmazni kell a mélységi védelem elvét és védelmi zónákat kell kialakítani. A mélységi védelem a nevéből is adódóan jól bemutatja, hogy a védendő objektumon belül a védendő vagyont, esetünkben a nukleáris anyagot, illetve a nukleáris biztonságra közvetlen hatást gyakorló technológiákat több védelmi vonallal kell körülni. A védelmi rendszer kialakítása során a tárolt vagy alkalmazott nukleáris anyag ismeretében védelmi szinteket kell meghatározni. A védelmi szintek megfelelő alkalmazásához és kialakításához a 190/2011 (IX.19.) korm. rendelet és mellékletei egyértelmű iránymutatást adnak. A jogszabály a kategóriába sorolt nukleáris, radioaktív anyagok függvényében egyértelműen meghatározza az alkalmazandó védelmi szinteket.

A jogszabály négy fizikai védelmi szintet fogalmaz meg. A meghatározásnak megfelelően a védelmi szinteket úgy kell kialakítani, hogy az biztosítsa a hozzá tartozó követelményeket:

- „A-szinten a szabotázs és a jogtalan eltulajdonítás megakadályozását,
- B-szinten a szabotázs és a jogtalan eltulajdonítás lehetőségének csökkentését,
- C-szinten a jogtalan eltulajdonítás lehetőségének csökkentését, és
- D-szinten az alapvető védelmi intézkedések alkalmazását.”

Az energiatermelő atomerőművekben az üzemanyagkötegek dúsításából adódóan a jogszabály szerinti védelmi szint besorolás alapján minimum B szintű védelmet kell kialakítani. A mélységi védelem elvei alapján a védelmi vonalak kialakításához védelmi zónákat kell létrehozni a védelmi szinteknek megfelelően. A fizikai védelmi zónáknak kívülről befelé haladva fokozatosan egyre magasabb biztonsági szintet nyújtó védelmi képességekkel kell rendelkezniük.

Fizikai védelmi zónák:

- ellenőrzött zóna
- őrzött zóna
- fokozottan őrzött zóna
- belső zóna [39]

A komplex fizikai védelmi rendszer hatékony kialakításához az egymáson belül elhelyezkedő zónákhoz hozzá kell rendelni a védelmi szinteket. Előzőekben már megállapításra került, hogy egy atomerőmű esetében a kötelezően alkalmazandó védelmi szint az a B védelmi szint. A nukleáris létesítmények fizikai védelmét szabályozó nemzetközi és hazai jogszabályok konkrétan meghatározzák, a védelmi szintek és védelmi zónák kapcsolatát. Az alkalmazott nukleáris anyag miatt B védelmi szintet kell alkalmazni. A B védelmi szintet a fokozottan őrzött zónában kell létrehozni. Ebből adódik, hogy bentről kifelé haladva a fokozottan őrzött zónát az őrzött zóna veszi körül C szintű védelemmel és azt pedig az ellenőrzött zóna D védelmi szinttel.

Grafikusan ábrázolva egy egyszerű sematikus rajzzal így mutatható be:



9. ábra - A fizikai védelmi zónák kialakítása a védelmi szintek függvényében

Élőerős védelem megtervezésénél a három szervezetenként egymástól elkülönült egységek alapvető feladatainak a többségét a vagyonsvédelmi törvény hatálya alá tartozó őrszolgálati feladatok elvégzésével megbízott szervezetnek kell végrehajtania. Az atomerőmű folyamatos működéséből adódóan az élőerős védelem minden résztvevője 0-24 órás váltóműszakos rendszerben kell működjön. A szervezetnek el kell látnia az erőművet üzemeltető, karbantartó és egyéb személyzetének a folyamatos ki és beléptetését. A ki és beléptetés során ellenőrizni kell a beléptető pontokhoz érkező személyek jogosultságát illetve a teherportán a gépkocsikat is. A beléptetési jogosultság ellenőrzését követően az áthaladó forgalom által ki és beszállított eszközök vizsgálatát és a nem személyi használatú tárgyak esetén azok engedélyezését. A beléptető pontokon üzemeltetni kell a fémkapukat, a sugárkapukat és az automata tolókapukat. Tekintettel a veszélyes ipari üzem mivoltára, el kell rendelni az üzemeltető személyzet területre való belépéskori véletlenszerű alkoholszondás és drogtesztes ellenőrzést.

A területet fel kell osztani különböző fizikai védelmi zónákra a technológia berendezések és a veszélyeztetettség figyelembevételével. Egy úgynevezett nyomottvizes atomerőművet példaként véve jól el lehet határolni a nukleáris folyamatot fenntartó technológia helyiségeket (primer kör, reaktor és berendezései) és a villamos energia előállításában közvetlen résztvevő technológiai berendezések (szekunder kör, turbó gépcsoport és berendezései) helyiségeit, amelyek önmagukban képezhetnek egy zónát. Ellenőrzött zónát kell kialakítani az objektum (atomerőmű) területi határán kezdődően. Ebben a zónában jellemzően a technológiai folyamatokat nem érintő épületek (irodák, raktárak és javító műhelyek) helyezkednek el. Őrzött zónát az ellenőrzött zónán belül kell kialakítani úgy, hogy az magába foglalja a szekunder technológiai épületeket és a termeléshez vagy a nukleáris biztonság biztosításához kapcsolódó épületeket, berendezéseket. Fokozottan őrzött zónát az őrzött zónán belül kell kialakítani úgy, hogy

az magába foglalja a primer technológiai (reaktorépületet) épületet. Valamint fokozottan őrzött zónát kell kialakítani a nukleáris biztonság szempontjából jelentős rendszert, rendszerelemet tartalmazó épületek, helyiségek körül. Ezek közé tartoznak a blokkvezénylők, számítógép termek és a reaktort szabályzó-és biztonságvédelmi rendszerét tartalmazó helyiségek.

A zónahatároknál zsilipes, illetve forgókeresztes beléptető rendszereket kell kialakítani, amelyek segítségével akár egy adott személy területi mozgása is meghatározható. A fokozottan őrzött védelmi zónába történő átlépés esetén, az FBŐ szolgálatot kell megbízni az őrzési védelmi feladatokkal a 27/1998. (VI. 10.) BM rendelet alapján, és a veszélyeztetés mértékének függvényében, a fegyveres biztonsági őrsg rövid lőfegyvertől eltérő nagyobb hatótávolságú, gépkarabélyokat kell rendszeresíteni. Általánosságban mondható, hogy a kiemelten fontos pontokon, illetve területen felállított őrt kell alkalmazni. Az erőműben felállított örök által nem biztosított körzetét járőrözéssel kell ellenőrizni. [40] Az örök éberségének fenntartása érdekében az őrzési, ellenőrzési pontokon a személyzet folyamatos 2 óránként rotációs váltásával kell lefedni a 0-24 órás szolgálati időt. A járőrözés hatékonyságát mindenképpen járőrellenőrző rendszer kiépítésével és a lefedetlen területeknél zárt láncú kamerarendszer alkalmazásával kell támogatni. További fő feladatként deklarált a különböző funkciókat ellátó elektronikai rendszerek, mint például a fémdetektálókapuk vagy a területre való fegyverek bejuttatását megakadályozó, illetve azok detektálását szolgáló rendszerek üzemeltetése. A fentiek figyelembevételével egy tervezett atomerőmű biztonsági rendszerének a kialakításakor ellenálló komplex védelmi megoldást lehet megvalósítani. Természetesen a fő feladatokat további alfeladatokra kell bontani az aktuális környezeti tényezőkhöz igazodva. Összegezve elmondható, hogy a védelmi rendszerek kialakítása összetett feladat, ami nagy odafigyelést és széleskörű szakmai ismereteket igényel, de az általam végzett elemzés egy teljesértékű védelmi terv kidolgozásához szükséges és elégséges követelményrendszer alkot. [41] [27]

### **3 ÉLŐERŐ HATÉKONYSÁGÁT BEFOLYÁSOLÓ HUMÁN TÉNYEZŐK VIZSGÁLATA**

Az élőerő a komplex védelem tekintetében a napjainkban alkalmazott objektumbiztonsági rendszerekben az egyetlen, beavatkozásra képes elhárító funkcióval rendelkező védelmi alrendszer. Ebből egyenesen következik, hogy kiemelt fontossággal kell kezelni a kialakításukat és az üzemeltetésüket. A hatékony komplex vagyónvédelmi rendszer csak akkor valósítható meg, ha az objektumvédelem komponensei összehangolt, optimalizált és kockázatokkal arányosan kerülnek alkalmazásra. [42] Az élőerő hatékonyságának befolyásoló tényezőit, a hatást gyakorló faktorok forrásoldali szempontjai, a kockázat statikus vagy dinamikus jellege és az élőerős védelem életciklus fázisai alapján vizsgálom.

A forrásoldali szempontként a rendszerszintű és az egyéni humán kockázati tényezőket azonosítottam.

A védelmet befolyásoló humán tényező statikus és dinamikus jellege alatt azt kell érteni, hogy a kockázat kizárására, illetve annak a legalacsonyabb szintre való redukálására hozott intézkedés, egyszeri vagy ismételt végrehajtásával valósítható-e meg.

Az élőerős védelmi rendszer életciklusát alapvetően két fázisra lehet bontani, amelyek a tervezés - kialakítás és az üzemeltetés. A leírt elemzési szempontok objektíven külön-külön nem vizsgálhatóak, mivel ezek egymással szoros kölcsönhatásban vannak. Ebből kifolyólag az életciklus fázisai köré csoportosítva mutatom be a hatékonyságot befolyásoló tényezőket.

#### **3.1 A tervezési fázisból származtatható élőerős védelmi rendszer hatékonyságát befolyásoló tényezők**

A komplex objektumvédelmi rendszer tervezési feladatainak végrehajtása a vagyónvédelem területeinek átfogó ismereteit igényli műszaki és humán vonatkozásban egyaránt. Az elmúlt években több tanulmány, publikáció és disszertáció is készült, amelyek rávilágítanak a hatékony és optimális vagyónvédelmi koncepció kialakításának nehézségeire. Ennek ellenére meg kell jegyezni, hogy a tanulmányok többsége csak valamelyik vagyónvédelmi alrendszert fókuszba állítva vizsgálja a témakört, így az élőerős védelemmel kapcsolatosan viszonylag kevés szakirodalom áll rendelkezésre. Az általam végzett vizsgálatot én is az élőerő megtervezésének középpontba állításával végeztem el

a technikai alrendszerek konstellációjában. A biztonsági szolgálat koncepciójának kidolgozása az adott intézmény, szervezet, vagy vállalkozás biztonságának és védelmének hatékony és átfogó megközelítését jelenti. Egy ilyen koncepció kialakítása fontos a kockázatok minimalizálása, a veszélyek megelőzése és a biztonságos környezet fenntartása érdekében. Ennek kulcsfontosságú lépési a következők, amelyeket figyelembe kell venni a tervezése során:

1. Szakértői csapat kialakítása: Előkészületi fázisban, a nulladik lépésként létre kell hozni egy szakértőkből álló csapatot, akik részt vesznek a biztonsági koncepció kialakításában. Ez a csapat magában foglalja a biztonsági szakembereket, informatikai szakembereket és más releváns szakértőket.
2. Kockázatértékelés: Az első lépés a kockázatértékelés végrehajtása. Nagyon fontos az alapos kockázatértékelés elvégzése a helyszínrre jellemző potenciális biztonsági fenyegetések és sebezhetőségek azonosítására. Az előerő vonatkozásában a kockázatok helyes megítélése szükséges a megfelelő létszám, felállítási helyek és munkarend meghatározásához.
3. Célok és prioritások meghatározása: Az alapján, hogy milyen veszélyeket azonosítottunk, meg kell határozni a biztonsági szolgálat fő célját és prioritásait. Fontos, hogy ezek a célok legyenek konkrétak, mérhetőek a biztonsági terv hatékonyságának értékeléséhez.
4. Létszám és ütemezés: A kockázatértékelés és a biztonsági célok alapján meghatározható a megfelelő számú biztonsági személyzet, amely az objektum, védendő terület megfelelő lefedéséhez szükséges. Ezt alapvetően a terület mérete, a belépési pontok száma és a fenyegetettség szintje határozza meg. Továbbá a feladatspecifikációból következhet, hogy különböző típusú őrszemélyzet (vagyonőr, fegyveres biztonsági őr) kerül alkalmazásra. Az objektum működéséhez kell igazítani a műszakbeosztást. Ez alatt azt értem, hogy a hétfőtől péntekig napi 8 órában üzemelő létesítmény, ami 0-24 órás Őrzést igényel, ott természetesen nem egyenletes az őrök terhelése.
5. Intézkedések és protokollok kidolgozása: A védelmi alrendszerek önmagukban rezsimitézkedések, szabályzatok nélkül nem képesek ellátni funkcióikat, ezért azok kidolgozásakor egy mindent átfogó biztonsági tervet kell készíteni, amely a védelem teljes spektrumát lefedi. [28] Biztosítani kell a technikai eszközök



szakszerű működtetését biztosító dokumentumokat, külső szabályzatokat, belső szabályzatokat, valamint az előre kidolgozott intézkedési terveket.

6. Kommunikáció és koordináció: Világos kommunikációs csatornákat kell létrehozni a biztonsági örök, a vezetőség és az érintett érdekelt felek között. A hatékony kommunikáció kulcsfontosságú az információk megfelelő áramlásához, az incidensekre, eseményekre való reagáláshoz és a vészhelyzetek során az erőforrások összehangolásához.
7. Rendszeres felülvizsgálatok: A biztonsági terveket rendszeresen felül kell vizsgálni és a vizsgálati eredmény függvényében frissíteni. A felülvizsgálatok során elemezni kell az esetleges változásokat a fenyegetések, a technológiai vagy a szervezet vonatkozásában. Folyamatosan fenn kell tartani a jogi szabályozásoknak való megfelelést és a változásokat le kell követni a belső szabályozókban
8. Minőségbiztosítás: A biztonsági örök teljesítményének és hatékonyságának ellenőrzésére szolgáló rendszer kialakítása és bevezetése elengedhetetlen. A rendszeres értékelések és visszajelzések segíthetnek azonosítani a fejlesztendő területeket és fenntartani a magas színvonalú biztonsági szolgálat működtetését.

Az élőerős alrendszer kialakításánál a fenti szempontok szerinti megvalósítás esetén olyan komplex védelmi rendszer alakítható ki, amelynél a humán tényezőtől fakadó kockázatok a minimálisra csökkenthetők.

### **3.2 Az üzemeltetési fázisból származtatható élőerős védelmi rendszer hatékonyságát befolyásoló tényezők**

Az élőerős védelmi alrendszer üzemeltetésének hatékonyság vizsgálatakor feltételeztek egy szinte „tökéletesen” végrehajtott megelőző tervezési fázist. Természetesen annak tudatában, hogy nincs tökéletes tervezés, ahogy 100%-os biztonság sincs. A kutatási, elemzési munkám szempontjából ez azt jelenti, hogy a tervezés pillanatában a létező összes biztonsági kockázat felismerésre került és azok megszüntetésére, illetve minimálisra csökkentésére alkalmas védelmi koncepció került kidolgozásra. Továbbá az őrség felállítása és üzemeltetése ennek megfelelően lett megvalósítva. Az élőerős szolgálat üzemeltetése során a humán tényezőkből adódó nehézségek jelentős mértékben befolyásolják az őrzésvédelmi tevékenység hatékonyságát és a biztonsági személyzet

teljesítményét. Az alábbiakban néhány olyan kockázatot sorolok fel, amelyek humán tényezőkből erednek:

1. Személyzet Felvétel és Megtartása: Megfelelően képzett és megbízható biztonsági személyzet toborzása és megtartása gyakran kihívást jelent. A magas fluktuáció és a verseny a munkaerőpiacon nehezítheti a képzett személyzet megtalálását.
2. Munkaidő és Műszakok: Biztonsági szolgálatok általában 24/7-es műszakrendben működnek, ami hosszú munkaidőket és éjszakai műszakokat jelenthet. Ez a személyzet fizikai és mentális egészségét befolyásolja, valamint megnehezíti a munka-magánélet egyensúlyának fenntartását.
3. Veszélyeztetettség: A biztonsági személyzet gyakran veszélyeztetett helyzetben dolgozik, és fizikai vagy verbális agresszióval találkozhat. Ez stresszt és traumaélményeket okozhat, amelyek kezeletlensége marandandó pszichikai degradációt okozhat a személyzetben.
4. Munkahelyi Stressz és Kiegészítés: A munkahelyi stressz és kiegészítés a magas nyomás és a veszélyhelyzetekkel való folyamatos szembesülés miatt gyakori lehet a biztonsági szolgálatoknál. A stressz és a mentális egészség problémáinak kezelése kiemelten fontos.
5. Munkavállalói konfliktusok: A személyzet közötti konfliktusok és problémák a hatékony munkavégzés zavarához vezethetnek. Ezeknek a konfliktusoknak kezelése és megelőzése fontos.
6. Ügyfélkapcsolatok: A biztonsági személyzetnek meg kell találnia az egyensúlyt az ügyfél elvárásai és a biztonság fenntartása között. Az ügyfélszolgálati problémák és panaszok kezelése kihívást jelenthet.
7. Etikai Dilemmák: A biztonsági személyzet találkozhat etikailag aggályos esetekkel. Például, ha olyan szóbeli utasítást kap, ami ellentmond vagy nincs összhangban a szabályozó dokumentumok utasításaival a törvényekkel vagy az emberi jogi normákkal. A védelmi szervezeten belül az ilyen esetek felismerésére és vállalhatóságára megfelelő protokollokat kell kidolgozni, különben előfordulás esetén jelentős mértékben csökkentheti a biztonság mértékét.
8. Munkavállalói Elégedettség: A biztonsági személyzet elégedetlensége erősen kihathat a munkavégzés minőségére és a szolgáltatás megbízhatóságára. A munkavállalók elégedettsége sok tényezőtől függ, de talán a legfontosabb a

megfelelő bérek és juttatások alkalmazása, ami arányos az elvégzett munka mennyiségével és az elvárt minőséggel.

9. Kommunikációs Nehézségek: A hatékony kommunikáció kritikus fontosságú a biztonsági szolgálatokban. Bármilyen hibás kommunikáció vagy információhiány komoly biztonsági problémákat okozhat. Az őrség kommunikációjába beleértendő a nem szolgálati információk áramlása is.

A fentiekben azonosított humán tényezőket rendszerszintű problémák közé sorolom, amelyek közül bármelyik bekövetkezése az élőrön belül a személyzet tagjaira egyedi negatív hatását fejt ki. A biztonsági őr munkájának során a legnagyobb kihívást a munka jellegéből adódó monotonitás jelenti. A monotonitás szerepe Tóth Levente „*Videó megfigyelő rendszerek hatékonyságnövelő lehetőségei a közterületi megfigyelés területén*” című értekezésében és Szabó Anikó „*Különböző rendeltetésű szervezetek objektumainak őrzésbiztonsági feladatait ellátó személy- és vagyonőrök gyakorlati képzési-fejlesztési lehetőségeinek vizsgálata és elemzése*” című disszertációjában is megjelennek, mint humán tényező, amely kiküszöbölésére jelentős figyelmet kell fordítani. [43],[44] A biztonsági őrök munkája gyakran magában foglal ismétlődő tevékenységeket, mint például folyamatos járőrözés vagy azonos ellenőrzések végzése. A monotonitás, vagyis az ismétlődő és egyhangú feladatok végzése hosszú távon negatív hatással lehet a biztonsági őr teljesítményére és éberségére. A monoton munka különösen akkor probléma, ha hosszú ideig tart, és nincs lehetőség a változatosságra. Amennyiben az élőrös védelmi szervezetben a monotonitás számottevő jelenségként megfigyelhető, akkor az negatív hatással fogja befolyásolni a biztonsági őr teljesítményét. A monotonitás negatív hatásának kifejtési módjai:

1. Csökkentett Éberség: Az ismétlődő feladatok és a monotonitás könnyen vezethetnek a figyelem elvesztéséhez. A biztonsági őröknek állandóan ébernek kell lenniük a veszélyek és a rendellenes események felismeréséhez, és ha a munka monotonná válik, könnyen megtörténhet, hogy nem veszik észre a veszélyeket.
2. Hibák és Figyelmetlenség: A monoton munka során a figyelmetlenség és a hibák kockázata megnő. A biztonsági őröknek pontosan és folyamatosan kell végrehajtaniuk az előírt feladatokat, és ha a munka unalmassá válik, könnyebben követhetnek el hibákat vagy hagyhatnak ki fontos részleteket.

3. **Motiváció Csökkenése:** A monoton munka hosszú távon csökkentheti a biztonsági örök motivációját. Az ismétlődő feladatok és a változatosság hiánya unalmat és elégedetlenséget okozhat a munkavállalók körében, ami negatívan befolyásolhatja a teljesítményüket. Napjainkban megfigyelhető jelenség a motiválatlanság növekvő tendenciája, ami nem csak a fiatalabb korosztályt érinti. Az őrásban vezető szerepet betöltő pozícióban dolgozóknak már a motiválatlanság kialakulási fázisában érdemes beavatkozni. [45]
4. **Kommunikációs Problémák:** A monoton munka könnyen vezethet a közönyhöz és az összehangolási problémákhoz a biztonsági személyzet között. A hatékony kommunikáció rendkívül fontos a biztonsági munka során, és a monotonitás zavarhatja ezt a kommunikációt.
5. **Fáradtság és Kényelmetlenség:** A hosszú órák alatt ismétlődő tevékenységek végzése fizikailag és mentálisan kényelmetlen lehet. A túlzott fáradtság és kényelmetlenség befolyásolhatja a biztonsági örök teljesítményét és éberségét.

Az élőerős alrendszer üzemeltetése során az általam összegzett rendszerszintű és egyéni kockázati tényezők mindegyike olyan tényező, amely nem feltételez szándékosságot, csak a személyzetre gyakorolt hatást jelenti.

### **3.3 A humán kockázati tényezők komplex vizsgálata gyakorlati megközelítésben**

A biztonsági szektorban is létező jelenség a szándékos, rosszindulatú cselekmények szervezeten belüli megjelenése. A jelenséget a szakirodalomban belső elkövető néven ismerhetjük. A jogszabályi szinten is megjelenik az ilyen jellegű cselekmények kockázati tényezőként való figyelembevétele. A 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló kormányrendelet 2. §-ban is megfogalmazásra kerül a belső elkövető fogalma: *„belső elkövető: a jogtalan eltulajdonítás vagy szabotázs végrehajtását elkövető, vagy a végrehajtást segítő olyan személy, aki a fizikai védelmi tervben meghatározott be- és kiléptetési rend alapján az adott létesítménybe belépésre jogosult”*. [46 2. §] A gyakorlatban ez azt jelenti, hogy olyan személyekről van szó, akik legálisan beléphetnek és tartózkodhatnak az adott objektum területére munkavégzés vagy más egyéb célból, de ezen belépési joggal visszaélve illegális tevékenységet folytatnak, megzavarva a létesítmény normál működését. Amennyiben a fenyegetések ténylegesen

be is következnek, akkor már incidensről beszélünk és a kockázat következményeivel kell számolnunk. A fenyegetések és a következmények elméleti megközelítésben nagyon sokrétű lehetőséget kínál a kockázatelemzés, amelyekre hozott intézkedések eredményességére csak egy valós esemény bekövetkezésekor kapunk választ. Feltételezéseim igazolása céljából több kriminalisztikai eseményt dolgoztam fel a kutatásom során, amelyből két belső elkövető által végrehajtott cselekménysort részletesebben is elemeztem, a humán kockázatok fókuszba állításával.

### **3.3.1 Energiatermelő atomerőmű ellen elkövetett szabotázs elemzése**

A belgiumi Doel 4 Atomerőműben történt nukleáris biztonságot és védettséget érintő 2014-es esemény elemzésének kiválasztási szempontja az elkövetési mód és az esemény következményei voltak. Az atomerőműben 2014 augusztusában a 4-es reaktorblokkhoz tartozó szekunder körüli turbinájáról elkövetők leeresztettek mintegy 65 m<sup>3</sup> mennyiségű kenőolaját. Az olaj leengedését a turbina vészleürítő rendszerének egyik zárt szelepének kinyitásával hajtották végre, ezzel a berendezés kenőanyag nélkül maradt, aminek következtében a turbina túlhevült és súlyosan károsodott. A cselekményt végrehajtó és az őt feltételezetten segítő személyek mindegyike érvényes belépővel rendelkeztek a létesítménybe, így rejtetten maradtak a fizikai védelmi rendszer előtt. A létesítmény jellegéből, védelmi rendszeréből következik, hogy a külső elkövetői végrehajtás szinte teljesen kizárható, mivel a berendezéshez való eljutáshoz, hozzáféréshez több védelmi zónán kellett volna átjutnia észrevétlenül, aminek igen kicsi a valószínűsége. További három fontos dolog volt szükséges a sikeres végrehajtáshoz, mégpedig a helyismeret, a megfelelő szakértelem a szelep kinyitásához, valamint átcímkezéséhez szükséges szerszámok. Az elkövetők teljesen tisztában voltak a szelep funkciójával és azzal is, hogy az olajrendszer leürítésével mekkora kárt tudnak okozni. Az elkövetők szakértelmét az is bizonyítja, hogy a szelep nyitását követően úgy címkézték át, hogy az a szelep zárt állapotát jelezte, ezzel észrevétlenné téve a beavatkozást. A sikeresen végrehajtott szabotázzsal olyan súlyos kárt okoztak, hogy a javítási munkák elvégzéséhez négy hónapos leállásra volt szükség. A javítási költségek és a négyhónapos termelés kieséssel közel 200 millió eurós kárt okoztak. Az esemény bevonult a nukleáris ipar történelmébe, mint az egyik legnagyobb gazdasági kárral járó szabotázs. Természetesen semmilyen radiológia következménnyel nem járt az eset, mivel a berendezés nem kapcsolódik közvetlenül a reaktorhoz és a primerköri hőhordozó berendezéseire. [47]

### 3.3.2 A világ legnagyobb gyémántbányájában elkövetett lopássorozat elemzése

A Nyugat-Ausztráliai Kelet-Kimberly régiójában található Argyle bányában végrehajtott gyémántlopásról elmondható, hogy egy hosszú időn keresztül folytatott belső elkövetői lopás volt, egy szervezett külső támogatóhálózattal bővítve. Ennek következtében a gyémántok a forrástól egészen a feketepiacig szabadon tudtak áramolni. A bányában elkövetett lopások időszaka 1988-tól 1993-ig tartott, amely idő alatt becslések szerint kb. 30 millió USA dollár értékű nyersgyémántot tulajdonítottak el és értékesítettek a feketepiacon. A gyémántbánya további sajátossága, hogy egy nagyon ritka rózsaszínű gyémántlelőhely, amelyből a világ rózsaszínű gyémánttermelésének mintegy 90% származik. Az ilyen különleges gyémántok értékének érzékeltetésére érdemes megemlíteni, hogy 2022-ben egy körte alakú 18 karátos rózsaszínű gyémánt 28,8 millió dollárért kelt el a genfi aukción. [48] A belső elkövető személye maga a biztonsági szolgálat vezetője volt, aki korábban a Victoria Szövetségi Államban szolgált rendőrként. A bányában betöltött pozíciójába is már egy külső segítség beszerző tevékenységének köszönhetően került. Betöltött beosztása következtében korlátlan hozzáférése volt az objektum teljes területén, ami lehetővé tette a teljes mozgásszabadságot és egyben elengedhetetlen volt a gyémántlopás sikere szempontjából. A hierarchikus rendszer lévén a biztonsági szolgálat vezető jogosultságát soha nem kérdőjelezték meg sem a beosztottjai, sem a gyémántok bányászatát és szortírozását végző munkások. Ez magyarázatot ad arra, hogy miért tudta a gyémántokat egy meglehetősen szokatlan film-tartó dobozban kiszállítani. A funkciójából adódóan részletesen ismerte a bányában érvényben levő védelmi intézkedéseket. Tudomása volt arról, hogy a gyémántoknak a bányában történő szortírozásának időpontja- és a lemérésük és regisztrálásuk időpontja között volt egy holtidő. Ismerte a videómegfigyelő rendszer, tartományát, a területi lefedettségét és működési időtartamaival is tisztában volt, továbbá ismerte a gyakran - egyedileg és rendszertelen időközönként - végrehajtott ellenőrzéseket is. Továbbá a feladatai közé tartozott a technikai rendszerek karbantartásával kapcsolatos tevékenységek felügyelete is. Feltételezhető, hogy a video megfigyelő rendszer meghibásodásainak javításait is szándékosan késleltette, illetve mulasztotta el, ezáltal csökkentve annak hatékonyságát.

Több rendőrségi vizsgálat is indult, de azok eredménytelenül zárultak. Végül az elkövető feleségének vallomása alapján indult harmadik vizsgálat nyomozása alapján bűnvádi eljárás indult, több elkövető ellen. Az elkövető vallomásában a kapzsi és magas anyagi

igényeket támaztó feleséget jelölte meg a bñncselekvény végrehajtásának motivációjaként.

### **3.4 Részkövetkeztetések**

Ebben a fejezetben bemutatam és vizsgáltam a humán kockázati tényezöket, valamint azok hatását a komplex védelmi rendszeren belül. Az elméleti vizsgálati részben a védelmi rendszer életciklusai szerinti bontásban sorakoztattam fel mind rendszerszintű, mind pedig egyéni szinten jelentkező kockázati tényezöket. A fejezet ezen része rámutat arra, hogy az emberi tulajdonságokból adódóan mindig is jelen vannak és lesznek az élöerő hatékonyságát befolyásoló humán kockázatok. Ki kell emelnem, hogy a komplex védelem területén az alrendszerek tekintetében az elektronikus védelmi alrendszer és a mechanikai védelmi alrendszer vonatkozásában nem vizsgáltam azok kockázatait, illetve feltételeztem, hogy azok a lehető legoptimálisabban kerültek kialakításra és üzemeltetésre. Az elemzésben kizártam azon tényezöket, amelyek e két alrendszer hiányosságaiból adódóan fejtenének ki negatív hatást az élöerő tekintetében.

A gyakorlati példákön, esettanulmányokon keresztül bemutatható az élöerős alrendszerből származó hiányosságok. A Doel Atomerómű esetében azonosítható a tervezési fázisban elvégzet kockázatelemzés és a rendszeres felülvizsgálatot leíró szabályozás üzemeltetési fázisban történő alkalmazásának elmulasztása. Ezen megállapításomat arra alapozom, hogy a szabotázs végrehajtásának idején az Európai Unió területén 2010 és 2014 között 16 terrorcselekményt hajtottak végre ezek közül kettőt Belgiumban és hetet a szomszédos államokban. [49] Ezzel párhuzamosan 2013-ban jelent meg Bryan R. Early és szerzötársainak azon tanulmánya, amely a nukleáris-radiológiai terrorizmus kockázatát vizsgálták. A kutatásban 152 ország 1992 és 2006 közötti időintervallumát elemezték, amelyben 80 támadást és 64 tervezett támadást azonosítottak. [50] Továbbá a szabotázs esemény következményeként a fizikai védelmi rendszer felülvizsgálatát követően új belső elkövetök elleni rezsimentézkedéseket vezettek be és technikai fejlesztéseket végeztek a videómegfigyelő rendszeren.[47] Tehát kijelenthető, hogy a fizikai védelmi rendszer külső fenyegetettsége megváltozott, amit egy preventív felülvizsgálat keretében észlelni kellett volna és az utólagosan hozott intézkedéseket megelőző intézkedésként be kellett volna vezetni.

Az Argyle gyémántbányai esettanulmány alapján több humántényezöből származó súlyos hiba is azonosítható, amit elsősorban az igazol, hogy az elkövető és segítői 5 éven

keresztül tudták folytatni a lopássorozatot. A biztonsági szolgálat vezetői beosztás személyi feltételei a legszigorúbb elvárásokat támasztja a betöltésre kiválasztandó személlyel szemben és egyben a legmagasabb biztonsági kockázatot is jelenti a rendszer egészére nézve. Ennek ellenére egy olyan személy tudta betölteni a vezetői munkakört, aki nem volt fedhetetlen, mivel egy beszerző tevékenység következtében került a beosztásába. Ez az üzemeltetési fázis első lépéseinek a nem megfelelő végrehajtását jelenti, mivel erkölcsileg fedhetetlen és megbízható személyzetet kell alkalmazni a védelmi rendszerben bármely feladatot ellátó munkavállaló tekintetében. Az esettanulmányban és az elméleti megközelítésben ismertetett információk alapján ezt a súlyos rendszerszintű hibák közé sorolom. A bányászati folyamatban a gyémántok szortírozása és regisztrálása között eltelt jelentős idő lehetőséget biztosított az elkövető számára, hogy nyomtalanul eltulajdonítsa a gyémántokat, amely az érintett objektumrészben a szokatlan és rendszeres megjelenését igényelte. A video megfigyelő rendszer karbantartásáért is Ő felelt. Vélhetően szándékosan késleltette vagy mulasztotta el a rendszerben keletkezett hibák elhárításának karbantartói megrendelését. Jelezni kellett volna a furcsa és sűrű biztonsági vezetői jelölést és a technikai rendszerelemek túlzottan hosszú üzemképtelenségeit. Mindent összegezve a motiváció csökkenése, az etikai dilemmák, a kommunikációs problémák és a csökkent éberség, mint humánkockázati tényezőket azonosítottam a személyzet munkája során, amelyek egymást erősítve fejtettek ki negatív biztonsági hatást.

Megállapítható, hogy ez a fejezet igazolja az első hipotézisemet, azaz napjainkban még mindig jelen vannak a komplex védelmi rendszerekben olyan élőerő hatékonyságát befolyásoló humán tényezők, amelyek számottevő kockázatokat jelentenek a védelmi rendszer egészére. A kiválasztott két esettanulmány egyike az 1990-es években történt, de a részletes elemzésére csak 2015-ben került sor a „*Belső fenyegetések: Nukleáris és nem-nukleáris esettanulmányokat bemutató oktatási kézikönyv*” -ben. [51]



## **4 A TECHNOLÓGIA FEJLŐDÉSŐL SZÁRMAZÓ BIZTONSÁGI KOCKÁZATOK, KIHÍVÁSOK**

Az élőrő hatékonyságát befolyásoló humán kockázati tényezők részletes elemzése mellett a kutatás szempontkából fontos a technológia fejlődés következtében megjelenő új biztonsági kihívásokat is tanulmányozni. A 2010-es évektől kezdődően az egyre kisebb elektronikai eszközök gyártását lehetővé tevő nanoelektronika robbanásszerű fejlődése gyakorlatilag a digitális világ teljes spektrumára kifejtette hatását. A globalizációs folyamat együtt jár az információ, tőke, munkaerő, áruk, szolgáltatások, politikai elvek és ideológiák szabad és gyors áramlásával. Ugyanakkor ez a folyamat összefonódik a technológiai fejlődéssel, mint például az elektronika, informatika, biogenetika, űrkutatás, mesterséges intelligencia és számos más műszaki tudományos terület robbanásszerű előrelépésével. Ezen fejlesztések kihatnak az IoT eszközök, IKT technológiák és a dróntechnológia rohamos fejlődésére, de formálja egyben a társadalmat is, aminek következménye, hogy sok elektronikai eszköz a mindennapi hétköznapiak részévé válik. [52] Az új technológiai eszközök használatának következtében felmerülő biztonsági kockázatok és problémák közül azt a két területet emeltem ki, amely a legelterjedtebb alkalmazást élvezi, illetve az elterjedésük rohamos tempóban növekszik. Ilyen eszközök az okostelefonok és a drónok.

Az elmúlt időszakban egyre szélesebb körben alkalmaznak pilóta nélküli légi járműveket (unmanned aerial vehicle továbbiakban: UAV) nem csak kutatási és hadiipari területeken, hanem a civil és kereskedelmi szektorban is. Ennek következtében a piac egyre sokoldalúbbá válik, és a gyártók igyekeznek minél több területen jelen lenni. Az ilyen eszközök elterjedésével kapcsolatban felmerülnek különböző kérdések a használat és üzemeltetés tekintetében.

Az biztonságtechnika területén is számos lehetőség mutatkozik ezeknek az eszközöknek a felhasználására, például a távfigyelés, a katasztrófa helyzetek értékelése vagy az infrastruktúra ellenőrzése terén. Azonban fontos kiemelni, hogy az ilyen technológiák potenciálisan veszélyesek is lehetnek, ha rosszindulatú célokra használják fel, mint például a magánélet megsértése, kémkedés vagy akár fizikai károk okozása. [53p. 168-169] Az ilyen eszközök elterjedésekor fontos az egyensúly megtalálása a hasznosítás és a biztonság között, hogy ezek a technológiák hozzájárulhassanak a társadalmi fejlődéshez anélkül, hogy veszélyeztetnék az egyéneket vagy a társadalom biztonságát.

Az okostelefonokról is elmondható, hogy a felgyorsult világban a használatuk nélkül nem lehet lépést tartani a mindennapi életben, ezért szinte mindig magánál tartja az ember. A gyártók annyira sok funkcióval látják el a telefonokat, hogy azok teljesítményükben és használatukban egy hordozható „zsebszámítógépnek” tekinthető. Ebből adódóan biztonsági szempontból egyben veszélyeket is hordoz magában. A kockázatok azonosításának elemzéséhez a nukleáris létesítményt választottam, mint védendő objektumot. A nukleáris létesítmények fizikai védelmi rendszere megfelelően tagolt és tudomásom szerint csak itt értelmezhető a légi szcenárió fogalma a nem katonai célú objektumoknál. Továbbá a 80-as 90-es években létesített nukleáris energiatermelő erőművek élettartam hosszabbítása és az új épülő erőművek technológiai rendszereinél egyre nagyobb teret hódít az IoT technológia és a digitalizáció. [54]

#### **4.1 A dróntechnológia elterjedéséből jelentkező új kockázatok azonosítása és elemzése nukleáris létesítmények vonatkozásában**

A kutatói munkám szempontjából fontosnak tartom az UAV-k potenciális veszélyeinek bemutatását nukleáris létesítmények szempontjából. Az UAV-k gyorsan fejlődő technológiák közé tartoznak, amelyek számos előnyt kínálnak, de növekvő fenyegetést is jelentenek a számuk és technológiai fejlődésük miatt. Nem szükséges alapos és mélyreható kutatást végezni ahhoz, hogy találjunk olyan eseteket, amikor drónokat használtak olyan cselekményekben, amelyek a nukleáris létesítmények elleni terrorcselekmények kategóriájába sorolhatók. Franciaországban például 2014-ben körülbelül harminc esetet dokumentáltak, amikor engedély nélküli drón repüléseket hajtottak végre nukleáris létesítmények felett. Az atomerőmű légterébe történő berepülések aggodalomra adnak okot, mivel nemcsak a drónok jelentenek problémát, hanem az is, hogy a biztonságért felelős hatóságok nem tudtak megfelelő magyarázatot adni ezekre az esetekre, és nem voltak képesek megakadályozni a drónok berepülését. [55] A berepüléseket a greenpeace aktivisták megbízásából hajtották végre azzal a céllal, hogy felhívják a figyelmet a nukleáris létesítmények sebezhetőségére. Ehhez egy supermant formázó drónt reptettek be a tiltott légtérbe és neki ütköztették a pihentető medencét tartalmazó épület falának. [56] Az eset nagyon tanulságos, mert magával a szabotázs végrehajtásával felhívhatják a figyelmét a nemzetközi terrorszervezeteknek arra, hogy egy fokozottan őrzött nukleáris objektum területére milyen egyszerűen lehet bejuttatni egy kereskedelmi fogalomban kapható pár száz dolláros eszközt. Amennyiben a pilóta nélküli légitársaságokban rejlik további technikai megoldások találkoznak a

terrorszervezetek ártó szándékú cselekményeinek céljaival, akkor már nem csak a berepülés tényével, hanem a keletkezett fizikai és reputációs károkkal is kell számolni. Annak valószínűségét nagyon nehéz megállapítani, hogy ilyen esemény valóban bekövetkezhet-e, de az alábbi nukleáris létesítmények terrorfenyegetésének statisztikája a valószínűség növekedését jelzi. A globális terrorizmus adatbázisában az 1966 és 1977 közötti időszakban tíz olyan terrorcselekmény található, amelyek európai erőművekkel vagy azokhoz kapcsolódó objektumokkal voltak összefüggésben. Az 1970 és 1999 közötti időszakban pedig összesen 167 eset került rögzítésre, amelyekben nukleáris célpontok érintettsége volt megfigyelhető. [38] A 2014-es évben Nagy Britanniában 37 olyan esemény történt, melyek során atomerőművek biztonsága volt veszélyeztetve, ezek közül egy alkalommal drón által. [57]

A 2001. szeptember 11-i tragikus események után világszerte a terrorizmus okozta globális fenyegetettség lényegesen nőtt. Egy arab újságíró szerint az al-Kaida eredetileg nukleáris létesítményekbe akart repülni eltérített repülőgépekkel a World Trade Center és a Pentagon helyett. Állítása szerint interjút készített a csoport két ötletgazdájával az Al-Jazeera televízió számára.[58] Ebben a kontextusban kiemelkedő fontosságú lett a nukleáris létesítmények elleni terrorfenyegetés elemzése. Természetesen az esemény után a témában készült tanulmányok többsége azt vizsgálta, hogy egy utasszállító repülőgép atomerőműre zuhanása milyen következményekkel járhat. 2007-ben jelent meg magyar nyelvű tudományos cikk, *„A nukleáris terrorizmus, mint potenciális fenyegetettség napjainkban”* címmel, amely vizsgálja a nukleáris fegyverek és erőművek működésének részleteit és elemzi, hogy terrorista csoportok milyen esélyekkel és milyen lehetséges forrásokból juthatnak hozzá nukleáris fegyverekhez. A publikáció megemlíti, hogy az újabb generációs erőművek tervezésénél már figyelembe veszik az, olyan repülőgép baleseteket, amelyek során érintve lehetnek az atomerőművek. [59] Az ABA MMT program keretében az Országos Atomenergia Hivatal (továbbiakban: OAH) megbízásából készült tanulmány *„A paksi Atomerőmű telephelye felett elhelyezkedő tiltott légtér méretének felülvizsgálata”* címmel. A tiltott légtér fontos védettségi szempontból és a véletlen vagy akár szándékos rázuhanás miatti nukleáris baleset kockázatának csökkentése érdekében is. A tanulmányban alkalmazott modell a rázuhanások éves valószínűségét elemzi és az alábbi következtetésre jutottak a munkában résztvevő tudományos munkatársak:

- „a tiltott légtér sugarának megduplázásával közel a felére csökkenne a rázuhanásokból származó kockázatok mértéke”
- „a légtér vízszintes kiterjedésének megváltoztatása (növelése) elősegítheti a védelemben résztvevő erők, szervezetek reakcióidejének növelését”
- „kis sebességű és kis magasságon repülő légjárművek ellen a tiltott légtér vízszintes kiterjedésének megnagyobbítása ténylegesen növeli az Atomerőmű védelmét”
- „a tiltott légtér köré egy további korlátozott légtér létrehozása indokolt”
- „a távirányítású repülőeszközök ellen a tiltott légtér kiterjedésének növelése, valamint a korlátozott légtér létrehozása nem elégséges védelem”
- „a repülőeszköz fedélzetéről indított pusztítóeszköz alkalmazása ellen a tiltott légtér kiterjedésének növelése, valamint a korlátozott légtér létrehozása nem elégséges védelem” [60 p. 5]

Az amerikai Légiközlekedési Szövetségi Légihatoság is vizsgálta a drónok polgári célú nagyarányú elterjedésének hatását és 2019 végén megkezdte az együttműködést az Energiaügyi Minisztériummal és a nukleáris ipar szereplőivel. Az egyeztetések megindításának kiváltó oka a megnövekedett drónos berepülések száma és az ellenük felmutatható arányos védelem és a szabályozások hiánya volt. Az atomerőmű biztonsági erőinek nincs felhatalmazása arra, hogy megkísérelje megakadályozni vagy elhárítani a létesítményeik felett repülő légi járművek berepülését, ideértve a drónokat is.

Magyarország területi légtérét két fő kategóriába sorolhatjuk: "ellenőrzött" és "nem ellenőrzött" légtér. Az ellenőrzött légtérben repülési tevékenységet kívánó személyeknek a felelős hatóság engedélyére van szükségük, amely felügyeli és szabályozza az ott zajló repüléseket. A Paksi Atomerőmű esetében a magyar hatóságok egy 3 kilométer sugarú, 5950 méter magas területet határoztak meg, amelyre vonatkozik a légiközlekedés tilalma. Ez a tiltott légtér a 26/2007.(III. 1.) GKM-HM-KvVM együttes rendelet alapján lett kijelölve. A rendelet hatályba lépése óta több alkalommal módosult először 2018-ban, miniszteri engedéllyel meghatározott okokból és időre a tiltott légtérbe békeidőben történhet berepülés. A második módosítás 2021-ben történt, amelyben egyik új elemeként a No Drone zóna került beiktatásra. [61] A jogszabály a zóna pontos meghatározásában a magyar légtér igénybevételéről szóló 4/1998. (I. 16.) Korm. rendelet 13. § 5. pontjára hivatkozik, mely szerint a No Drone zóna: olyan légtér, amelyben a pilóta nélküli légi járművek működtetése - az e rendeletben foglalt kivételekkel – tiltott. Ezzel

egyidőben a magyar légtér igénybevételéről szóló 4/1998. (I. 16.) Korm. rendelet 9 § 4. pontja előírja a Paksi Atomerőmű üzemeltetője számára, hogy az LHP1 légtérben köteles pilóta nélküli légi jármű detektálására. [62] Az előzőekben bemutatott adatok alapján megállapítható, hogy Magyarország nukleáris létesítményeinek védelme a pilóta nélküli légi járművekkel szemben hasonló helyzetben van, mint az amerikai nukleáris létesítmények esetében, tehát a biztonsági szolgálat személyzete nincs felhatalmazva a drónok elleni védelmi intézkedések végrehajtására.

#### **4.1.1 Kockázatok vizsgálata hipotetikus légi scenáriók mentén**

A nukleáris létesítmény légtérsértésének lehetséges eszközeként a kereskedelmi forgalomba kapható drónokat veszem alapul. A véletlen behatolás lehetőségét két okból is kizárom a vizsgálatból, az egyik ok, hogy a legtöbb gyártó termékeibe felprogramozásra kerülnek a No Drone zónák. Ennek következtében például egy tiltott légtérben fel se száll az eszköz vagy ha a határához ér ott az irányító utasításait felülbírálja és egyszerűen nem repül tovább. A másik ok pedig az, hogy ha esetlegesen az adott drón nem ismeri a No Drone zónákat, a véletlenszerű berepülés mögött nincs ártó szándék. A drónok hasznos teherszállítási képességét 1 kilogrammban határozom meg, mert ezek felületi mérete jellemzően nem haladja meg a 0,2 m<sup>2</sup>-t. Fontos paraméter még a maximális repülési idő és a hatótáv. A hatótávolság minimum 5 km és a repülési idő minimum 45 perc kell legyen.

A drónpilóta ártó szándéka szerint három scenáriót vizsgálok:

1. Drón reptetés a terület felett videofelvételek készítése céljából, amelyeket online vagy későbbi időpontban megoszt, egy social media felületen demonstrációs céllal.
2. : Berepülés a terület fölé video és fényképek készítése céljából, ami egy későbbi fizikai behatolás előkészítéséhez szolgáltat információkat
3. : Berepülés a területre, pontosan kiválasztott célpont felrobbantása céljából. (maximum 1kg robbanóanyag)

A drónos berepülések okozta fenyegetések biztonságra gyakorolt hatásának vizsgálatához a lehetséges károk mértékét is szükséges meghatározni. Kiindulási alapként a nemzetközi és hazai gyakorlatokban alkalmazott veszélyhelyzeti terminológiákat alkalmazom, valamint a nukleáris létesítményeknél jelentőséggel bíró nem fizikai jellegű károkat. A károkozás mértéke szerint három eshetőséget feltételezek:

1. Reputációs kár: A nukleáris létesítmények körül gyakran merülnek fel nukleáris biztonsági és védettségi aggályok, valamint az atomenergia alkalmazásával kapcsolatos politikai és társadalmi viták. Ha például egy atomerőműben bekövetkezik egy baleset vagy szabotázs, az a hírnevét veszélyeztető kárt okozhat az erőmű üzemeltetőjének, az iparágak és az államnak is. A reputációs kár csökkentheti az emberek bizalmát az atomenergia iránt, megnehezítheti új atomerőművek engedélyezését, és negatívan befolyásolhatja az atomenergiaipar fejlesztését és fenntarthatóságát.
2. Termelésbiztonsági veszélyhelyzet: A nukleáris létesítmény üzemeltetése során olyan helyzet vagy nem várt esemény következmény, amely normál üzemeltetési folyamatok működését veszélyezteti.
3. Nukleáris veszélyhelyzet: *„rendkívüli esemény következtében előálló állapot, amelyben a lakosságot érintő következmények elhárítása vagy enyhítése érdekében intézkedésekre van vagy lehet szükség”* [30 2. § 22.]

A nemzetközi ajánlások szerint fontos, a nukleáris veszélyhelyzeteket súlyosságuk szerint kategorizálni vagy csoportosítani. Ezáltal könnyebb lehet az intézkedések, a reagálás és az erőforrások felosztása, mivel a veszélyhelyzetek eltérő mértékű súlyosságot jelenthetnek. A csoportosítás lehetővé teszi, hogy a reagáló egységek hatékonyabban kezeljék a helyzetet, és a megfelelő intézkedéseket hozzák meg a veszélyeztetett területeken. Az Országos Balesetelhárítási Intézkedési Tervből (továbbiakban: OBEIT) származó információk alapján négy nukleáris veszélyhelyzeti osztályt lehet azonosítani atomerőműveknél:

1. Potenciális veszélyhelyzet: egyéb, a reaktorblokkokat közvetlenül nem érintő veszélyek
2. Létesítményi veszélyhelyzet: egy reaktorblokkot érintő veszélyek
3. Telephelyi veszélyhelyzet: több reaktorblokkot érintő veszélyek
4. Általános veszélyhelyzet: valamennyi reaktorblokkot érintő veszélyek [63]

A felsorolt nukleáris veszélyhelyzeti osztályokat kiterjesztem a termelésbiztonsági veszélyhelyzetre is. A három hipotetikus forgatókönyv sikeres végrehajtása esetén a következő káresemények valósulhatnak meg.

Az 1. számú szcenárió kockázatának vizsgálata:

- Cselekmény: Drón felhasználása a terület feletti videofelvételek készítésére, amelyeket online vagy későbbi időpontban egy közösségi média platformon történő közzététel céljából történik, ezzel demonstrálva a létesítmény védelmi képességeinek hiányosságait.
- Veszélyhelyzet: Az esemény a potenciális termelésbiztonsági veszélyhelyzetek közé sorolható. A berepülés hagyományos légvédelmi eszközökkel nem detektálható. Nagyon kicsi eséllyel az erőmű területén tartózkodó személy által vizuálisan észlelhető, de az elkövetői szándék nem azonosítható
- Kár mértéke: A fizikai kár okozása, csak a képzetlen pilóta vagy az eszköz meghibásodása esetén valósulhat meg, aminek bekövetkezési valószínűsége igen kicsi és az okozott kár a lezuhant drón következtében jelentéktelen. Az eseménnyel kizárólag reputációs kár okozható.

#### A 2. számú szcenárió kockázatának vizsgálata:

- Cselekmény: A terület fölé való drónrepülés során videofelvételeket és fényképeket készítése annak érdekében, hogy későbbi fizikai behatolás előkészítéséhez információkat szolgáltatasson.
- Veszélyhelyzet: Az esemény a potenciális termelésbiztonsági veszélyhelyzetek közé sorolható, hasonlóan, mint az 1. számú szcenáriónál.
- Kár mértéke: A fizikai kár okozása kizárható. Az eseménnyel okozható kár nem határozható meg, csak későbbiekben lehet következtetéseket levonni, amennyiben valóban végrehajtanak egy fizikai behatolást. Ehhez is az szükséges, hogy a két cselekmény között egyértelműen kimutatható legyen a közvetlen kapcsolat.

#### A 3. számú szcenárió kockázatának vizsgálata:

- Cselekmény: Berepülés a területre, pontosan kiválasztott célpont felrobbantása céljából, maximum 1kg robbanóanyag felhasználásával.
- Veszélyhelyzet: A berepülés bekövetkezése pillanatában a potenciális veszélyhelyzet áll fenn. A robbanóanyag célba juttatásakor és felrobbantásakor létesítményi és telephelyi veszélyhelyzet alakulhat ki a kiválasztott célpont és a robbantás hatékonyságának függvényében. A nukleáris veszélyhelyzet kialakulásának bármelyikét teljes mértékben kizárom.
- Kár mértéke: A fizikai kár okozásának mértéke a bejuttatott robbanóanyag mennyiségétől és a kiválasztott célponttól függ. A robbantást az üzem területén

gyakorlatilag bárhol végre lehet hajtani, de a legnagyobb valószínűséggel olyan rendszerek vagy berendezések elleni támadásra kerülhet sor, amelyeknek a megrongálása a legnagyobb mértékű termelés kiesést és gazdasági kárt okozhatja. Egy kilogramm robbanóanyaggal 5 méteres sugarú körben súlyos károsodásokat, 10 méteres körzetben pedig erős károkat lehet okozni. [63][44] Az elkövető a célpont kiválasztásakor arra is figyelhet, hogy az adott objektum őrzése kevésbé szigorú legyen, ami segítheti a szabotázs cselekmény végrehajtását. Az anyagi kár a megrongált berendezés javítási költségeiből és az esetleges termelés kiesés következtében, akár milliárd forintos tétel is lehet.

## **4.2 Az IoT technológia elterjedéséből jelentkező új kockázatok azonosítása és elemzése nukleáris létesítmények vonatkozásában**

Az IoT mint fogalom meghatározása első látásra nem egy egzakt egyértelműen leírható fogalmat takar. A téma meghatározására több fogalommal is találkozhatunk. A kézzelfogható eszközök szemszögéből nézve egyszerűen megfogalmazva azon eszközök csoportját jelenti, amelyek rendelkeznek egyedi azonosítóval, képesek vezetékes vagy vezeték nélküli hálózatokon keresztül az internetre csatlakozva önállóan egymással kommunikálni, illetve adatokat megosztani [64]. Ide lehet sorolni bármely olyan fizikai eszközt, amely rendelkezik IP címmel és képes az interneten keresztül kommunikálni, ilyenek például a napjainkban gyártott autók, okos hűtő, smart TV, smart telefon, smart watch, tablet és az okos otthon összes berendezése akár a fűtési rendszer szobatermosztátja is. A felsorolt eszközök közül az okos telefonra és órára mostanság már személyes tárgyként kell tekintenünk. Habár okos órával, ha nem is, de okos telefonnal a fejlett világ minden állampolgára rendelkezik. Több esetben akár két készülékkel is rendelkezik egy személy, egy magán és egy vállalati telefonnal. Az IoT működés számára a fizikai eszközökön túl elengedhetetlen a kommunikációs csatornák megléte. Alapvetően vezetékes és vezeték nélküli átviteli csatornákat lehet megkülönböztetni a fizikai eszközök közötti adatátvitelnél. Jellemző, hogy a két adatkapcsolati mód vegyesen kerül alkalmazásra egy ipari létesítmény, gyáregység IT rendszereiben, beleértve a nukleáris létesítményeket. A biztonsági kockázatok vizsgálatánál a fókusz ezért az okostelefonokra helyeztem a vezeték nélküli kommunikációs csatorna tükrében.



#### 4.2.1 Okostelefon funkciói és kockázatai

Az okostelefonok vonatkozásában a hétköznapi nyelvezetben azon mobiltelefonokról beszélhetünk, amelyek gyakorlatilag egy PC szinte összes funkcionalitását magába foglalja, valamint a hagyományos mobiltelefonoktól eltérően érintőképernyőn keresztül lehet működtetni. Továbbá fontos még megjegyezni, hogy a mobileszközök saját operációs rendszerén (IOS, Android) futatott alkalmazásokon (APP-ok) keresztül érhetőek el a különböző funkciók. A kockázatelemzés aspektusából tekintsünk át néhány fontosabb funkciót:

- fotó/videofelvétel készítés
- sms/mms/e-mail küldés
- wifi hotspot létrehozás
- Bluetooth kommunikáció
- internet csatlakozás
- helymeghatározás
- tárhely/adathordozó

A felsorolt funkciók külön – külön és együttes alkalmazásuk, alkalmasak lehetnek arra, hogy ártó szándékú cselekményeket, szabotázsokat lehessen végrehajtani, amennyiben a mobil eszköz fizikailag a fokozottan őrzött zónában üzemelő IT eszközökkel azonos időben van jelen. Ez az jelenti, hogy a nukleáris létesítmény ezen területein, olyan IT rendszereket is alkalmaznak, amelyek vezeték nélküli kommunikációs lehetőségeket biztosítanak. Ezenfelül meg kell még említenem az egyre jobban elterjedt olyan terepi ipari készülékeket, amelyek rendelkeznek Bluetooth kommunikációval a gyors helyszíni üzembehelyezést segítve. [54] [65]

#### 4.2.2 Egy hipotetikus atomerőmű fokozottan őrzött üzemi területének IT eszközei

A nukleáris energia békés célú felhasználása során a nukleáris biztonság megfelelő szintjének elérése érdekében az alaptechnológián kívül különböző védelmi és ellenőrző rendszert kell üzemeltetni. Az egyik kiemelten fontos rendszer a reaktorvédelmi rendszer. A reaktorvédelmi rendszer feladata a működő reaktor blokk számos technológia paraméterének (neutronfluxus, hőmérséklet, nyomás stb.) folyamatos monitorozása és az egyes paraméter limitek elérése, illetve meghaladása esetében figyelmeztető jelzések generálása és szükség esetében a blokk automatikus leállítása. Az atomerőmű

üzemeltetése során ellenőrzésre kerülnek a reaktorfizikai paraméterek a zónaellenőrző rendszeren keresztül, amely segítségével a zónakiégettség mértéke és az esetleges zónatorzulás kialakulása határozható meg. Az üzemi terület radiológiai állapotát a sugárzásellenőrző rendszer segítségével lehet ellenőrizni és limit túllépés esetében riasztást kiadni. Mindhárom rendszerről elmondható, hogy a nukleáris biztonság tekintetében fontos rendszerekről beszélünk. A rendszerek feladataik tekintetében igen eltérőek, viszont az IT infrastruktúrájuk nagymértékben hasonlóak. A rendszerek alsó szintjén az analóg és digitális szenzorok és végrehajtók helyezkednek el, amelyek közt szerepelnek Bluetooth-os eszközök is. A topológia középső szintjén találhatóak az adatgyűjtők, illetve a PLC-k. A rendszerek felső szintjén pedig az IT hardware és software eszközök.

Az IT rendszert alkotó hálózat aktív eszközei a kliens számítógépek, a szerverek, a routerek, a switch-ek és esetlegesen Wifi AP-ok.

A kliens számítógépeken keresztül valósul meg az ember gép kapcsolat. Jellemzően a kliensgépek a funkciójukat tekintve munkaállomások, ahol az üzemeltető személyzet számára különböző szoftverek segítségével kerülnek megjelenítésre a technológiai paraméterek. Nem nagy számban, de vannak olyan kliensek is, amelyeken keresztül beavatkozásra is van lehetőség a technológiai folyamatokba egy berendezés ki/bekapcsolásával. Egy adott rendszerben több kliensgép helyezkedik el, amelyek a switcheken vagy router-eken keresztül kapcsolódnak a szerverekhez. A switchek teszik lehetővé a számítógépek hálózatba szervezését különböző topológiai kialakítás mentén. Ezek eszközök konfigurációja határozza meg, hogy a hálózaton belül melyik számítógép melyikkel kommunikálhat. [65]

#### **4.2.3 Kockázatok vizsgálata hipotetikus scenáriók mentén**

A kockázatelemzésben a területi behatárolást két részre osztom. Az első scenárió a létesítmény teljes területére kiterjed míg a többinél csak azon fokozottan őrzött zónák területére, amelyekben B védelmi szintű nukleáris anyag található, illetve olyan IT rendszereket tartalmaz, amelyek sikeres szabotázs jelentős radiológia következményeket vonhat maga után. A mobiltelefonok jelentette veszélyek esetében a fizikai védelem tekintetében két alapesetet lehet megkülönböztetni. Egyik esetben a fizikai védelemre gyakorolt közvetlen hatást lehet vizsgálni, míg a másik esetben az IT rendszereken keresztül végrehajtott szabotázs (mint fizikai védelmi esemény) nukleáris

biztonságra és fizikai védelemre gyakorolt hatást kell figyelembe venni. A kockázatok tételes vizsgálatát a mobiltelefonok funkcióinak tükrében a nukleáris védelethez gyakorolt hatás függvényében vizsgálom.

Az elkövető ártó szándéka szerint három scenáriót vizsgálok:

1. : A okostelefon használója a létesítmény bármely zónájában szándékosan fotó-és videofelvételeket készít. Rögzíti a fizikai védelmi rendszer és a technológiai rendszer berendezéseit, valamint megközelítési útvonalakat, azzal a szándékkal, hogy későbbi fizikai támadáshoz információt szolgáltatson.
2. : A okostelefon használója Bluetooth technológia és szükséges applikációk segítségével csatlakozik egy vagy több terepi eszközhöz és annak konfigurációját átállítja.
3. : A okostelefon használója Wifi technológia és szükséges applikációk segítségével csatlakozik egy vagy több hálózati eszközhöz és azon keresztül valamelyik nukleáris biztonságot megvalósító rendszer működését módosítja.

Az okostelefon ártó szándékú használata okozta fenyegetések biztonságra gyakorolt hatásának vizsgálatához a lehetséges károk mértékét is szükséges meghatározni. A feltételezett scenáriók sikeres végrehajtásának következményei nem jelentkeznek minden esetben azonnal és nagy valószínűséggel az elkövető törekszik is erre. Az elkövető kiléte és az esemény csak akkor tud rejtve maradni, ha a beavatkozások időben később fejtik ki hatásukat. [66] A három hipotetikus forgatókönyv sikeres végrehajtása esetén a következő káresemények valósulhatnak meg.

Az 1. számú scenárió kockázatának vizsgálata:

- Cselekmény: A okostelefon használója a létesítmény bármely zónában olyan felvételeket készít, amelyek fizikai védelmi rendszer elemeit is tartalmazzák. Felvételt készít az áteresztő pontok pontos elhelyezkedéséről, kialakításáról, illetve még a működéséről is. Rögzíti a megfigyelő kamerák pontos elhelyezkedését. Olyan videofelvételt készít, amely során rögzíti a zónahatártól akár a reaktortartályig vezető útvonalat. Felvételeket készít a technológiai berendezések típusáról elhelyezkedéséről és működéséről. A rögzített képek és videofelvételeket tárolja a telefonján és mobilinternet kapcsolaton keresztül feltölti a felhőben.

- Kár mértéke: Az eseménnyel okozható kár nem határozható meg, csak későbbiekben lehet következtetéseket levonni, amennyiben valóban végrehajtanak egy fizikai behatolást. Ehhez is az szükséges, hogy a két cselekmény között egyértelműen kimutatható legyen a közvetlen kapcsolat. Ha ez bekövetkezik, akkor a fizikai szabotázs következményeiből lehet a kár mértékét meghatározni.

#### A 2. számú scenárió kockázatának vizsgálata:

- Cselekmény: A okostelefon használója Bluetooth technológia és szükséges applikációk segítségével csatlakozik egy vagy több terepi eszközhöz és annak konfigurációját átállítja. A konfigurációkat úgy módosítja, hogy az meghamisítsa a rendszerben mért értékeket és ez egy működés elmaradást okozzon.
- Kár mértéke: A kár mértéke az elkövetés pillanatában nem határozható meg csak amikor a működéselmaradásból származó üzemzavar megtörténik. A kár az üzemzavar okozta termelés kiesés mértéke lesz. Nagyobb kárt nem lehet okozni anélkül, hogy fény derüljön a beavatkozásra, mivel redundáns rendszerek vannak kiépítve. Amennyiben több vagy nagyobb mértékű módosítást hajt végre akkor, arra előbb derülne fény minthogy kiváltta károsító hatását.

#### A 3. számú scenárió kockázatának vizsgálata:

- Cselekmény: A okostelefon használója Wifi technológia és szükséges applikációk segítségével csatlakozik egy vagy több hálózati eszközhöz és azon keresztül valamelyik nukleáris biztonságot megvalósító rendszer működését módosítja.
- Kár mértéke: A kár mértéke óriási is lehet, akár nukleáris katasztrófa is okozható. Természetesen a végrehajthatósághoz a tudomány több területén is igen jártas elkövetőre van szükség.

A felsorolt és értékelt kockázatok közül valamennyi kockázat esetében fontos kiemelni, hogy bármelyik bekövetkezése csak belső elkövetői magatartás tanúsítása esetén feltételezhető. A kockázatok közül a 2. és a 3. scenárió a kiberbiztonsági területet érint, amely elleni védekezés megfelelőségének megvitatása az értekezés terjedelmén kívül mutat. Ennek ellenére a lehetőséget vizsgáltam, mivel a nemzetközi gyakorlatok és a hazai jogszabályok értelmében a fizikai védelmi rendszernek kell a veszélyeztetések elleni hatékony védelmet biztosítania.

### 4.3 Részkövetkeztetések

A világ technikai fejlődése mindig is magában hordozza a veszélyeket és beláthatatlan következményekhez vezethet, ha azokat a tudomány területén dolgozó szakemberek, tudósok nem tudják kellő gondossággal felismerni és kezelni. Gondoljunk csak a Csernobili balesetre vagy akár a Paksi Atomerőműben történt INES hármas eseményre. A Csernobili baleset alap kiváltó oka a grafitmoderátoros reaktortípusban rejlő konstrukciós hiba volt, amit az USA-ban a 40-es években Teller Ede és kollégái fedeztek fel és Teller-Effektusnak nevezték el. Az 50-es években az ilyen típusú reaktorokat leállították és befejezték a további fejlesztésüket. [67] A 2003-as paksi üzemzavar egyik hozzájáruló okként a vezetői szinten jelentkező túlzott magabiztosságot azonosította az OAH. [68 p. 18] Mindent összevetve nagyon fontosnak tartom, hogy a nemzeti érdekeket szolgáló objektumok vélt és valós kockázatait bemutatásra kerüljenek, mint például egy atomerőműnél. Ebből adódóan a fejezetben részletesen bemutattam és elemeztem a technikai fejlődés következtében jelentkező új kockázatokat. Az elemzésben, olyan objektumot választottam, ahol a fenyegetéseknek való kitettség igazolható. A témával kapcsolatos több tudományos esettanulmányt dolgoztam fel. Bemutattam a dróntechnológia és az IoT technológia jelentette új kockázatokat egy hipotetikus nukleáris létesítmény védelmi rendszerén keresztül. Az elemzésben feltételeztem, hogy az objektum nem rendelkezik drónelhárításra alkalmas védelmi megoldásokkal. A feltételezésemet a nukleáris iparban eltöltött 20 éves tapasztalataimra alapozom. Továbbá a jogi szabályozásból és a nemzetközi tapasztalatokból egyértelműen megállapítható, hogy a létesítmény üzemeltetőjét nem ruházza fel a drónelhárítás lehetőségével, és az állam által ellátandó feladatok közé sincs besorolva. Az IoT technológia is jelen van az üzemidő hosszabbítás következményeként és az emberek mindennapi használati tárgyává váltak az okostelefonok, ezzel biztosítva a technológiák egyidejű jelenlétét az objektum területén. Megállapítható, hogy a fejezetben elvégzett elemzői munka igazolja a második hipotézisemet, mégpedig az elektronikai, az IT eszközök fejlődésével, valamint a világ nagyléptékű digitalizációjával új jelentős kockázatok jelennek meg az objektumvédelem vonatkozásában, amelyek csökkentésére még nincsenek műszaki védelmi intézkedések bevezetve.

## **5 AUTONOM MŰKÖDÉSŰ AKTÍV BEAVATKOZÁSRA IS KÉPES ELEKTRONIKUS VAGYONVÉDELMI RENDSZEREK**

Az autonóm vagy más néven önműködő rendszer egy olyan technológiai vagy szervezeti rendszert jelent, amely képes önállóan működni, döntéseket hozni és feladatokat végrehajtani anélkül, hogy folyamatos emberi beavatkozásra lenne szükség. Napjainkban az autonóm rendszereket különböző területeken már használják vagy az utolsó tesztelési fázisban vannak, például az autonóm járművek, drónok, robotok, és az informatikában is az MI-t alkalmazó szoftverek, hálózatok és szerverek területén is megtalálhatók.

Az autonóm rendszereknek általában többféle érzékelőre és szoftverre van szükségük, amelyek segítségével képesek érzékelni és értelmezni a környezetüket, majd az adatok alapján döntéseket hozni és feladatokat végrehajtani. Az autonóm rendszerek használatának előnyei közé tartozik az emberi hibák csökkentése, a hatékonyság növelése és olyan feladatok végrehajtása, amelyek az ember számára veszélyesek vagy nehezek. Az autonóm drón alkalmazás kapcsán elterjedt a köztudatban a 4D kritériumrendszer, amivel csökkenteni akarták a veszélyeket és az emberi tényezőt. A kritériumrendszerben a négy D az angol szavak kezdőbetűit jelenti:

- Dangeorus (veszélyes)
- Dirty (piszkos)
- Distans (távoli)
- Dull (unalmas)

A kritériumrendszert elsősorban az olajipari tengeri fúrótornyok karbantartásánál alkalmazták, de magas ipari kéményeknél, nagyfeszültségű távvezeték hálózattoknál és még sok más területen is alkalmazható hatékonyságnövelés céljából.[69] [70] [71]

Az autonóm rendszerek sokféle alkalmazási területen találhatók meg, amelyek folyamatosan fejlődnek és terjednek az ipari, közlekedési, mezőgazdasági és informatikai területeken, de a biztonságtechnikában ez nem mondható el. Néhány magyar rendszertelepítő cég magát autonóm őrzőrendszer telepítőjeként mutatja be, de ez még mindig csak a vizuális megfigyelés video-analitikai megoldásait jelenti.[72] A kutatás szempontjából fontosnak tartom az autonóm beavatkozásra is képes aktív elektronikus vagyonvédelmi rendszer meghatározását.

Autonóm beavatkozásra is képes aktív elektronikus vagyónvédelmi rendszer, egy olyan elektronikai érzékelőkből, eszközökből felépített rendszert jelent, amely képes önállóan működni, döntéseket hozni, valamint késleltető, feltartoztató és beavatkozó funkciókat, feladatokat végrehajtani anélkül, hogy folyamatos emberi beavatkozásra lenne szükség.

A továbbiakban kizárólag a nukleáris létesítmények objektumvédelmi kutatását fogom szemléltetni, ahol az őrzési tevékenység a nukleáris létesítmény jellegéből adódik, és olyan sokrétű feladatokat takar, amelyek miatt a biztonsági szolgálatnak szerteágazó őrzésvédelmi feladatokat kell ellátnia.

## **5.1 Autonóm elektronikai védelmi rendszer eszközeinek meghatározása**

Az autonóm rendszer kialakításának alvető feltétele, hogy a védendő objektum rendelkezzen az elektronikus vagyónvédelem alterületeit képező beléptető rendszerrel, video megfigyelő rendszerrel, behatolás jelző rendszerrel és periméter védelmi rendszerrel. A védelmi koncepciónak alkalmaznia kell a mélységben tagolt védelmi elveket és az elektronikus védelmi rendszereknek magasfokú integráltsággal kell rendelkeznie. Ezen feltételek mentén kialakított „hagyományos” elektronikai védelmi rendszer képezi az alapját annak, hogy a rendszer aktivitását fokozni lehessen, illetve új funkciókkal lehessen kiegészíteni, a védelmi rendszer optimalizálása, a kockázatok további költséghatékony csökkentése, valamint az előerős védelem létszámának csökkentése érdekében. A megvalósíthatóság szempontjából az autonóm rendszernek további kritikus feltételeket kell teljesítenie:

- **Megbízható érzékelés:** A rendszernek képesnek kell lennie környezetét megbízhatóan érzékelni. Ehhez szenzorokra van szükség, amelyek információkat gyűjtenek a környezetről és pontosan észlelik a fenyegetéseket úgy, hogy az önműködő beavatkozásra alkalmas legyen.
- **Döntéshozatal:** Az rendszernek rendelkeznie kell döntéshozatali mechanizmussal, amely alkalmas a fenyegetés elleni gyors reakciók indítására.
- **Vezérlés és cselekvés:** A rendszernek képesnek kell lennie a környezetével való kölcsönhatásra, amihez megfelelő aktuátorokra van szükség. Az aktuátorok végzik el a rendszer cselekvéseit, például mozgást, kommunikációt vagy más tevékenységeket.

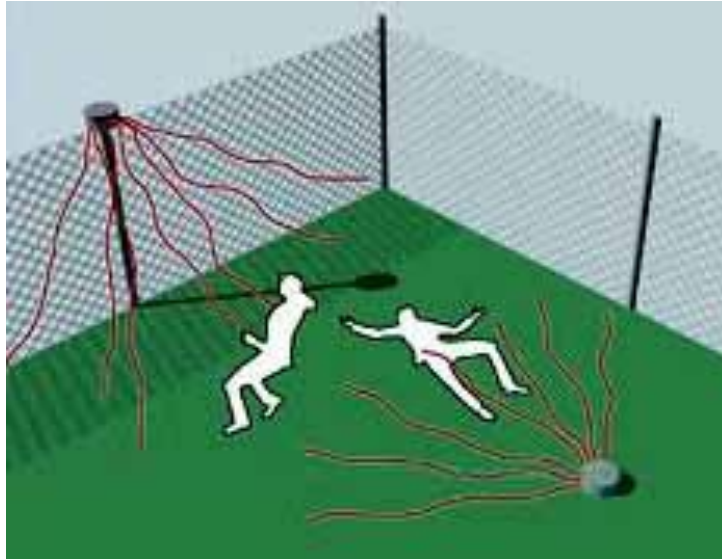
- **Alkalmazkodás:** A rendszernek képesnek kell lennie a tanulásra és az alkalmazkodásra a változó környezeti feltételekhez, gépi tanulási vagy mesterséges intelligencia algoritmusok alkalmazásával.

A követelményrendszer alapján, olyan érzékelőket, beavatkozókat és nem hardveres eszközöket mutatok be, amelyek az autonóm rendszer részét képezhetik. A bemutatásra kerülő eszközök között vannak létező vagyonvédelemben is alkalmazott megoldások, de azok képességei napjainkban alacsony mértékben vannak kihasználva vagy az elterjedésük igen alacsony. Ezen felül nem vagyonvédelmi eszközök is megjelennek, amelyek alkalmasak lehetnek a feladatok végrehajtására.

### **5.1.1 Nemhalálos fegyverek**

A nem halálos fegyverek közzé tartoznak mindazon eszközök, melyeket a veszélyeztetés elhárítására alkalmaznak, de nem az emberi élet kioltására terveznek, gyártanak és alkalmaznak. A nemhalálos fegyverek közé tartoznak például az elektromos sokkolók. Az első prototípust 1970-es évek közepén fejlesztették ki, de szélesebb körben való alkalmazásuk később, a 1990-es években indult el. Az Egyesült államokban az Air TASER Model 34000 került először rendszeresítésre. Azóta a taser a legtöbb amerikai rendőrségi szervezet felszerelésének része. Az alkalmazása nemcsak az Egyesült Államokban, hanem szerte a világ minden részén elterjedt. Magyarországon a rendőrség 2022 - ben kezdte meg a Taser X2 Model rendszeresítését. [73] A Taser gyártója a 2000 években kifejlesztett több típusú területvédelmi önműködő és távvezérelhető elektromos sokkolókat. A fejlesztések végeredményeként megszületett a TADD és a TRAD típusú területvédelmi eszköz. A taser terület védelmi eszközt a fejlesztő első sorban az amerikai nukleáris létesítmények védelmi rendszerének modernizálási szándékával fejlesztette ki. A kialakítása pedig a robbanótöltetes taposóaknak kiváltását célozta meg. Az aknába helyeztek 12 elektródapárt, ami 120° -os szögű 5-7 méter sugarú körívknyi területet képes lefedni. Telepítés szempontjából földfelszíni vagy föld feletti lehet. Az eszköz képes a beépített szenzorok alapján működésbe lépni vagy távvezérléssel is indítható. A telepített akkumulátora összesen 200-szor 3 másodperces impulzus leadására képes. [74]





10. ábra - Terület Védő Eszköz TADD [74]

A taser távolsági területvédelmi eszköz egy továbbfejlesztés eredménye, melynek köszönhetően jelentősen nagyobb területet képes lefedni és akár 100 méteres távolságból is aktiválható. Működtetése szintén történhet autonóm módon vagy távvezérléssel egyaránt. Egyszerűen és gyorsan telepíthető a kis súlya és hordozható kivitele következtében.



11. ábra - Távolsági Terület Védő Eszköz (TRED) [74]

A leginnovatívabb elképzelése a gyártónak, hogy egy kézi taser-re adat-portot helyeztek el, ezzel megteremtve a távvezérlés lehetőségét. Területvédelmi megoldásként, azt találták ki, hogy egy PTZ kamerához rögzítenek egy távvezérelhető taser-t. A biztonsági személyzet a kamerarendszer vezérlőjén keresztül becélazza a célszemélyt, majd az adat-porton keresztül működteti a lézer irányzékot és az elsütő szerkezetet.

A sokkoló működési elvéből adódóan az érintett személy 5 másodpercig teljes mozgásképtelen lesz és azt követően további élettani hatások jelentkeznek. Ezek a sokkoló működési idejével arányosan és az érintett személy bioelektromos jellemzőinek függvényében kialakulhat:

- egyensúlyvesztés
- tájékozódási képesség ideiglenes elvesztése
- az agyműködés átmeneti zavara
- több perces tudatzavar (ez átlagosan 15 perc)

A sokkolás összes hatását figyelembe véve az a személy, akin alkalmazták a sokkolót, átlagosan 10-15 percre teljesen harc képtelen, illetve jelentősen csökkent harcértéket képviselő személlyé válik. A gyakorlatban azt jelenti, hogy a reagáló erőknél nagyságrendekkel megnő az intézkedésekre rendelkezésére álló ideje.

### **5.1.2 Intelligens video analitika és video megfigyelési eszközök**

Az intelligens videó egy gyűjtő kifejezés a videómegfigyelő rendszerek területén, amely alatt olyan funkciókat, feladatokat és elemzéseket értünk, amelyeket a rendszer autonóm módon lát el. A feladatokat valós idejű és archivált felvételek esetén is el tudja végezni. A videó tartalom elemzésnél nem a kezdeti mozgásdetektálási algoritmusokkal ellátott eszközökre gondolok, hanem azon eszközökre és rendszerekre, amelyek a mozgáson belüli magatartási és viselkedési minták elemzésére is képesek. A procedurális és deklaratív programozással készített video analitikai eljárások nem alkalmasak a disszertációban későbbiekben megfogalmazott feladatok ellátására. A neurális hálózatok elvén működő vagy a mesterséges intelligenciát használó algoritmusok viszont alkalmazhatóak, mivel párhuzamos felépítésűek és tanulási képességekkel rendelkeznek. A rendszer képalkotó eszközeinek szempontjából kizárólag IP technológiás kamerák jöhetnek szóba, amik lehetnek hagyományos, infra és hőkamera.

Megkülönböztetünk centralizált és decentralizált video analitikát. A centralizált videótartalom elemzésnél a hagyományos IP kamerákból érkező video adatfolyamot a központi rögzítő dolgozza fel, elemzi és tárolja. A decentralizált rendszereknél a képek feldolgozása és elemzése közvetlenül a kamerában zajlik, és nem a rögzítő eszközben. A videótartalom elemzése a kamera intelligens algoritmusainak és processzorának összehangolt működésével valósul meg. Ezáltal az intelligens kamera határozza meg, hogy a megfigyelt területen történik-e olyan esemény, amelyet érdemes archiválni és továbbítani a hálózati rögzítő eszköznek. Egyes megoldásoknál a kamera metaadatokat is generál, amit a video streammel egyben küld át a rögzítőnek. A metaadatok rövid text alapú üzenetek az esemény idejéről, a viselkedési mintáról vagy más lényeges információról. Mivel a metaadatok jóval kisebb kiterjedésűek, mint a tömörített video állomány, így könnyen átküldhetőek, kevés helyet foglalnak, és a legfontosabb, hogy lényegesen megkönnyítik az archivált eseményekben a keresést.

A különböző képelemzési algoritmusokkal az alábbi analitikai funkciók valósíthatók meg:

- Arcfelismerés
- Bóklászás érzékelés
- Eltűnt tárgyak érzékelése
- Elhagyott tárgyak érzékelése
- Futásérzékelés
- Haladási irány megfigyelése
- Mozgásérzékelés
- Objektumkövetés
- Rendszámfelismerés
- Vonallátépés érzékelés

A rengeteg funkció ellenére a VCA technológiát a legtöbb esetben csak az incidensek rögzítésére és az utólagos nyomozások segítésére használják, nem pedig proaktív módon megelőző jelleggel. A meta adatok videófolyamból történő kinyerése lehetővé teszi a kockázatos helyzetek korai felismerését, a károk minimalizálását és ideális esetben a veszélyhelyzetek teljes elkerülését. A megelőző jellegű alkalmazásokhoz egyidejűleg több különböző funkcióval rendelkező videóanalitikai megoldást kell alkalmazni centralizált és decentralizált rendszerstruktúrában, amelyre javaslatokat fogok tenni.

### 5.1.3 Dróndetektáló, elhárító eszközök és a drón

A pilóta nélküli légi járművek elterjedése a polgári és ipari felhasználásban számos előnnyel jár, de ugyanakkor negatív következményeket is hozhat magával. Az eszközök könnyű hozzáférhetősége és az ellenőrizetlen felhasználás új veszélyeket teremthet, amelyek egy szűk szegmensét a 4.1-es fejezetben bemutattam. Az elmúlt öt évben a drón technológiában rejlő potenciális alkalmazási lehetőségekről számos publikáció jelent meg az ipari szektorban is, a mezőgazdaságtól kezdődően a termelő egységek hatékonyságnövelésén keresztül a biztonságtechnikáig. [75] [76] [77] Az elektronikus védelmi alrendszernek egyszerre kell a drónok nyújtotta számos új technológiai előnyöket kihasználnia és a technológia elterjedéséből származó fenyegetésekkel szemben hatékony védelmet nyújtania.

Az elektronikus védelmi alrendszerben a drónokra úgy tekintek mint, egy hely-és helyzetváltoztatásra képes platform, amely az alapját képezi egy többcélú aktív beavatkozásra is képes elektronikai védelmi eszköznek. Túlmenően a saját beépített funkcióin további szenzorok és aktuátorok csatlakoztatására is alkalmas és más rendszerekből érkező indítójelek fogadására is képes. A védelmi tevékenységek ellátására alkalmas drón meghatározásához szükséges a drón jellemzőinek és képességeinek azonosítása. A specifikációban elsőként a drónok többféle szempont szerinti csoportosítása nyújt segítséget:

- méret
- meghajtás
- szárnyszerkezet
- vezérlés típusa

Az összes lehetséges kialakítási és működési módozatot nem mutatom be, csak a beavatkozó drón feladat specifikációhoz szükséges paraméterek alapján készítettem egy csoportosítást.

<b>Kategória</b>	<b>Összsúly</b>	<b>Üzemeltethetőségi magasság</b>	<b>Hatótávolság</b>	<b>Üzemidő</b>	<b>Hasznos teher</b>
Micro	< 2 kg	< 140 m	5 km	< 1 óra	< 1 kg
Mini	2-25 kg	< 1000 m	25 km	2-8 óra	< 10 kg
Kicsi	25-150 kg	< 1700 m	50 km	4-12 óra	< 50 kg

#### 4. táblázat - drónok csoportosítása a NATO class I alapján

A táblázatban felsorolt drónkategóriáknak megfeleltethetőek a kereskedelmi forgalomban kapható drónok. Ilyen például a DJI Mavic 2 ami a micro kategóriának felel meg, a DJI Inspire 2 ami a mini kategóriának felel meg és a Scorpion 3 ami a kicsi kategóriának felel meg. Az alap paramétereken kívül további fontos képességekkel kell rendelkezni a kiválasztásra kerülő eszköznek:

- Ütközés érzékelés és elkerülés
- RTK vezérlés
- Autonóm működés belső és külső vezérléssel
- Objektum követés
- Automatizált döntéshozatal
- Skálázhatóság
- Környezeti paramétereknek való megfelelés
- Automata töltés

Az aktív védelmi funkciók megvalósításához az elvégzett elemzés eredményeként az 4. táblázat mini kategóriájú drónt választom ki. Természetesen az alap paramétereken felül a fenti képességekkel is rendelkeznie kell.

A drónok detektálása hasonlóan a hagyományos repülőgépekhez a működésükből eredő „zajok” és az üzemeltetésükből származó elektromágneses hullamák érzékelésén alapszik. A fenyegetést jelentő drón érzékelése, olyan érzékelőből vagy érzékelőkből áll, amelyek képesek az elektromágneses vagy akusztikus spektrumból extrapolált információkat összegyűjteni, az érintett technológiától és jelfeldolgozástól függően. Általában az észlelési művelet a következő fázisokra osztható:

- Észlelés: Az objektum vagy objektumok megtalálása a légtérben, amelyre a megfigyelés irányul. Ebben az első fázisban a rendszer még nem tudja megkülönböztetni, hogy az észlelt tárgy valóban drón-e. Ezt a fázist a két indikátorral az észlelési aránnyal és a hamis riasztási aránnyal jellemezhetjük, amelyek a helyes észlelés, illetve a téves riasztás valószínűségét fejezik ki.
- Osztályozás: Ha az észlelési esemény megtörtént, ellenőrizni kell, hogy az észlelt objektum valóban jelen van-e, és hogy drónról van-e szó. Megtörténhet például, hogy az előző fázisban észlelt célpont egy madár, amelynek az elektromágneses jellemzői (radar keresztmetszet) hasonlóak lehetnek a drónokhoz. Ez az ellenőrzés

maga az azonosítás. Ezt követően a rendszer extrapolálja a drón néhány kiemelkedő attribútumát, mint például a típus, a méret, a meghajtás típusa, a rotorok száma, a modell vagy akár a távoli pilóta lehetséges elhelyezkedése és a hasznos teher jelenléte.

- Lokalizáció/követés: A célpont helyzetének szögben és távolságban való becsülésével határozható meg. Háromszögelési technikák használhatók a pontosság növelésére. Miután a célpont lokalizálva lett, a repülése során végig követni kell. Néhány detektáló rendszer képes a repülési pályát is megjósolni.

Az észlelési folyamat megvalósítására különböző technológiák állnak rendelkezésre. [78] Az érzékelők kategorizálása során az legfontosabb jellemzőjük alapján a technológiai megkülönböztetés az aktív és passzív érzékelés között történik. Ez a két típus lényeges különbséget mutat az energiefelhasználás terén a térben található objektumok érzékeléséhez. Az aktív érzékelők elektromágneses vagy akusztikus sugárzást bocsátanak ki, amely segítségével közvetlenül mérhető az objektumok távolsága a sugárzás kibocsátása és visszavisszaverődése közötti időkéssleltetésen alapulva. Például a radarok és LiDAR érzékelők ebbe a kategóriába tartoznak. Másrészt a passzív szenzorok az energiát a környezetükből és az észlelni kívánt objektumokból nyerik, amelyekből hasznos információkat lehet kinyerni. Az elterjedt passzív érzékelők közé tartoznak az optikai és infravörös kamerák. Az érzékelők fizikai működésének ismertetésével kapcsolatosan több publikáció is megjelent, ami részletesen leírja a szenzorok technológia felépítését és működési elvét. Ezen technológiák közül én csak azokat vizsgálom, amelyek a 4.1.1 fejezetben leírt scenáriók végrehajtásához szükséges paraméterekkel rendelkező drónok detektálására alkalmas. A scenáriókban szereplő drónok a 4. táblázat mini és micro besorolású drónoknak feleltethető meg.

Az akusztikus érzékelők a drón repülése közben keltett hangokat detektálja. A drónok motorjai és propellerjei olyan akusztikus hullámokat bocsátanak ki, amelyek a 20 Hz és 20 kHz közötti frekvenciatartományba esnek. Ezek az akusztikus hullámok a drón akusztikus jellemzői, másnéven az akusztikus aláírása. Egy mikrofonnal is lehet már ezeket az információkat érzékelni. Az azonosítási fázisban a drón akusztikus aláírását egy előre rögzített akusztikus aláírásokat tartalmazó könyvtárral hasonlítja össze a rendszer, így azonosítva a drónt megkülönböztetve más objektumoktól. Ezzel az eljárással a típusát, méretét és több mikrofonos rendszer esetében az érkezési irány is beazonosítható.

Az optikai érzékelők olyan eszközök, amelyek az elektromágneses hullámokat az infravörös (300 GHz) és az ultraibolya (790 THz) frekvenciatartomány között érzékelik, és kétdimenziós képet készítenek a környezetükről. Ezek az érzékelők két fő kategóriába sorolhatók attól függően, hogy milyen frekvenciasávban működnek, és képesek-e az emberi szem által észlelhető tartományon belül működni. Az első kategóriába tartoznak az optikai kamerák, amelyek az 430–790 THz frekvenciatartományban képesek elektromágneses sugárzást érzékelni. A második kategóriába pedig a hőkamerák sorolhatók, melyek az infravörös sugárzást (300–430 THz) alakítják képpé. Az optikai érzékelők és a számítógépes látáson alapuló képfeldolgozási technikák segítségével ma már lehetővé válik a drónok felismerése, osztályozása és nyomon követése, amik a látómezőjükbe kerülnek.

A rádiófrekvenciás érzékelők rögzítik a drón vagy a távoli pilóta rádióvezérlésének elektromágneses jeleit, ha vannak ilyenek. Ez tehát egy passzív módszer, amely nem igényel elektromágneses hullámok sugárzását, ezért nincs korlátozás a használatára ipari vagy városi környezetben. Az RF-detektálás ismert protokollon vagy a spektrális mintázat felismerésén alapuló technikákkal végezhető. A legtöbb kereskedelmi drón uplink rádiócsatornát használ a távirányító parancsokhoz, és egy downlink csatornát a telemetriai és videojelekhez. Az autonóm drónok is jellemzően rendelkeznek a downlink kapcsolattal a földi irányító állomás felé.

A radar lehet aktív és passzív rendszerű is. Az aktív radar a lokátorállomás által kibocsátott elektromágneses hullámok és repülő tárgyról visszavert jel érzékelése között eltelt idő mérésére visszavezethető elv alapján működik. A passzív radar nem bocsát ki jeleket, hanem külső források jelei használják. Ilyenek lehetnek a földi sugárzású rádió és tévé csatornák átjátszó tornyai. A radar maga is érzékeli az ún. megvilágító forrást közvetlenül az adótoronyról és ugyanezen torony céltárgyról visszaverődött jelét is. A források elhelyezkedése miatt az egyes jelkomponensek eltérő időben érkeznek a vevőbe, ami alapján képes meghatározni az ismeretlen drón helyzetét. Az aktív radar a 3 MHz és a 300 GHz közötti frekvencia tartományban működik.

A LiDAR elektromágneses sugárzást használ az optikai és infravörös hullámhosszon. Ez egy aktív szenzorú rendszer, amely elektromágneses hullámokat bocsát ki és a visszavert hullámokat a radar működéséhez hasonlóan érzékeli. A frekvenciatartománya viszont, 200 THz és 400 THz közötti. Az emittált és visszaver jel közötti időkülönbség

kiszámításának köszönhetően lehetőség nyílik a környezet 3D-s feltérképezésére, és ezáltal a régtérben jelenlévő objektumok helyzetének, irányának és sebességének meghatározására. A sebesség a mozgó tárgyak miatt a Doppler-effektusból is számítható.

A drónelhárítás alapját a drón detektáló rendszer határozza meg elsősorban. A detektáláshoz alkalmazott eszközök különböző pontossággal tudják észlelni, osztályozni, lokalizálni és követni a betolakodó drónt. Először bemutatom a napjainkban legelterjedtebb műszaki megoldásokat a drónelhárítás területén, ami lehet:

- Elektronikai alapú semlegesítő rendszer
- Kinetikus-mechanikus semlegesítő rendszer

Az elektronikus semlegesítők egyik csoportjának működési elve azon alapul, hogy a semlegesítő zavarja a drón repüléséhez szükséges külső jelként érkező elektromágneses hullámokat, oly mértékben, hogy az nem tud eljutni a kijelölt célállomásra. Ennek két típusa van a rádiófrekvenciás zavarás és a GPS alapú zavarás.

Az RF zavarási technikák lehetővé teszik az drónelhárító rendszert üzemeltetők számára a rosszindulatú drón és a távirányítója közötti kommunikáció megzavarását, minőségromlását vagy akár a teljes megszakítását. Ennek eredményeként a LOS tartományon kívül nem lesz képes a drónt irányítani.

A GNSS zavarás alapműködését tekintve hasonló az RF zavaráshoz, csak annyi a különbség, hogy a zavarás nem a távirányító és a drón közötti kommunikációt lehetetleníti el, hanem a drón pozíció meghatározási képességét csökkenti vagy teljesen megakadályozza. Az ilyen technikáknak az autonóm drónok elleni védekezésnél van jelentőségük, mivel ezen típusú drónoknál a repülés egy előre meghatározott útvonalon történik, így nincs szükség távirányítóra.

Létezik még a protokoll alapú zavarás, ahol a kommunikációs szabványok sérülékenységeit használják ki és DoS alapú szolgáltatásmegtagadás támadási eljárást használnak. A drón és a távirányító közötti például WIFI kapcsolat, úgy zavarható meg hogy a drónelhárító rendszer nagymennyiségű kommunikáció felvételét célzó csomagot küld a drónnak. Erre a drón a kommunikáció kialakításához szükséges válasz csomagot küld majd várakozik és ha nem kap választ akkor még háromszor megismétli a küldést. Ezt nevezzük háromutas kommunikációnak. [79 p. 11] [80] A kapcsolatfelvételi eljárás idejére a handshake üzenetek tárolásra kerülnek. Ennek a memória szegmensnek a



kapacitása véges így, ha megfelelően nagy mennyiségű üzenetet küldünk a drón felé, akkor a memória telítődhet és túlsordulhat. A memória terület telítődésével megvalósul a túlterheléses támadás, mivel nem lesz képes újabb kapcsolati kezdeményezések kialakítására, ami a drón használó szempontjából a szolgáltatás működésképtelenségét jelenti.

A hamisítás technológia egy nagyon bonyolult eljárás, itt nem elegendő az adatkommunikáció fizikai rétegének ismerete, hanem a protokoll veremk ismerete is szükséges. Ezt a technológiát alkalmazó drónzavaró rendszerek egy olyan elfogadható hamis jelet küldenek a drón vevője részére, amelyet úgy érzékel mintha az lenne a valós vezérlő jel. Ennek hatására a drón felett át lehet venni az irányítást és ki lehet vezetni a védett objektum területén kívülre és ott biztonságosan le lehet szállni vele. Az elfogott drónból, így további információk gyűjthetők a kinyert metaadatok segítségével.

A kinetikus-mechanikus semlegesítők képesek fizikailag blokkolni vagy akár megsemmisíteni a behatoló drónt. Az elhárító rendszer hatékony működéséhez szükséges a hatástalanítani kívánt drón pontos célzása, illetve követése. Valójában ezeknek a semlegesítőknél a lehető legközelebb kell kerülniük a támadott drónhoz. A semlegesítés történhet:

- lövedékekkel,
- hálókkaal,
- ütköző drónokkal.

A lövedék és a háló alkalmazása esetében is célszerű azt légi platformról indítani, mivel ezeknek az eszközöknek a célba juttatását nagyobb távolságról erősen befolyásolja a szél és a csapadék, viszont egy drónról indítva ezek a hatások a jelentősen kisebb akár néhány méteres távolság miatt teljesen kiküszöbölhetőek.

#### **5.1.4 A vagyonvédelemben alkalmazott eszközök továbbfejlesztési lehetőségei**

A jelenleg rendelkezésre álló elektronikus, illetve elektromechanikus objektumvédelmi eszközök fejlesztési és alkalmazásuk középpontjában még mindig „csak” a jelzés és riasztás funkció áll, holott az elektronika és informatika ugrásszerű fejlődése lehetővé tenné ezen védelmi eszközöknél számos többletfunkció kialakítását. Az objektumvédelmi rendszer komplex szemléletű vizsgálata során arra a következtetésre jutottam, hogy apró módosításokkal és kiegészítésekkel az elektronikus rendszereknél is kialakítható a

mechanikai vagy előerős védelem funkciói, ami a késleltetés és elhárítás. Természetesen nem a teljes alrendszer helyettesítésére kell gondolni, hanem az elektronikus rendszer néhány olyan képességgel való felruházására, amely átvesz a másik két alrendszertől funkciókat vagy annak hatékonyságát növeli.

A személy beléptetési és ellenőrzési pontok többsége, úgy van kialakítva, hogy a belépési pont kapui, a személyátvizsgáló kapu és a csomagvizsgáló berendezés külön-külön önálló készülékek, amelyek között nincs semmilyen elektronikus logikai kapcsolat. Egyedül a beléptető rendszer képes automatikusan áteresztetni, illetve korlátozni a belépni kívánó személyt a belépési jogosultság vizsgálata után. A többi eszköznél is ki kell alakítani azt a lehetőséget, hogy az adott csomag és egy fémvizsgáló vagy robbanóanyag detektáló kapu vizsgálati eredménye egyértelműen hozzárendelhető legyen az adott személyhez. A funkció megvalósításához el kell látni a fémvizsgáló kaput, a csomagröntgent és a robbanóanyag detektáló kaput a személy azonosításra alkalmas elektronikus berendezéssel. Ezek jellemzően belépőkártya olvasók vagy biometrikus olvasók. Végül a személy azonosítására is alkalmas vizsgáló berendezéseket be kell integrálni a beléptető rendszerbe.

A gépjármű beléptetési pontok nukleáris létesítményeknél jellemzően zsilip rendszerű kialakításúak, a sorompók és kapu vegyes használatával, amit az első fejezetben részletesen ismertettem és illusztrációs képpel is bemutattam. A mechanikai akadályt a kapu jelenti a sorompónak inkább csak forgalom korlátozó szerepe van. A gépjármű belépési pontokon szintén nincs kapcsolat a gépjármű beléptető és a személy beléptető rendszerek között. A kockázatok csökkentése érdekében a gépjármű beléptetési pontot ki kell egészíteni egy automatizált tüskés vagy késes útakadállyal. [81]

Az objektumok nyílászáróinak jellemzően az üvegfelülettel nem rendelkezőknek a másodlagos rejtett késleltetési funkciója alakítható ki. Általánosságban a nyílászárókat nyitásérzékelőkkel, illetve az ajtó mögötti helyiség térvédelmi érzékelőkkel vannak felszerelve, ami következtében egy illetéktelen behatolás már a mechanikai gát leküzdését követően kerül detektálásra. Kutatásaim során már találok az okosajtó kifejezéssel, de ezek nem feltétlenül a biztonság fokozását szolgálják, hanem inkább egy kényelmi funkciót. Egy biztonsági bejárati ajtókat forgalmazó cég öt lehetőséget javasol, ami okosajtvá teszi a hagyományos bejárati ajtót:

- kártyás ajtónyitás

- okos zár
- kódkilincs
- pánikzár
- digitális kitekintő [82]

A felsorolásból jól látszik, hogy csak az ajtó elektronikus nyitás különböző lehetőségeit kínálja és egyéb kényelmi funkciókat, viszont a mechanikai állóképesség fokozására nem kínál semmilyen megoldást. A másodlagos és egyben rejtett késleltetési funkció kialakítható érzékelők és elektromechanikus reteszek segítségével. Az ajtót fel kell szerelni rezgésérzékelővel, testhangérzékelővel és lángérzékelővel, ami lehetővé teszi az összes behatolási kísérlet felismerését a kezdeti pillanatban. Majd ezen érzékelőkkel kell vezérelni egy vagy több nagyszilárdságú elektromechanikus reteszt, aminek az lesz a következménye, hogy az elkövető által sikeresnek gondolt ajtó feltörés végén még mindig egy zárt ajtóval találkozik. Ugyanezen érzékelőkkel és beavatkozókval ellátott ajtót úgy is lehet működtetni, hogy a reteszműködés csak azután aktiválódik, mikor már a behatoló belépett az objektumba, így őt csapdába ejtve. Ennek a működtetési módnak viszont az a feltétele, hogy az objektum összes nyílászárója el legyen látva elektromechanikus reteszeléssel és egyidőben lépjenek működésbe.

## **5.2 Autonóm működésű aktív rendszerek kialakítási koncepciói**

Az autonóm működés megvalósításához szükséges rendszerelemeket meghatároztam az előzőekben. Ezen rendszerelemekből, olyan aktív autonóm beavatkozásra képes rendszereket alakítok ki, amelyek a nukleáris létesítmények komplex védelmi rendszerének a hatékonyságát növelik, csökkentik a humán eredetű és a technikai fejlődésből jelentkező kockázatokat, valamint optimalizálják az élőerő létszámigényét.

### **5.2.1 Belső elkövetők hatékony kiszűrése aktív védelmi rendszerekkel**

A belső elkövetői kockázatokat a harmadik és negyedik fejezetekben részletesen ismertettem, de ezen kockázatok csökkentéséről még nem esett szó. A nukleáris létesítmények belső elkövetők elleni védekezésben fontos szerepet játszik a humánbiztonsági szakterület. A nemzetközi és hazai jogszabályok alapján az OAH fizikai védelmi útmutatót adott ki. A belső elkövetők elleni védelem címmel. Az útmutató ajánlásokat tartalmaz és meghatározza a belső elkövető azonosításának, cselekményei megelőzésének, megakadályozásának, valamint azok következményei csökkentésének értékelési módszertanát. Ennek ellenére még maga az útmutató is úgy fogalmaz, hogy a

belső elkövetők kiszűrése egy igen nehéz feladat és a hatékonysága nem mérhető. „*A potenciális belső elkövető kizárása az összes megelőző intézkedéssel együtt nehéz, de az alkalmazott intézkedések (mint a megbízhatóság ellenőrzése a foglalkoztatás előtt és alatt) vélelmezhetően hatékonyan csökkenti – bár teljesen nem zárja ki – a belső elkövető lehetőségét. Ezek az intézkedések észszerű és körültekintő óvintézkedések még akkor is, ha azok eredménye mennyiségileg nem értékelhető.*” [83 p. 23] Az útmutató a megelőzésre fekteti a hangsúlyt és a detektálás és megakadályozás szempontjából szinte csak adminisztratív intézkedéseket javasol. Átfogó megközelítés kialakítási javaslat részben említést tesz a technikai rendszerekről, de csak annyit, hogy többszintű védelmet kell kialakítani nyomon követéssel és késleltetéssel. A belső elkövetőnek a rosszindulatú cselekmény végrehajtásához szerszámokra, eszközökre van szüksége, amelyek vagy rendelkezésre állnak a védendő objektumban vagy magának kell bejuttatnia azt legálisan vagy illegálisan. A fizikai védelmi zónákat, védelmi szinteket és a komplex védelem kialakítását az második fejezben ismertettem. Belépve egy nukleáris létesítmény területére az ellenőrzött zónába az első védelmi zónába jutunk, amihez egy beléptetési ponton kell áthaladnunk. Ezen a zónahatáron jellemzően a biztonsági személyzet végzi a belépőkártya meglétét és jogosult használatát, valamint a csomag/poggyász átvizsgálását, aminek a hatékonysága jelentősen csökkenhet a frekvenciált időtartományokban, amikor rövid időn belül (5-10 perc) több száz ember halad át. A beléptetési pont megfelelő áteresztő képességéhez egyidejűleg 4-6 beléptető terminál alkalmazása szükséges, ami természetesen ugyanennyi élőerőt is jelent.

A személyek beléptetési pontjainak aktív elektronikus védelmi rendszeré alakítása, úgy lehetséges, ha azt egy zsiliprendszerre alakítjuk át, magába foglalva a jogosultság ellenőrzést, a személyazonosság ellenőrzést és a csomagvizsgálatot. Ezek soros logikai reteszelésként kell, hogy képezzenek. A zsilip első ellenőrzési lépése a fényképes belépőkártya olvasó, numerikus panel (pin kód bevitel) és a beléptető rendszerbe integrált arcfelismerő kamera együttes alkalmazása. A beléptető adatbázisában mentet fénykép és a kamera megjelenített képe összehasonlításra kerül az arcfelismerő algoritmusban, valamint a kártyához tartozó pin kód a numerikus billentyűn bevitt kóddal, és egyezés esetén engedélyezi a zsilip ajtajának automatikus nyitását. Második lépésként a csomagvizsgáló röntgenbe behelyezi a nála lévő táskát és személyes eszközt és ismételten kártyát olvastat. Az ismételt kártyaolvastatással összerendelésre kerül a csomag és a személy. A csomagröntgennek rendelkeznie kell intelligens video analitikával, hogy a

készített képet automatikusan ki tudja értékelni és autonóm tudja szabályozni az áthaladást. A csomagvizsgálattal egyidejűleg a személy áthalad a fémvizsgáló kapun. A két berendezés engedélyezi a zsilip kijárati ajtajának nyitását, ha a vizsgálatok eredménye megfelelő volt. A zsiliprendszert mindkét irányba ki kell alakítani. A fentiek alapján kialakított rendszerrel a beléptetési folyamat teljes autonóm működésűvé válik, kizárva a humánkockázati tényezőket. A beléptetési pont teljes mértékben nem hagyható élőrő nélkül, mert jogosultsággal nem rendelkező vagy tiltott tárgy bevitelét megkísérlő személlyel szemben intézkedni kell. A létszám viszont irányonként egy -egy főre redukálható.

A mobiltelefonok bevitele a fokozottan őrzött zónába adminisztratív módon tiltott. A szabály betartásának ellenőrzése élőrős személyzetet igényel. A mobiltelefon fokozottan őrzött zónába való bevitele szintén megakadályozható autonóm elektronikus védelmi rendszerrel. Az ellenőrzött zóna belépési pontján kialakított autonóm aktív beléptető zsilip alkalmazásával annyi kiegészítéssel, hogy mobiltelefon detektorral ellátott fémvizsgáló kaput kell alkalmazni. Olasz mérnökök kifejlesztettek egy MSD detektort, ami képes érzékelni a mobiltelefont és megkülönböztetni az egyéb fémtárgyaktól.



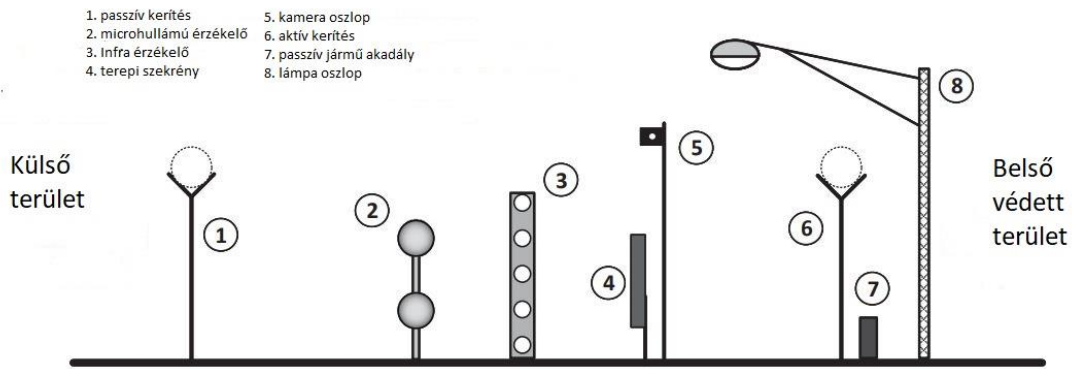
12. ábra - Mobiltelefon detektoros fémvizsgáló kapu [84]

A detektor fejlesztése és a fémvizsgáló kapuba integrálása nagy előrelépést jelent az objektumvédelem tekintetében, de meg kell jegyezni, hogy a berendezés ebben a formában „csak” elektronikus jelzésre alkalmas.

A gépjárműveket nehezebb átvizsgálni, mint a személyeket, ezért a kockázatok csökkentésének a leghatékonyabb módja, ha korlátozásra kerül az érzékeny területekre belépési engedéllyel rendelkező gépjárművek száma. [83] Ez a korlátozás viszont már nem alkalmazható az ellenőrzött zóna gépjármű beléptetési pontjánál, ami a kockázatok növekedését eredményezi. A probléma feloldására egy aktív tüskés vagy késes útakadályt kell alkalmazni. Az eszközt a zsilip kimeneti sorompója után kell elhelyezni. Az alapállapota mindig felnyitott kell legyen és amikor az ellenőrzési folyamat lezárul a kimeneti sorompó nyitással, akkor kell lecsukódnia ameddig át nem halad a jármű. A jármű áthaladást az úttestbe épített induktív hurkokkal kell érzékelni, ami lehetővé teszi az autonóm működést.

### **5.2.2 Behatóló ártalmatlanítása aktív védelmi rendszerrel**

A jogtalan belépési kísérlet az objektum területére két szárazföldi szcenárió mentén valósulhat meg. Az egyik a belépési ponton történő erőszakos áthaladás a másik az objektumot körül határoló periméter védelmi rendszer mechanikai akadályainak leküzdése. Az ellenőrzött zóna határán kiépített kerítésrendszer az első akadály a mélységben tagolt védelemben. Ezt további kerítések és építmények követik egészen a belső zónáig. A Nemzetközi Atomenergiái Ügynökség előírásai egyértelműen meghatározzák a kerítések kialakításának technikai paramétereit, amit a „*Kézikönyv a nukleáris anyagok és nukleáris létesítmények fizikai védelmi rendszerek tervezéséhez*” című kiadványában találhatunk. [85] Az ellenőrzött zóna kerítés rendszerét két egymástól 6 méter távolságban elhelyezett párhuzamos kerítéssel kell kiépíteni, így kialakítható egy nyomsáv, ahol az elektronikus védelmi eszközök telepíthetők. Az egyik kerítés passzív, ami csak mechanikai késleltetést valósít meg, a másik kerítés viszont aktív, mert az elektronikai eszközökkel van ellátva, ami képes detektálni bármilyenű szabotázszt. A periméter védelmi elektronikai érzékelő rendszernek több detektálási vonallal kell rendelkeznie. Egyik lehetséges megoldása, ha a külső kerítéstől befelé indulva mikrohullámú érzékelőpárt, majd aktív infra sorompót és végül video analitikával rendelkező dual szenzoros kamerarendszert telepítünk. Légvégül a belső kerítésre rezgésérzékelőkből kialakított rendszert kell telepíteni. A rendszert az alábbi ábra jól szemlélteti.



13. ábra - Ellenőrzött zóna periméter védelmi rendszer [85]

A védelmi rendszer aktivitás fokozása, úgy valósítható meg, hogy az 13-as ábrán szereplő rendszer kiegészítésre kerül az 5.1.1. fejezetben bemutatott TADD vagy TRAD területvédelmi eszközzel és egy automatikus hangalapú figyelmeztetést lejátszó berendezéssel. A nyomsáv teljes szélessége 6 méter, míg a két eszköz hatótávolsága 5-7 méter, ami lehetővé teszi a két kerítés közötti teljes területi lefedettséget. Az autonóm működés megvalósításához a detektáló rendszer első védelmi vonalát szakaszonként logikai kapcsolatba kell hozni az adott szakaszon elhelyezett területvédelmi eszközökkel, hogy az élőerő és más aktív rendszerek felé küldött jelzésen kívül élesítse a területvédelmi eszközöket, amelyeket a saját érzékelőik fognak működésbe hozni. A kikerülő őrszemélyzet a helyszínen egy ártalmatlanított, de mindenképpen csökkentett harcképességű behatolóval fog szembesülni, aki még valószínűleg az aktív kerítésen sem jutott át. Az OAH FV-4-es számú útmutatója szerint egy 2,5 méter magas kerítés leküzdési ideje átlagosan 12 másodperc, de minimum késleltetési időként 6 másodperc van meghatározva. Az átlagos idővel számolva a két kerítésen való átjutás beleszámolva a nyomsávot is 26 másodperc alatt végrehajtható. Majd sík terepen kb. 400 méter megtételével elérhetővé válnak a biztonság szempontjából fontos berendezéseket tartalmazó épületek. A 400 méteres táv megtételéhez maximum 10 kg-os felszereléssel 100 másodperc szükséges. Feltételezhetően a 400 méteres távon minimum még egy kerítést le kell küzdeni, ami szintén átlagosan 12 másodperc. [86] Összesítve az adatokat a külső területről egy olyan épületig, ami fontos berendezéseket tartalmaz 2 perc 18 másodperc alatt lehet eljutni. Ennyi ideje van, illetve ennél 10-15 másodperccel kevesebb az élőerőnek reagálni úgy, hogy a támadó és a védendő objektum közé érkezen és megszakítsa a támadási folyamatot. Megállapítható, hogy az aktív beavatkozó területvédelmi eszköz rendszerbe integrálása és annak eredményes működése esetén nagyságrendekkel több ideje van a reagáló erőknek a szabotázs cselekmény

felszámolására. A sokkoló 5 másodpercre mozgásképtelenné teszi a behatolót és további 10-15 perces, olyan élettani hatásokat vált ki, aminek következtében az érintett személy harcképtelenné válik.

### **5.2.3 Drónok az előerő szolgálatában**

A drónok polgári, ipari célú felhasználására számtalan megoldás található, amelyből a rendvédelmi, biztonságtechnikai alkalmazásukra nagyságrendekkel kevesebb gyakorlattal találkozhatunk. A tudományos közlemények tekintetében is elmondható, hogy a drónokkal kapcsolatosan egyre több publikáció jelenik meg, de témájukat tekintve jelentős hányaduk a használatuk kockázatait, a drónok elleni védekezést, az alkalmazásuk jogi kérdéseit és az ipari szegmensben való felhasználásuk más területeit dolgozza fel. Az objektumvédelmi felhasználásról nagyon kevés példával lehet találkozni, ezért a védelmi rendszerbe integrálásának feladatát, valamint specifikációját új megközelítésnek tekintem. A fejezet első részében specifikált képességekkel rendelkező mini kategóriájú forgószárnyas drón és további drónra applikálható eszközök felhasználásával meghatározok egy, olyan aktív védelmi drónrendszert, amely képes az előerő számos tevékenységét hatékonyabbá tenni és bizonyos esetekben kiváltani, csökkentve a komplex védelmi rendszer kockázatait.

A rendszer kialakítását a kockázatokkal arányos válaszingtézkedések tükrében a megvalósítandó funkciókra alapozva határozom meg:

- Járőrözési funkció megvalósítása
- Riasztási esemény kivizsgálása
- Első beavatkozási feladatok megvalósítása
- Vezetéstámogatás a szabotázs alatt
- Emelt szintű fizikai védelmi feladatok
- FBŐ gyakorlati képzés támogatása

A fentiek alapján jól látható, hogy a drón bevetetősége a védelmi rendszerben igen sokrétű. A feladatok maradéktalan ellátásához három különböző összeállításra van szükség.

Alapkiépítésben a drónon elhelyezendő egy kétlencsés kamera, amely egyik csatornája a látható fény tartományában a másik csatornája pedig a 8-14  $\mu\text{m}$  hullámhossz tartományban működik. Elhelyezhető lenne egy normál és egy hőkamera is, de a kétlencsés megoldás jelentős súlycsökkenést és alacsonyabb tápellátási igényt jelent. A



kamera kimeneti jelét vezeték nélküli kommunikáció segítségével továbbítani kell a video megfigyelő rendszerbe, ahol a rögzítés mellett video analitikai szoftver segítségével alarm, illetve trigger jelek képezhetőek a drón autonóm működését vezérlő rendszerhez. A kamerán kívül egy kétirányú átbeszélőt is fel kell szerelni a drónra, a párját pedig az őrségközpontban. Az átbeszélő eszköz első alkalommal egy előre felvett hangüzenetet játszik le (például: ön az atomerőmű területét túlságosan megközelítette kérem hagyja abba tevékenységét) majd, ha ez hatástalan, akkor az őrszemélyzet tud kapcsolatba lépni az észlelt személlyel és további utasításokat adni. Az alapkonfiguráció szerinti drón alkalmazható járőrözési, riasztási esemény kivizsgálási és vezetéstámogatási feladatok ellátására.

A beavatkozásra is képes drón kialakításához az alakiépítésen túl el kell helyezni egy Taser-t. A kívánt hatótávolság függvényében az M26-os típus 3-7 méteres hatótávolsággal, vagy az XREP 15-20 méteres hatótávolsággal alkalmazható. A Taser M26-os rendelkezik adatkommunikációs port-tal, amin keresztül a távműködtetés valósítható meg. A Taser XREP egy sörétes puskából kilőhető kapszula, amely magába foglalja az akkumulátort és a sokkoló berendezést. Az XREP elsütéséhez viszont még egy kioldószerkezetre is szükség van, amit a drónra kell szerelni. A két eszköz jelentős méret és súly béli különbsége, miatt az M26-os típusú eszköz alkalmazását találok megfelelőbbnek. A katonai fejlesztések területén már a végső fejlesztési tesztelési fázisban vannak a drónokra helyezett gépkarabélyok alkalmazási lehetőségének vizsgálata, sőt Törökország már exportálja is a terméket.



14. ábra - ASISGUARD gyártmányú SONGAR csapásmérő drón [87]

Az FBŐ intézkedéstaktikai eljárásokkal végrehajtott gyakorlati képzésének a támogatása egy csapat mód funkcióval rendelkező távirányítású drónnal oldható meg a leghatékonyabban. A csapat mód lehetővé teszi, hogy egyidőben két vezérlőn keresztül két kezelő külön-külön irányítsa a drónt és a kamerát. Az intézkedéstaktikai eljárások oktatására nem találtam olyan jellegű forrásanyagot, amely ezt pontosan leírná, hogy milyen elemekből épül fel, csak a 27/1998. (VI. 10.) BM rendelet a fegyveres biztonsági őrség Működési és Szolgálati Szabályzatának kiadásáról szóló rendelet 73. § 2. bekezdés c pontja tartalmazza az önvédelmi ismereteket, mint képzési, felkészülési követelményt. Az intézkedéstaktikai gyakorlati képzés pontosabb megismerése céljából szakmai egyeztetést folytattam a nukleáris létesítmények képzési előadóival és őrségparancsnokaival. Az intézkedéstaktikai képzések tartalmát teljeskörűen nem ismertették velem, mert az már érzékeny információ harmadik félnek való átadását jelentené, de a munkám segítése céljából a minősített adatokra vonatkozó törvény betartása mellett néhány példát megemlítettek. A szabotázs felszámolása közben alkalmazandó taktikák példái: terület zárás, biztosított kiszálás, elszakadás és átkarolás.

Az előerő munkáját segítő, illetve drónnal kiváltható összes feladat egyidejű ellátása a védendő objektum teljes területi lefedettsége mellett egyszerre több drón alkalmazásával valósítható meg. A járőrözési feladatok, az emelt szintű fizikai védelmi feladatok és a riasztási esemény kivizsgálására használható drónok számának meghatározásánál első sorban a maximális repülési időt és az akkumulátor feltöltési időt veszem alapul. Külön kell választani az alapfenyegetettség és megnövekedett fenyegetettségkor ellátandó feladatokat. Az alapfenyegetettség fennállásakor elvégzendő tevékenységek közé tartozik a járőrözés és a riasztási esemény kivizsgálása. Erre a feladatra összesen hat darab drón szükséges 4 db járőrözési feladatok ellátására és 2 darab eseménykivizsgálási feladatra. A drónok mennyiségének meghatározásánál figyelembe vett paraméterek:

- repülési idő minimum 45 perc
- töltési idő 1 óra
- repülési magasságok 30 méter és 50 méter
- az objektum területe maximum 300 hektár
- repülési sebesség 3 m/s
- kamera látószög 80°

A négy darab járőröző drón dokkolóit az ellenőrzött zóna kerítésein belül megfelelő védelmet nyújtó távolságban a terület középpontjától a négy legtávolabbi pontján kell elhelyezni, ahonnan indulnak és ahová érkeznek a drónok. Megközelítőleges méréseket végeztem a védendő objektum területét illetően google maps műholdas felvételeket használva hat üzemelő atomerőműnél. Kettő, négy és hatblokkos kiépítésű erőművek területmeghatározásának eredménye 121 hektártól 283 hektárig terjedt, így a védendő terület méretét 5%-os mérési bizonytalanságot alkalmazva 300 hektárnak állapítottam meg. A mérésekből kiszámolható, hogy az objektum periméter védelmi vonala 7 km hosszú. Az egyidejű rotációs négydrónos járőrözéssel a teljes nyomvonal 3 m/s-os sebességgel 30 méter magasságból 10 perc alatt teljesíthető, amennyiben nem észlel a videóanalitika eltérést, személyt vagy akár elhagyott tárgyat. A járőrözést követően 20 perces töltési fázis következik, majd az adott dokkolóhoz tartozó egynegyednyi terület teljes pásztázása 50 méteres magasságból, ami szintén 10 percet vesz igénybe és ismét 20 perces töltési ciklus következik. A pásztázó terület bejárásának útvonalát és az objektumhatár vonalában végzet járőrözés irányát random módon változtatnia kell az autonóm működést biztosító algoritmusnak. A specifikált autonóm járőrfunkcióval biztosított a teljes terület óránkénti vizuális átvizsgálása. Az elektronikus védelmi rendszerekből származó riasztások kivizsgálására, akkor van szükség, amikor az adott területről érkező riasztás nem behatolási kísérlethez köthető. A drón helyszínre küldésével hatékonyabban végezhető el a feladat, mint a telepített videó megfigyelő rendszer fix és magaslati PTZ kameráival, valamint élőerőt se kell a helyszínre vezényelni. A járőröző drónnal megegyező specifikációjú két kivizsgáló drónt a védendő objektum középpontjában kell elhelyezni, hogy a lefedett terület különböző pontjaira azonos idő alatt tudjon odaérni. A két darabos szükségességet az egynél több egyidejű riasztás indokolja.

Az emeltszintű fizikai védelmet a hirtelen megnövekedett fenyegetettség következtében az állam rendelheti el a kötelezett részére. Az emelt szintű fizikai védelem a fizikai védelmi funkciók elrendelt megerősítését jelenti, amelynek a konkrét intézkedéseit a Fizikai Védelmi Terv (továbbiakban: FVT) tartalmazza. Az FVT nemzeti minősített dokumentum, ezért a konkrét intézkedésekről nincs információ. Általánosságban a fenyegetettség növekedése esetén ésszerű intézkedés a folyamatos járőrözés elrendelése vagy a járőrözési terület kibővítése a létesítmény jogi határain kívüli területre. A jogszabályi környezet lehetővé teszi a kötelezett részére, hogy állami segítséggel hajtsa

végre a feladatot (például rendőrség). [88] Amennyiben a védendő atomerőmű rendelkezik autonóm járőröző drónokkal, abban az esetben az eszközöket tud biztosítani a rendőrség számára.

Az objektumot érő valós szabotázsakor reagáló drónokat lehet alkalmazni az őrsemélyzet veszélyeztetettségének csökkentése és az elhárítás hatékonyságának növelése érdekében. A reagáló drónok számát 4 darab beavatkozó és két darab járőröző képességekkel rendelkező, azaz összesen 6 darabban határozom meg, tekintettel a Taser M26-os képességeire (kétszer két elektródapár) és a nemzetközi gyakorlatban figyelembe vett támadási scenáriókra. [63] A maximálisan figyelembe vehető támadók száma 6 fő és maximum egy időben két behatolási ponton keresztül hajtják végre a szabotázs cselekményt, így egy kétszer háromfős csoportról beszélhetünk. A nukleáris létesítményekről elmondható, hogy nem puha célpontok, így a támadók biztosan alapos felkészülés és jól megtervezett előkészületek után kísérik meg a szabotázs akció végrehajtását. A sikeres előkészítés eredménye, akár az is lehet, hogy eredményesen megzavarják vagy esetleg kiiktatják a nyomsvonal egy adott szakaszának az autonóm területvédelmi eszközeit, így a mechanikai akadályok késleltetési idejére számíthatunk csak, ami a korábbi adatok alapján átlagosan 26 másodperc. Ebből az időből még le kell számítani az észlelési időt is, ami maximum 2 másodperc. Az élőerő kiérkezéséhez rendelkezésre álló idő 24 másodperc, amiből az következik, hogy a véderők nem a behatolási pontnál tudják feltartoztatni, hanem valahol biztosan a kerítés és a reaktorblokkok közötti területen. Mindezt egyidőben két behatoló csoporttal szemben kell teljesíteni. Az esemény elhárítási folyamata beavatkozó drónok alkalmazásával egy lehetséges megoldása a következőképpen alakul. A kerítésvédelmi rendszer érzékeli a behatolást és riasztási jelet generál az élőerő és az autonóm drónrendszer vezérlője felé. A riasztási jel tartalmazza a behatolás lokációs adatait, ami a drón számára meghatározza a repülési irányt és a célt. A beérkező riasztáskor felszál a két beavatkozó és egy megfigyelő drón és elindul a cél felé. A helyszínre érkezéshez szükséges idő 20 m/s-os repülési sebességgel 34 másodperc, de ekkor már az elkövetők 40 méterre eltávolodtak a kerítéstől, ami nem olyan nagy távolság, hogy az érkező drón ne tudná beazonosítani az elkövetői csoportot. Azonosítást követően meg kell győződni az elkövetői szándékról és a behatolót fel kell szólítani, hogy hagyja abba a tevékenységet. A sikertelen felszólítást követően megközelíti hatótávolságon belülre, célba veszi és működteti a Taser-t mindkét beavatkozó drón. A megfigyelő drón ezzel egyidőben a helyszínre érkezve magaslati képet

továbbít az eseményekről az őrségközpont felé, ami segítségével az őrparancsnok meggyőződhet a beavatkozás eredményéről. Természetesen a riasztás észlelésekor az őrszemélyzet is megkezdi a válaszingtezkedések végrehajtását.

#### **5.2.4 Drón detektálás és elhárítás**

A drón detektáló és elhárító rendszereket egyben vizsgálom, mint aktív védelmi rendszer. Két okból is célszerűnek tartom a két rendszer együttes kezelését. Az egyik, hogy az elhárítás nem valósítható meg drón detektálás nélkül, a másik pedig, hogy a kockázatoknál vizsgált szcenárióban az elkövetői szándék a robbanóanyag bejuttatása a védendő objektum területre. Drónelhárító rendszer nélkül teljesen értelmetlen, csak detektáló rendszert kiépíteni. A fejezet első felében bemutattam a lehetséges detektálási és elhárítási megoldások széles skáláját. A drónelhárító rendszer konfigurációjának kiindulási paraméterei:

- elhárítandó drón osztálya mikro és mini az 4. táblázat alapján
- dróntámadás szcenáriója a 4. fejezet alapján berepülés felderítés céljából és robbanóanyag bejuttatása a védendő objektum területére
- a drónelhárítási mód nem veszélyezteti az objektumot
- a detektálás hatótávolsága legalább 3 kilométer
- a hatékonyságát nagymértékben nem befolyásolhatja az időjárás

A drónok detektálására kifejlesztett különböző eljárások változó hatékonysággal képesek ellátni a feladatukat. Önállóan csak egy érzékelési eljárás nem képes ellátni teljes mértékben a detektálási feladatot. Mindegyik megoldásnak van valamilyen nehezen elfogadható korlátja, például nagy érzékelési tartomány, cserébe alacsony osztályozási képesség. Ugyanez elmondható az elhárító rendszerekre is. A kereskedelmi forgalomban jelenleg rendelkezésre álló drónok semlegesítésére szolgáló eszközök nem biztosítják a létesítmény hatékony védelmét. A drónsemlegesítő rendszert ezért különböző technológiájú drónsemlegesítő eszközökből kell felépíteni, hogy a semlegesítés valószínűsége elég magas legyen. A különböző elveken működő eszközök használata biztosítja, hogy a rendszer minden körülmények között teljesítse feladatát, azaz semlegesítse a drónt. A detektáló és elhárító rendszer koncepciója is csak körvonalakban írható le az objektum és környezetének ismerete nélkül. A rendszer telepítéséhez pontosan ismerni kell az objektum és a környezet számos paraméterét:

- időjárási viszonyok

- levegő tisztaság átlátszóság
- területre jellemző szélereőség
- sík vagy hullámzó a terep
- növényzet magassága az objektumban és környezetében
- észlelési magasság

Az érzékelési módszereket a korábbiakban bemutattam, de nem értékeltem a jellemzőik alapján. A legegyszerűbb értékelési mód a fő jellemzők mentén egy táblázatos összehasonlítással oldható meg.

Módszer	Működési feltételek	Hatótávolság
Aktív radar	Részben az időjárési viszonyok befolyásolják	Nagy hatótávolságú (~5 km)
Passzív radar	Részben az időjárési viszonyok befolyásolják	Nagy hatótávolságú (~5 km)
RF érzékelő	RF interferencia és részben az időjárési viszonyok befolyásolják	Középtávú (~2 km)
Akusztikus érzékelő	Az időjárési/zajviszonyok befolyásolják	Rövid hatótáv (~500 m)
optikai érzékelés	Az időjárési viszonyok befolyásolják, nappal/éjjel	Közepes hatótávolság (~1 vagy 2 km)

5. táblázat - detektálási módszerek összehasonlítása

A különböző detektálási módszerekből egy teljes rendszert lehet kialakítani, fő és kiegészítő technológiákat alkalmazva.

Feladat	Fő technológia	Kiegészítő technológia
Érzékelés	Radar, Akusztikus, RF	Optikai
Osztályozás	Optikai, RF, akusztikus	Radar
Lokalizáció/követés	Radar, optikai, akusztikus	RF akusztikus

6. táblázat - Fő és kiegészítő detektálási technológiák az észlelési feladat függvényében

Az összes paramétert figyelembe véve a hatótávolságtól a működési feltételeken keresztül a detektálási feladatokig, egy nukleáris létesítmény drón detektálási rendszerének az RF/akusztikus/optikai érzékelőkből álló fő technológiájú rendszert javaslok kiegészítve aktív radarral. Drónelhárító rendszerek működési elvei is bemutatásra kerültek. A nukleáris létesítményeknél a legalkalmazhatóbb megoldás a hamisítás, mivel az elhárító rendszeren keresztül át lehet venni a drón vezérlését és biztonságosan az objektum területén kívül le lehet szállni. Majd a drónból kinyerhető az összes meta adat, ami segíthet az elkövető megtalálásához. Ez a módszer jól alkalmazható mindkét támadási szcenárió esetén kivéve, ha autonóm repülést hajtanak végre. A szóba jöhető másik megoldás a kinetikus elhárítási módok egyike lehet, mégpedig a drónról kilőtt háló. Viszont ehhez mindenképpen a Mini osztályú (25 kg) drónt kell alkalmazni és olyan hálót, ami ejtőernyővel is rendelkezik.

## **6 PRIMER KUTATÁS KÉRDŐÍVES ADATFELVÉTELI MÓDSZERREL**

A kutatás szekunder szakaszában tett megállapításaim további igazolására és alátámasztására egy kérdőíves primer kutatási szakaszt iktattam be. Továbbá a szekunder kutatási szakaszban nem volt lehetőségem a drón gyakorlati képzésben való alkalmazást az irodalomkutatás módszerével igazolni, megfelelő mennyiségű szakirodalom hiányában.

### **6.1 A primer kutatás módszertani leírása**

Kutatásom módszertani alapját az irodalomkutatás, az adatelemzés és értékelés, valamint a szakmai tapasztalataimból származó kutatási eredmények alkotják. Az elektronikus vagyonvédelmi eszközök aktivitás fokozásának vizsgálatai során, arra a következtetésre jutottam, hogy nem elegendő bemutatni a műszaki megoldásokat, illetve azok koncepcióit, hanem empirikus módszerrel vizsgálni kell a komplex védelmi rendszerbe integrálásának hatásait. Az empirikus kutatásnál a kvantitatív módszert alkalmaztam, azon belül az adatfelvételi eljárások közül a kérdőíves módszert választottam. A fókuszcsoporthként a fizikai védelmi rendelet hatálya alá tartozó létesítmények fegyveres biztonsági őrését választottam, leszűkítve azon létesítményekre, ahol a kültéri védelmi eszközöknek számottevő szerepe van a védelmi rendszerben és az élőerő létszáma meghaladja a 20 főt. A disszertációban bemutatott aktivitás fokozási lehetőségek közül a drónt alkalmazó műszaki megoldásokkal kapcsolatos véleményükre fókuszáltam. A papír alapú kérdőív zárt kérdéseket tartalmaz, amelyekre egy négy pontos Likert-skálán lehet válaszolni. A kérdőíves felmérésnek a „Drónok az élőerő szolgálatában?” nevet adtam. A kérdéseim fókusza az volt, hogy a drón mint védelmi eszköz alkalmazhatóságáról és a komplex fizikai védelemben való illeszthetőségéről milyen véleménnyel van az élőerős személyzet. Továbbá azt is nagyon fontosnak ítélem meg, hogy az új technológia megjelenése mennyire feszéjezi a személyzetet és véleményük szerint helyettesíthetőek-e ők a rendszerben technikai eszközökkel. A kérdésekre adott válaszokat nem vizsgáltam Khi négyzet próbával, mivel a kutatás szempontjából nincs jelentősége a Likert-skálák közötti kapcsolatok vizsgálatának. A kiértékelésben a válaszok normális eloszlásából vontam le következtetéseket.



## 6.2 A kutatásban résztvevő fegyveres biztonsági őrök eloszlása létesítményenként

Három létesítményben volt lehetőségem elvégezni a kérdőíves felmérést. A három létesítmény pontos nevét nem adathatom meg és a létesítményben szolgálatot teljesítők számát sem, csak a válaszadók összlétszámát és a felmérésben résztvevők százalékos arányát létesítményenként. A védelmi erők létszámát ugyan nyílt határozat tartalmazza, de a létesítmények rendészeti vezetői nem járultak hozzá a létszámadatok egyenkénti közléséhez és az volt a kérésük, hogy a létesítmények nevét se szerepeltessem a kutatási eredményeim közlésekor. A két nukleáris létesítmény és egy radioaktív hulladék tárolót Létesítmény 1, Létesítmény 2 és Létesítmény 3 néven szerepeltettem. Az 7. táblázat a három létesítményben az összes válaszadó számát, valamint a létesítményekben megkérdezettek és válaszadók arányát szemlélteti.

	Létszám	Kérdezett/válaszadók aránya
Létesítmény 1	---	90,07 %
Létesítmény 2	---	84,45 %
Létesítmény 3	---	85,71 %
Összesen	195 fő	88, 23 %

7. táblázat - Kutatásban résztvevő és a megkérdezett biztonsági őrök százalékos eloszlása

## 6.3 A dróntechnológia ismertségére és a fegyveres erőknél szolgált időtartamra vonatkozó kérdések kiértékelése

A kérdőívben fontosnak tartottam, olyan jellegű kérdések megfogalmazását, amelyek befolyásolhatják, illetve torzíthatják a kutatási eredményeket. Az objektivitás megítélhetőségéhez két kérdést tettem fel arra vonatkozólag, hogy mennyire ismerik a dróntechnológiát vagy találkoztak-e rendvédelmi, rendőrségi, illetve katonai célú felhasználással. Továbbá két kérdést, ami arra irányult, hogy mennyi ideje dolgozik az FBŐ kötelékében és a jelenlegi munkahelyét megelőzően szolgált-e bármilyen fegyveres szervezetnél. A kérdőív erre irányuló kérdései:

- Milyen mértékben ismeri az UAV-okat (pilóta nélküli légijármű), drónokat?

- A drónok felhasználhatósági területe igen széles a polgári és a rendfenntartói körökben is. Hallott-e rendvédelmi, rendőrségi, illetve katonai célú drónok alkalmazásáról?
- Jelenlegi foglalkozását megelőzően szolgált-e hivatásos fegyveres állományban?
- Mennyi ideje dolgozik fegyveres biztonsági őrként?

A válaszok eredményeit, olyan szempontból vizsgáltam, hogy a technológia ismerete vagy a fegyveres erőknél eltöltött idő befolyásolja-e a többi kérdésre adott választ.

A fenti négy kérdésre adott válaszok alapján megállapítottam, hogy a dróntechnológiával kapcsolatos ismereteik és a drón alkalmazhatóságára irányuló kérdésekre adott válaszok között egyértelmű összefüggés nem mutatható ki és a válaszaikat nem befolyásolták. A fegyveres erőknél eltöltött idő és a többi kérdésre adott válaszként is szintén, arra a következtetésre jutottam, hogy ok okozati összefüggés nem állapítható meg.

#### **6.4 A drónok védelmi rendszerbe integrálhatóságára irányuló kérdések kiértékelése**

Öt kérdést fogalmaztam meg, hogy megtudjam a véleményüket a drónok alkalmazhatóságával kapcsolatban. Az új technológiák bevezetése mindig azon áll vagy bukik, hogy a felhasználóknak milyen a hozzáállásuk. Mennyire tartják azt hasznosnak, vagy csak úgy tekintenek rá, mint egy újabb haszontalan eszközre, amit muszáj üzemeltetniük. A negatív hozzáállás jelentős mértékben rontja a technológia hatékonyságát. Továbbá a fegyveres biztonsági őrök véleménye alapján megállapítható, hogy a drónt be lehet-e integrálni a komplex védelmi rendszerbe. Ennek megállapítására az alábbi kérdéseket fogalmaztam meg számukra:

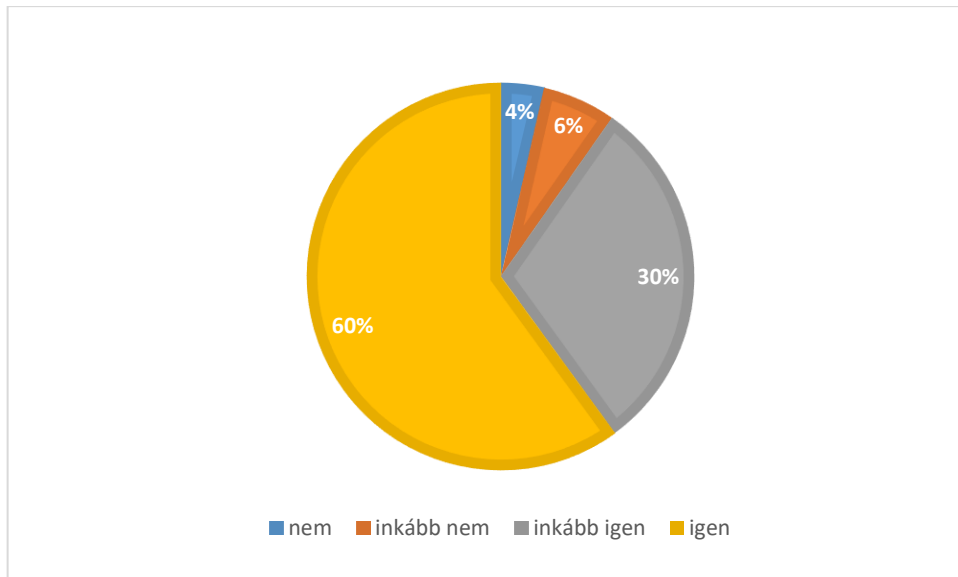
- Véleménye szerint megfelelő minőségű és funkciójú (normál és hőkamera, esetleg mindkét) kamerával felszerelt drónt lehet-e alkalmazni a telepített CCTV kamerarendszer kiegészítésére?
- Véleménye szerint a „legkülső” zónahatáron keletkezett jelzés valódiságának megállapítására alkalmazható- e egy megfelelő kamerával ellátott drón?
- Véleménye szerint egy nem halálos fegyverrel vagy a behatolót lelassító eszközzel (könnygránát, hang-fény gránát, hálövető puska) felszerelt drón alkalmazható-e az FBŐ kötelékében?

A drónra felszerelt kamera jól alkalmazható a vezetéstámogatási feladatok ellátására, a növényzet és épületrészek által kitakart területek időnkénti átvizsgálására és akár egy fix kamerával megfigyelt terület más perspektívából való megfigyelésére. A kérdésekre adott válaszok a következők alapján alakultak.

	Nem	Inkább nem	Inkább igen	Igen
Létesítmény 1	4 %	2 %	37 %	57 %
Létesítmény 2	16 %	8 %	16 %	60 %
Létesítmény 3	7 %	20 %	36 %	37 %
Összesen	7 %	6 %	33 %	54 %

8. táblázat - Véleménye szerint megfelelő minőségű és funkciójú (normál és hőkamera, esetleg mindkét) kamerával felszerelt drónt lehet-e alkalmazni a telepített CCTV kamerarendszer kiegészítésére?

Az őrzési feladatok ellátása során előfordulnak olyan jelzések, riasztások az elektronikus rendszereknél, amelyek a jelzőrendszer szempontjából valós érzékelésen alapul, de a későbbiek során az objektum védelme szempontjából téves riasztásnak minősül. Az ilyen típusú jelzéseket kiválthat esetleg a kerítés közelében mozgó vad, vagy például a megnövekedett aljnövényzet is. Az elektronikus védelmi rendszer minden egyes riasztását az elsődleges gyors helyzetfelismerés után alaposan ki kell vizsgálni, hogy pontosan meghatározásra kerüljön a téves riasztást generáló esemény. Erre a feladatra alkalmasnak találok egy normál és egy hőkamerával felszerelt drón helyszínrre küldésével elvégzett kivizsgálást. A három létesítmény FBŐ személyzetének összesített véleményét az 15.-ös ábra szemlélteti.



15. ábra - Véleménye szerint a „legkülső” zónahatáron keletkezett jelzés valódiságának megállapítására alkalmazható- e egy megfelelő kamerával ellátott drón?

A videó megfigyelő rendszer kiegészítésén és a helyszínre küldött riasztási esemény kivizsgálásán felül, tovább lehet fokozni a védelmi rendszerben az elektronikus vagyonvédelmi eszközök aktivitását egy beavatkozásra is képes autonóm drón alkalmazásával. Az ötödik fejezetben specifikáltam egy Taser-rel felszerelt elhárító drónt. A kérdőívben ennél egy jóval szélesebb skálán mozgó beavatkozó drón alkalmazhatóságáról kérdeztem meg a kutatásban résztvevő fegyveres biztonsági őroket. A véleményüket az 9. táblázat mutatja be.

	Nem	Inkább nem	Inkább igen	Igen
Létesítmény 1	9 %	15 %	27 %	49 %
Létesítmény 2	5 %	19 %	29 %	47 %
Létesítmény 3	7 %	23 %	33 %	37 %
Összesen	4 %	6 %	30 %	60 %

9. táblázat - Véleménye szerint egy nem halálos fegyverrel vagy a behatolót lelassító eszközzel (könnygránát, hang-fény gránát, hálövető puska) felszerelt drón alkalmazható-e az FBŐ kötelékében?

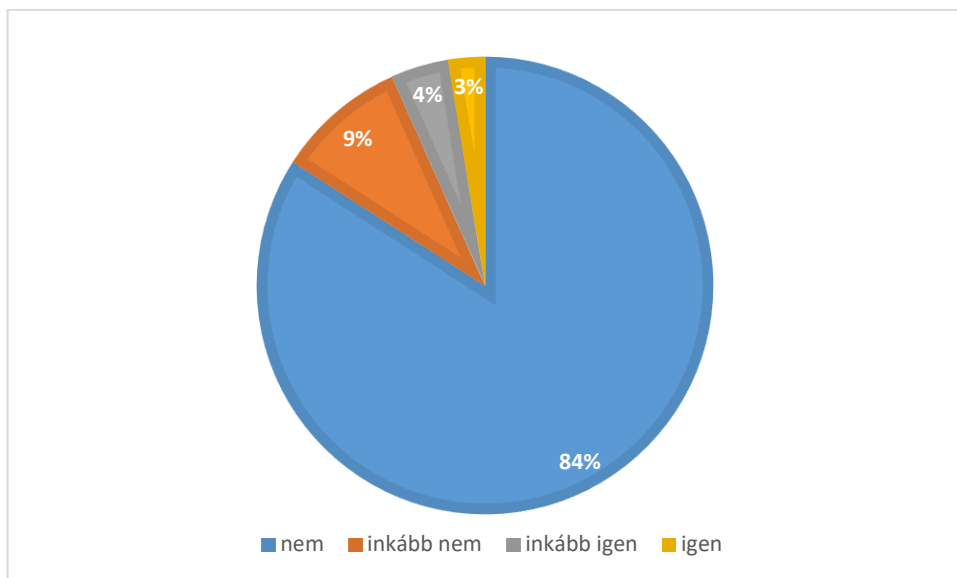
Az adatokból egyértelműen kijelenthető, hogy a megkérdezett 195 fő nagy többsége alkalmasnak tartja az általam felvázolt műszaki megoldást a rendszerbe való integrálhatóságra. A létesítmények FBŐ személyzete külön-külön is, és összesítetten vizsgálva is pozitív megítélésben vélekedett az alkalmazhatóságról. Ez az állítás még

akkor is igaz, ha csak az egyértelmű igen válaszokat veszem figyelembe az összlétszám tekintetében.

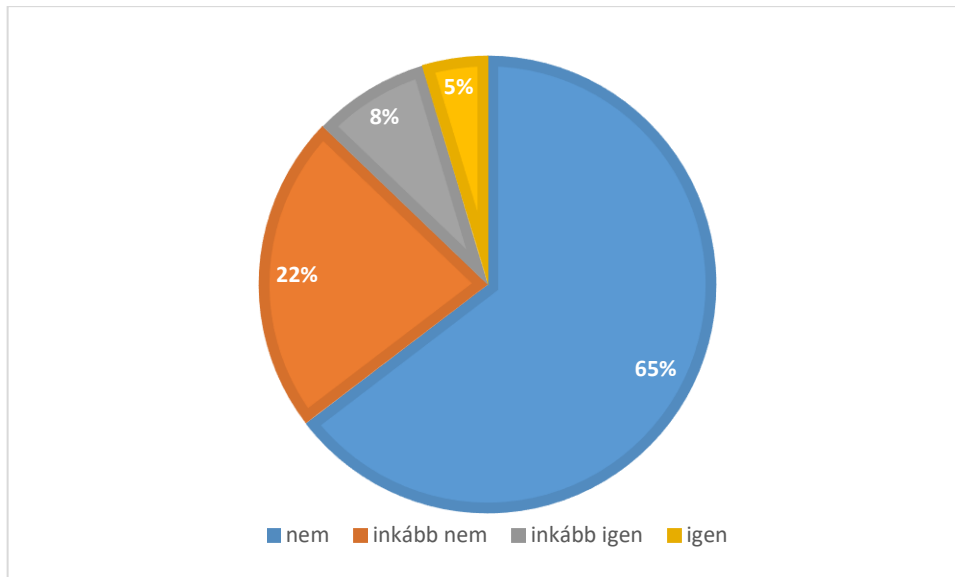
A kutatás szempontjából fontosnak tartom, hogy kiderüljön a technológiával kapcsolatos aggályaik is az FBŐ személyzetének. Ennek felmérésére két kérdést fogalmaztam meg:

- Véleménye szerint egy nem halálos fegyverrel vagy a behatolót lelassító eszközzel (könnygránát, hang-fény gránát, hálövető puska) felszerelt drón helyettesítheti-e teljes mértékben magát a fegyveres biztonsági őrt?
- Véleménye szerint, ha alkalmazásra kerülne egy drón kellene-e attól tartania, hogy az őrt helyettesítve megszűnik a munkahelye?

A kérdésekre adott válaszokat csak a 195 fő összesített válasza alapján jelenítem meg, mert a létesítményenkénti kiértékelés során a kapott eredmények az adott kérdésekre 5 %-os szóráson belül voltak.



16. ábra - Véleménye szerint egy nem halálos fegyverrel vagy a behatolót lelassító eszközzel (könnygránát, hang-fény gránát, hálövető puska) felszerelt drón helyettesítheti-e teljes mértékben magát a fegyveres biztonsági őrt?



17. ábra - Véleménye szerint, ha alkalmazásra kerülne egy drón kellene-e attól tartania, hogy az őrt helyettesítve megszűnik a munkahelye?

Az adatokból egyértelműen kijelenthető, hogy a megkérdezett 195 fő túlnyomó többsége nem gondolja azt, hogy helyettesíthető lenne egy elektronikus védelmi eszközzel és nem tart attól, hogy a drónok térnyerése a komplex védelmi rendszerben az élőerő rovására következne be. A kutatásom egyik feltételezése, hogy a drónok alkalmazásával optimalizálható az élőerő létszáma. A két diagram külön-külön szemlélve a feltételezésemnek ellentmondó eredményt mutat, de ha két diagrammot együtt vizsgáljuk, akkor kiolvasható, hogy a munkahely elvesztésének lehetőségét 6%-kal nagyobb arányban gondolják úgy, mint a helyettesíthetőséget, és az egyértelmű nem válaszok száma is 19%-kal alacsonyabb.

## 6.5 Gyakorlatok és képzések alkalmával készített drónos videófelvevételek jelentőségére irányuló kérdések kiértékelése

A fegyveres biztonsági őrök képzésének fontos eleme a gyakorlati képzés is, amely intézkedéstaktikai elemeket is tartalmaznak. Ennek a leghatékonyabb elsajátítási lehetősége, ha egy objektum elleni támadást és a megfelelő védelmi válaszingtezkedéseket szcenáriók mentén begyakorolják. A nukleáris létesítményeknek és radioaktív hulladéktárolóknak évente igazolni kell a komplex fizikai védelmi rendszer hatékonyságát. Az OAH és az illetékes megyei rendőrfőkapitányság részvételével évente komplex fizikai védelmi gyakorlatokat tartanak. A gyakorlatok elsődleges kiértékelése a helyszíni megfigyelők segítségével kerül végrehajtásra. [89] A 2008-as atomerőművi minősített oktatói képzésem során talákoztam egy meglehetősen hatékony módszerrel,

amelynek az volt az alapja, hogy az oktatói előadásokat videófelvételen rögzítették és azt később kielemezték. A legfontosabb eleme az volt, hogy magának az előadónak kellett az andragógiai elméleti tudása alapján értékelnie a saját előadását. Ezt a módszert alkalmasnak tartom a fegyveres biztonsági őrök gyakorlati képzésének fejlesztésére is. A feltételezésem igazolása vagy elvetése érdekében két kérdést fogalmaztam meg a kérdőívben:

- A gyakorlati képzések alkalmával egy feltételezett szcenárió elhárításának gyakoroltatása közben videofelvétel készül egy drón segítségével madártávlatból. Mennyire ért egyet azzal, hogy egy ilyen video segítheti az őr felkészülését?
- Véleménye szerint egy force on force vagy komplex gyakorlat végrehajtásakor, egy madártávlati videofelvétel segíthetné-e a gyakorlat kiértékelését?

A fegyveres biztonsági őrök véleményét a 10-es és a 11-es táblázat tartalmazza.

	Nem	Inkább nem	Inkább igen	Igen
Létesítmény 1	9 %	7 %	34 %	50 %
Létesítmény 2	13 %	11 %	21 %	55 %
Létesítmény 3	3 %	10 %	50 %	37 %
Összesen	9 %	8 %	34 %	49 %

10. táblázat - A gyakorlati képzések alkalmával egy feltételezett szcenárió elhárításának gyakoroltatása közben videofelvétel készül egy drón segítségével madártávlatból. Mennyire ért egyet azzal, hogy egy ilyen video segítheti az őr felkészülését?

	Nem	Inkább nem	Inkább igen	Igen
Létesítmény 1	5 %	2 %	31 %	61 %
Létesítmény 2	8 %	13 %	16 %	63 %
Létesítmény 3	3 %	7 %	40 %	50 %
Összesen	5 %	5 %	30 %	60 %

11. táblázat - Véleménye szerint egy force on force vagy komplex gyakorlat végrehajtásakor, egy madártávlati videofelvétel segíthetné-e a gyakorlat kiértékelését?

A létesítmények őrsegparancsnokaival folytatott gyakorlati képzésekkel kapcsolatos szakmai egyeztetések során a képzési hatékonyság kérdéseiről is beszélgettünk. Egyikük az alábbi tapasztalatokat osztotta meg velem:

Alap taktikai eljárásokkal végrehajtott gyakorlásakor (elszakadás, átkarolás, biztosított kiszállás stb.) az értékelést rendkívüli módon segíti elő egy madártávlati felvétel. A

tapasztalatok alapján két féle végrehajtó létezik. Az egyik csoport tagjait nem lehet meggyőzni felvétel nélkül arról, hogy hibázott, a másik csoport tagjait pedig arról, hogy jól hajtotta végre a feladatát. Egy áttekintő felvétel segít abban, hogy helyes következtetéseket vonjunk le a manőverek komplex vizsgálatakor – mind a támadók, mind a védők oldalán – akár az eltérések, akár a jó gyakorlatok azonosításakor. Profi kiképzők is csak az események 60-70 %-át tudják jól értékelni a helyszínen látottak alapján. Például a fegyverek csövének állásából a taktikai manőverek iránya, a végrehajtó szándéka pontosan megállapítható egy felsőnézetű videófelvételről. Nem utolsó sorban olyan üzemekben, objektumokban, ahol a védelmi tevékenység során az irányítók magaslati pontokon elhelyezett vagy drónról készített kameraképekből irányítják a válaszüzemi résztvevőket, alkalmas a megoldás az operatív vezetők képzésére, fejlesztésére is.

A válaszokból és a szakmai egyeztetésen átadott információkból megállapítottam, hogy a gyakorlati képzési események alakalmával nagyon hasznos lenne egy drónos madártávlati felvétel és jelentős mértékben növelné a képzési hatékonyságot.



## ÖSSZEGZETT KÖVETKEZTETÉSEK

A kutatási munkám általános célkitűzése alapján áttekinttem a komplex objektumvédelemben alkalmazott védelmi alrendszereket. Vizsgáltam a technikai és az élőerős rendszerek egymásra gyakorolt hatását. Részletesen bemutattam három különböző fenyegetettségű objektum kockázatokkal arányos komplex védelmi rendszerét. Az első kutatási szakasz eredményeként, arra a következtetésre jutottam, hogy az eredeti kutatási tervemhez képest eltérő mélységű és irányú kutatómunkát kell folytatnom. Ennek eredményeként további fontos vizsgálandó területet határoztam meg, ami a komplex védelmi rendszerben rejtőző humán és újonnan megjelenő kockázatok vizsgálatát jelenti.

A harmadik fejezetben bemutattam azon humán eredetű kockázati tényezőket, amelyek a védelmi rendszerben napjainkban még mindig jelen vannak és jelentős degradáló hatásúak. A humán kockázatokot rendszereztem forrásoldali szempontok, statikus vagy dinamikus jellege alapján és a tervezési/üzemeltetési fázisa szerint. A beazonosított humánkockázati tényezők mentén elemeztem gyakorlati esettanulmányokat és igazoltam a humánkockázatok jelenlétét és azok negatív hatását a komplex objektumvédelmi rendszerben. Az első esettanulmány részletes elemzése során bebizonyítottam, hogy a megnövekedett mértékű külső fenyegetés az élőerős védelem rendszerszintű hiányossága okán nem került azonosításra, amit egy felülvizsgálat során be kellett volna azonosítani és megelőző intézkedések bevezetésével csökkenteni a bekövetkezési valószínűséget. A második esettanulmány feldolgozása során bebizonyítottam, hogy a motiváció csökkenése, az etikai dilemmák, a kommunikációs problémák és a csökkent éberség, mint humánkockázati tényezők a személyzet munkájára kihatottak és egymást erősítve fejtettek ki negatív biztonsági hatást.

A humánkockázatok vizsgálati struktúráját alkalmazva végeztem el a technikai fejlődésből származó új kockázati tényezők beazonosítását. Igazoltam az önmagukban külön-külön is kockázatot jelentő technológiák egyidejűségét logikai összefüggések levezetésével. Végül a negyedik fejezetben bemutattam hipotetikus scenáriók mentén, hogy az új technológiák megjelenése valódi kockázatot jelent a nukleáris létesítményekre, különös tekintettel a dróntechnológia.

Az elektronikus vagyonvédelmi rendszer aktivitás fokozási lehetőségének az alapja, hogy a védendő objektum rendelkezzen autonóm beavatkozásra is képes aktív elektronikus

vagyonvédelmi rendszerrel. Az ötödik fejezetben első lépésben meghatároztam az autonóm elektronikus vagyonvédelmi rendszer fogalmát. Ezt követően részletesen elemeztem a napjainkban alkalmazott elektronikus vagyonvédelem eszközeit és rendszereit fókuszálva az aktivitás fokozási lehetőségeire. Az eszközök tekintetében azt vizsgáltam, hogy alkalmas lehet-e a védelmi rendszerben a detektálási funkciókon felül egy beavatkozó rendszerben feltartóztató vagy esetleg elhárító funkció megvalósítására. A vizsgálatot szenzor és aktuátor oldalról is elvégeztem és meghatároztam azon hardver és szoftver komponenseket, amelyek kielégítik az autonóm működés kritériumait. A fejezet második részében az autonóm működésű aktív rendszerek kialakításának koncepcióit állítottam össze a kockázatok jelentős mértékű csökkentésére és az előerő hatékonyságának növelésére alkalmas műszaki megoldásokon keresztül. Nagy hangsúlyt fektettem a drónok rendszerszintű integrálhatóságának kérdésére. Meghatároztam két féle védelmi drón specifikációját. Az eszközszinten specifikált képességekkel rendelkező mini kategóriájú forgószárnyas drón és további drónra applikálható eszközök felhasználásával meghatároztam egy, olyan aktív védelmi drónrendszert, amely képes az előerő számos tevékenységét hatékonyabbá tenni és bizonyos esetekben kiváltani, csökkentve komplex védelmi rendszer kockázatait. A rendszer kialakítását a kockázatokkal arányos válaszintézkedések tükrében a megvalósítandó funkciókra alapozva határoztam meg. Végül összeállítottam a beavatkozó drón konfigurációját és az elhárítási funkciót megvalósító rendszert. Továbbá vizsgáltam a drónt mint a fegyveres biztonsági őrök gyakorlati képzésre alkalmas eszközt.

Primer kutatási fázisban kérdőíves adatfelvételi módszerrel feltártam a fegyveres biztonsági őrök véleményét az aktív védelmi drón alkalmazhatóságával és elfogadottságával kapcsolatosan. A felmérés kiértékelése bebizonyította az aktív védelem részét képező drón alkalmazhatóságát, mit védelmi, mint oktatási célokra egyaránt.

### **Új tudományos eredmények**

Meghatároztam az autonóm beavatkozásra is képes aktív elektronikus vagyonvédelmi rendszer fogalmát.

A kutatásom során az elektronikus vagyonvédelmi rendszer aktivitás fokozásának lehetőségeire, meghatároztam a rendszer felépítéséhez szükséges komponenseket, majd azokat felhasználva elkészítettem a rendszerspecifikációt és megalkottam számos aktív

védelmi rendszer koncepcióját. Ennek részeként öt tézist fogalmaztam meg, amelyek a célkitűzéseimre és a kutatási kérdésekre adnak választ.

A kutatói munkám során az igazolt téziseket új tudományos eredményt jelentenek:

### **Tézis 1**

A humán kockázatok elméleti rendszerezését követően esettanulmányok elemzésén keresztül bebizonyítottam, hogy napjainkban még mindig olyan humán kockázati tényezők terhelik a komplex védelmi rendszert, amelyek befolyásolják az élőrő hatékonyságát számottevő kockázatot jelentve az objektumvédelmi rendszer egészére.

### **Tézis 2**

A digitalizációs technológia fejlődésnek következtében megjelenő új kockázatok hipotetikus scenáriókon keresztüli elemzésével igazoltam, hogy a kockázatok jelentősen csökkentik a nukleáris létesítmények védelmi képességeit és bebizonyítottam a műszaki védelmi intézkedések hiányát.

### **Tézis 3**

Az autonóm beavatkozásra is képes aktív vagyonvédelem eszközeinek specifikálásával és a rendszerszintű koncepciók elkészítésével, bebizonyítottam, hogy kialakítható egy olyan védelmi rendszer, amely képes csökkenteni az új kockázatokat és növelni a komplex védelem hatékonyságát

### **Tézis 4**

A kutatásom eredményeivel igazoltam, hogy fizikai védelmi rendszerbe integrálható aktív védelmi drón a fegyveres biztonsági őrök részéről pozitív megítélésű és alkalmasnak tartják a fizikai védelmi rendszerbe integrálására.

### **Tézis 5**

Empirikus kutatási módszerrel bebizonyítottam, hogy a fegyveres biztonsági őrök gyakorlati képzése drónról készített videófelvétel készítésével és annak elemzésével hatékonyabbá tehető.

## **Ajánlások**

A disszertációm jó alapját képezi a kritikus infrastruktúrák objektumvédelmi aspektusának felülvizsgálatához és ajánlom a nukleáris létesítmények fizikai védelmi

rendszerrel szembeni fenyegetettség mértékét meghatározó országos DBT bizottság figyelmébe.

Ajánlom azoknak a szakembereknek a figyelmébe a kutatási munkám eredményeit, akik olyan objektumok védelmi tervezésével foglalkoznak, ahol a légi fenyegetettséggel is kell számolni.

A drónokkal kapcsolatos tudományos eredményeim jelenleg nem alkalmazhatóak, azon objektumoknál, ahol az objektum fölött tiltott légtér helyezkedik el. Ezért javaslom a jogalkotóknak, hogy vizsgálják meg a lehetőségét a tiltott légtér feloldásának az objektumot üzemeltetők részére. További jogi kérdések tekintetében is fontos lenne a jogszabályok módosítása.

Ajánlom a munkám a biztonságtechnikai tervezők és a vagyonvédelmi eszközt gyártók részére is.

# IRODALOMJEGYZÉK

- [1] L. Berek, T. Berek és L. Berek: Személy- és vagyonbiztonság, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, OE-BGK 3071, Budapest, 2016.
- [2] Jurás Zsolt Építőipari nagyberuházások során alkalmazandó élőerős védelmet támogató technikai rendszerek továbbfejlesztése aktív funkciókkal, In: Kollár, Csaba /szerk./ Berek Hetven: Egy élet a hadtudomány és a művészet szolgálatában, a hetvenéves Berek Lajos professzor és szobrászművész köszöntése, Budapest: Óbudai Egyetem, Biztonságtudományi Doktori iskola, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar (2019) pp. 79-88.
- [3] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, Budapest, ZMNE Katonai Műszaki Doktori Iskola doktori (PhD) értekezés, 2009.
- [4] Nivó Kerítés Kft. Acél kerítések online: (letöltve: 2022.05.19.)  
<https://nivokerites.hu/accel-kerites#&gid=1&pid=5>
- [5] EZI Security System comp. EntraQuickfolding gate online: (letöltve: 2021.05.19.)  
<https://www.ezisecurity.com.au/wp-content/uploads/2020/08/EntraQuick-I-30-1-scaled-1-380x250.jpg>
- [6] Product, Industrial Land Trading Ltd. online: (letöltve: 2021.05.19.) <https://ilt-sa.com/wp-content/uploads/2019/11/Avon-RB780CR-Road-Blocker-38.jpg>
- [7] Tóth Attila, Tóth Levente: Biztonságtechnika; NKE, Budapest, 2014
- [8] Országos Atomenergia Hivatal, Fizikai Védelmi Útmutató FV-4, Budapest 2022 online: (letöltve: 2023.05.19.)  
[https://www.haea.gov.hu/web/v3/OAHPortal.nsf/FD0CBD7B6AFE26EEC1257BE9003E-DF32/\\$FILE/FV-4\\_v4\\_v%C3%A9gleges.pdf](https://www.haea.gov.hu/web/v3/OAHPortal.nsf/FD0CBD7B6AFE26EEC1257BE9003E-DF32/$FILE/FV-4_v4_v%C3%A9gleges.pdf)
- [9] Bencsik Balázs, Kovács Zsolt, Dénes Levente: Az ablakok légzárási teljesítményének változása a környezeti hőmérséklet függvényében, Faipar, NyME, LX. évfolyam 2012. I. szám. online: (letöltve: 2021.05.19.)  
[http://epa.oszk.hu/02300/02321/00032/pdf/EPA02321\\_Faipar\\_2012\\_01\\_10-16.pdf](http://epa.oszk.hu/02300/02321/00032/pdf/EPA02321_Faipar_2012_01_10-16.pdf)
- [10] Barabás A. T., Rózsa S. Windt Sz., Eisinger A., Gaulang E., Magi A., Tolvaj-kulcs A BETÖRÉSES LOPÁSOK VIZSGÁLATA AZ ELKÖVETŐK SZEMSZÖGÉBŐL In: Barabás A. T. ISBN 798-963-89468-7-4, Országos Kriminológiai Intézet, Budapest, 2014.
- [11] Zárszervíz, Letis Magyarország Kft, online: (letöltve: 2021.05.19.)  
[http://static.letis.hu/Uploaded/Products/Picture/3/6/6/366\\_300x300\\_fill.png](http://static.letis.hu/Uploaded/Products/Picture/3/6/6/366_300x300_fill.png)
- [12] Zárbetétek, Zárrendszerek Zárkirály Kft. online: (letöltve: 2021.05.19.)  
[http://www.zarkiraly.hu/cms/upload/image/article/10\\_pic8\\_m.jpg](http://www.zarkiraly.hu/cms/upload/image/article/10_pic8_m.jpg)
- [13] Kiss István Csaba, Behatolásjelző rendszerek biztonsági szintjét befolyásoló tényezők In: Hadmérnök NKE, Bp., IX. évfolyam 2. szám 2014., ISSN1788-1919., pp. 25-36.
- [14] Safety & Security Review Africa: AGIL Fence completes integration with Milestone XProtect 2020 R2 online: (megtekintve: 2021.05.19.)  
<https://safetyandsecurityafrica.com/wp-content/uploads/2020/12/Milestone-Integration.jpg>
- [15] Bunyitai Ákos, A beléptető rendszerek helye és szerepe a vagyonvédelemben In: Hadmérnök NKE, Bp., VI. évfolyam 4. szám 2011., ISSN1788-1919., pp. 17-25.
- [16] CCTV története, Oktel Szolgáltató Kft. <https://oktel.hu/szolgalattas/kamerarendszer/a-kepalkotas-alapjai/a-cctv-tortenete/> online: (megtekintve: 2021.05.19.)

- [17] HORVÁTH J.: A zárláncú videó megfigyelő rendszerek jövője. In: Hadmérnök NKE, Bp., VIII. évfolyam 1. szám 2013., ISSN1788-1919., pp. 15-22. online: (megtekintve: 2021.05.19.) [http://hadmernok.hu/2013\\_1\\_horvathj.pdf](http://hadmernok.hu/2013_1_horvathj.pdf)
- [18] Kameratípusok, Oktel Szolgáltató Kft. <https://oktel.hu/szolgalattas/kamerarendszer/kamerak/kameratipusok/> online: (megtekintve: 2021.05.19.)
- [19] Tóth A.: Az élőerő munkáját segítő technikai megoldások. In: Hadmérnök NKE, Bp., XIII. évfolyam 2. szám 2018., ISSN1788-1919., pp. 29-36. (letöltve: 2022.02.05) [http://www.hadmernok.hu/182\\_03\\_toth.pdf](http://www.hadmernok.hu/182_03_toth.pdf)
- [20] Source Security, PTZ compact camera (letöltve: 2022.02.05) <https://www.sourcesecurity.com/img/products/400/axis-214-ptz.jpg>
- [21] IFSEC GLOBAL Security technical portal, Simon Lambert: 3 Key Elements of any CCTV system <https://www.ifsecglobal.com/installers/3-key-elements-cctv-system/> online: (megtekintve: 2021.05.19.)
- [22] Szabó A., Papp J., Kovács T., Szűcs E., Berek T.: A személy- és vagyonőrök és a fegyveres biztonsági őrök tevékenységének összehasonlítása a MÁV Zrt.-n keresztül, Műszaki Katonai Közlöny, XXVIII. évfolyam, 4. szám 2018 online: (megtekintve: 2021.05.19.) <https://folyoirat.ludovika.hu/index.php/mkk/article/view/1534/851>
- [23] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól online: (megtekintve: 2021.05.19.)
- [24] 1997. évi CLIX. törvény a fegyveres biztonsági őrsegről, a természetvédelmi és a mezei őrszolgálatról online: (megtekintve: 2021.05.19.)
- [25] Secblog today Quo vadis magánbiztonság 2 rész – Dr Fialka György írása <https://secblog.today/2017/09/17/quo-vadis-maganbiztonsag-2-resz-dr-fialka-gyorgy-irasa/> (letöltve: 2021.10.21.)
- [26] Horváth Tamás., Elektronikus megfigyelő-, és ellenőrző rendszerek objektumorientált kialakítása különös tekintettel a biztonsági kockázatok rendszerére, Budapest, Óbudai Egyetem Biztonságtudományi Doktori Iskola doktori (PhD) értekezés, 2018. (letöltve: 2021.10.21.)
- [27] Jurás Zsolt: Atomerőmű, mint kritikus infrastruktúra egy elemének veszélyeztetése, őrzésének és védelmének fő feladatai, Bánki Közlemények, 1. évf. 3. szám, pp. 32-37., 2018
- [28] Szabó Anikó., A szabályzatok szerepe az objektumok őrzésvédelmében, Műszaki Katonai Közlöny, XXVII. Évfolyam, 1. szám, 2017
- [29] Berek Lajos: Biztonságtechnika, NKE Budapest, 2014, , <http://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf> , Letöltve: 2017.04.05
- [30] 1996. évi CXVI. törvény az atomenergiáról online: (megtekintve: 2021.05.19.) <https://net.jogtar.hu/jogszabaly?docid=99600116.tv>
- [31] MABISZ ajánlás, Betöréses lopás- és rablásbiztosítás technikai feltételei telephelyek és létesítmények, helyiségek őrzésének, vagyontárgyak tárolásának, szállításának szabályai online: (megtekintve: 2023.05.19.) <http://www.pluto.hu/A/A2.html>
- [32] MABISZ ajánlás, Értéktárolók biztosítók számára ajánlott értékhatárai online: (megtekintve: 2023.05.19.) [https://mabisz.hu/wpcontent/uploads/2018/08/%C3%89rt%C3%A9kt%C3%A1rol%C3%B3k-kock%C3%A1ztatv%C3%A1llal%C3%A1si-%C3%A9rt%C3%A9khat%C3%A1rai-2023\\_.pdf](https://mabisz.hu/wpcontent/uploads/2018/08/%C3%89rt%C3%A9kt%C3%A1rol%C3%B3k-kock%C3%A1ztatv%C3%A1llal%C3%A1si-%C3%A9rt%C3%A9khat%C3%A1rai-2023_.pdf)

- [33] David Cameron nyilatkozata <http://vs.hu/kozelet/osszes/piszkos-bomba-veszelyere-figyelmeztetdavid-cameron-0401> (letöltve: 2018.04.12.)
- [34] Rácz László István: Kritikus infrastruktúra védelem hazai és nemzetközi szabályozási rendszere, 2012. Hadmérnök, online: (letöltve: 2018.04.12.) [http://hadmernok.hu/2012\\_2\\_racz.pdf](http://hadmernok.hu/2012_2_racz.pdf)
- [35] 2080/2008. (VI. 30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról online: (megtekintve: 2022.07.19.)
- [36] Vass Attila – Dr. Maros Dóra – Prof. Dr. Berek Lajos: Az interdependencia kérdése az energetikai rendszer és a híradástechnika esetén a kritikus infrastruktúra biztonsága védelmében, 2015. Bolyai szemle, online: (megtekintve: 2022.07.19.) [http://unike.hu/uploads/media\\_items/bolyai-szemle-2015-03.original.pdf](http://unike.hu/uploads/media_items/bolyai-szemle-2015-03.original.pdf)
- [37] Infostrat Hírportál [Elítéltek egy amerikai apácát, mert behatolt egy nukleáris létesítménybe - Infostart.hu](http://infostrat.hu/Elitelt-egy-amerikai-apacat-mert-behatolt-egy-nuklearis-letesitmenybe) online (letöltve: 2017.03.07.)
- [38] Global Terrorism Database <https://www.start.umd.edu/gtd/contact/download?t=e0c0788297f511edaf000e5194896103> online (letöltve: 2022.03.07.)
- [39] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), p 14. IAEA, Vienna,
- [40] BEREK Lajos-VASS Attila: Gázturbinás erőműi objektum védelme, In: Hadmérnök, NKE, Bp., IX. évfolyam 2. szám 2014., ISSN1788-1919., pp. 5-15. [http://www.hadmernok.hu/142\\_01\\_berekl.pdf](http://www.hadmernok.hu/142_01_berekl.pdf) (letöltve: 2017.01.07.)
- [41] Máté Solymosi, Zsolt Jurás., Review the basics of nuclear security in case of nuclear power plants, through a hypothetical scenario.: 2022 IEEE 5th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE). IEEE, 2022.
- [42] Csege Gy.- Gáll, T.: Az élőerős vagyonvédelem problematikája. Hadmérnök IX:(4) 2014 pp. 5-10. ISBN 1788-1919
- [43] Szabó Anikó Őrzésbiztonsági feladatokat ellátó vagyonőrök képzési rendszerének vizsgálata, a kor változó követelményeinek megfelelő fejlesztési terv kidolgozása Budapest, Óbudai Egyetem Biztonságtudományi Doktori Iskola doktori (PhD) értekezés, 2023
- [44] Tóth Levente.: Videó megfigyelő rendszerek hatékonyságnövelő lehetőségei a közterületi megfigyelés területén Budapest, Óbudai Egyetem Biztonságtudományi Doktori Iskola doktori (PhD) értekezés, 2023
- [45] Major Zs, Kovács T.: A vagyonőrök alkalmassági vizsgálatának koncepciója; Belügyi Szemle, 70. évf. 5. szám, 2022, pp.943-959 online: (megtekintve: 2022.07.19.) <http://realj.mtak.hu/20728/37/BSZ%20-%202022-05.pdf>
- [46] 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről online: (megtekintve: 2022.07.19.)
- [47] Matthew Bunn: Belgium Highlights the Nuclear Terrorism Threat and Security Measures to Stop it 2016 (letöltve: 2022.10.03.) <https://www.belfercenter.org/publication/belgium-highlights-nuclear-terrorism-threat-and-security-measures-stop-it>
- [48] The Indian Express: 18-carat pink diamond reaps \$28.8 million at Geneva auction <https://indianexpress.com/article/lifestyle/life-style/18-carat-fortune-pink-diamond-reaps-28-8-million-at-geneva-auction-christies-8258889/> (letöltve: 2023.01.15.)

- [49] Ambrus Andrea.: A tömeges migráció és az iszlamista terrorizmus közti kapcsolat az Európai Unióban, Stratégiai Védelmi Kutató Központ (Elemzések) 2018/11 Nemzeti Közszolgálati egyetem 2018. online (letöltve: 2022.06.07.)
- [50] Early, B. et al.: Atoms for Terror? Nuclear Programs and Non-Catastrophic Nuclear and Radiological Terrorism, *British Journal of Political Science*, 43(4), 915-936. online: (megtekintve: 2022.07.19.) [doi:10.1017/S000712341200066X](https://doi.org/10.1017/S000712341200066X)
- [51] C Hobbs, M. Moran.: Insider Threats: An Educational Handbook of Nuclear and Non-Nuclear Case Studies." King's College London. 2015. online (letöltve: 2022.04.19.)
- [52] PETERSEN, T-STEINER, F.: The Bigger Picture, How globalization, digitalization and demographic change challenge the world. [https://rsm-bst-live.bertelsmann-stiftung.de/fileadmin/files/user\\_upload/MegatrendBrief MT The Bigger Picture How globalization digitalization and demographic Change challenge the world 2019.pdf](https://rsm-bst-live.bertelsmann-stiftung.de/fileadmin/files/user_upload/MegatrendBrief_MT_The_Bigger_Picture_How_globalization_digitalization_and_demographic_Change_challenge_the_world_2019.pdf) (letöltve: 2023.01.12.)
- [53] G. Major: Ésszerű szabályozás vagy tiltás, avagy mit lehet kezdeni a drónokkal? *Repüléstudományi Közlemények*, Vol. 27, no. 1. pp. 168–169. 2015. online: (megtekintve: 2022.07.19.) <https://doi.org/10.32560/rk.2015.1.11>
- [54] Runyan-Beebe, Christopher Alan.: The Rise in the Utilization of IoT Devices in Nuclear Facilities. No. SAND-2020-6994R. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2020. online: (megtekintve: 2021.03.19.) <https://www.osti.gov/biblio/1638782>
- [55] O. Becker: Nukleáris létesítmények terrorfenyegetettsége. *Energiaklub*, 2018. Online: <https://energiaklub.hu/tanulmany/nuklearis-letesitmenyek-terrorfenyegetettsege-4602> (letölve: 2022.11.24.)
- [56] Central Digitális Média Kft; gardenista.hu: A Greenpeace drónt repített be egy francia atomerőműbe. online: (megtekintve: 2020.07.19.) <https://gardenista.hu/2018/07/04/a-greenpeace-dront-repitett-be-egy-francia-atomeromube/>
- [57] C. Wheeler, Terror Threat Alert: UK's nuclear plants are at serious risk of terrorist drone strikes. *Express*, 2015. online: (megtekintve: 2022.07.19.) [www.express.co.uk/news/uk/559718/Nuclear-plants-are-at-risk-from-a-terrorist-strike-by-unmanned-drones](http://www.express.co.uk/news/uk/559718/Nuclear-plants-are-at-risk-from-a-terrorist-strike-by-unmanned-drones)
- [58] BBS News, Middle East: Al-Qaeda Plotted nuclear attacks [http://news.bbc.co.uk/2/hi/middle\\_east/2244146.stm](http://news.bbc.co.uk/2/hi/middle_east/2244146.stm) online (letöltve: 2022.11.24.)
- [59] Hanka László, Vincze Árpád, Solymosi József.: A nukleáris terrorizmus, mint potenciális fenyegetettség napjainkban. 2007 *Hadmérnök*, II. évfolyam 4: 4-24.
- [60] Kovács L et al.: A paksi Atomerőmű telephelye felett elhelyezkedő tiltott légtér méretének felülvizsgálata, *Nemzeti Közszolgálati Egyetem* 2014 online: (megtekintve: 2021.07.19.) [http://www.oah.hu/web/v3/OAHPortal.nsf/371C5096A5F4CB45C1257E580024FCCB/\\$FILE/302\\_TSO\\_NKE\\_KovacsL\\_public.pdf](http://www.oah.hu/web/v3/OAHPortal.nsf/371C5096A5F4CB45C1257E580024FCCB/$FILE/302_TSO_NKE_KovacsL_public.pdf)
- [61] 26/2007. (III. 1.) GKM-HM-KvVM együttes rendelet a magyar légtér légiközlekedés céljára történő kijelöléséről online: (megtekintve: 2022.07.19.)
- [62] 4/1998. (I. 16.) Korm. rendelet a magyar légtér igénybevételéről online: (megtekintve: 2022.08.12.)
- [63] Rónaky, J., et al.: A nukleáris létesítmények katonai terror-fenyegetettségének értékelése II.: A Paksi Atomerőmű katonai terror-fenyegetettségének értékelési eljárása. *Hadmérnök*, II 2 2007., 32–49. o.



- [64] IoT Agenda, M. Rouse,.: What is IoT (Internet of Things) and How Does it Work? online: (megtekintve: 2022.08.12.)  
<https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>
- [65] Solymosi Máté, Zsolt Jurás.: Review the basics of nuclear security in case of nuclear power plants, through a hypothetical scenario. 2022 IEEE 5th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE). IEEE, 2022. DOI:10.1109/CANDO-EPE57516.2022.10046358
- [66] Cserhádi András: A Stuxnet vírus és az iráni atomprogram Fizikai Szemle, 61. évf. 5. szám, 2011, pp.150-155 online: (megtekintve: 2021.08.12.)  
<http://fizikaiszemle.hu/archivum/fsz1105/FizSzem-201105.pdf>
- [67] Világhíres Feltalálók, Teller-Effektus  
<http://www.feltalalok.hu/tudosok/tellerede/html/teledetal2.htm>
- [68] Jelentés az Országos Atomenergiái Bizottság számára a Paksi Atomerőműben 2003. április 10-én bekövetkezett esemény hatósági kivizsgálásáról, Országos Atomenergiái Hivatal 2003. online: (megtekintve: 2021.08.12.)  
<https://www.parlament.hu/irom39/10836/10836-0001.pdf>
- [69] A. KOURANI - N. DAHER: Marine locomotion: A tethered UAV-Buoy system with surge velocity control, in Robotics and Autonomous Systems 145. évf. (2021) online: (megtekintve: 2022.08.12.) <https://doi.org/10.1016/j.robot.2021.103858>
- [70] Jurás, Zsolt, Drones in Smart Cities: Repüléstudományi Közlemények 2021 33. évfolyam 2. szám pp: 7-17.
- [71] Jurás Zsolt: The Role of Drones in Enhancing Production Efficiency of Nuclear Facilities: Repüléstudományi Közlemények 2021 33. évfolyam 2. szám pp. 143-152.
- [72] City Group Kft., Robot Őr online: (megtekintve: 2022.09.12.)  
[https://www.citygroup.hu/?gclid=CjwKCAjwkNOpBhBEEiwAb3MvvUfGXh4K87rUiXpu2w\\_LiLdJLYvQcZfjYDCyu9erg0wPbyOhmRuwhoCHIUAQAvD\\_BwE](https://www.citygroup.hu/?gclid=CjwKCAjwkNOpBhBEEiwAb3MvvUfGXh4K87rUiXpu2w_LiLdJLYvQcZfjYDCyu9erg0wPbyOhmRuwhoCHIUAQAvD_BwE)
- [73] Fenyvesi Beáta; Rendszerben a sokkoló, Zsaru Magazin 2022.02.03 (letöltve: 2023.04.13.) <https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/rendszerben-a-sokkolo>
- [74] Duncan Graham-Rowe; Non-lethal landmine zaps intruders with 50,000 volts, NewScientist 2003 online (letöltve:2022.10.21.)  
[https://www.newscientist.com/article/dn3650-non-lethal-landmine-zaps-intruders-with-50000-volts/?\\_ptid=%7Bkpx%7DAAAAsHTW-BTzdQoKcmJhNGYxWmNwZRIQbG81a3FnOWgzbiNqMXE0dxoMRVg0T11JVEzZRUU2liUxODIzNHBnMDdnLTAwMDAzMnI2N2xlaXIzMG5tM2VmYXEyaDVnKhtzaG93VGVtcGxhdGU2MjRIQkxSUVSUkExMTkwAToMT1RDTzJDnlc2NEhGUhJ2LXYA8BZwa2N4YnE5czVaCzg0LjEuOTUuMTMwYgNkd2Nos-zoqQZwFHgE](https://www.newscientist.com/article/dn3650-non-lethal-landmine-zaps-intruders-with-50000-volts/?_ptid=%7Bkpx%7DAAAAsHTW-BTzdQoKcmJhNGYxWmNwZRIQbG81a3FnOWgzbiNqMXE0dxoMRVg0T11JVEzZRUU2liUxODIzNHBnMDdnLTAwMDAzMnI2N2xlaXIzMG5tM2VmYXEyaDVnKhtzaG93VGVtcGxhdGU2MjRIQkxSUVSUkExMTkwAToMT1RDTzJDnlc2NEhGUhJ2LXYA8BZwa2N4YnE5czVaCzg0LjEuOTUuMTMwYgNkd2Nos-zoqQZwFHgE)
- [75] Dorota Ziemkowska, Nemcsak fényképezni, járművet követni is tudnak a spanyol rendőr-drónok, trans.info 2021.07.14 (letöltve: 2022.09.23.) <https://trans.info/hu/nemcsak-fenykepezni-jarmuvel-kovetni-is-tudnak-a-spanyol-rendor-dronok-245852>
- [76] Zsolt Jurás: The Role of Drones in the Electricity Sector, Repüléstudományi Közlemények 33. évfolyam 2. szám pp: 57-63.
- [77] Bebesi Zoltán, Zsolt Jurás. RELEVANT TASKS FOR UAV PROTECTION SYSTEMS IN RELATION TO THE AERIAL SCENARIO OF NUCLEAR FACILITIES: Science & Military Journal 18.1 (2023).
- [78] Besada, Juan A., et al.: Review and simulation of counter-UAS sensors for unmanned traffic management. Sensors Volume 22. Issue1 (2021): 189. online: (megtekintve: 2022.09.12.) <https://doi.org/10.3390/s22010189>

- [79] RFC793: Transmission Control Protocol online: (megtekintve: 2022.09.12.)  
<https://datatracker.ietf.org/doc/html/rfc793>
- [80] Tom Thomas: Hálózati biztonság. Panem Könyvkiadó, 2005.
- [81] Balogh Zsuzsanna, Katonai táborok korszerű kialakítása. Műszaki Katonai Közlöny XXII. évfolyam, 2012. 1. szám online (letöltve: 2021.11.13.)  
<https://folyoirat.ludovika.hu/index.php/mkk/article/view/2771>
- [82] HISEC DOOR Biztonságtechnikai Kft., 5 nagyszerű kiegészítő, ami bármilyen bejárati ajtót okossá varázsol. online (megtekintve: 2022.10.13.) <https://hisecddoors.hu/hisec-okos-bejarati-ajto>
- [83] Országos Atomenergia Hivatal, Fizikai Védelmi Útmutató FV-13, Budapest 2022 online: (megtekintve: 2022.09.12.)  
[https://www.haea.gov.hu/web/v3/oahportal.nsf/E522D4B4B4CAC989C1257BE9003EDF3F/\\$FILE/FV-13\\_v4\\_v%C3%A9gleges.pdf](https://www.haea.gov.hu/web/v3/oahportal.nsf/E522D4B4B4CAC989C1257BE9003EDF3F/$FILE/FV-13_v4_v%C3%A9gleges.pdf)
- [84] Schütz Gergely, Mobiltelefon detektor Z&Z Biztonságtechnika Kft. online (megtekintve: 2022.10.13.) <https://znz.hu/mobiltelefon-detektor/>
- [85] IAEA NSS No. 40-T Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities Vienna 2021 ISBN 978-92-0-105419-7 (megtekintve: 2022.09.12.) [https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1875\\_web.pdf](https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1875_web.pdf)
- [86] Országos Atomenergia Hivatal, Fizikai Védelmi Útmutató FV-4, Budapest 2022 online: (megtekintve: 2022.09.12.)  
[https://www.haea.gov.hu/web/v3/OAHPortal.nsf/FD0CBD7B6AFE26EEC1257BE9003EDF32/\\$FILE/FV-4\\_v4\\_v%C3%A9gleges.pdf](https://www.haea.gov.hu/web/v3/OAHPortal.nsf/FD0CBD7B6AFE26EEC1257BE9003EDF32/$FILE/FV-4_v4_v%C3%A9gleges.pdf)
- [87] RailyNews, ASISGUARD Continues to Export SONGAR Armed Drones (megtekintve: 2023.04.15.) <https://railynews.com/2022/03/asisguard-songar-silahli-drone-ihracatina-devam-ediyor/>
- [88] Országos Atomenergia Hivatal, Fizikai Védelmi Útmutató FV-15, Budapest 2022 online: (megtekintve: 2022.09.12.)  
[https://www.haea.gov.hu/web/v3/oahportal.nsf/5E46C5E0D3D3D7A9C1257BE9003EDF39/\\$FILE/FV-15\\_v4\\_v%C3%A9gleges.pdf](https://www.haea.gov.hu/web/v3/oahportal.nsf/5E46C5E0D3D3D7A9C1257BE9003EDF39/$FILE/FV-15_v4_v%C3%A9gleges.pdf)
- [89] Országos Atomenergiái Hivatal, Lezajlott a Paksi Atomerőmű fizikai védelmi gyakorlata, Hírek 2021.11.29. online: (megtekintve: 2022.09.12.)  
<https://www.haea.gov.hu/web/v3/oahportal.nsf/web?OpenAgent&article=news&uid=639030FDAE877A31C125879C003899C8#>

## RÖVIDÍTÉSJEGYZÉK

IKT	Infokommunikációs Technológia
IoT	internet of Things
IP	Internet Protocoll
IT	információs technológia
MABISZ	Magyar Biztosítók Szövetsége
CCD	charge-coupled device
CMOS	Complementary metal-oxide semiconductor
PTZ	Pen/Tilt/Zoom (forgatás billentés és zoomolás)
CCTV	Zárt Láncú Televízió
UTP/FTP	árnyékolt sodrott érpár
FIR	Folyamatirányító Rendszer
OAH	Országos Atomenergia Hivatal
OBEIT	Országos Balesetelhárítási Intézkedési Terv
PLC	Programozható Logikai Vezérlő
TADD	Terület Védő Eszköz
TRAD	Távolsági Terület Védő Eszköz
VCA	Video Content Analysis
RTK	Real Time Kinematic
LiDAR	Lézer alapú távérzékelés
GPS	Globális Helyzetmeghatározó Rendszer
GNNS	Globális Navigáció Műhold Rendszer
LOS	loss of signal
FVT	Fizikai Védelmi Terv
UAV	Unmanned Aerial Vehicle

## TÁBLÁZATJEGYZÉK

1. táblázat - Mechanikai ellenálló képesség paraméterei összefoglalás .....	19
2. táblázat - a fegyveres biztonsági őr és a személyi-és vagyonőr jogosultságainak összehasonlítása [23][24].....	37
3. táblázat - A komplex védelem kialakításához szükséges védelmi formák különböző objektumok tekintetében [31] [32] .....	41
4. táblázat - drónok csoportosítása a NATO class I alapján .....	85
5. táblázat - detektálási módszerek összehasonlítása.....	102
6. táblázat - Fő és kiegészítő detektálási technológiák az észlelési feladat függvényében .....	102
7. táblázat - Kutatásban résztvevő és a megkérdezett biztonsági őrök százalékos eloszlása.....	105
8. táblázat - Véleménye szerint megfelelő minőségű és funkciójú (normál és hőkamera, esetleg mindkét) kamerával felszerelt drónt lehet-e alkalmazni a telepített CCTV kamerarendszer kiegészítésére?.....	107
9. táblázat - Véleménye szerint egy nem halálos fegyverrel vagy a behatolót lelassító eszközzel (könnygránát, hang-fény gránát, hálóvető puska) felszerelt drón alkalmazható-e az FBŐ kötelékében?.....	108
10. táblázat - A gyakorlati képzések alkalmával egy feltételezett scenárió elhárításának gyakoroltatása közben videofelvétel készül egy drón segítségével madártávlatból. Mennyire ért egyet azzal, hogy egy ilyen video segítheti az őr felkészülését? .....	111
11. táblázat - Véleménye szerint egy force on force vagy komplex gyakorlat végrehajtásakor, egy madártávlati videofelvétel segíthetné-e a gyakorlat kiértékelését? .....	111

## ÁBRAJEGYZÉK

1. ábra - Lakossági utcafronti kerítés [4] .....	17
2. ábra - személy-és gépjármű beléptetési pont [5] .....	17
3. ábra - Komplex ellenőrzési pont kapu és sorompó zsilip vegyes alkalmazásával.....	18
4. ábra - Aktív és passzív úttorlasz [6].....	18
5. ábra - Egybeépített biztonsági zár és biztonsági zárbetét [11] [12] .....	21
6. ábra - Felügyeleti állomáson a periméter védelmi rendszer megjelenítése [14].....	25
7. ábra - Scout videokamera szerkezeti ábra [19].....	28
8. ábra - PTZ kompakt kamera [20].....	29
9. ábra - A fizikai védelmi zónák kialakítása a védelmi szintek függvényében.....	53
10. ábra - Terület Védő Eszköz TADD [74].....	81
11. ábra - Távolsági Terület Védő Eszköz (TRED) [74].....	81
12. ábra - Mobiltelefon detektoros fémvizsgáló kapu [84].....	93
13. ábra - Ellenőrzött zóna periméter védelmi rendszer [85] .....	95
14. ábra - ASISGUARD gyártmányú SONGAR csapásmérő drón [87] .....	97
15. ábra - Véleménye szerint a „legkülső” zónahatáron keletkezett jelzés valódiságának megállapítására alkalmazható- e egy megfelelő kamerával ellátott drón? .....	108
16. ábra - Véleménye szerint egy nem halálos fegyverrel vagy a behatolót lelassító eszközzel (könnygránát, hang-fény gránát, hálóvető puska) felszerelt drón helyettesítheti-e teljes mértékben magát a fegyveres biztonsági őrt?.....	109
17. ábra - Véleménye szerint, ha alkalmazásra kerülne egy drón kellene- e attól tartania, hogy az őrt helyettesítve megszűnik a munkahelye?.....	110

## KÖSZÖNETNYILVÁNÍTÁS

Elsősorban köszönettel tartozok a családomnak, feleségemnek és gyermekeimnek a türelmükért és kitartásukért, hogy a tanulmányaim alatt bátorítottak és nem sajnálták a kutatási munkámra fordított időt.

Szeretnék köszönetet mondani témavezetőmnek **Dr. Prof. Berek Lajosnak**, a témavezetése alatt nyújtott szakmai segítségért és a rengeteg bátorításért, amivel a nehéz pillanatokban átlendített az akadályokon.

Hálás köszönettel tartozok az Óbudai Egyetem Biztonságtudományi Doktori Iskola tanárainak, különösképpen a komplex vizsgám bizottsági tagjainak, akik segítettek a tudományos munkám helyes irányának a megtalálásában.

Végül de nem utolsó sorban köszönetet mondok **Lévay Katalin** és **Hronyecz Erika** titkársági előadóknak, akik segítettek eligazodni az adminisztrációs tennivalók rengetegében.