Doktori (PhD) értekezés

Vásárhelyi Örs László

2026

NEMZETI KÖZSZOLGÁLATI EGYETEM

HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR

KATONAI MŰSZAKI DOKTORI ISKOLA

Vásárhelyi Örs László

A veszélyes üzemek biztonságos üzemeltetésének eljárási és műszaki feltételei, ezek fejlesztési lehetőségei a 21. század kihívásaival szemben, különös tekintettel a lakosságvédelem hatékonyságának növelésére ezen üzemek környezetében

Doktori PhD értekezés

Tudományos témavezetők:

.....	.....
Dr. habil. Dobor József	**Dr. Ambrusz József**
tű. alezredes PhD	**tű. ezredes PhD**

BUDAPEST, 2026.

Tartalomjegyzék

BEVEZETÉS 6
A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA 6
A téma jelentősége, időszerűsége 7
KUTATÁSI HIPOTÉZISEK 11
KUTATÁSI CÉLKITŰZÉSEK 11
KUTATÁSI MÓDSZEREK 12
RELEVÁNS SZAKIRODALOM ÁTTEKINTÉSE 14
AZ ÉRTEKEZÉS FELÉPÍTÉSE 23
1. IPARBIZTONSÁGOT SZOLGÁLÓ IRÁNYÍTÁSI RENDSZEREK HATÉKONYSÁGÁNAK FEJLESZTÉSI LEHETŐSÉGEI 26
1.1 Hazai veszélyes üzemek szabályozása 27
1.1.1 A veszélyes anyagokkal foglalkozó üzemek fogalma és kategóriái 28
1.1.2 Az üzemeltetői kötelezettségek rendszere 29
1.1.3 Balesetmegelőzési politika és biztonsági irányítási rendszer 29
1.1.4 Veszélyazonosítás és kockázatelemzés 30
1.1.5 Védelmi tervezés 30
1.2 A felügyeleti hatóság szerepe és eljárásai 31
1.2.1 Hatóság szerepe a védelmi tervezésben 33
1.2.2 Lakosság tájékoztatása 34
1.3 Európai Uniós direktívák hatása a veszélyes üzemekre 34
1.3.1 CER irányelv ismertetése 35
1.3.2 NIS2 irányelv ismertetése 37
1.3.3 NIS2 hazai implementáció és a „fehér folt” 39
1.4 A GRC, mint integráló meta keret 41
1.4.1 A nemzetközi szabványok GRC-be illesztése 43
1.5 Integrált GRC-alapú biztonsági modell veszélyes üzemek számára 44
1.5.1 keretrendszerek hierarchikus bemutatása 45
1.6 GRC alapú biztonságirányítás mérhetősége és érettségi modellje 48
1.6.1 Veszélyes üzemek biztonsági irányítási rendszere hatékonyságának lehetséges mérése 57

1.6.2 A szervezeti integritás, mint biztonsági faktor 58
1.6.3 Az iparbiztonsági hatósági munka hatékonyságának növelése 60
1.7 Fejezet részkövetkeztetései 61
2. IPARI BALESETEK KEZELÉSE, KÜLÖNÖS TEKINTETTEL A BEAVATKOZÓ ÁLLOMÁNY ÉS AZ ÉRINTETT LAKOSSÁG VÉDELMÉRE 63
2.1 Lakosságvédelem a 21. században 63
2.1.1 Lakosság katasztrófavédelmi felkészítése 68
2.1.2 Digitális lakosságtájékoztatás 69
2.1.3 A lakosságvédelem nemzetbiztonsági aspektusai 72
2.2 A Rouen-i Lubrizol ipari baleset tanulságai 76
2.2.1 A Lurbizol baleset kezelésének hiányosságai 80
2.3 Magyarország baleset elhárítási – és lakosságvédelmi képességei 83
2.3.1 Elhárítás és helyreállítás 83
2.3.2 A modern kockázatok kezelése 86
2.4 A kiber-incidensek kivizsgálásának lehetőségei 88
2.5 A katasztrófavédelmi helyreállítás rendszere és kiterjesztésének szükségessége 92
2.6 Egy ingyenes terjedés-modellező szoftver fejlesztési lehetősége 96
2.7 A rendszer gyakorlati használata 100
2.7.1 Rendszerkapcsolatok és adatbevitel 100
2.7.2 Az eredmények vizualizált megjelenítése a Google Earth Pro-n keresztül 103
2.7.3 Alkalmazási lehetőségek 103
2.7.4 Veszélyes anyag terjedési modellezése és az MI kapcsolata 104
2.8 Lakossági kitettség becslése, a fejlesztett applikáció koncepciója 107
2.8.1 A fejlesztett alkalmazás működése és alkalmazási lehetőségei 107
2.9 A fejlesztett rendszer-ökoszisztéma alkalmazásának bemutatása 110
2.9.1 Fiktív szcenárió 111
2.10 Fejezeti részkövetkeztetések 116
3. VESZÉLYES ANYAGOKKAL FOGLALKOZÓ ÜZEMEK 21. SZÁZADI KIHÍVÁSAI 118
3.1 A veszélyes üzemek fenyegetései 118
3.2 Az információbiztonság szerepe a veszélyes anyagokkal foglalkozó üzemek kiberkitettségének csökkentésében 119

3.3 OT rendszerek és az ipari környezet 125
3.4 Ipari vezérlőrendszereket érintő esettanulmányok 129
3.4.1 Ausztrál szennyvízkezelő elleni kibertámadás (2000) 129
3.4.2 Németországi acélmű elleni kibertámadás (2014) 131
3.4.3 Olaszországi Vízkezelő Üzem Támadása (2023) 133
3.4.4 Libanoni vízkezelő rendszerek ellen elkövetett Izraeli kibertámadás (2024) 134
3.5 Kiberbiztonsági mutatók, trendek 135
3.5.1 Az IT rendszerek sérülékenységei 135
3.5.2 Az ipari rendszerek kitettsége 146
3.6 A NIS2 irányelv és hazai implementációja 154
3.7 Veszélyes üzemek kiberrezilienciájának kialakítási lehetőségei 159
3.7.1 A kiberbiztonsági keretrendszer módszertani háttere 162
3.8 Fejezetbéli részkövetkeztetések 168
ÖSSZEGZETT KÖVETKEZTETÉSEK 170
ÚJ TUDOMÁNYOS EREDMÉNYEK 174
aZ ÉRTEKEZÉS AJÁNLÁSAI 176
a KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGA 178
Hivatkozott irodalom jegyzéke 179
A TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓIM 190
MELLÉKLETEK 191
Alkalmazott rövidítések és szakkifejezések jegyzéke 192
Témához kapcsolódó jogszabályok és belső szabályozó eszközök jegyzéke 195
Ábrák és táblázatok jegyzéke 198
„Safety driven” kontrollkatalógus 199
Kohéziós táblázat 203

BEVEZETÉS

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A veszélyes anyagokkal foglalkozó üzemek működése napjainkban egyre összetettebb kihívások elé néz, különösen az információbiztonság és a kiberfenyegetések területén. Az Ipar 4.0 technológiák, mint az IoT (Internet of Things)[1], a kiber-fizikai rendszerek, az automatizálás és a valós idejű adatfeldolgozás rohamos térnyerése forradalmasította az ipari folyamatokat, de egyben új sebezhetőségeket is teremtett. Az ipari rendszerek digitalizációja globális szinten új típusú kockázati környezetet hozott létre, amelyben a kiber- és fizikai rendszerek egyre szorosabb integrációban működnek.

A mai ipari környezetben a kockázatkezelés és a szabályozási kötelezettségeknek való megfelelés csak akkor lehet hatékony, ha integrált módon kezeli a technológiai, jogi, szervezeti és kiberbiztonsági szempontokat is. Ennek megfelelően kiemelt jelentőségű a veszélyes üzemek üzembiztonságának vizsgálata a GRC[2] (Governance – Risk Management – Compliance) szemlélet mentén, amely elősegítheti az üzemi biztonság holisztikus erősítését és a veszélyes üzemek teljes körű rezilienciájának növelését.

A digitális átalakulással párhuzamosan a kibertérből érkező fenyegetések is egyre kifinomultabbá válnak. Kiemelten fontos tudományos kérdés, hogy a veszélyes anyagokat kezelő létesítmények védelmi képességeinek kialakításában mennyiben nyújt hatékony keretet a meglévő jogi szabályozás. Bár a különböző európai uniós direktívák és hazai jogszabályok, valamint biztonsági irányelvek törekednek a biztonsági szintek egységes magas szintű harmonizálására, kérdéses, hogy ezek valóban alkalmazkodnak-e gyakorlatban a digitalizált ipari környezet komplexitásához és gyorsan változó kockázataihoz, valamint valóban minden hazai SEVESO irányelv hatálya alá tartozó üzem a vonatkozó kiberbiztonsági jogszabályok hatálya alá is tartozik-e.

A modern ipari környezet működéséből fakadóan azonosíthatóvá vált az a tudományos rés, hogy egy kiber-fizikai rendszer elleni célzott támadás következményeként akár lakosságvédelmi feladatok is előállhatnak. Egy ilyen esemény túlmutathat az üzemi károkon,

[1] A dolgok internete, olyan hálózatba kapcsolt fizikai eszközök rendszere, amelyek érzékelők és kommunikációs technológiák segítségével adatokat gyűjtenek, továbbítanak és automatikusan együttműködnek egymással vagy központi rendszerekkel.

[2] a szervezeti irányítás, a kockázatkezelés és a megfelelőség integrált megközelítése (meta-keret), amely a szervezeti célok biztonságos és szabályozott megvalósítását támogatja.

és komoly veszélyt jelenthet a környező lakosság egészségére és vagyonára. Az ilyen típusú incidensek kezelésére a katasztrófavédelmi szervek és a társhatóságok közötti együttműködés, a jól kidolgozott vészhelyzeti tervek megléte, valamint a hiteles lakosságtájékoztatás elengedhetetlenek. Ebből következően a biztonság értelmezése nem korlátozódhat az üzem határain belülre, hanem szükségessé válik a társadalmi hatások figyelembevétele is.

A kiber-fizikai rendszerek elleni támadások közvetlen hatással lehetnek az üzembiztonságra, az üzemfolytonosságra, valamint az emberi élet és a környezet biztonságára is. Ez indokolttá teszi olyan üzembiztonság-központú és kockázatarányos védelmi megközelítések vizsgálatát, amelyek figyelembe veszik az ipari vezérlőrendszerek sajátos működési követelményeit.

A fentiek alapján a tudományos probléma abban ragadható meg, hogy a veszélyes anyagokkal foglalkozó üzemek esetében jelenleg nem áll rendelkezésre olyan egységes, integrált megközelítés, amely képes a kiber-fizikai kockázatok, az üzembiztonság, a szervezeti reziliencia, valamint a lakosságvédelmi következmények együttes kezelésére.

Kutatásaim indítékát az a meglátás adta, hogy a veszélyes anyagokkal foglalkozó üzemek működésében az Ipar 4.0 technológiák megjelenésével párhuzamosan, jelentős mértékben megnőtt az információbiztonsági kockázatok súlya, miközben a kibertérből érkező fenyegetések ellen megalkotott jelenleg hatályos hazai jogszabályok nem teljeskörűen vonatkoznak valamennyi veszélyes anyagokkal foglalkozó üzemre. A jelenlegi jogi szabályozás és üzemirányítási gyakorlat nem minden esetben képes hatékonyan kezelni az új típusú kibertámadások hatásait. Azt is fontosnak tartottam feltárni, hogy a GRC szemlélet alkalmazása milyen lehetőségeket kínál az üzembiztonság fejlesztésére, és hogy egy esetleges kiber-fizikai támadás során milyen lakosságvédelmi kihívásokkal kell számolni, különös tekintettel arra, hogy a meglévő lakosságvédelmi eszközrendszer mennyiben képes alkalmazkodni az ilyen típusú, komplex kockázati helyzetekhez.

E hiányosság indokolja egy olyan integrált, interdiszciplináris megközelítés kidolgozását, amely képes a veszélyes ipari rendszerek biztonságának rendszerszintű újraértelmezésére.

A téma jelentősége, időszerűsége

A 21. század elejére a kiberbiztonság kérdésköre globális szinten a több ágazat működésének egyik meghatározó kockázati tényezőjévé vált. A digitalizáció, az Ipar 4.0 és az ipari rendszerek hálózatosodása következtében a korábban elszigetelt ipari vezérlőrendszerek

(ICS)[3] fokozatosan integrálódtak az informatikai hálózatokba a folyamatos adatkommunikáció révén a termelés hatékonysága növelhető ugyan, ám ezzel együtt új sérülékenységek is megjelennek, különösen a kibertámadásokkal szemben. A nemzetközi kiberbiztonsági jelentések, többek között a IBM X-Force[4] és a Cisco Talos[5] elemzései, egyértelműen rámutatnak arra, hogy az elmúlt években a kibertámadások fókusza egyre inkább az ipari és kritikus infrastruktúrákat érintő szektorok felé tolódott el.

Különösen figyelemre méltó, hogy a gyártóipar, az energetikai és a petrokémiai ágazat a leginkább célzott szektorok közé került. Az IBM X-Force több egymást követő évben is kimutatta, hogy a gyártóipar a kibertámadások elsődleges célpontjává vált, míg más jelentések az ellátási láncok és ipari vezérlőrendszerek elleni célzott támadások növekedését hangsúlyozzák. E támadások sajátossága, hogy nem csupán adatvesztést vagy pénzügyi károkat okoznak, hanem közvetlen hatással lehetnek a fizikai folyamatokra, ezáltal veszélyeztetve az üzembiztonságot, a környezetet és a környező lakosságot is.

Ezen globális trendek tükrében a veszélyes anyagokkal foglalkozó üzemek biztonsága napjainkban olyan kihívás elé néz, amely már nem kizárólag technológiai vagy jogi kérdésként értelmezhető, hanem egyértelműen interdiszciplináris kutatási területként jelenik meg. A kutatás középpontjában álló veszélyes anyagokkal foglalkozó üzemek és alapvető szolgáltatást nyújtó szervezetek biztonság kérdésköre ugyanis három, egymással szorosan összefonódó és egymást erősítő pillérre épül: a kiberbiztonságra, az üzembiztonságra (iparbiztonság), valamint a lakosságvédelemre. E három terület szinergikus kapcsolódása teremti meg azt az átfogó szemléletet, amely lehetővé teszi a valóban teljes körű reziliencia kialakítását a kritikus infrastruktúrák és veszélyes üzemek esetében.

A téma aktualitását hűen tükrözi, hogy az Európai Unió 2022 december végén elfogadott, majd 2024. október 18 óta hatályos Az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló, az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (a továbbiakban: NIS2) hasonló kérdéskört feszeget. Célul tűzi ki, hogy valamennyi alapvető és fontos szervezet Uniós szinten egységes, magas biztonsági képességgel rendelkezzen az informatikai rendszerei és szervezeti működése tekintetében. Valamint a

[3] olyan hardver- és szoftveralapú rendszerek összessége, amelyek ipari technológiai folyamatok felügyeletét, vezérlését és automatizált működtetését biztosítják.
[4] Az IBM globális kiberbiztonsági kutató- és incidenskezelő szervezete
[5] A CISCO globális kiberbiztonsági kutató és kiberfenyegetés-elemző szervezete

kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről szóló, az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (a továbbiakban: CER irányelv) a kritikus szervezetek rezilienciájának fokozását tűzi ki célul, vagyis az Unió területén található létfontosságú rendszerelemet birtokló szervezeteknek nem csak a kiberbiztonság területén, de fizikai biztonság területén is magas szintű ellenállóképességgel kell, hogy rendelkezzenek.

A jövő technológiai és társadalmi trendjeit kiválóan megragadja Alvin Toffler gondolata:

„*A technológia önmagát táplálja. A technológia újabb technológiát hoz létre.”* [1]

Ez az idézet különösen érvényes a veszélyes üzemek és a lakosság biztonságát érintő kérdésekre, a modern ipari és kritikus infrastruktúrák digitalizációjának folyamatára, ahol az automatizáció, az IoT-alapú rendszerek, valamint az IT–OT konvergencia új képességeket és hatékonyabb működést eredményeznek, ugyanakkor új biztonsági és kockázatkezelési kihívásokat is teremtenek. A veszélyes üzemek esetén ezért a technológiai fejlődéssel párhuzamosan a biztonsági irányítási rendszerek, kiberbiztonsági és lakosságvédelmi képességek folyamatos fejlesztése is szükségessé válik.

Kutatásom során egy komplex, többdimenziós tudományos rést azonosítottam. A veszélyes anyagokkal foglalkozó ipari üzemek és a kritikus infrastruktúrák digitális kitettsége, valamint ennek komplex és integrált kezelése, különösen a kiberbiztonság, az üzembiztonság és a lakosságvédelem összekapcsolása, jelenleg nem kellőképpen feltárt és rendszerezett terület. A meglévő szakirodalmak többsége jellemzően egy-egy aspektusra, például a technikai sebezhetőségekre vagy a jogszabályi megfelelésre, fókuszál, miközben hiányzik az átfogó, interdiszciplináris megközelítés, amely figyelembe veszi az egyes alrendszerek közötti kölcsönhatásokat és egymásra gyakorolt hatásaikat.

A kutatás ennek megfelelően e komplex tudományos rés három, egymással összefüggő vetületét vizsgálja:

Egyrészt a kutatás a biztonsági irányítási rendszerek továbbfejlesztésének és integrációjának lehetőségeit vizsgálja, különös hangsúlyt fektetve az egyes irányítási rendszerek, így különösen az információbiztonsági, üzletmenet-folytonossági és egyéb vállalatirányítási rendszerek, összehangolására. E megközelítés célja annak feltárása, hogy az egymástól gyakran

elkülönülten működő szabályozási és irányítási struktúrák miként alakíthatók át egy koherens, egységes biztonsági metakeretté.

A vizsgálat ennek keretében kiterjed a kiberbiztonsági és iparbiztonsági dimenziók integrált értelmezésére is, amelyben kiemelt szerepet kap a Governance, Risk and Compliance szemlélet alkalmazhatóságának elemzése. A GRC, mint meta-szintű keretrendszer, lehetőséget teremt a különböző biztonsági és kockázatkezelési folyamatok összehangolására, a szervezeti működés átláthatóságának növelésére, valamint a folyamatbiztonság hatékonyságának javítására a veszélyes ipari környezetben.

Másrészt a disszertáció kiemelten foglalkozik a lakosságvédelem kérdéskörével, amely nem csupán a hagyományos védelmi intézkedések szintjén kerül értelmezésre, hanem kiterjed a digitális technológiák által nyújtott lehetőségekre is. A kutatás ennek keretében vizsgálja a lakosság tájékoztatásának korszerű, digitális platformokon megvalósítható formáit, valamint olyan rendszerkomponensek és alkalmazási megoldások fejlesztését, amelyek közvetlenül támogatják a lakosság biztonságának növelését és a veszélyhelyzeti reagálás hatékonyságát.

Harmadrészt a kutatás szakít a hagyományos és jelenleg domináns IT-OT biztonsági fokúszú szemlélettel és üzembiztonsági (safety) szemléletből kiindulva vizsgálja a kiberkockázatok kezelésének lehetőségeit. E megközelítés célja annak bemutatása, hogy a kiberfenyegetések miként értelmezhetők és kezelhetők a veszélyes ipari folyamatok biztonságának kontextusában.

A kutatás ennek keretében egy integrált követelményrendszer kialakítására tesz javaslatot, amely a biztonsági irányítási rendszerek fejlesztését és összehangolását támogatja, és amely kifejezetten a veszélyes anyagokkal foglalkozó üzemek sajátosságaira épül. A megközelítés szemléltetésére a disszertáció egy követelménykatalógust dolgoz ki, amely a kiberbiztonsági és üzembiztonsági szempontok egységes rendszerben történő kezelését teszi lehetővé.

Ez a tudományos megközelítés ezért nemcsak elméleti, hanem gyakorlati szempontból is időszerű és jelentős. A cél egy olyan reziliens rendszerkép kialakítása, amely képes alkalmazkodni a gyorsan változó kockázati környezethez, és amelyben a digitális védelem, az ipari működésbiztonság és a társadalmi biztonság szerves egységet alkot.

A hazai és nemzetközi irányelveket, jogszabályokat elemezve arra a következtetésre jutottam, hogy a különböző védelmi intézkedések mind az adott szervezetekre vonatkozóan kerülnek meghatározásra, az üzem és ügymenet fenntartásának folytonossága szempontjából, azonban a

lakosság ellenállóképességeinek fokozására csak közvetetten az üzemek és létesítmények biztonságának fokozásával van lehetőség. A lakosság a közvetlen élőterében lévő alapvető szolgáltatást nyújtó szervezeteknek való kitettségének kockázatával kevés szakirodalom foglalkozott ezidáig. E hiányosság rámutat arra, hogy a veszélyes anyagokkal foglalkozó üzemek és kritikus szervezetek biztonságának értelmezése nem korlátozódhat kizárólag szervezeti és technológiai dimenziókra, hanem szükségessé válik egy olyan komplex megközelítés alkalmazása, amely a kiberbiztonsági, üzembiztonsági és társadalmi szempontokat egységes rendszerben kezeli, és ezáltal képes a reziliencia valódi, rendszerszintű értelmezésére.

KUTATÁSI HIPOTÉZISEK

Az értekezés kidolgozása során az alábbi hipotéziseket állítottam fel:

1. Megítélésem szerint a felső és alsó küszöbértékű veszélyes anyagokkal foglalkozó üzemekre vonatkozó előírások és azok alapján készült szabályrendszer összehasonlítása alapján a veszélyes anyagok és technológiák hatékonyabban meghatározhatóak. Az általános vezetési rendszer és biztonsági irányítási rendszer nemzetközi szabványok ajánlásaival, valamint a PDCA vagy a PDSA ciklussal való kibővítésével az üzemeltetés biztonsága növelhető, a balesetek kialakulásának kockázata csökkenthető.

2. Feltételezem, hogy a valós idejű és előrejelzett meteorológiai adatokra épülő digitális anyagterjedés-modellezési és döntéstámogatási rendszerek alkalmazásával hatékonyabban támogatható a veszélyhelyzeti helyzetértékelés, valamint csökkenthető a beavatkozó állomány és a potenciálisan veszélyeztetett lakosság egészségkárosodásának kockázata, ami tovább mérsékelhető a digitálisan támogatott és hiteles lakosságtájékoztatás alkalmazásával.

3. Feltételezem, hogy különösen az alsó és felső küszöbértékű veszélyes anyagokkal foglalkozó üzemek esetén a kibertérből érkező támadásokkal szembeni kitettség jelentős mértékű és ez a tendencia az elkövetkező években folyamatos növekedést fog mutatni.

KUTATÁSI CÉLKITŰZÉSEK

A kutatási célkitűzéseimet - a hipotézisek meghatározásánál már ismertetett - három kutatási részterületen fogalmazom meg:

1. Célul tűztem ki a veszélyes anyagokkal foglalkozó üzemekre vonatkozó hazai és nemzetközi szabályozási, biztonságirányítási és kockázatkezelési megközelítések vizsgálatát annak érdekében, hogy

meghatározhatók legyenek azok az integrált irányítási és reziliencia-központú módszertani elemek, amelyek hozzájárulhatnak az üzembiztonság növeléséhez, a modern kori kihívások hatékonyabb kezeléséhez és a súlyos ipari balesetek megelőzéséhez.

2. Célkitűzésem, hogy megvizsgáljam és bemutassam a felderítésben résztvevő állomány egészségi állapotának megőrzését és hatékonyabb felderítési és elemzési folyamatokat eredményező, a jelenleg rendelkezésre álló veszélyes anyag terjedését modellező szoftverek fejlesztési lehetőségeinek vizsgálata és bemutatása, különös tekintettel a lakosságvédelmi döntéstámogatás, a helyzetértékelés és a digitálisan támogatott lakosságtájékoztatás lehetőségeire.

3. Egy modern műszaki, technikai és adminisztratív keretrendszer és eljárásrend kidolgozását tűztem ki célul, amely a kiber-fizikai eszközök (OT) és azokkal párhuzamosan működő IT rendszerek magas szintű kibervédelmi képességeinek kialakításához szükséges.

KUTATÁSI MÓDSZEREK

A kutatás során interdiszciplináris módszertani megközelítést alkalmaztam, amely ötvözi a jogtudományi, biztonságtudományi és informatikai aspektusokat. A vizsgálati célkitűzések teljes körű feltárása és megalapozott megválaszolása érdekében többféle kvalitatív és analitikus módszert alkalmaztam, amelyek egymást kiegészítve biztosították a kutatás tudományos mélységét és gyakorlati relevanciáját.

A kutatás első lépéseként szisztematikus szakirodalmi és jogszabálykutatást végeztem, amely során a hazai és nemzetközi szintű releváns dokumentumok, szakkönyvek, tudományos cikkek, EU-irányelvek, biztonságpolitikai stratégiák és ipari szabványok tanulmányozására került sor. A cél a tématerület elméleti és szabályozási kereteinek feltérképezése volt, különös tekintettel az információbiztonság, kiberbiztonság, iparbiztonság és lakosságvédelem metszéspontjaira.

A begyűjtött jogi és szabályozási dokumentumok alapján elemző-logikai tevékenységet folytattam. E módszer segítségével értékeltem a jelenlegi szabályozási környezet erősségeit, hiányosságait, valamint azonosítottam a szabályozási réseket és alkalmazási problémákat. Az elemzésekből levont következtetések alapján fejlesztési javaslatokat fogalmaztam meg a veszélyes üzemek rezilienciájának növelése érdekében.

A kutatás empirikus része a vizsgált szakterületen – különösen a katasztrófavédelem, és információbiztonság területén szerzett többéves szakmai tapasztalatra épült. A gyakorlati tapasztalat lehetővé tette az elméleti megállapítások valóságalapú ellenőrzését, validálását és árnyalt értelmezését.

Külön figyelmet fordítottam a hazai jogszabályok, valamint a nemzetközi irányelvek és szabványok gyakorlati végrehajtása során jelentkező nehézségek azonosítására. A feltárt akadályok nemcsak a szabályozási környezet hiányosságaira, hanem az implementációs gyakorlat gyengeségeire is rámutattak. A hazai kiberbiztonsági követelményeket és auditokra vonatkozó módszertant javasolt lehet újra gondolni, különösen az ipari rendszerek sajátosságainak figyelembevételével, valamint a hatóság munkájának gördülékenyebbé tétele miatt.

A kutatás során Design Science Research (DSR)[6] módszertant alkalmaztam, amely lehetőséget adott innovatív megoldások tervezésére és értékelésére konkrét gyakorlati problémák kezelése érdekében. A módszert különösen az ingyenes terjedésmodellező szoftver digitális meteorológiai állomásának fejlesztése során használtam, így a szoftver a valós idejű és prediktív meteorológiai adatok integrálásával képes a veszélyes anyag kibocsátások környezeti hatásainak pontosabb, a valósághoz közelebb álló becslésére. A fejlesztés során alkalmazott matematikai képletek és algoritmusok kerültek beépítésre a légköri terjedési jelenségek pontosabb szimulációjához, miközben a rendszer valós szoftverfejlesztési környezetben készült. A DSR módszertan lehetővé tette egy olyan prototípus-szintű eszköz kialakítását, amely elősegítheti a veszélyes üzemek balesetelhárító képességének fejlesztését, valamint az elsődleges beavatkozók egészségének magasabb szintű védelmét, és a lakosságvédelmi döntések gyorsabb és megalapozottabb meghozatalát, melyet egy kiegészítő alkalmazás is támogat.

A kutatás során született rész- és végeredmények folyamatos dokumentálása és publikálása szerves részét képezte a munkának. Az eredményeket hazai és nemzetközi tudományos fórumokon, konferenciákon és folyóiratokban mutattam be, lehetőséget teremtve a tudományos közösséggel való szakmai diskurzusra.

[6] olyan kutatásmódszertani megközelítés, amely gyakorlati problémák megoldására új artefaktumok, például architektúra-rendszerek vagy prototípus-rendszerek, tervezésén, fejlesztésén és értékelésén keresztül hoz létre tudományos eredményeket.

A módszertan fontos eleme volt a szakmai konzultációk lefolytatása hazai szakértőkkel. E megbeszélések során lehetőség nyílt a kutatás közbenső eredményeinek véleményezésére, kiegészítésére és validálására, elősegítve a kutatás többdimenziós, szakmailag megalapozott szemléletének kialakulását.

Ez a módszertani keret biztosította, hogy a kutatás eredményei elméleti megalapozottságuk mellett gyakorlati alkalmazhatósággal és adaptálhatósággal is rendelkezzenek, különösen a kritikus infrastruktúrák és a veszélyes üzemek védelme és a reziliencia megvalósítása terén. A fejlesztési munka során egy ESP32[7]-alapú fizikai mikrokontroller is felprogramozásra került, amely képes valós idejű és prediktív meteorológiai adatok gyűjtésére és továbbítására. A szoftver és a hordozható eszköz közötti kommunikáció révén lehetőség nyílik arra, hogy a szoftver dinamikusan reagáljon az aktuális környezeti viszonyokra, és pontosabb prediktív becsléseket adjon egy esetleges veszélyes anyag kibocsátás esetén.

RELEVÁNS SZAKIRODALOM ÁTTEKINTÉSE

A kutatási célkitűzések eléréséhez elengedhetetlen a témához kapcsolódó, hazai és nemzetközi szinten mértékadónak tekintett szakirodalom tömör áttekintése. A kutatómunka megalapozását a választott tématerülethez kapcsolódó hazai és nemzetközi jogi szabályozások, valamint a releváns szakirodalmi források feldolgozása biztosította.

A kutatás középpontjában a veszélyes anyagokkal foglalkozó üzemek üzembiztonsági és információbiztonsági képességeinek, valamint ezen üzemek környezetében lévő lakosság védelmének fejlesztése áll. Ebben a kontextusban korábban még dokumentáltan itthon nem került vizsgálatra ez a komplex és koherens interdiszciplináris kutatási terület.

Magyarország Kiberbiztonsági Stratégiája a víziójában szintén egy átfogó és komplex szemléletet képvisel. A nemzeti kiberbiztonsági stratégia célja Magyarország digitális jólétének és ellenálló képességének megerősítése a globális kihívásokkal szemben. Ennek érdekében egy olyan átfogó kiberbiztonsági rendszer kialakítását tűzi ki, amely képes kezelni a változó fenyegetéseket, támogatja a társadalom és a gazdaság biztonságos digitalizációját, növeli az állampolgárok tudatosságát, valamint erősíti az állami, gazdasági és társadalmi szereplők együttműködését.

[7] Egy alacsony fogyasztású, beépített Wi-Fi és Bluetooth képességekkel rendelkező 32 bites mikrokontroller-platform.

Kutatásom egyik kiindulópontja, hogy a veszélyes anyagokkal foglalkozó üzemek rezilienciája nem értelmezhető kizárólag műszaki kérdésként, hanem olyan összetett védelmi rendszerként, amelyben az intézkedések és tevékenységek több szinten kapcsolódnak egymáshoz. Ennek keretében a védelmi intézkedések átfogó fogalomként értelmezhetők, amelyek a lakosság, a beavatkozó állomány, az ipari folyamatok és rendszerek biztonságát egyaránt szolgálják. Ernyőfogalom, ami a védelmi intézkedéseken belül kiterjed a megelőző jellegű intézkedésekre is, amelyek célja a biztonsági incidensek bekövetkezési valószínűségének minimalizálása. Amennyiben mégis bekövetkezik egy kiberbiztonsági vagy üzembiztonságot érintő esemény, a reagálási és beavatkozási tevékenységek biztosítják a gyors detektálást, az érintett rendszerek izolálását, valamint a beavatkozó állomány biztonságának megőrzését. Az incidens utáni helyreállítási tevékenységek már a normál ügy- és üzemfolytonosság biztonságos visszaállítására és a hosszú távú reziliencia erősítésére irányulnak. A védelmi intézkedések részét képezik továbbá a kifejezetten lakosságvédelmi intézkedések, mint a riasztási és tájékoztatási mechanizmusok, valamint az evakuációs protokollok, amelyek a civil lakosság védelmét szolgálják. E komplex megközelítés biztosítja, hogy a veszélyes anyagokkal foglalkozó üzemek teljeskörű rezilienciája ne elszigetelt technikai feladatként, hanem átfogó, társadalmi és gazdasági hatásokkal bíró védelmi rendszerként jelenjen meg.

A hazai katasztrófavédelem, valamint azon belül a polgári védelem és az iparbiztonság fejlesztése összhangban áll a nemzetközi, európai uniós és az ezekre épülő hazai jogi szabályozásokkal, kormányzati stratégiákkal és koncepciókkal. E fejlesztési irányokat támogatják azok az állami és szakmai törekvések is, amelyek célja a kritikus infrastruktúrák védelmének és rezilienciájának növelése. Itt a Katasztrófavédelem mellett a Nemzetbiztonsági Szolgálat Nemzeti Kibervédelmi Intézete (NBSZ NKI) is megjelenik, amely a kiberreziliencia előmozdításáért tett intézkedéseivel hozzájárul a veszélyes üzemek és más létfontosságú rendszerek teljeskörű rezilienciájának kialakításához. Ezen szervezetek működése erősíti a nemzeti szintű reagálóképességet a kibertérben jelentkező fenyegetésekkel szemben, elősegítve ezzel a komplex biztonsági környezethez való alkalmazkodást.

A kutatás során számos nemzetközi adatbázist vizsgáltam, mint az Európai Unió által működtetett MINERVA portált, ahol az Európai Unió területén bekövetkezett ipari baleseteket regisztrálják digitálisan, valamint az Amerikai Egyesült Államokbeli Cybersecurity &

Infrastructure Security Agency (CISA)[8] kampányait és a hazai Nemzeti Kibervédelmi Intézet beszámolóit. Továbbá kiemelt figyelmet fordítok a MITRE ATT&CK® [9]tudásbázisára, mely révén konkrét kiberfenyegetési modelleket és módszereket tudtam feltérképezni.

A Nemzeti Közszolgálati Egyetem és annak jogelődjének Katonai Műszaki Doktori Iskolája által jelentős számú katasztrófavédelmi témájú és a biztonságos infókommunikációval foglalkozó doktori értekezés és habilitációs tézisfüzet készült, amelyek szintén iránymutatásul szolgáltak kutatómunkám során.

Nemzetközi és hazai jogi szabályozás és szervezetrendszer bemutatása

A veszélyes anyagokkal foglalkozó üzemek biztonságának vizsgálata olyan összetett szabályozási és szervezeti környezetben értelmezhető, amelyben az iparbiztonsági, kiberbiztonsági, kritikus szervezeti rezilienciai és lakosságvédelmi szempontok egyidejűleg jelennek meg. A kutatás szempontjából ezért nem elegendő egyetlen szabályozási terület áttekintése, hanem szükséges annak bemutatása, hogy a különböző jogi és intézményi alrendszerek miként kapcsolódnak a veszélyes üzemek működésbiztonságához, digitális kitettségéhez és a környezetükben élő lakosság védelméhez.

Európai Uniós szinten a veszélyes anyagokkal foglalkozó üzemek biztonságának egyik meghatározó jogi alapját a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyeinek kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről szóló, az Európai Parlament és a Tanács 2012/18/EU irányelve (a továbbiakban: Seveso III irányelv) jelenti, amely a súlyos balesetek megelőzésére, következményeinek korlátozására, valamint a veszélyes anyagokkal kapcsolatos ipari tevékenységek kockázatainak kezelésére irányul. Az irányelv logikája alapvetően az ipari baleseti kockázatok azonosítására, a biztonsági dokumentációk elkészítésére, a hatósági ellenőrzésre és a lakosság tájékoztatására épül. Ez a megközelítés a veszélyes üzemek klasszikus iparbiztonsági szabályozásának alapját képezi.

A kiberbiztonsági szabályozási környezet Uniós szinten a NIS2 irányelv hatálybalépésével jelentősen megerősödött. Az irányelv célja, hogy az Európai Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedések jöjjenek létre, különösen az irányelv hatálya alá tartozó szervezetek vonatkozásában. A NIS2 a korábbi NIS irányelvhez képest

[8] Az USA kiberbiztonsági és kritikus infrastruktúra-védelmi ügynöksége, amely a kibervédelmi fenyegetések megelőzéséért, kezeléséért és a létfontosságú rendszerek rezilienciájának fokozásáért felel.
[9] A MITRE nonprofit kutató szervezet által üzemeltetett nyílt tudásbázis a kibertámadásokról

szélesebb ágazati hatályt, erősebb kockázatkezelési követelményeket, incidensbejelentési kötelezettségeket és felügyeleti mechanizmusokat vezetett be. A szabályozás jelentősége a jelen kutatás szempontjából abban áll, hogy a digitalizált ipari működés biztonságát már nem pusztán informatikai kérdésként, hanem szervezeti, üzem- és üzletmenetfolytonossági kockázatként kezeli.

A kritikus szervezetek fizikai és szervezeti ellenállóképességének európai uniós szintű megerősítését a CER irányelv szolgálja, amely a kritikus szervezetek rezilienciájának fokozását tűzi ki célul. A CER irányelv a kritikus szolgáltatások folytonosságát, a szervezetek kockázatértékelési és rezilienciafejlesztési kötelezettségeit, valamint az állami és szervezeti szintű védelmi intézkedések összehangolását helyezi előtérbe. A NIS2 és a CER irányelvek kiegészítik egymást, együttes értelmezésük szükséges, aminek eredményeként az európai uniós szabályozás a kiberbiztonságot és a fizikai-szervezeti rezilienciát egymást kiegészítő területként kezeli, ez a megközelítés releváns lehet a veszélyes anyagokkal foglalkozó üzemek esetében.

A hazai szabályozási környezetben a veszélyes anyagokkal foglalkozó üzemek biztonsága elsődlegesen a katasztrófavédelmi szabályozás rendszerében jelenik meg. A legfontosabb jogszabályok a katasztrófavédelemről és annak egyes módosításairól szóló 2011. évi CXXVIII. törvény és annak végrehajtásáról szóló 234/2011. (XI. 10.) Korm. rendelet, valamint a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X. 20.) Korm. rendelet, mely a SEVESO III irányelv hazai implementációját valósítja meg. E szabályozási környezet meghatározza a veszélyes üzemek azonosítását, a biztonsági jelentések és biztonsági elemzések elkészítését, a belső és külső védelmi tervezés követelményeit, valamint a hatósági ellenőrzési és beavatkozási feladatokat. A hazai iparbiztonsági szervezetrendszerben kiemelt szerepet tölt be a katasztrófavédelem, amely egyszerre lát el hatósági, ellenőrzési, tervezési, beavatkozási és lakosságvédelmi feladatokat.

A kibertérből érkező fenyegetések kezelése ugyanakkor a hazai szabályozásban elkülönült kiberbiztonsági szervezetrendszerhez is kapcsolódik. Magyarországon a kiberbiztonsági szabályozási környezetet jelenleg a kiberbiztonságról szóló 2024. évi LXIX. törvény határozza meg, amely a NIS2 irányelv hazai implementációjának alapját képezi. A törvény meghatározza az érintett szervezetek körét, a kockázatkezelési és incidenskezelési kötelezettségeket, valamint a felügyeleti és ellenőrzési mechanizmusokat, ezzel biztosítva a magas szintű kiberbiztonsági követelmények érvényesítését.

A jogszabályi környezet fontos kiegészítő eleme a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló 1/2025. (I. 31) SZTFH rendelet, amely a gazdálkodó szervezetek kiberbiztonsági auditjainak részletszabályait határozza meg. A rendelet rögzíti az auditálási követelményeket, az auditok végrehajtásának rendjét, valamint az érintett szervezetek megfelelőségének értékelési szempontjait. Ezzel a kiberbiztonsági felügyeleti rendszer gyakorlati végrehajtásának egyik kulcsfontosságú normatív eszközét jelenti.

A hazai szervezetrendszerben a kiberbiztonsági felügyelet, a nemzeti kibervédelmi feladatok, az incidenskezelés, valamint az iparbiztonsági hatósági és lakosságvédelmi tevékenység több szervezet feladat- és hatáskörébe tartozik. Ez a többpólusú intézményi környezet önmagában indokolja annak vizsgálatát, hogy a veszélyes anyagokkal foglalkozó üzemek biztonsága miként értelmezhető integrált módon. A kutatás szempontjából különösen fontos kérdés, hogy a szervezeti szintű kiberbiztonsági kötelezettségek, az iparbiztonsági védelmi tervezés, a katasztrófavédelmi reagálás és a lakosságvédelmi eszközrendszer milyen módon illeszthető egységes rezilienciaalapú megközelítésbe.

Nemzetközi szakirodalom bemutatása

A nemzetközi szakirodalomban és ajánlásrendszerekben ezzel párhuzamosan egyre hangsúlyosabbá vált az ipari vezérlőrendszerek védelme. A NIST SP 800-82 ajánlásokat megfogalmazó útmutató külön kiemeli, hogy a kiber-fizikai rendszerek sajátosságai eltérnek a hagyományos informatikai rendszerektől, mivel ezek közvetlenül fizikai folyamatokat irányítanak vagy befolyásolnak, ezért védelmük során a rendelkezésre állás, a megbízhatóság és a safety-követelmények is meghatározó jelentőségűek. [2]

A szabványok esetén az ipari vezérlőrendszerek védelmének egyik legátfogóbb keretrendszerét az IEC 62443 szabványsorozat jelenti. A szabvány kifejezetten az ipari automatizálási - és vezérlőrendszerek (IACS – Industrial Automation and Control Systems) biztonságára fókuszál, és strukturált követelményrendszert biztosít mind a gyártók, mind az üzemeltetők számára. A szabvány a rendszerek életciklusának teljes spektrumát lefedi, beleértve a tervezést, implementációt, üzemeltetést és karbantartást, valamint hangsúlyozza a „defense-in-depth” elv alkalmazását, a biztonságos szegmentációt és a biztonságos kommunikációs kapcsolatok kialakítását. [3]

A nemzetközi szabványok és ajánlások mellett a kutatás során számos olyan adatbázis került feldolgozásra, amelyek gyakorlati szempontból támogatják a veszélyes üzemek komplex

kockázatainak értelmezését. Ezek közé tartozik az Európai Unió által működtetett MINERVA portál, amely az ipari balesetekkel kapcsolatos események rendszerezett adatbázisát biztosítja, valamint az Egyesült Államok Cybersecurity and Infrastructure Security Agency (CISA) által publikált kampányok és figyelmeztetések. Valamint a MITRE ATT&CK for ICS tudásbázis pedig az ipari vezérlőrendszereket célzó támadói taktikák és technikák rendszerezésével támogatja a fenyegetések strukturált értelmezését. [4] [5] [6]

A nemzetközi szakirodalomban az utóbbi években egyre nagyobb hangsúlyt kapnak az integrált irányítási és kockázatkezelési megközelítések, amelyek a biztonságot nem kizárólag technológiai, hanem szervezeti és működési kérdésként értelmezik. E szemlélet egyik meghatározó keretrendszere az Open Compliance and Ethics Group (OCEG) által kidolgozott GRC Capability Model, amely a governance, kockázatkezelés és megfelelés integrált kezelését a szervezeti teljesítmény és reziliencia alapvető feltételeként határozza meg.

A modell a „Principled Performance” koncepció mentén a szervezeti működést nem csupán a kockázatok csökkentése, hanem az értékteremtés és fenntartható működés irányából közelíti meg. A Learn–Align–Perform–Review ciklus alkalmazásával biztosítja a folyamatos visszacsatolást és fejlesztést, valamint hangsúlyozza a kockázatok, lehetőségek és megfelelőségi követelmények együttes kezelésének szükségességét. [7]

A GRC mint meta-szintű keretrendszer a szervezeti irányítás és kockázatkezelés alapelveit és követelményeit fogalmazza meg, míg a Secure Controls Framework (SCF) az ezekhez illeszkedő operatív kontrollszintet képviseli. Az SCF Integrated Controls Management (ICM) modellje a védelmi intézkedések integrált kezelését biztosítja, lehetővé téve a különböző szabványokból és előírásokból származó követelmények egységes alkalmazását.

Ez az integrált kontrolltérkép lehetővé teszi a szervezetek számára, hogy a párhuzamos vagy átfedő követelményeket egységes struktúrában kezeljék, ezáltal csökkentve a redundanciát és növelve a biztonsági intézkedések átláthatóságát és hatékonyságát. [8]

Míg a GRC modellek elsősorban a szervezeti irányítás, a kockázatkezelés és a szabályozásoknak való megfelelőség stratégiai szintű összehangolását célozzák, addig az SCF az ezen elvek mentén megvalósítandó konkrét védelmi intézkedések operatív szintű integrációját támogatja. Ennek megfelelően az SCF nem pusztán kiegészíti a GRC szemléletet, hanem annak gyakorlati megvalósításához biztosít strukturált eszközrendszert.

A lakosságvédelem nemzetközi szakirodalmában meghatározó szerepet tölt be az UNDRR által kidolgozott Sendai Framework for Disaster Risk Reduction (2015–2030), amely a katasztrófakockázat csökkentésének globális stratégiai keretrendszerét adja. A keretrendszer hangsúlyozza a kockázatok rendszerszintű értelmezésének szükségességét, valamint kiemelt jelentőséget tulajdonít a lakosság felkészítésének, a kockázatkommunikációnak, valamint a reziliencia fejlesztésének. [9]

A Sendai Framework egyik alapvető megállapítása, hogy a katasztrófák hatásainak csökkentése nem valósítható meg kizárólag technikai vagy szervezeti intézkedések révén, hanem elengedhetetlen a társadalmi szereplők, kiemelten a lakosság, aktív bevonása és tudatosságának növelése. A keretrendszer ezért kiemelten foglalkozik a korai előrejelző (early warning) rendszerekkel, a riasztási mechanizmusokkal, valamint a hatékony és célzott tájékoztatással. A válságkommunikáció és a társadalmi bevonás fontosságára a World Health Organization által kidolgozott Risk Communication and Community Engagement (RCCE) keretrendszer is felhívja a figyelmet és meghatározza ennek alapelveit.

A WHO megközelítése szerint a hatékony lakosságvédelem nem korlátozódhat kizárólag a riasztási és beavatkozási mechanizmusokra, hanem kiemelt jelentősége van az időben, hitelesen és célzottan közvetített információknak, amelyek befolyásolják a lakosság viselkedését és döntéseit veszélyhelyzetekben. A keretrendszer hangsúlyozza a bizalomépítés, az információk érthetősége, valamint a különböző társadalmi csoportok sajátosságaihoz igazított kommunikáció fontosságát. [10]

Hazai mértékadó szakirodalom bemutatása

A veszélyes anyagokkal foglalkozó üzemek iparbiztonsági vizsgálatában meghatározóak azok a hazai kutatások, amelyek a súlyos ipari balesetek megelőzésével, a biztonsági dokumentációk tartalmával, valamint a belső és külső védelmi tervezés gyakorlati kérdéseivel foglalkoznak. Dobor József és Szendi Rebeka munkája a veszélyes üzemek belső védelmi terveinek gyakorlati alkalmazhatóságát vizsgálja, különös tekintettel a vegyi felderítés, mentesítés, valamint az erő- és eszközszükséglet meghatározásának problémáira. Kutatásuk rámutat arra, hogy bár a belső védelmi tervek formálisan tartalmazzák a jogszabályban előírt elemeket, a konkrét eseménysorokra, végrehajtási láncokra és kapacitásszámításokra vonatkozó részletek több esetben hiányosak. Ez a megállapítás a jelen értekezés szempontjából azért bír jelentőséggel, mert alátámasztja, hogy a veszélyes üzemek biztonságának fejlesztése

nem merülhet ki a formális, adminisztratív jellegű megfelelésben, hanem szükségessé válik a követelmények gyakorlati működőképességének vizsgálata is. [11]

A hazai kutatások, különösen Kátai-Urbán Lajos és Mesics Zoltán munkája rámutatnak arra, hogy a veszélyes ipari létesítmények biztonságos működtetésének kulcseleme a hatékony biztonsági irányítási rendszer kialakítása és folyamatos fejlesztése. A szerzők hangsúlyozzák, hogy a súlyos ipari balesetek jelentős része nem kizárólag technikai meghibásodások következménye, hanem szervezeti, irányítási és emberi tényezők együttes hatására vezethető vissza. E megközelítés a biztonságot nem statikus állapotként, hanem folyamatosan fejlesztendő, dinamikus rendszerként értelmezi.

A biztonsági irányítási rendszerek működésének alapját a kockázatalapú szemlélet képezi, amely magában foglalja a veszélyek azonosítását, a kockázatok értékelését és a megelőző intézkedések rendszerszintű alkalmazását. A szerzők kiemelik a folyamatos monitoring, a belső auditok és a vezetői felülvizsgálatok szerepét, amelyek biztosítják a rendszer működésének visszacsatolását és fejlesztését. Emellett hangsúlyozzák, hogy a biztonsági kultúra és a szervezeti „tanulás” fejlesztése nélkül a technikai intézkedések önmagukban nem képesek garantálni a balesetek megelőzését. [12]

E megállapítások közvetlen párhuzamba állíthatók a jelen értekezés megközelítésével, amely az irányítási rendszereket nem izolált elemekként, hanem egymással összefüggő, integrált rendszerként értelmezi. A hazai szakirodalom ugyanakkor arra is rámutat, hogy a különböző biztonsági területekhez kapcsolódó követelmények, így az iparbiztonsági, információbiztonsági és szervezeti kockázatkezelési elemek, jellemzően elkülönülten jelennek meg, és hiányzik azok egységes, rendszerszintű integrációja. Ez indokolja a jelen kutatás azon irányát, amely a biztonsági irányítási rendszerek integrációját, valamint egy egységes követelménykatalógus kialakítását vizsgálja, kifejezetten üzembiztonsági (safety) megközelítésből.

A települési és környezeti kockázatkezelés vonatkozásában Vass Gyula doktori értekezése mértékadó hazai szakirodalomnak tekinthető. Kutatása a településrendezési tervezés szerepét vizsgálja a veszélyes anyagokkal kapcsolatos súlyos ipari balesetek megelőzésében, és rámutat arra, hogy a lakott területek és veszélyes ipari létesítmények térbeli viszonya alapvetően befolyásolja egy esetleges baleset hatásainak súlyosságát. A szerző kiemeli, hogy a Seveso-szabályozás egyik fontos célja a súlyos ipari balesetek megelőzése mellett azok emberre és környezetre gyakorolt hatásainak csökkentése, és ennek egyik eszköze a településrendezési

tervezésbe beépített hosszú távú (több évtizedes) kockázatcsökkentés. Valamint felhívja a figyelmet az adott település társadalmi kockázati értékének folyamatos monitorozására, annak érdekében, hogy folyamatosan biztosított legyen a meghatározott kockázati érték. [13] Ezt a megközelítést tovább erősíti Cimer Zsolt, Kátai-Urbán Lajos és Vass Gyula közös kutatása, amely rámutat arra, hogy a jelenlegi szabályozási környezet nem minden esetben biztosít teljeskörű védelmet a lakosság számára, különösen azon létesítmények esetében, amelyek nem tartoznak a szigorúbb iparbiztonsági előírások hatálya alá. A szerzők kiemelik továbbá az urbanizáció és a növekvő népsűrűség szerepét a kockázatok súlyosságának növekedésében, ami a jelen kutatás lakossági kitettséget vizsgáló dimenziójával közvetlen kapcsolatban áll. [14]

A harmadik kutatási terület a lakosságvédelem, amely a hazai szakirodalomban elsősorban a polgári védelem, a lakosságfelkészítés, a riasztás és a veszélyhelyzeti tájékoztatás témaköreiben jelenik meg. Halász László és Kovács Judit megállapításai jól értelmezhetők a doktori kutatás során kialakított rendszerarchitektúra kontextusában. A szerzők hangsúlyozzák, hogy a katasztrófavédelmi döntések hatékonysága nagymértékben függ a rendelkezésre álló információk minőségétől, gyorsaságától és feldolgozhatóságától. [15] A kutatás során fejlesztett ESP32 mikrovezérlő-alapú digitális meteorológiai állomás és a hozzá kapcsolható lakosságkitettség-becslő alkalmazás ezt a megközelítést gyakorlati oldalról szemlélteti. A rendszerarchitektúra demonstrálja, hogy alacsony költségvetésű, decentralizált adatgyűjtő és döntéstámogató rendszerekkel is korszerűsíthetők az életciklusuk végén járó lakosságvédelmi és iparbiztonsági megoldások. A valós idejű meteorológiai adatok integrálása lehetővé teszi a veszélyes anyagok terjedésének pontosabb modellezését, míg a lakosságkitettség-becslő modul támogatja a megalapozott védelmi intézkedések gyors meghozatalát.

A fejlesztés rámutat arra, hogy a modern katasztrófavédelmi döntéstámogatás területén az alacsony költségű, decentralizált és skálázható megoldások is támogató szerepet tölthetnek be.

A lakossági tájékoztatás és felkészítés korszerűbb megközelítésében több hazai mű is kiemlhető, köztük Ambrusz József és Beke Zoltán közös publikációja hangsúlyozza, hogy a lakosság megfelelő tájékoztatása nem pusztán kommunikációs feladat, hanem a védekezés hatékonyságának egyik alapfeltétele. A szerzők rámutatnak arra, hogy a lakosság riasztási jelzésekkel, követendő magatartási szabályokkal és veszélyhelyzeti információkkal kapcsolatos ismereteit célzottan fejleszteni szükséges, különösen azon területeken, ahol a lakosság fokozottan ki van téve veszélyes anyagok hatásainak. E gondolat közvetlenül kapcsolódik a jelen kutatás digitális lakosságtájékoztatási és alkalmazásfejlesztési irányához. [16]

Ambrusz József doktori kutatása külön hangsúlyt helyez a helyreállítási szakasz jelentőségére is, rámutatva arra, hogy a lakosság biztonsága nem ér véget a közvetlen veszélyhelyzet megszűnésével, hanem a fizikai helyreállítás, a szolgáltatások normál működésének visszaállításának és a hosszú távú ellenállóképesség kialakításának kérdéseivel folytatódik. [17]

Kátai-Urbán Irina kutatása a veszélyes anyaggal foglalkozó telephelyek riasztási és területkiürítési hatékonyságát vizsgálja, és rámutat arra, hogy a riasztási eszközök, kommunikációs megoldások és védelmi tervek gyakorlati alkalmazhatósága több esetben korlátozott. Különösen fontos megállapítása, hogy a lakossági riasztás és tájékoztatás nem lehet kizárólag általános jellegű, hanem figyelembe kell vennie a helyi sajátosságokat, a veszélyeztetett terület kiterjedését és az alkalmazott eszközrendszer tényleges működőképességét. Ez a jelen értekezés szempontjából azért jelentős, mert alátámasztja a digitális platformokon megvalósítható, célzottabb és helyspecifikusabb lakosságtájékoztatás szükségességét. [18]

Összességében megállapítható, hogy a hazai szakirodalom jelentős eredményeket mutat fel az iparbiztonság, a települési kockázatkezelés és a lakosságvédelem területén, azonban e kutatások jellemzően elkülönülten kezelik az egyes szakterületeket. A veszélyes üzemek kiber-rezilienciája, az integrált irányítási megközelítés, valamint a veszélyes ipari környezetben jelentkező kiber-fizikai kockázatok és azok lakosságvédelmi következményeinek együttes vizsgálata a hazai szakirodalomban csak korlátozott mértékben jelenik meg, ami megalapozza a jelen értekezés kutatási célkitűzéseit.

AZ ÉRTEKEZÉS FELÉPÍTÉSE

A tudományos célkitűzéseim alapján a doktori értekezést három egymásra épülő, egymással korreláló tartalmi fejezetre bontva dolgozom ki.

Az értekezés nyolcadik fejezetében áttekintem és elemzem a hazai és nemzetközi veszélyes anyagokkal foglalkozó üzemekre vonatkozó üzemeltetési kötelezettségeket, elsődlegesen katasztrófavédelem és az üzembiztonság vonatkozásában. Továbbá a hazai üzembiztonság megteremtése érdekében felügyeletet gyakorló hatóságok vertikális és horizontális irányítási rendszerében megvalósuló, a következmények felszámolásával és a helyreállítási feladatok végrehajtási kompetenciáit, irányítási, vezetési feladataikat, kapcsolati rendszerüket térképezem fel. Bemutatom azon faktorokat, melyek kritikus szerepet játszhatnak egy üzem

biztonságában, illetve azon védelmi intézkedéseket, melyek képesek az üzemeltetési és kiber kockázati értékeket mitigálni.

A disszertáció kilencedik fejezetében esettanulmányokon keresztül igazolom, hogy a veszélyes anyagokkal foglalkozó üzemeket ért balesetek negatív hatásai potenciálisan veszélyeztetik az üzem környezetében lévő lakosság egészségét. Számba veszem a lehetséges lakosságvédelmi intézkedéseket kiváltó forgatókönyveket, javaslatokat fogalmazok meg a lakosságvédelem során alkalmazott eszközrendszer fejlesztésére vonatkozóan. Valamint a kárelhárításban résztvevő beavatkozó állomány egészségének megőrzése érdekében egy a kutatás során fejlesztett rendszert mutatok be, valamint a jövőben továbbfejleszthető mesterséges intelligencián alapuló lakosságvédelmi intézkedések meghozatalát elősegítő döntéstámogatási modul fejlesztési lehetőségeit ismertetem részletesen. Továbbá javaslatokat fogalmazok meg a lakosság tájékoztatásának fejlesztési lehetőségeire vonatkozóan, különösen a válság kommunikáció területén.

Az értekezés tizedik fejezetében nemzetközi kiberbiztonsággal foglalkozó szervezetek biztonsági jelentésein és esettanulmányokon keresztül igazolom, hogy a veszélyes anyagokkal foglalkozó üzemeknek minősített létesítmények potenciális célpontjaivá válhatnak a kibertámadásoknak. kidolgozok egy kiberbiztonsági kontrollokat is tartalmazó védelmi keretrendszert, ami az IT mellet OT biztonsági követelményeket is előírna az kutatás hatókörébe tartozó üzemek üzemeltetésének. A kutatás során először lefektetem a vizsgálati keretrendszer elméleti alapjait, majd kidolgozom a megvalósításához szükséges követelménykatalógust. Ez a katalógus nagymértékben empirikus kutatásra épül, és kialakításánál figyelembe veszem a nemzetközi és hazai jó gyakorlatokat, valamint a releváns jogszabályi környezetet.

A doktori értekezésem célkitűzéseinek meghatározásakor a következő főbb szűkítéseket és elhatárolási szempontokat vettem figyelembe:

- Elsősorban Magyarország területén működő veszélyes anyagokkal foglalkozó üzemekkel foglalkozom, illetve azon kritikus szervezetnek minősülő entitásokkal, melyek egyúttal a Kat. tv. IV. fejezete alapján veszélyes anyagokkal foglalkozó üzemnek is minősülnek (egy szervezet akár több jogszabályok által meghatározott kritériumrendszernek is megfelelhet).
- Főként a veszélyes anyagokkal foglalkozó üzemek környezetében élő lakosság biztonságának fokozási lehetőségeit vizsgálom.

- A károk elhárítása és helyreállítás esetén nem csak az egyes ipari balesetek során kialakuló negatív hatások elleni védekezést és helyreállítást értem, hanem ezen üzemek elektronikus információs és kiber-fizikai rendszereiket ért károkkal szembeni védekezést és az ezekből való helyreállítást is.

A kutatásaimat 2026. 05.15. zártam le.

1. IPARBIZTONSÁGOT SZOLGÁLÓ IRÁNYÍTÁSI RENDSZEREK HATÉKONYSÁGÁNAK FEJLESZTÉSI LEHETŐSÉGEI

Az értekezés ezen fejezetének célja az iparbiztonságot szolgáló irányítási rendszerek hatékonyságának vizsgálata és fejlesztési lehetőségeinek feltárása, különös tekintettel a veszélyes anyagokkal foglalkozó üzemek működésére. A korszerű ipari környezetben a biztonság már nem kizárólag műszaki vagy szabályozási kérdésként értelmezhető, hanem komplex, többdimenziós irányítási feladatként jelenik meg, amely magában foglalja a szervezeti, technológiai és információbiztonsági tényezők integrált kezelését. A fejezet egyben az első hipotézis igazolására is fókuszál, amely szerint a felső és alsó küszöbértékű, veszélyes anyagokkal foglalkozó üzemekre vonatkozó előírások és az azok alapján kialakított szabályozási rendszerek összehasonlító elemzése lehetővé teszi a veszélyes anyagok és technológiák pontosabb azonosítását, ezáltal hozzájárul a kockázatok hatékonyabb kezeléséhez. Ennek megfelelően a vizsgálat kiterjed a különböző szabályozási és irányítási megközelítések értékelésére, valamint azok gyakorlati alkalmazhatóságára a beavatkozási tevékenységek során.

Kiemelt hangsúlyt kap továbbá annak bemutatása, hogy az általános vezetési rendszerek és a biztonságirányítási rendszerek miként járulnak hozzá az ipari biztonság növeléséhez, különösen akkor, ha azok nemzetközi szabványok ajánlásaival, valamint a PDCA ciklus vagy PDSA ciklus alkalmazásával kerülnek kiegészítésre. E ciklikus, folyamatos fejlesztésen alapuló megközelítések lehetővé teszik a működési és védelmi folyamatok rendszeres felülvizsgálatát és optimalizálását, amely közvetlen módon hozzájárul a balesetek kialakulási valószínűségének csökkentéséhez, valamint a bekövetkezett események hatékonyabb kezeléséhez.

A fejezet tehát integrált módon vizsgálja a szabályozási, irányítási és operatív védelmi intézkedésekhez köthető aspektusokat, hangsúlyozva, hogy a beavatkozó állomány, a lakosság és a környezet védelme csak komplex, rendszerszintű megközelítés alkalmazásával biztosítható.
A fejezet fő fókuszában a vonatkozó hazai jogszabály által elvárt biztonsági irányítási rendszer (BIR) továbbfejlesztését is támogató, integrált GRC (Governance, Risk, Compliance) meta keretrendszer áll, amely egységes struktúrába rendezi az irányítási, kockázatkezelési és megfelelőségi követelményeket. A megközelítés célja, hogy a veszélyes anyagokkal foglalkozó üzemek működésében jelenlévő biztonsági, üzemeltetési és kiberbiztonsági szempontok

összehangolt kezelését tegye lehetővé, ezáltal növelve a szervezet átláthatóságát és irányíthatóságát.

A keretrendszer részét képezik mindazon részszabályok, kontrollok és követelmények, amelyek az üzem biztonságos működéséhez szükségesek, különös tekintettel a kockázatok azonosítására, értékelésére és kezelésére. Ezzel összhangban meghatározásra kerülnek azok a mérőszámok és teljesítménymutatók is, amelyek alkalmasak az üzembiztonság szintjének objektív értékelésére, valamint a fejlesztési intézkedések hatékonyságának nyomon követésére.

A bemutatott megközelítés kiemelt célja az üzembiztonság növelése mellett a szervezet teljeskörű rezilienciájának erősítése, amely magában foglalja a fizikai, technológiai és információbiztonsági dimenziók integrált kezelését. A megfelelően kialakított és folyamatosan felügyelt és fejlesztett biztonsági irányítási rendszer így nemcsak a balesetek megelőzéséhez járul hozzá, hanem a bekövetkezett eseményekre adott válaszok hatékonyságát és a helyreállítási képességet is jelentős mértékben javítja.

A modern, komplex ipari rendszerek biztonságának értelmezése jelentős paradigmaváltáson ment keresztül az elmúlt évtizedekben. Nancy G. Leveson rendszerszemléletű megközelítése szerint a balesetek nem kizárólag komponenshibák vagy eseményláncok következményei, hanem a rendszerben érvényesítendő biztonsági korlátok (safety constraints) nem megfelelő működéséből, illetve a hierarchikus kontrollstruktúrák hibáiból erednek. Ebben az értelmezésben a biztonság nem statikus állapot, hanem egy dinamikus kontrollfolyamat, amely a technikai, humán és szervezeti szintek kölcsönhatásában valósul meg. [19]

Ezt a rendszerszintű megközelítést erősítik meg a legújabb kutatások is, amelyek rámutatnak arra, hogy a komplex kiber-fizikai rendszerekben a kockázatok nem izoláltan jelennek meg, hanem egymással összekapcsolódó, hálózatos struktúrákban, ahol egy esemény láncreakciós hatásokat válthat ki a rendszer különböző elemei között. [20] Ennek megfelelően a biztonság értelmezése csak integrált, többdimenziós és rendszerszintű megközelítésben lehetséges.

1.1 Hazai veszélyes üzemek szabályozása

A veszélyes anyagokkal foglalkozó üzemek szabályozása az Európai Unióban egységes elveken alapul, amelyek kiindulópontját a Seveso-balesetek tapasztalatai képezik. A Seveso III

direktíva[10] célja a súlyos ipari balesetek megelőzése, valamint azok emberi egészségre és környezetre gyakorolt hatásainak csökkentése. Az irányelv kockázatalapú megközelítést alkalmaz, amely a veszélyes anyagok jelenlétéhez és mennyiségéhez igazítva határozza meg az üzemeltetői kötelezettségeket és a hatósági felügyelet kereteit.

A hazai jogrendben az irányelv rendelkezései elsősorban a 219/2011. (X.20.) Korm. rendelet révén kerültek átültetésre, amely meghatározza a veszélyes anyagokkal foglalkozó üzemek azonosításának, működésének és felügyeletének részletes szabályait. A rendelet a BM Országos Katasztrófavédelmi Főigazgatóság (BM OKF) hatáskörébe és illetékességi körébe tereli a Seveso-előírások végrehajtását, figyelembe véve a hazai ipari és igazgatási sajátosságokat.

Magyarországon a veszélyes üzemek létesítését katasztrófavédelmi engedély birtokában lehet csak megvalósítani. A veszélyes üzemekre irányadó hazai jogszabályok a következők: 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzákapcsolódó egyes törvények módosításáról szóló, valamint a 219/2011 (X.20.) Kormányrendelet *a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről*.

1.1.1 A veszélyes anyagokkal foglalkozó üzemek fogalma és kategóriái

A szabályozás értelmében veszélyes anyagokkal foglalkozó üzemnek minősül minden olyan létesítmény, ahol a meghatározott veszélyes anyagok jelenléte, akár gyártás, feldolgozás, tárolás vagy felhasználás során, elér egy meghatározott küszöbértéket. Az Seveso III direktíva ennek megfelelően két alapvető kategóriát különböztet meg:

- alsó küszöbértékű üzemek,
- felső küszöbértékű üzemek.

A besorolás alapját a jelenlévő veszélyes anyagok típusa és mennyisége képezi, amely egyben meghatározza az alkalmazandó biztonsági követelmények szigorúságát is. A felső küszöbértékű üzemek esetében a szabályozás részletesebb dokumentációs és kockázatkezelési kötelezettségeket ír elő, tekintettel a potenciálisan súlyosabb következményekre.

A magyar szabályozás ugyanakkor az uniós irányelvhez képest egy további kategóriát is bevezet a 219/2011. (X.20.) Korm. rendelet keretében. Ennek megfelelően megkülönböztethetők az úgynevezett küszöbérték alatti üzemek. Ezen kategóriába eső

[10] Az Európai Parlament és a Tanács 2012/18/EU irányelve (2012. július 4.) a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről

szervezeteknél a jelenlévő veszélyes anyag mennyisége nem éri el az alsó küszöbértéket, azonban annak legalább 25%-át eléri.

Ennek a kategória bevezetésének oka, hogy ezen létesítmények bár formálisan nem tartoznának a Seveso irányelv hatálya alá, mégis hordozhatnak olyan kockázatokat, amelyek indokolttá teszik bizonyos biztonsági követelmények alkalmazását. Ennek megfelelően a küszöbérték alatti üzemekre is vonatkoznak előírások, bár ezek jellemzően enyhébbek, mint az alsó és felső küszöbértékű üzemek esetében. A követelmények elsősorban a veszélyazonosításra, az alapvető megelőző intézkedésekre, valamint a hatósági nyilvántartásba vételre és ellenőrzésre terjednek ki.

A háromszintű besorolási rendszer sajátossága, hogy lehetővé teszi a kockázatarányos szabályozást, ugyanakkor egyben rámutat arra is, hogy a veszélyes anyagokkal kapcsolatos kockázatok nem kizárólag a Seveso-hatály alá tartozó üzemekben jelennek meg. Ez különösen fontos szempont napjaink komplex digitális ipari környezete és az ellátási láncok vizsgálata során, ahol a kisebb, de hálózatosan kapcsolódó üzemek is jelentős szerepet játszhatnak a rendszerszintű kockázatok alakulásában.

1.1.2 Az üzemeltetői kötelezettségek rendszere

A veszélyes üzemek üzemeltetőinek kötelezettségei több szinten jelennek meg, és alapvetően a megelőzés, a felkészülés és a következménykezelés hármas logikájára épülnek.

1.1.3 Balesetmegelőzési politika és biztonsági irányítási rendszer

Az üzemeltető köteles kialakítani és működtetni egy balesetmegelőzési belső szabályozási környezetet, amely meghatározza a szervezet biztonsági céljait és alapelveit. Ennek operatív megvalósítását a biztonsági irányítási rendszer (BIR) biztosítja, amely magában foglalja:

- a szervezeti struktúrát és felelősségi rendet,
- a technológiai berendezések üzemeltetési és karbantartási eljárásait,
- a változáskezelési mechanizmusokat,
- az alkalmazott teljesítménymutatók meghatározását,
- az oktatási és képzési rendszert,
- az ellenőrzési és felülvizsgálati folyamatokat,

- jelentéstételi eljárásrendeket.

A BIR célja, hogy strukturált módon biztosítsa a biztonsági követelmények folyamatos érvényesülését az üzem teljes életciklusa során.

1.1.4 Veszélyazonosítás és kockázatelemzés

Az üzemeltető köteles azonosítani a lehetséges veszélyforrásokat és elemezni a súlyos ipari balesetek bekövetkezésének lehetőségeit, valamint azok következményeit. Erre vonatkozóan a jogszabály nem határoz meg expilicit módszereket, az alkalmazott kockázatkezelési módszert az üzemeltető felelősségkörébe helyezi.

Az üzemeltető által végzett kockázat azonosítási és kockázatelemzési eljárásoknak ki kell terjedniük:

- a technológiai folyamatok elemzésére,
- a veszélyes anyagok tulajdonságainak értékelésére,
- a lehetséges baleseti forgatókönyvek meghatározására,
- a hatásterületek és érintett lakosság becslésére.

A felső küszöbértékű üzemek esetében ezt a tevékenységet részletes biztonsági jelentés formájában kell dokumentálni, míg az alsó küszöbértékű veszélyes üzemek ezt a biztonsági elemzés részeként végzik el.

1.1.5 Védelmi tervezés

Az üzemeltető feladata a belső védelmi terv elkészítése, amely meghatározza a baleseti helyzetek kezelésének módját. A terv tartalmazza:

- a riasztási és kommunikációs rendet,
- a beavatkozási eljárásokat,
- a személyzet feladatait és felelősségét,
- az együttműködés kereteit a hatóságokkal.

A védelmi tervben foglalt eljárásokra és eszközök alkalmazására valamennyi dolgozót fel kell készíteni és évente szimulált gyakorlatok által szükséges ellenőrizni a dolgozók egy meghatározott része által végrehajtandó beavatkozás tényleges hatékonyságát és megfelelőségét. Három évente pedig a teljes személyzetnek szükséges gyakorlatot végeznie.

A belső védelmi terv kiegészül a hatóság által készített külső védelmi tervvel, amely a lakosság védelmét és a környezeti károk mérséklését szolgálja.

A hivatásos katasztrófavédelmi szerv területi szerve, az illetékes polgármesterrel együttműködve, a külső védelmi tervben foglaltak megvalósíthatóságát rendszeresen ellenőrzi. Ennek érdekében évente lefolytatnak olyan gyakorlatot, ahol a tervben megjelölt szervezetek valamely részét, valamint háromévente olyan gyakorlatot, ahol a tervben megjelölt szervezetek egészét gyakoroltatják.

A polgármester és az érintett szervezetek a veszélyes anyagokkal kapcsolatos súlyos baleset vagy egyéb biztonsági esemény bekövetkezésekor a külső védelmi tervben foglalt intézkedéseket azonnal foganatosítják.

Az üzemeltető a jelentési rendszer részeként köteles biztosítani:

- a hatóságok részére történő rendszeres adatszolgáltatást,
- veszélyes anyagokkal kapcsolatos súlyos baleset esetén az eseményről, annak bekövetkezését vagy az arról való tudomásszerzést követő 24 órán belül írásbeli adatszolgáltatást nyújt az iparbiztonsági hatóság részére.
- a lakosság tájékoztatását a veszélyekről és a követendő magatartási szabályokról,
- a biztonsági dokumentáció naprakészen tartását.

1.2 A felügyeleti hatóság szerepe és eljárásai

A veszélyes üzemek felügyeletét Magyarországon a katasztrófavédelem iparbiztonsági hatósága látja el, amely a jogszabályi előírások betartását ellenőrzi és biztosítja a lakosság védelmét.

A hatóság feladata:

- az üzemek azonosítása és besorolása,
- a biztonsági jelentések, biztonsági elemzések és súlyos káresemény elhárítási tervek elbírálása,
- az üzemek létesítésének és működésének engedélyezése.

A felügyeleti hatóság a veszélyes anyagokkal foglalkozó üzemek működését folyamatos ellenőrzési és felügyeleti tevékenység keretében vizsgálja. Az ellenőrzések célja annak biztosítása, hogy az üzemeltetők a jogszabályi követelményeket ténylegesen betartsák, valamint, hogy a biztonsági irányítási rendszerek ne csupán formálisan, hanem a gyakorlatban is megfelelően működjenek.

Az ellenőrzések két fő típusa különböztethető meg:

- tervezett ellenőrzések, amelyek a hatóság által előre meghatározott éves ellenőrzési terv alapján történnek,
- eseti ellenőrzések, amelyek rendkívüli eseményekhez, bejelentésekhez vagy hatósági észlelésekhez kapcsolódnak.

A hatóság az ellenőrzések során átfogó módon vizsgálja az üzem biztonsági működését, különös tekintettel a biztonsági irányítási rendszer (BIR) tényleges működésére és hatékonyságágra, a veszélyazonosítási és kockázatelemzési tevékenységek megalapozottságára és naprakészségére, az üzemeltetési és karbantartási gyakorlat megfelelőségére, valamint a belső védelmi tervek végrehajthatóságára és a szervezet felkészültségére.

Az ellenőrzések nem kizárólag dokumentáció-ellenőrzésre korlátozódnak, hanem kiterjednek a helyszíni vizsgálatokra, az üzemeltetési gyakorlat értékelésére, valamint szükség esetén a személyzet felkészültségének ellenőrzésére is. A helyszíni vizsgálatok alkalmával kerülnek az üzemben jelen lévő veszélyes anyagokról és azok mennyiségéről vezetett nyilvántartás is ellenőrzésre.

A felügyeleti tevékenység kockázatalapú megközelítésben valósul meg, amelynek keretében az ellenőrzések gyakoriságát és mélységét az adott üzem veszélyességi szintje, a jelenlévő veszélyes anyagok mennyisége, valamint az üzem működésének komplexitása határozza meg. Ennek megfelelően a felső küszöbértékű üzemek esetében jellemzően gyakoribb (legalább éves szintű) és részletesebb ellenőrzések történnek, míg az alacsonyabb kockázati kategóriába tartozó létesítmények esetében a felügyelet arányos mértékű.

A kockázatalapú ellenőrzési rendszer célja, hogy a hatósági erőforrások a legnagyobb potenciális veszélyt jelentő létesítményekre koncentrálódjanak, ugyanakkor biztosított maradjon a hazai veszélyes üzemek teljes spektrumának átfogó felügyelete. Ez a megközelítés összhangban áll a kockázatarányos megközelítéssel, amely biztosítja, hogy a védelmi

intézkedések mértéke és erőforrásigénye igazodjon az azonosított kockázati értékek nagyságához.

A hatóság amennyiben hiányosságokat tapasztal, szankcionálás eszközével élhet, ezek közé tartozik a katasztrófavédelmi bírság alkalmazása, amelynek részletes szabályait a katasztrófavédelmi bírság részletes szabályairól, a katasztrófavédelmi hozzájárulás befizetéséről és visszatérítéséről szóló 208/2011. (X.12.) Korm. rendelet határozza meg. A bírság kiszabására abban az esetben kerül sor, ha az üzemeltető nem tesz eleget a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzésére és következményeinek csökkentésére vonatkozó jogszabályi kötelezettségeinek. Ezenfelül az a hatóság kötelezheti az üzemeltetőt a hiányosságok megszüntetésére, korlátozhatja vagy felfüggesztheti a tevékenységet és súlyos esetben megtilthatja az üzem további működését.

A bírságolási rendszer a biztonsági irányítási rendszer (BIR) külső kontrollmechanizmusaként értelmezhető, amely biztosítja a szabályozási követelmények kikényszerítését.

1.2.1 Hatóság szerepe a védelmi tervezésben

A hatóság egyik alapvető feladata a külső védelmi terv elkészítése és folyamatos karbantartása a felső küszöbértékű üzemek esetében. A külső védelmi terv célja, hogy meghatározza a baleseti helyzetekben végrehajtandó intézkedéseket a lakosság, a környezet és az anyagi javak védelme érdekében. A terv kidolgozása során a hatóság figyelembe veszi az üzemeltető által készített biztonsági jelentést, valamint az abban szereplő baleseti forgatókönyveket és hatásterületeket.

Ennek keretében a hatóság:

- meghatározza a veszélyeztetett területeket, amelyek kijelölése a modellezett baleseti események hatásterülete alapján történik;
- kialakítja a lakosságvédelmi intézkedések rendszerét, beleértve az elzárkóztatás, kitelepítés, kimenekítés vagy egyéb védelmi intézkedések alkalmazásának feltételeit;
- meghatározza a beavatkozásban részt vevő szervezetek körét, valamint azok feladatait és együttműködésének rendjét;
- meghatározza a riasztási és tájékoztatási rendszerek működését, biztosítva, hogy a lakosság időben és megfelelő formában értesüljön a veszélyhelyzetről és a szükséges intézkedésekről.

1.2.2 Lakosság tájékoztatása

A jogszabály külön hangsúlyt helyez a lakosság előzetes tájékoztatására és felkészítésére, amelynek keretében a veszélyeztetett területen élők számára rendszeresen hozzáférhetővé kell tenni az alapvető információkat, így különösen:

- az adott üzem által jelentett veszélyek jellegét,
- a lehetséges baleseti eseményeket és azok hatásait,
- a riasztási jelzéseket és azok jelentését,
- a veszélyhelyzet esetén követendő magatartási szabályokat.

A tájékoztató kiadvány alapjául szolgál az alsó küszöbértékű üzem biztonsági elemzése, a felső küszöbértékű üzem biztonsági jelentése, valamint, ha készült, akkor a külső védelmi terv tartalma is.

A külső védelmi tervek hatékonyságának biztosítása érdekében a hatóság rendszeresen gyakorlatokat és felülvizsgálatokat szervez, amelyek célja a tervek végrehajthatóságának ellenőrzése, valamint a beavatkozó szervezetek közötti együttműködés fejlesztése. A tervek felülvizsgálata indokolt minden olyan esetben is, amikor az üzem működésében, a veszélyes anyagok mennyiségében vagy a környezeti feltételekben jelentős változás következik be.

A védelmi tervezés rendszere így biztosítja, hogy a súlyos ipari balesetek bekövetkezése esetén ne csupán az üzemeltető belső intézkedései, hanem egy összehangolt, hatóság által irányított külső beavatkozási struktúra is rendelkezésre álljon. Ez a megközelítés összhangban áll a Seveso szabályozás alapelveivel, amelyek a megelőzés mellett kiemelt hangsúlyt helyeznek a következmények kezelésére és a lakosság védelmére.

1.3 Európai Uniós direktívák hatása a veszélyes üzemekre

Európában a második világháború óta a jugoszláviai háborút leszámítva nem jellemezték geopolitikai konfliktusok, azonban az elmúlt bő egy évtizedben az orosz-ukrán konfliktus ezt a tendenciát felborította. Az Európai Unió tagállamainak szervezetei gyakran váltak kiberbiztonsági és szürke zónás műveletek áldozataivá. Ezen okokból kifolyólag az Európai Uniónak lépnie kellett. Ennek nyomán az Európai Unió kritikus szervezeteinek és kritikus infrastruktúráinak fokozott kiber-kitettségei és fizikai sebezhetőségei ellen az Európai Parlament és a Tanács még 2022 decemberében kiadta a két irányelvét, hogy előmozdítsa az Unióban lévő fontos és alapvető szolgáltatást nyújtó szervezetek teljes körű rezilienciájának kialakítását. Az Unió felhívja a tagállamok figyelmét, hogy ezt a két irányelvet koherens

megközelítést alkalmazva implementálják hazai jogrendjeikbe. Továbbá mindkét irányelv a kockázatalapú megközelítés alkalmazását követeli meg a tagállamoktól.

Az irányelvek hatályai alól kizárásra kerülnek azon közigazgatási szervek, melyek tevékenységeiket túlnyomórészt a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés területén végzik.

Az irányelveket a tagállamoknak a nemzeti jogszabályi környezetükbe legkésőbb 2024. október 17-ig implementálniuk kellett, melynek hazánk eleget is tett.

Jelenleg kiemelten kritikus ágazatokat és egyéb kritikus ágazatokat különböztet meg a direktíva, valamint alapvető és fontos szervezeteket. A CER irányelv azon veszélyes anyagokkal foglalkozó üzemeknél releváns, melyek rendelkeznek kritikus infrastruktúrával, vagy az általuk nyújtott szolgáltatás alapvető fontosságú a társadalom számára. Nem minden veszélyes üzem kritikus szervezet, azonban néhány hazai szervezet lehet egyszerre veszélyes üzemként is azonosítva, valamint olyan alapvető szolgáltatást nyújtó szervezet, amelyet a kijelölő hatóság a vonatkozó törvényben meghatározottak szerint kijelölt és elengedhetetlen Magyarország társadalmi, gazdasági stabilitásához és a biztonság, a környezet, a közegészségügy, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához

1.3.1 CER irányelv ismertetése

Az irányelv szükségességét a dinamikusan változó fenyegetések, mint a hibrid hadviselés és a terrorizmus, valamint az infrastruktúra és az ágazatok közötti növekvő kölcsönös függőségek és a szélsőséges időjárás okozta kihívások indokolják. Fontos volt, hogy minden tagállamban a kritikus ágazatokat elismerjék és védelmüket egységes magasszinten biztosítsák.

Célul tűzte ki, hogy harmonizált minimumszabályokat kell megállapítani az alapvető belső piaci szolgáltatások, a kritikus szervezetek rezilienciájának fokozása, valamint az illetékes hatóságok közötti, határokon átnyúló együttműködés javítása érdekében.

Figyelmet fordít az olyan alacsony valószínűségű nagy hatású kockázatokra, mint amilyen a Covid19-világjárvány volt, ugyanis a járvány rámutatott az egyre inkább egymásra utalt társadalmaink sebezhetőségére a nagy hatású, de csekély valószínűségű kockázatokkal szemben.

A digitális infrastruktúra ágazat esetén érintett szervezetek kategóriái nagy mértékben a NIS2 irányelvben meghatározott szolgáltatókból áll.

Valamennyi tagállamnak meg kell határoznia a saját a kritikus szervezetek rezilienciájának erősítését célzó stratégiáját. A dokumentumban kiemelt figyelmet kell fordítani a NIS2 irányelv miatt kijelölt nemzeti hatóság és a CER irányelv miatt kijelölésre kerülő hatóság közötti gördülékeny együttműködés meghatározására. A stratégiát 2026. január 17-ig el kell készíteni és valamennyi, a direktíva által meghatározott ágazatot le kell fednie.

A kritikus szervezetek azonosítására és rezilienciájának biztosítására irányuló tagállami intézkedéseknek kockázatalapú megközelítést kell követniük, amely az alapvető fontosságú társadalmi funkciók vagy gazdasági tevékenységek ellátása szempontjából leginkább releváns szervezetekre koncentrál. Az ilyen célzott megközelítés biztosítása érdekében egy összehangolt kereten belül minden egyes tagállamnak el kell végeznie az olyan releváns természeti és ember okozta kockázatok értékelését – ideértve a több ágazatot érintő, illetve a határokon átívelő kockázatokat is –, amelyek hatással lehetnek az alapvető szolgáltatások nyújtására, beleértve a baleseteket, a természeti katasztrófákat, a népegészségügyi szükséghelyzeteket, így például a világjárványokat és a hibrid fenyegetéseket vagy egyéb ellenséges fenyegetéseket. A tagállamok általi kockázatértékelésnek elkészítési határideje 2026 január 17. ennek a kockázatelemzésnek releváns pontjait a kritikus szervezetként azonosítottak is megkaphatják saját kockázatelemzésük és intézkedési tervük megvalósításának elősegítése érdekében.

A tagállamok által létrehozott stratégiák és egyéb dokumentumok elemzése, továbbá a legjobb gyakorlatok meghatározása érdekében létrehozták a kritikus szervezetek rezilienciájával foglalkozó csoportot.

A tagállamok a CER irányelv által meghatározott 11 ágazatban és az azokhoz tartozó alágazatokban szereplő kritikus szervezeteket legkésőbb 2026. július 17-ig azonosítják, majd benyújtják a Bizottság részére az alapvető szolgáltatások jegyzékét, a mellékletben meghatározott egyes ágazatok és alágazatok, valamint az egyes szervezetek által nyújtott alapvető szolgáltatás vagy szolgáltatások tekintetében azonosított kritikus szervezetek számát, valamint az alkalmazott küszöbértékeket.
Minden tagállamnak szükséges kijelölnie egy egyedüli kapcsolattartó pontot, mely a többi tagállam egyedüli kapcsolattartó pontjaival és az uniós kritikus szervezetek rezilienciájával foglalkozó csoporttal tart fenn gördülékeny kommunikációt, információcserét. A kijelölt nemzeti kapcsolattartó pontok 2028. július 17-ig összefoglaló jelentést készítenek a

Bizottságnak és kritikus szervezetek rezilienciájával foglalkozó csoportnak, a bejelentésre került biztonsági eseményekről.

A kritikus szervezetek a kockázatelemzés és értékelés elvégzését követően (mely támaszkodik az adott tagállam kockázatértékelésén) az azonosított kockázatokra intézkedéseket hoznak, hogy saját rezilienciájukat biztosítsák. A szervezetek által hozott intézkedéseket részletesen ismertetni kell a reziliencia terv dokumentumban.

Ahogyan a jelenleg hatályos hazai jogszabályok is elvárják valamennyi kritikus infrastruktúra esetén a biztonsági összekötő személy alkalmazását a hatóságokkal való kapcsolattartás érdekében, úgy a CER irányelv is megköveteli ennek a szerepkörnek a meglétét.

Az irányelv kiterjed a kritikus szervezetek által alkalmazott humán erőforrás háttérellenőrzésének kérdésére is, ami egy rövid határidejű hatóság által végzett vizsgálatot jelentetne a szervezeten belüli jogosultságokkal való visszaélések csökkentése végett.

Az irányelv a szankciók mértékét az egyes tagállamok önrendelkezésére bízza, azonban ennek részleteit legkésőbb 2024. október 17-én meg kell küldeni a Bizottság részére. [21]

1.3.2 NIS2 irányelv ismertetése

A NIS2 irányelvben a korábbinál több ágazat került meghatározásra, tizenegy kritikus ágazat és hét egyéb kritikus ágazat, valamint számos alágazat. A fenti ágazatokba tartozó szervezeteket a direktíva alapvető – és fontos szervezetként nevez.

A direktíva hatálya alá a meghatározott ágazat azon szervezetei fognak tartozni, melyek 50 fő feletti foglalkoztatottal rendelkeznek és / vagy nettó árbevétele meghaladja a 10 millió Eurót (kb. 3.7 milliárd Huf) ezek alól kivételt képeznek például a minősített bizalmi szolgáltatást nyújtó szervezetek, DNS szolgáltatók, legfelső szintű domain név-nyilvántartók, digitális infrastruktúrák alapvető szolgáltatói, tehát alapvetően a közép és nagyvállalatok érintettek.

1. ábra NIS 2 direktíva hatálya alá tartozó vállalatok méret szerint, forrás: [22]

Az alapvető és fontos szervezetek jegyzékét valamennyi tagállam összeállítja és 2025. április 17-ig a Bizottság részére megküldi.

Az irányelv a kockázat alapú megközelítést alkalmazza, csakúgy, mint a CER irányelv. Nem az egyes információs rendszerekre fókuszál, hanem a teljes üzleti folyamatra terjed ki hatálya, beleértve a beszállítói láncok biztonságát.
Bevezeti az IKT fogalmat, mint infokommunikációs technológia fogalmát. Az ENISA által kidolgozásra fog kerülni egy Európai Uniós nyilvántartás, mely tartalmazni fogja valamennyi azonosított IKT termék és - szolgáltatás sérülékenységeit.

A nagyszabású kiberbiztonsági események és válságok kezelésére minden tagállam kijelöl egy vagy több illetékes hatóságot, valamint a számítógép – biztonsági események kezelésére létrehoz egy vagy több nemzeti CSIRT-et.
Létrehozásra kerül az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe), aminek fő feladata a jelentős kiberbiztonsági események és válságok operatív szintű összehangolt kezelésének támogatása, továbbá kapcsolattartás a tagállamok és az Unió intézményei, szervei, hivatalai és ügynökségei között. [23]
Kiberbiztonsági együttműködési csoport kerül létrehozása, mely hasonlóan a CER irányelv esetén létrejövő munkacsoporthoz itt is az irányelv átültetésének megvalósítását támogatja, valamint a stratégiák és egyéb benyújtott dokumentumok elemzéséből az iparági legjobb gyakorlatokat kívánják meghatározni.

Az alapvető szervezetek esetén a szankcionálás mértéke amennyiben súlyos eltérés kerül feltárásra legalább 10 millió Euró vagy a szervezet előző évi bevételének akár a 2%-a lehet közigazgatási bírság formájában. Fontos szervezet esetén ez az összeg némileg alacsonyabb, mint a fenti értékhatárok.

Az irányelv, csak úgy, mint a CER irányelv szintén kiemelt figyelmet fordít a humánerőforrás okozta kockázatokra ezért például folyamatos szervezeten belüli biztonságtudatosság növelő képzések megtartását szorgalmazza, kiterjesztve a vezetőségre, valamint hangsúlyozva a vezetőség felelősségét. Ösztönzi az alapvető és fontos szervezeteket a zero trust szemlélet alkalmazására, ezzel ugyanis a szervezetek képesek fokozni a hálózati biztonságot, mivel minden felhasználót és eszközt folyamatosan ellenőriznek, és csak a szükséges erőforrásokhoz való hozzáférést engedélyezik, minimalizálva ezzel a támadási felületet. [24] [25]

A direktíva a szállítási ágazatot is szabályozni kívánja, így az intelligens közlekedési infrastruktúra, valamint a vasúti pályahálózatot működtetők a kibertámadásokkal szemben kockázat arányos védelmi képességgel fognak rendelkezni, mely katasztrófavédelmi szempontból a veszélyes áru szállítást tenné biztonságosabbá a meglévő ADR, RID és ADN szabályzók mellett. Hiszen a közlekedési infrastruktúrát ért kibertámadások, akár közvetlen hatást is képesek gyakorolni a veszélyes áru szállítás biztonságára. [26]

Ebből jól látható, hogy hazánkban döntően a felső küszöbértékű veszélyes üzemek és az alsó küszöbértékű veszélyes üzemek egy jelentős része került a kiberbiztonsági törvény hatálya alá a méret és árbevétel korlátok miatt.

1.3.3 NIS2 hazai implementáció és a „fehér folt”

Az ipari rendszerek digitalizációjával és az IT–OT konvergencia erősödésével a kritikus infrastruktúrák és ipari létesítmények kiberbiztonsága kiemelt szabályozási területté vált az Európai Unióban. Ennek egyik legfontosabb eszköze a NIS2 direktíva, amely a hálózati és információs rendszerek egységes, magas szintű biztonságát célozza a tagállamokban.
A NIS2 irányelv jelentős előrelépést jelent a korábbi NIS irányelvhez képest, mivel kiterjeszti a szabályozás hatályát, pontosítja az érintett szervezetek körét, valamint szigorúbb követelményeket ír elő a kockázatkezelés, az incidenskezelés és a felügyelet területén.
Magyarországon a NIS2 irányelv rendelkezései a 2024. évi LXIX. törvény révén kerültek átültetésre, amely meghatározza a kiberbiztonsági követelmények hazai keretrendszerét. A törvény célja a kritikus és a kockázatos szervezetek kiberrezilienciájának növelése, valamint a kibertérből érkező fenyegetésekkel szembeni védekezés megerősítése.

A törvényt kiegészítik a végrehajtási rendeletek, különösen a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI.24.) MK rendelet, és a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló 1/2025. (I.31.)

MK rendelet, amelyek részletesen szabályozzák az elektronikus információs rendszerek biztonsági osztályba sorolását, a kockázatkezelést szolgáló védelmi intézkedések katalógusát, az incidensjelentési kötelezettségeket, a felügyeleti és ellenőrzési eljárásokat.

A hazai implementáció középpontjában a kiberbiztonsági kockázatok azonosítása, értékelése és kezelése áll. A NIS2 szabályozás egyik lényeges sajátossága, hogy hatálya meghatározott kritériumokhoz kötött. Azon szervezetek képezik a szabályozás tárgyi hatályát, amelyek megfelelnek a törvény által meghatározott ágazati besorolásnak, méret- és bevételi korlátnak, és vagy a szervezet által nyújtott szolgáltatás kritikus jellegű.
E megközelítés következtében azonban egy jelentős szervezeti kör kívül maradhat a szabályozás hatályán, ami releváns a veszélyes anyagokkal foglalkozó üzemek kapcsán is. Azon alsó küszöbértékű üzemek és küszöbérték alatti üzemek lehetnek érintettek, akik bár nem kiemelten kockázatos üzemek, mégis jelenős mennyiségű veszélyes anyagot kezelnek, és potenciálisan súlyos következményekkel járó események forrásai lehetnek.

Ez a helyzet egy úgynevezett szabályozási „fehér foltot” eredményez, ahol a fizikai (safety) kockázatok szabályozottak, azonban a kiberbiztonsági dimenzió nem, vagy csak korlátozottan. A hazai NIS2 implementáció egyik sajátossága, hogy a kiberbiztonsági követelményrendszer alapját a NIST SP 800-53 Rev.5 kontrollkatalógus képezi, amely eredendően informatikai környezetekre lett kialakítva. Ennek következtében az ipari vezérlőrendszerek és egyéb OT rendszerek is egységesen elektronikus információs rendszerként kerülnek kezelésre, és az ellenőrzések során ugyanazon követelmények alkalmazása történik. Ez a megközelítés nem veszi teljes mértékben figyelembe az OT rendszerek sajátos működési és biztonsági követelményeit. Ez a jelenség értelmezhető a szabályozási „fehér folt” egy speciális eseteként, amely nem a lefedettség hiányából, hanem a módszertani megközelítés korlátjaiból fakad.
A probléma jelentőségét tovább növeli, hogy a modern ipari környezetben a rendszerek nem izoláltan működnek, hanem komplex, hálózatos struktúrák részei. Ennek következtében egy, a NIS2 hatályán kívül eső üzem kockázatot jelenthet a beszállítói láncokban különösen, ha az egy nemzetgazdaság vagy nemzetbiztonság szempontjából jelentős szervezetnek is beszállít. További kockázat, ha az üzem által használt technológiai platformok megosztásra kerülnek más szervezetekkel is.
Számos nemzetközi kiberbiztonsági jelentés rámutat arra, hogy a támadók a supply kill chain részeként a beszállítói lánc legsebezhetőbb szereplőinek digitális infrastruktúrájában található sérülékenységeket kihasználva jutnak be, és ezeken keresztül teremtenek belépési pontot egy kritikus fontosságú szervezet elleni támadáshoz. [27] Ez azt eredményezi, hogy a szabályozás

hatályán kívül eső, de kockázatos üzemek rendszerszintű sérülékenységet hozhatnak létre, amely túlmutat egy „stand-alone” létesítmény kockázati szintjén.
A kialakuló szabályozási hiátus jól értelmezhető a Governance–Risk–Compliance (GRC) keretrendszer perspektívájából. A GRC szemlélet nem kizárólag a jogszabályi megfelelésre épít, hanem a szervezeti célok és a kockázatok összhangjára. Ennek megfelelően a „fehér folt” problémája rámutat arra, hogy a pusztán szabályozás-alapú megközelítés nem elegendő a komplex kiber-fizikai rendszerek biztonságának szavatolására.

1.4 A GRC, mint integráló meta keret

Napjaink veszélyes üzemei biztonságának és megbízható működésének biztosítása egyre inkább olyan integrált megközelítést igényel, amely túlmutat az egyes szakterületek elkülönült kezelésén. Ebben a kontextusban kiemelt jelentőséggel bír a GRC megközelítés, amely a szervezeti működés három alapvető dimenzióját egységes keretben értelmezi. A GRC szemlélet egyik legismertebb és legszélesebb körben alkalmazott modelljét az OCEG által kidolgozott GRC Capability Model adja, amely a szervezeteket komplex, adaptív rendszerekként kezeli.

A modell alapfeltevése szerint a szervezeti működés nem írható le statikus szabályrendszerek mentén, hanem dinamikus kölcsönhatások hálózataként értelmezhető, ahol a célok, a kockázatok és a működési korlátok folyamatosan alakítják egymást. Ennek megfelelően a GRC nem egy különálló funkcionális terület, hanem egy olyan integráló képességrendszer, amely biztosítja, hogy a szervezet céljait a meghatározott keretek között, a kockázatok tudatos kezelése mellett érje el. A sikeres szervezeti működés nagyfokú flexibilitást és adaptációs képességet is jelent. A modell központi fogalma a „principled performance”, amely azt fejezi ki, hogy a teljesítmény csak akkor tekinthető fenntarthatónak, ha az a kockázatok és kötelezettségek figyelembevételével valósul meg. [7]

A hagyományos biztonsági és irányítási rendszerek jelentős része compliance-központú logikát követ, amelynek elsődleges célja a jogszabályi és szabványi követelmények teljesítése. Ugyanakkor a kizárólagos compliance-orientáció több szempontból is korlátozott. Egyrészt a compliance jellegéből adódóan reaktív megközelítést képvisel, amely elsősorban a már ismert kockázatokra és előírásokra reagál. Másrészt a szabályozás szükségszerűen általánosított, így nem képes teljes mértékben lefedni az egyedi szervezeti és technológiai sajátosságokat. Ennek következtében előállhat az a helyzet, hogy egy szervezet formálisan megfelel az előírásoknak, ugyanakkor működése ténylegesen nem tekinthető biztonságosnak, mert az elvárt

követelmények nem kerültek testre szabásra a szervezeti működéshez, folyamatokhoz és rendszerekhez.

A compliance-központú megközelítés további korlátja, hogy nem ösztönzi a kockázatok proaktív kezelését és a szervezeti tanulást. A szabályok betartása önmagában nem garantálja a nem várt, komplex vagy emergens jellegű kockázatok kezelését, különösen olyan környezetekben, ahol a technológiai és szervezeti változások gyors ütemben zajlanak. A szabályok és szabványok konkrétan nem ösztönzik a legújabb trendeknek megfelelő vagy előremutató technológiai megoldások alkalmazását. Ez különösen igaz a kiber-fizikai rendszerek esetében, ahol a kockázatok gyakran nem lineáris módon, több tényező kölcsönhatásából alakulnak ki.

A GRC modell egyik kulcseleme a governance, amely a szervezeti irányítás azon szintjét jelenti, ahol a stratégiai célok, az értékek és a működési keretek meghatározása történik, jellemzően board vagy tulajdonosi kört takarja. Ez egy magasabb szintű irányadó funkció, amely kijelöli azt a keretet, amelyen belül a szervezet működhet.

A governance szerepe különösen fontos a komplex rendszerek esetében, ahol a döntések következményei több szinten és időtávon jelentkeznek. A megfelelő irányítás biztosítja, hogy a szervezet ne csupán rövid távú célokat kövessen, hanem figyelembe vegye a hosszú távú kockázatokat és következményeket is. Emellett a governance teremti meg azt a keretrendszert, amelyben a különböző szakterületek tevékenysége összehangolható, így a biztonságot is széleskörűen értelmezi a szervezet egészére. Valamint itt kerül magas szinten meghatározásra a szervezet kockázati étvágya is. A governance hiánya vagy gyengesége gyakran vezet fragmentált működéshez, ahol az egyes funkciók elszigetelten, eltérő célok mentén működnek. Ez különösen problémás a veszélyes anyagokkal foglalkozó üzemek esetében, ahol a safety és security szempontok közötti konfliktusok megfelelő irányítás nélkül nem kezelhetők hatékonyan.

A GRC megközelítés harmadik alappillére a kockázatkezelés, amely nem önálló funkcióként, hanem a döntéshozatal integráns részeként jelenik meg. A modell értelmezésében a kockázat a bizonytalanság hatása a szervezeti célokra, amely lehet negatív (veszteség) vagy pozitív (lehetőség) jellegű is. A kockázatkezelés integrációja azt jelenti, hogy a szervezet nem utólag, külön folyamatként kezeli a kockázatokat, hanem már a stratégiai és operatív döntések során figyelembe veszi azokat. Ez különösen fontos olyan környezetekben, ahol a döntések gyorsan változó feltételek mellett születnek, és ahol a kockázatok jelentős része nem előre

definiált. Ezért szükséges a kockázatkezelési folyamatokat ciklikus és eseti jelleggel folyamatosan elvégezni. Valamint szükséges naprakészen tartani a szervezet működési tevékenységével és az aktuális geopolitikai helyzettel összefüggő fenyegetéseket.

A modern ipari környezetekben a kockázatok gyakran a technológiai, szervezeti és humán tényezők kölcsönhatásából erednek, így kezelésük csak integrált megközelítésben lehetséges.

A 219/2011. (X.20.) Korm. rendelet által előírt biztonsági irányítási rendszer (BIR) elemzése rámutat arra, hogy annak struktúrája jelentős hasonlóságot mutat a modern GRC keretrendszerekkel. A BIR tartalmazza a szervezeti irányítás (governance), a kockázatkezelés (risk), valamint a jogszabályi megfelelés (compliance) alapvető elemeit, azonban ezek nem kiegyensúlyozott módon jelennek meg.

A jogszabály által elvárt biztonsági irányítási rendszer működésében domináns szerepet tölt be a megfelelési és biztonsági logika, amely elsősorban a súlyos ipari balesetek megelőzésére és a jogszabályi követelmények teljesítésére fókuszál. Ezzel szemben a GRC keretrendszer a szervezeti teljesítmény, a kockázatkezelés és a megfelelés integrált kezelésére törekszik, ahol a kockázat nem csupán elkerülendő tényezőként, hanem a döntéshozatal részét képező, potenciálisan értékteremtő elemként is megjelenik.

1.4.1 A nemzetközi szabványok GRC-be illesztése

A modern veszélyes anyagokkal foglalkozó üzemek esetében különösen igaz, hogy a safety, a security, a megfelelés és a szervezeti működés szorosan összefonódnak. Ennek megfelelően szükségessé válik egy olyan integrált megközelítés, amely képes ezen dimenziók egységes értelmezésére és kezelésére. Ezt a szerepet töltheti be a Governance–Risk–Compliance (GRC) keretrendszer, amely nem önálló szabványként, hanem integráló elméleti és gyakorlati modellként értelmezhető.

A GRC szemlélet alapja, hogy a szervezeti működés három alapvető dimenzió – az irányítás (governance), a kockázatkezelés (risk) és a megfelelés (compliance) – egységében ragadható meg. E három terület nem elkülönülten, hanem egymással kölcsönhatásban határozza meg a szervezet működését és biztonsági szintjét. A GRC Capability Model ezt a megközelítést egy dinamikus, életciklus-alapú rendszerként írja le, amely a kontextus megértésére, a célok és keretek meghatározására, a végrehajtásra, valamint a visszacsatolásra épül.

A biztonságirányítás gyakorlati megvalósítása során számos nemzetközi szabvány és ajánlás áll rendelkezésre, amelyek különböző aspektusait fedik le a biztonságnak. Ezek közül kiemelkedő jelentőségű az ISO/IEC 27001, amely a szervezeti szintű információbiztonsági irányítási rendszer kialakításához biztosít keretet. A szabvány kockázatalapú megközelítést alkalmaz, és meghatározza a szükséges irányítási struktúrákat, folyamatokat és felelősségeket, ezáltal elsősorban a governance és risk dimenziókat támogatja. [28]

Ezzel szemben a NIST SP 800-53 egy részletes kontrollkatalógust nyújt, amely konkrét biztonsági intézkedéseket definiál. A szabvány erőssége a strukturált, auditálható követelményrendszer, amely elsősorban a compliance dimenziót erősíti, ugyanakkor önmagában nem biztosít teljes körű irányítási keretet. [29]

Az ipari környezet sajátosságait az IEC 62443 szabványsorozat, valamint a NIST SP 800-82 kezeli, amelyek kifejezetten az OT rendszerek védelmére fókuszálnak. Ezek a keretrendszerek figyelembe veszik az ipari rendszerek működési sajátosságait, és olyan technikai és szervezeti intézkedéseket határoznak meg, amelyek biztosítják a kiber- és fizikai folyamatok integrált védelmét. [3] [2]

Az üzembiztonsági dimenziót a hazai szabályozásban a 219/2011. (X.20.) Korm. rendelet által előírt biztonsági irányítási rendszer (BIR) képviseli, amely a súlyos ipari balesetek megelőzésére és következményeinek kezelésére biztosít strukturált keretet. Ezzel párhuzamosan az ISO 45001 a munkavédelem és az egészségvédelem területén alkalmaz kockázatalapú irányítási megközelítést, amely a szervezeti működés és a biztonsági kultúra integrációját hangsúlyozza. [30]

1.5 Integrált GRC-alapú biztonsági modell veszélyes üzemek számára

A GRC Capability Model egyik központi eleme a Learn–Align–Perform–Review (LAPR) ciklus, amely a szervezeti működést egy folyamatos, visszacsatoláson alapuló rendszerként írja le. Ez a megközelítés lehetővé teszi a különböző szabványok és szabályozási keretek funkcionális integrációját azáltal, hogy azokat nem statikus kategóriákba sorolja, hanem a működési folyamat különböző fázisaihoz rendeli.

A „Learn” fázisban a szervezet a működési környezetet, a kockázatokat és a külső felek elvárásait értelmezi, amelyhez az ISO/IEC 27001 és az ISO 45001 kockázatértékelési mechanizmusai, valamint az OT-specifikus ajánlások, például a NIST SP 800-82 nyújtanak

alapot. Az „Align” fázisban kerül sor a célok, politikák és irányítási keretek meghatározására, amelyben az ISO szabványok mellett az etikai dimenzió meghatározó szerepet játszik. [30] [28]

A „Perform” fázis a kontrollok tényleges megvalósítását jelenti, ahol a NIST SP 800-53 kontrollkatalógusa, az IEC 62443 ipari biztonsági követelményei, valamint a jogszabály által nevesített biztonsági irányítási rendszer (BIR) biztosítják a működési alapot. A „Review” fázisban a rendszer működésének értékelése történik auditok, hatósági ellenőrzések és visszacsatolási mechanizmusok révén. [29] [3]

A szervezeti kultúra és integritás nem egyetlen fázishoz köthető, hanem a teljes ciklust átható tényezőként jelenik meg, amely alapvetően befolyásolja a kontrollok tényleges működését.

1.5.1 keretrendszerek hierarchikus bemutatása

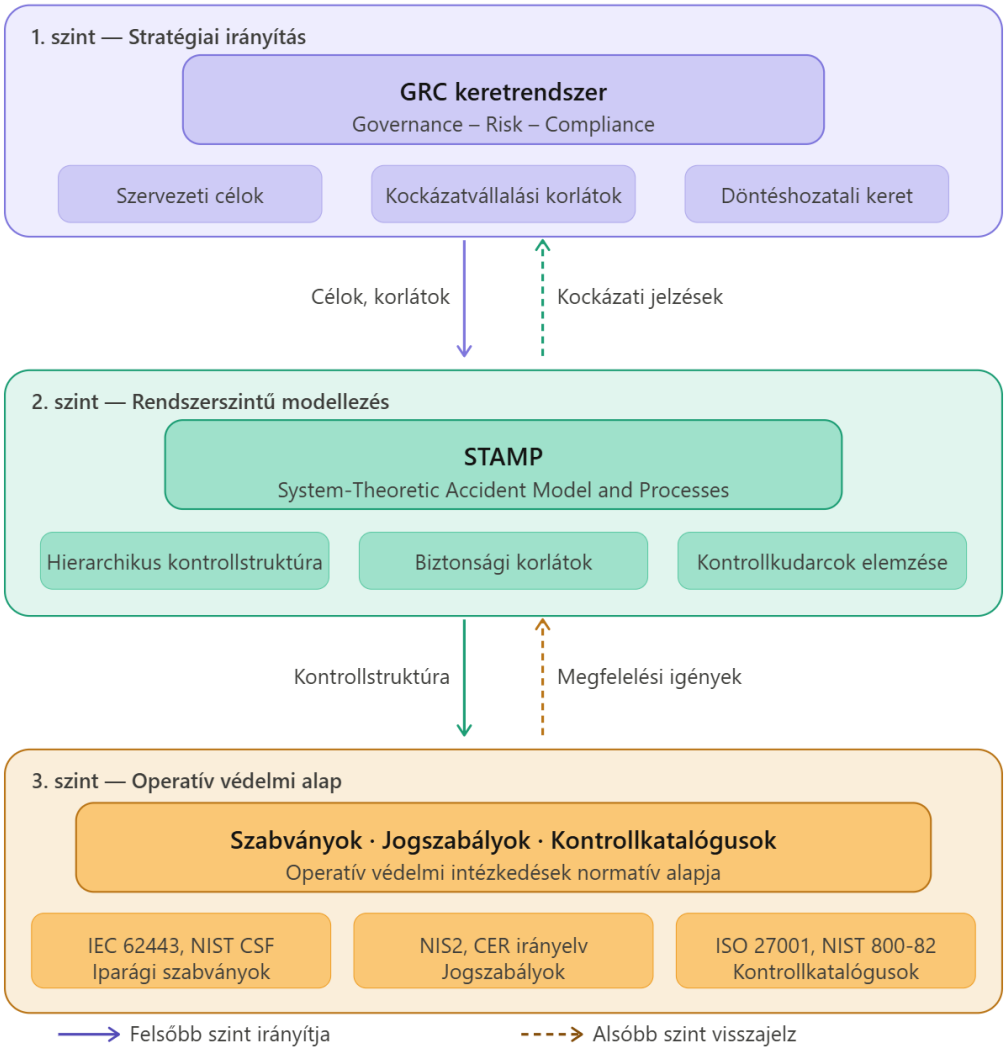
A nemzetközi szabványok GRC keretrendszerbe történő illesztése során kiemelt jelentőséggel bír a rendszerszemléletű megközelítés alkalmazása, amely lehetővé teszi a különböző szabályozási és irányítási elemek egységes struktúrába rendezését. E tekintetben releváns az Engineering a Safer World című műben bemutatott STAMP (System-Theoretic Accident Model and Processes) modell, amely a biztonságot nem a hibák hiányaként, hanem a rendszer viselkedését meghatározó biztonsági korlátok érvényesüléseként értelmezi. A modell alapfeltevése szerint a balesetek elsődleges oka nem az egyes komponensek meghibásodása, hanem a hierarchikus kontrollstruktúrák elégtelen működése és a biztonsági korlátok nem megfelelő érvényesítése.

Ez a megközelítés szoros párhuzamba állítható a GRC keretrendszerrel, amely a szervezeti működést szintén egy több szintből álló, kontrollalapú rendszerként írja le. A governance funkció kijelöli a szervezeti célokat és működési kereteket, a kockázatkezelés a bizonytalanságok hatásait értelmezi és kezeli, míg a compliance biztosítja a meghatározott korlátok betartását. Ennek megfelelően a STAMP modellben megjelenő biztonsági korlátok megfeleltethetők a GRC rendszerben alkalmazott jogszabályi, szabványi és kockázati követelményeknek, amelyek meghatározzák a szervezet elfogadható működési tartományát. A GRC keretrendszer értelmezhető a rendszerszemléletű biztonsági modellek, különösen a STAMP szervezeti szintű kiterjesztéseként.

A két megközelítés közös alapja a korlátalapú (constraint-based) gondolkodás, amely szerint a biztonság nem az egyes események közvetlen kontrolljával, hanem a rendszer viselkedésének

szabályozásával biztosítható. E szemlélet különösen alkalmassá teszi a nemzetközi szabványok, például az ipari kiberbiztonsági és információbiztonsági keretrendszerek, GRC struktúrába történő integrálására, mivel azok lényegében a működési korlátok és kontrollmechanizmusok formalizált megjelenési formáinak tekinthetők. [19]

A STAMP és a GRC modellek ilyen módon történő együttes értelmezése lehetőséget teremt arra, hogy a szabványokban megfogalmazott követelmények ne elszigetelt előírásokként, hanem egy egységes, hierarchikus kontrollrendszer elemeiként kerüljenek alkalmazásra. Ez nemcsak a megfelelőség biztosítását támogatja, hanem megalapozza a biztonságirányítási rendszer mérhetőségét és fejleszthetőségét is, mivel a kontrollok és korlátok teljesülése objektív módon értékelhetővé válik a GRC keretrendszerben alkalmazott mérőszámok és visszacsatolási mechanizmusok segítségével.
A bemutatott összefüggések rendszerszintű értelmezését a következő ábra szemlélteti, amely a GRC keretrendszer, a STAMP modell, valamint az operatív kockázatelemzési módszerek egymásra épülő, hierarchikus kapcsolatát mutatja be.



2. ábra A keretrendszerek egymásra épült hierarchiája, készítette a szerző MI promt által

Ennek megfelelően a BIR értelmezhető a GRC keretrendszer egy szűkebb, domain-specifikus implementációjaként, amely elsősorban a safety dimenzióra koncentrál, és kevésbé jeleníti meg a teljesítményorientált megközelítést. A rendszer működése ugyanakkor jól leírható a rendszerszemléletű biztonsági modellek, különösen a Engineering a Safer World által bevezetett STAMP modell segítségével, amely lehetőséget ad a kontrollmechanizmusok hatékonyságának és kölcsönhatásainak mélyebb elemzésére.

1.6 GRC alapú biztonságirányítás mérhetősége és érettségi modellje

Egy gyártási ágazatban működő modern szervezet működésének védelme, valamint komplex irodai és ipari rendszerei biztonságának hatékony irányítása nem valósítható meg megfelelő mérési és értékelési mechanizmusok nélkül. A biztonságirányítás eredményességének vizsgálata túlmutat a hagyományos „checklist" szintű ellenőrzéseken és egyre inkább a szervezeti működés átfogó teljesítményének értékelésére irányul. A hagyományos megfelelőségi szemlélet gyakran bináris logikát követ: egy követelmény teljesül vagy nem teljesül. Ez az auditálhatóság szempontjából hasznos, de nem ad kellően árnyalt képet a szervezet tényleges biztonsági képességéről. Egy kontroll formálisan létezhet, de működése lehet esetleges, nem dokumentált, nem mért vagy nem integrált más folyamatokkal. Ezzel szemben az érettségi modell fokozatos fejlődési állapotokat különböztet meg, és lehetővé teszi annak értékelését, hogy a szervezet mennyire képes ismételhető, mérhető, adaptív és folyamatosan fejlesztett módon kezelni a biztonsági kockázatokat. A GRC megközelítés, különösen az OCEG által kidolgozott koncepció, olyan keretet biztosít, amely lehetővé teszi a biztonságirányítás mérhetőségének és érettségének strukturált értelmezését.

A GRC modell központi eleme a „principled performance", amely a szervezeti teljesítményt nem kizárólag operatív vagy gazdasági dimenzióban értelmezi, hanem figyelembe veszi a kockázatok és kötelezettségek teljesítését is. Ennek megfelelően a biztonságirányítás mérhetősége csak akkor értelmezhető teljeskörűen, ha az a szervezeti célok, a kockázati kitettség és a megfelelési állapot együttes vizsgálatán alapul.
Az érettségi modellek alkalmazása lehetővé teszi a biztonságirányítási rendszerek fejlettségének és hatékonyságának összehasonlítható értékelését. A veszélyes anyagokkal foglalkozó üzemek esetében ez különösen fontos, mivel a formális megfelelés önmagában nem garantálja a tényleges biztonsági szintet.
A GRC alapú megközelítésben az érettség nem csupán a szabályok meglétére, hanem azok működésének minőségére és integráltságára vonatkozik. Ennek megfelelően az alábbi, egymásra épülő érettségi szintek különböztethetők meg:

- kezdeti (ad hoc) szint, ahol a biztonsági intézkedések eseti jellegűek és nem strukturáltak;
- megfelelés-orientált szint, ahol a szervezet teljesíti a jogszabályi követelményeket, azonban a működés elsősorban dokumentáció-központú fajsúlyosabb az adminisztratív rész;

- kockázatalapú szint, ahol a döntéshozatal már a kockázatok figyelembevételével történik;
- integrált szint, ahol a biztonság a szervezeti működés szerves részévé válik, és a különböző dimenziók koordináltan működnek;
- adaptív (reziliens) szint, ahol a szervezet képes a változó környezethez dinamikusan alkalmazkodni, és a visszacsatolások alapján folyamatosan fejleszti működését.

Ez a megközelítés túlmutat a hagyományos auditálási szemléleten, és lehetővé teszi a biztonságirányítás fejlődési pályájának meghatározását. A GRC-alapú érettségi értékelés lehetővé teszi, hogy a szervezet azokat a területeket azonosítsa, ahol a kockázati kitettség és az érettségi hiány együttesen a legnagyobb veszélyt jelenti. [31]

Az OCEG modell egyik fontos kiterjesztése a „total performance” fogalma, amely a szervezeti teljesítményt többdimenziós módon értelmezi. Iparbiztonsági kontextusban ez különösen releváns, mivel a biztonság nem választható el a működés egyéb aspektusaitól.

A total performance dimenziói az alábbi fő területekre bonthatók:

- operatív teljesítmény, amely az üzemeltetés folyamatosságát és hatékonyságát jelenti;
- biztonsági teljesítmény, amely a balesetek megelőzésére és a kockázatok csökkentésére irányul;
- megfelelési teljesítmény, amely a jogszabályi és szabványi követelmények teljesítését méri;
- kockázati teljesítmény, amely a bizonytalanság kezelésének hatékonyságát értékeli;
- szervezeti integritás és bizalom, amely a működés hitelességét és társadalmi elfogadottságát tükrözi. [7]

A veszélyes üzemek esetében e dimenziók szoros kölcsönhatásban állnak, és együttesen határozzák meg a rendszer biztonságát és fenntarthatóságát. Iparbiztonsági kontextusában a Total Performance megközelítés értelmezhető safety, security, compliance és governance dimenziók integrált rendszerében.

A biztonságirányítás mérhetőségének gyakorlati megvalósítását egy integrált indikátorrendszer biztosítja, amely egyaránt tartalmaz teljesítmény-, kockázati és kontrollmutatókat.

KPI (Key Performance Indicator):

Ez a mozakiszó talán a leginkább elterjedt a magyar nyelvben a három indikátor rendszer közül, bár leginkább a sales és marketing üzletágakban szokás itthon használni, valójában sokkal széleskörűbben alkalmazható megközelítés. A kulcs teljesítménymutatók (KPI) a biztonságirányítás mérési rendszerének alapvető elemei, amelyek a szervezet működésének eredményességét, valamint a kitűzött célok teljesülésének mértékét írják le. A KPI-k elsődleges szerepe, hogy objektív, kvantifikálható módon támogassák a teljesítmény értékelését, valamint lehetővé tegyék a szervezeti működés időbeli összehasonlítását és fejlesztését. Olyan célorientált mutatók, amelyek közvetlen kapcsolatban állnak a szervezet stratégiai és operatív céljaival. Önmagukban nem értelmezhetők, mindig az adott célokkal vagy elvárt állapottal kell összevetni őket. A legjellemzőbb célok egy veszélyes anyagokkal foglalkozó üzem esetén, például a működésfolytonosság és a balesetmegelőzések lehetnek, valamint az IT – OT rendszerek magasszintű rendelkezésre állása és biztonságos üzemeltetése.

A hatékony KPI-k kialakítása során a szakirodalom több alapvető tulajdonságot határoz meg. A KPI-knek mindenekelőtt egyértelműen definiáltnak kell lenniük, vagyis pontosan meg kell határozni, hogy mit mérnek és milyen módszerrel. Emellett elengedhetetlen a mérhetőség, amely biztosítja, hogy az indikátorok objektív, kvantifikálható adatokon alapuljanak. A KPI-knek továbbá relevánsnak kell lenniük, azaz közvetlen kapcsolatban kell állniuk a szervezet céljaival és kritikus folyamataival.
A stratégiai KPI-k a szervezet átfogó céljainak teljesülését mérik, és elsősorban a felsővezetői döntéshozatal támogatására szolgálnak. Ezek hosszabb időtávon értelmezhetők, és olyan mutatókat foglalnak magukban, mint például a működési hatékonyság, a megbízhatóság vagy a biztonsági teljesítmény aggregált szintje. Iparbiztonsági környezetben ide sorolható például a súlyos események előfordulási gyakorisága vagy a teljes rendszer rendelkezésre állása. Az operatív KPI-k ezzel szemben rövidebb időtávon értékelik a működést, és közvetlenül az üzemeltetési folyamatok hatékonyságára fókuszálnak. Ilyen mutatók lehetnek például a karbantartási feladatok végrehajtási ideje, az üzemzavarok gyakorisága, vagy a hibajavítási ciklusidők. Ezek a KPI-k közvetlen visszacsatolást biztosítanak az operatív működés számára.

A funkcionális KPI-k egy-egy szervezeti területhez – például karbantartás, információbiztonság vagy üzemeltetés – kapcsolódnak, és az adott funkció teljesítményét mérik. Ezek a mutatók egyaránt lehetnek stratégiai vagy operatív jellegűek, attól függően, hogy milyen időtávon és milyen célhoz kapcsolódnak. A KPI-k értelmezése során kiemelt jelentőséggel bír a vezető (leading) és késleltetett (lagging) indikátorok megkülönböztetése. A vezető indikátorok

előrejelző jellegűek, és a jövőbeni teljesítményre vagy kockázatokra utalnak, míg a késleltetett indikátorok a már bekövetkezett események eredményeit tükrözik. A hatékony biztonságirányítás mindkét típus együttes alkalmazását igényli, mivel ez teszi lehetővé a proaktív és reaktív megközelítések egyensúlyát.

A KPI-k alkalmazása gyakran strukturált keretrendszerekben valósul meg, amelyek támogatják a célok és mérőszámok összehangolását. Ilyen megközelítés például a célok szerinti irányítás (Management by Objectives – MBO), amely a szervezeti célokat egyéni szintre bontja le, vagy az Objectives and Key Results (OKR) modell, amely konkrét célokhoz rendelt mérhető eredményeken keresztül biztosítja a teljesítmény nyomon követését. Hasonlóan releváns a Balanced Scorecard megközelítés, amely a szervezeti teljesítményt több nézőpontból, például pénzügyi, működési, belső folyamatok és tanulás-fejlődés, értékeli, és ezekhez rendel KPI-ket. Fontos követelmény a folyamatos monitoring, amely lehetővé teszi az időbeli változások és trendek elemzését, valamint a teljesítmény folyamatos értékelését. Végül a KPI-knek döntéstámogató jelleggel is rendelkezniük kell, vagyis alkalmasnak kell lenniük arra, hogy konkrét beavatkozásokat és fejlesztési intézkedéseket alapozzanak meg. Annak érdekében, hogy egy szervezet hatékony KPI-kat állítson fel, fontos, hogy egyeztetni szükséges azokkal a személyekkel, akik a KPI-riportokat használják, annak érdekében, hogy feltárásra kerüljenek céljaik és a mutatók tervezett felhasználási módjai. Ezzel elősegítve a valóban releváns és hasznos mutatók létrehozását. A KPI-kat stratégiai célokhoz szükséges kapcsolni, hogy illeszkedjenek az átfogó stratégiai célrendszerhez, még abban az esetben is, ha azok egy-egy funkcionális területhez, például humánerőforrás-menedzsmenthez vagy marketinghez, kapcsolódnak.

A KPI-k akkor tekinthetők igazán hatékonynak, ha a kitűzött cél megfelel a SMART kritériumrendszernek, ami a egy mozaik szó az alábbi szavakból áll: Specific – a kitűzött céloknak konkrétnak kell lenniük, mérhetőnek (Measurable), elérhetőnek (Attainable), reálisnak (Realistic), valamint időben meghatározottnak (Time-bound) kell lenniük. Példaként említhető egy adott időszakra vonatkozó, meghatározott mértékű teljesítménynövekedés elér A kulcs teljesítménymutatók alkalmazása számos előnnyel jár a biztonságirányítás területén, különösen a veszélyes anyagokkal foglalkozó üzemek esetében, ahol a működés komplexitása és a kockázatok súlya indokolja az adatvezérelt döntéshozatalt. A KPI-k hozzájárulnak a működés átláthatóságához azáltal, hogy objektív, mérhető információkat biztosítanak a szervezet teljesítményéről. Ez lehetővé teszi a kritikus folyamatok állapotának folyamatos nyomon követését, valamint a problémás területek korai azonosítását. Emellett a megfelelően

kialakított mutatók támogatják az operatív és vezetői döntéshozatalt, erősítik az elszámoltathatóságot, valamint ösztönzik a szervezeti és egyéni szintű felelősségvállalást. A KPI-k alkalmazása a veszélyes üzemekben hozzájárulhat a biztonsági kultúra erősítéséhez is, mivel egyértelmű teljesítményelvárásokat és visszacsatolást biztosít a dolgozók számára. Ez elősegíti a tudatosabb működést és a biztonsági szempontok integrálását a napi tevékenységekbe. Továbbá a KPI-k alkalmasak annak kimutatására, hogy a bevezetett biztonsági intézkedések milyen mértékben járulnak hozzá a kockázatok csökkentéséhez és a működés stabilitásához.

Ugyanakkor a KPI-k alkalmazása számos kockázatot is hordoz, különösen akkor, ha azok nem megfelelően kerülnek kialakításra vagy értelmezésre. A túlzottan szűken meghatározott mutatók úgynevezett „tunnel vision” jelenséghez vezethetnek, amelynek következtében a szervezet kizárólag a mért indikátorokra koncentrál, miközben az infrastruktúra egészének biztonsága háttérbe szorulhat. Ez a veszélyes üzemek esetében különösen kritikus, mivel a biztonság rendszerszintű tulajdonság, amely nem redukálható néhány kiválasztott mutatóra. További problémát jelenthet, ha a KPI-k irreálisan magas célértékeket határoznak meg, amely demotiváló hatást gyakorolhat a személyzetre, vagy akár nem kívánt viselkedési mintákhoz vezethet. Ilyen esetekben előfordulhat, hogy a dolgozók a mutatók teljesítésére törekednek a tényleges biztonsági célok rovására, ami torzítja a valós teljesítményt és növelheti a kockázatokat. Hasonlóképpen, a rövid távú KPI-k túlhangsúlyozása a hosszú távú biztonsági és fenntarthatósági szempontok háttérbe szorulását eredményezheti. [32]
A túlzottan merev KPI-k emellett korlátozhatják az innovációt és a rugalmas problémamegoldást, mivel a szervezeti működést előre meghatározott mutatók mentén próbálják szabályozni. Ez különösen problémás lehet a dinamikusan változó ipari és kiber-fizikai környezetben, ahol az adaptív és preventív megközelítések elengedhetetlenek. Ennek megfelelően megállapítható, hogy a KPI-k hatékony alkalmazása a veszélyes üzemekben nem pusztán technikai kérdés, hanem a megfelelően kialakított indikátorrendszer és a szervezeti kultúra összhangját igényli. A KPI-k csak abban az esetben járulnak hozzá a biztonság növeléséhez, ha azok a rendszer egészét tükrözik, és nem torzítják a döntéshozatalt vagy a működési prioritásokat.

Az informatikai rendszerek esetén alkalmazott KPI-k lehetnek például a szerverek rendelkezésre állása és üzemideje, amely a kritikus rendszerek folyamatos működésének egyik alapvető indikátora. Hasonlóan fontos a válaszidők és késleltetés mérése, amelyek a rendszerek

terhelhetőségére és teljesítményére utalnak, és közvetve hatással lehetnek az operátori beavatkozások hatékonyságára is. A hibakezelési folyamatok értékelését támogatja az incidenskezelési vagy hibajegy-kezelési idő (ticket resolution time), amely a problémák elhárításának gyorsaságát jelzi.

A veszélyes anyagokkal foglalkozó üzemek esetében ezek a mutatók nem pusztán informatikai teljesítményindikátorokként értelmezhetők, hanem a folyamatbiztonságot közvetetten befolyásoló tényezőkként is. Az IT rendszerek és az OT rendszerek egyre szorosabban kapcsolódnak egymáshoz, a teljes termelési folyamatciklusban mindkét környezet rendszereinek meg van a saját szerepük, így a teljesítménybeli eltérések akár közvetlen biztonsági kockázatokat is generálhatnak.

KRI (Key Risk Indicator):

Olyan mérőszámok, amelyek a szervezet aktuális és jövőbeli kockázati kitettségének alakulását írják le, és lehetővé teszik a potenciális veszélyek korai azonosítását (például a kritikus hibák gyakorisága vagy a rendszerterhelés). A KRI-k elsődleges célja nem csupán a bekövetkezett események utólagos értékelése, hanem a kockázati profil változásának folyamatos nyomon követése, a sérülékenységek feltárása, valamint a megelőző intézkedések időbeni elindításának támogatása. Ennek megfelelően a KRI-k a folyamatos kockázatmonitoring eszközeként értelmezhetők, amelyek kapcsot képeznek az operatív működés és a stratégiai döntéshozatal között. Fontos, hogy a KRI-k kialakítása során az egymással összefüggő paraméterek egyidőben jelenjenek meg. A jó KRI-k relevánsak, mérhetők, és objektívek. További fontos jellemzőjük, hogy időszerűek, vagyis a kockázatok már a korai szakaszban észlelhetőkké váljanak és ezt egészíti ki a prediktív jelleg az előrejelzés érdekében.

A hatékony alkalmazhatóság miatt a mutatóknak küszöbértékekkel és riasztási szintekkel kell rendelkezniük, amelyek egyértelmű döntési pontokat biztosítanak a szervezet számára.

További lényeges követelmény a rendszeres felülvizsgálhatóság és adaptálhatóság, amely biztosítja, hogy a KRI-k a változó működési és fenyegetési környezethez igazíthatók legyenek. Emellett kiemelt szerepet kap a kommunikálhatóság és érthetőség, vagyis az, hogy a mutatók a különböző szervezeti szinteken, az operatív végrehajtástól a felsővezetői döntéshozatalig, egyaránt értelmezhetők és felhasználhatók legyenek. A KRI-knek továbbá akcióorientáltnak

kell lenniük, azaz alkalmasnak kell lenniük konkrét intézkedések kiváltására, nem pusztán információszolgáltatásra.

3. ábra A kulcs kockázati indikátorok kialakításának lépései, készítette: a szerző, MI promt által [33]

Fontos hangsúlyozni, hogy a nem megfelelően kialakított KRI-k torz képet adhatnak a szervezet kockázati helyzetéről, és akár hamis biztonságérzetet is kelthetnek. Ez különösen kritikus a komplex kiber-fizikai rendszerek esetében, ahol a kockázatok gyakran nem közvetlenül, hanem közvetett indikátorokon keresztül jelennek meg.
Gyakorlati példák a KRI-kre, a szakirodalom a KRI-ket több kategóriába sorolja, amelyek segítségével lefedhető a szervezet komplex működési struktúrája.

Pénzügyi dimenzióban a KRI-k a szervezet gazdasági stabilitásával és kitettségével kapcsolatos kockázatokat írják le. Ilyen mutató például a likviditási ráta (forgóeszköz/rövid lejáratú kötelezettség), amely a rövid távú kötelezettségek teljesíthetőségét jelzi, az adósság/tőke arány, amely a finanszírozási struktúra kockázataira utal, vagy a bevételkoncentráció mértéke, amely egyes kulcsügyfelektől való függőséget mutatja.

Az operatív dimenzióban a KRI-k a működés folytonosságát és megbízhatóságát érintő kockázatokra fókuszálnak. Ide sorolható például a berendezések kiesési ideje, amely

közvetlenül hat a termelési folyamatokra, a készletszintek alakulása, amely az ellátási lánc stabilitását befolyásolja, valamint a munkaerő fluktuációja, amely a szervezeti tudás és kompetencia megtartásának kockázatait jelzi.

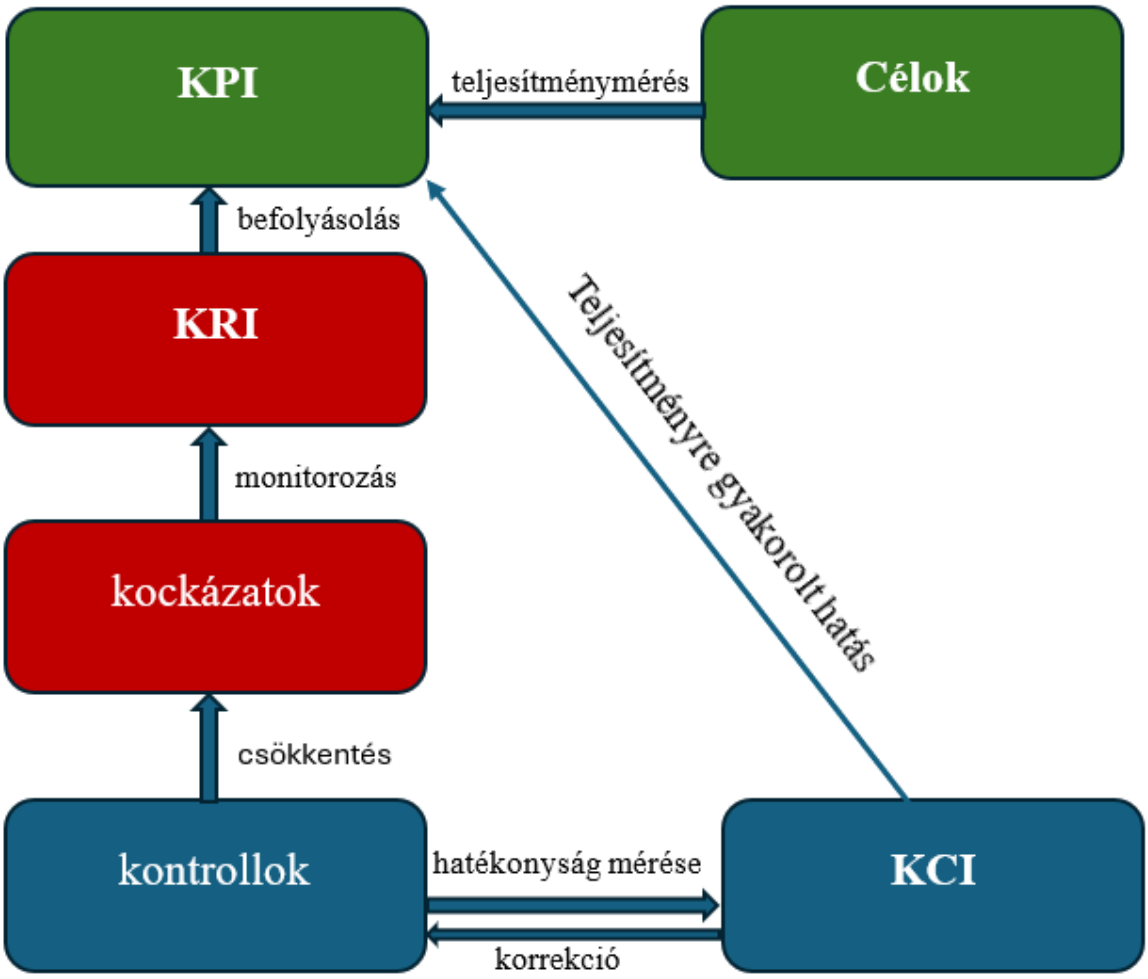
A megfelelési dimenzióban a KRI-k a jogszabályi és szabványi követelmények teljesülésével kapcsolatos kockázatokat mérik. Ilyen mutatók lehetnek a szabályozás megsértéseinek száma, az auditmegállapítások jellege és darabszáma, valamint az információbiztonsági incidensek vagy adatvédelmi események előfordulása. [33]

Az integrált megközelítésben a KRI-k szoros kapcsolatban állnak a KPI-okkal és a KCI-kkel. Míg a KPI-k a szervezet teljesítményét és célmegvalósítását mérik, addig a KRI-k a potenciális eltérések és veszélyek előrejelzésére szolgálnak, a KCI-k pedig a kontrollmechanizmusok működésének hatékonyságát értékelik. Amennyiben a kockázati mutatók kedvezőtlen irányba változnak, úgy ehhez kapcsolódó teljesítménycélok határozhatók meg, és a kontrollok hatékonysága is célzottan vizsgálható. A veszélyes anyagokkal foglalkozó üzemek esetében ez különösen fontos, mivel a pénzügyi, operatív és megfelelési kockázatok közvetlen hatással lehetnek a folyamatbiztonságra és a lakosság védelmére. Ennek megfelelően a KRI-k kialakítása során elengedhetetlen a különböző dimenziók integrált kezelése.

KCI (Key Control Indicator):

A KCI a szervezet védelmi intézkedéseinek hatékonyságát méri és követi nyomon. A KCI-k mérésének relevanciájához elengedhetetlen, hogy azok kapcsolódjanak egyrészt magához a kontrollhoz, másrészt ahhoz a kockázathoz is, amely mitigálása érdekében az adott védelmi intézkedés bevezetésre került, ennek értelmében a KCI-knek mind a KPI-okhoz, mind a KRI-khoz kötődniük kell.

A KCI-k általában több kontrollhoz kapcsolódnak egyszerre, ahogyan a KRI-k is jellemzően több kockázatot fednek le, és egy KPI-hoz több KRI is tartozhat. Ez egy egymásba ágyazott, ökoszisztémaszerű rendszert alkot.



GRC alapú indikátorrendszer

4. ábra Az indikátorok egymásra hatása a GRC meta-keretben, készítette: a szerző

Egy konkrét példán keresztül illusztrálva: ha egy KPI új földrajzi piacra való terjeszkedést céloz meg, és ehhez két KRI is kapcsolódik (pl. szabályozási megfelelés kockázata és bennfentes fenyegetések kockázata), akkor ezekhez kontrolok kerülnek bevezetésre, például külső szakértők bevonása a jogszabályi változások monitorozására, illetve technológiai és adatvédelmi megoldások, amelyek hatékonyságát a KCI-k mérik. [34]

E három indikátortípus integrációja lehetővé teszi a biztonságirányítás átfogó értékelését, és támogatja a döntéshozatalt mind operatív, mind stratégiai szinten. Az indikátorrendszerek alkalmazása nem iparág-specifikus, hanem általános irányítási eszköz, amely megfelelő adaptáció mellett az iparbiztonsági környezetben is hatékonyan alkalmazható.

1.6.1 Veszélyes üzemek biztonsági irányítási rendszere hatékonyságának lehetséges mérése

Veszélyes anyagokkal foglalkozó üzemek esetén a gyakorlatban javasolt olyan integrált indikátorrendszert kialakítani, amik kiemelten képesek kezelni azokat a területeket, ahol a üzembiztonsági (safety) és kiberbiztonsági (security) szempontok konfliktusba kerülhetnek. Az OT sérülékenységmenedzsment területén a hagyományos, kizárólag IT-szemléletű KPI-ok korlátozottan alkalmazhatók. Egy olyan mutató, mint például a „kritikus sérülékenységek javítása 15 napon belül", veszélyes ipari üzemekben önmagában nem tekinthető megfelelő teljesítménymérőnek, mivel egy validálatlan biztonsági frissítés technológiai vezérlőrendszerre történő telepítése a kiberkockázat csökkentése mellett akár új safety kockázatokat is előidézhet. Ugyanakkor az sem tekinthető elfogadható megközelítésnek, ha a szervezet a technológiai folyamatok biztonságára hivatkozva határozatlan ideig elhalasztja az ismert sérülékenységek kezelését. A kiber-fizikai környezetben ezért a sérülékenységkezelésnek kockázatarányos, validációhoz kötött és a technológiai folyamatok működési sajátosságait figyelembe vevő megközelítésen kell alapulnia. [2]

Az indikátorok kialakításánál fontos elv, hogy azok ne idézzenek elő nem kívánt szervezeti magatartást. Például, ha a szervezet kizárólag az incidensek számának csökkentését méri, akkor az aluljelentés kockázata növekedhet. Ha kizárólag a gyors patch-elést méri, akkor a validáció és a safety-impact elemzés kerülhet háttérbe. Ha kizárólag a megfelelési hiányosságok számát méri, akkor a szervezet a valós kockázatok feltárása helyett a dokumentáció és az adminisztratív intézkedések kozmetikai javítására koncentrálhat. Ezért az indikátorokat mindig kiegyensúlyozott módon, egymással összefüggésben kell értelmezni. [35]

Egy veszélyes anyagokkal foglalkozó üzem integrált biztonságirányítási rendszerében a mérhetőség nem korlátozódhat kizárólag technikai kiberbiztonsági teljesítménymutatók alkalmazására. Indokolt olyan komplex indikátorrendszer kialakítása, amely egyidejűleg képes támogatni a kiberbiztonsági, az üzem- és technológiai folyamat biztonsági, az üzemfolytonosság, valamint a szervezeti governance és compliance folyamatok értékelését.

Egy lehetséges integrált indikátorrendszer a következő területeket foglalhatja magában:

- kritikus OT vagyonelemek nyilvántartásának teljessége és naprakészsége,
- az OT rendszerek zóna- és konduitalapú szegmentációs lefedettsége,
- a távoli hozzáférések szabályozottsága és monitorozottsága,

- a kritikus sérülékenységek kockázatértékelési aránya,
- a kompenzáló kontrollokkal kezelt sérülékenységek aránya,
- a safety kritikus változtatások előzetes jóváhagyási aránya,
- az incidensészlelési és reagálási idő,
- az OT naplózási, monitorozási és eseménykorrelációs lefedettség,
- a beszállítói és külső partneri kiberbiztonsági értékelések aránya,
- a hatósági és belső auditmegállapítások lezárási ideje,
- az OT-specifikus biztonságtudatossági képzések és gyakorlatok teljesítési aránya,
- a reziduális kockázatok vezetői felülvizsgálatának rendszeressége.

A felsorolt indikátorok együttesen képesek támogatni az integrált biztonságirányítás működésének értékelését, valamint a kiberbiztonsági és safety szempontok közötti egyensúly fenntartását a veszélyes ipari környezetben.

A biztonságirányítás integrált megközelítése nem korlátozódhat a technikai és szabályozási aspektusokra, hanem ki kell terjednie a szervezeti működés etikai és kulturális dimenzióira is. Ebben a kontextusban kiemelt szerepet kaphat például az ISO 37001, amely a korrupció megelőzésére és az etikus működés biztosítására fókuszál. [36]

Egy formálisan megfelelően kialakított biztonsági rendszer is sérülékennyé válhat, ha a szervezeti kultúra nem támogatja a szabályok betartását, vagy ha a döntéshozatal során rövid távú érdekek felülírják a biztonsági szempontokat.

1.6.2 A szervezeti integritás, mint biztonsági faktor

A GRC megközelítés hangsúlyozza, hogy a szervezeti integritás nem csupán etikai kérdés, hanem a kockázatkezelés és a biztonság alapvető eleme. Belső szinten a hitelesség azt jelenti, hogy a szervezet működése összhangban áll a deklarált értékekkel és szabályokkal, míg külső szinten a szervezet megbízható és transzparens módon viselkedik az érintettek, így különösen a környező lakosság és a szabályozó hatóságok, irányába. A szervezet csak akkor tekinthető fenntarthatónak és hitelesnek, ha nemcsak teljesít és kockázatot kezel, hanem következetesen betartja az önkéntes és kötelező vállalásokat is. Az integritás értelmezhető a szervezet által tett és ténylegesen betartott vállalások közötti összhang mértékeként. Ebben az értelemben az integritás nem pusztán etikai kategória, hanem a szervezeti működés

konzisztenciájának és hitelességének mérőszáma, melynek aránya az alábbi ábrával szemléltethető:

$$integritás = \frac{\text{betartott vállalások}}{tett\ vállalások}$$

Ez a kettős értelmezés különösen releváns a veszélyes anyagokkal foglalkozó üzemek esetében, ahol a szervezeti működés közvetlen hatással van a környező lakosság biztonságára és bizalmára. A lakosság felé történő hiteles kommunikáció, a kockázatok átlátható kezelése, valamint a biztonsági intézkedések következetes alkalmazása nem csupán jogszabályi kötelezettség, hanem a társadalmi elfogadottság és a működési legitimitás alapfeltétele is.

A GRC megközelítés hangsúlyozza, hogy a szervezeti integritás nem csupán etikai kérdés, hanem a kockázatkezelés és a biztonság alapvető eleme. Az önként vállalt normák és értékek, amelyek túlmutatnak a jogszabályi kötelezettségeken, hozzájárulnak a biztonsági kultúra erősítéséhez és a transzparenciával kapcsolatos kockázatok csökkentéséhez.

A fejezetben bemutatott elemzések alapján megállapítható, hogy a felső és alsó küszöbértékű veszélyes anyagokkal foglalkozó üzemekre vonatkozó szabályozási és irányítási rendszerek összehasonlítása alkalmas a veszélyes anyagokhoz és technológiákhoz kapcsolódó kockázatok pontosabb azonosítására és strukturált kezelésére. Az eltérő szabályozási szintek követelményeinek vizsgálata rámutat arra, hogy a biztonságirányítási rendszerek hatékonysága nem csupán a megfelelőség biztosításán, hanem a kockázatokhoz illeszkedő, arányos intézkedések alkalmazásán alapul.

A nemzetközi szabványok (különösen az ipari és információbiztonsági keretrendszerek) által meghatározott irányítási elvek, valamint a PDCA/PDSA ciklus alkalmazása lehetővé teszi a biztonságirányítás folyamatos fejlesztését, visszacsatolását és adaptív működését. A GRC megközelítésben ez a ciklikusság a LAPR (Learn – Align – Perform – Review) modell formájában értelmezhető, amely a szervezeti tanulást, az összehangolt működést és a folyamatos visszacsatolást helyezi középpontba. Ennek megfelelően megállapítható, hogy a GRC-alapú biztonságirányítás nem csupán integrálja az irányítási, kockázatkezelési és megfelelőségi dimenziókat, hanem azok ciklikus, folyamatos fejlesztését is biztosítja. A LAPR modell alkalmazása lehetővé teszi a biztonsági intézkedések hatékonyságának rendszeres értékelését és finomhangolását, ezáltal támogatva az adaptív működést és a kockázatok dinamikus kezelését. [7]

A kutatás eredményei alapján megállapítható, hogy a GRC szemlélet alkalmas keretet biztosít ezen követelmények egységes kezelésére. A GRC-alapú megközelítés integrálja:

- az irányítási (governance) struktúrákat és döntési mechanizmusokat,
- a kockázatkezelési (risk) folyamatokat,
- valamint a jogszabályi és szabványi megfelelőségi (compliance) követelményeket.

Ez az integrált szemlélet biztosítja, hogy a biztonságirányítási rendszer ne elszigetelt elemekből álljon, hanem egy mérhető, auditálható és fejleszthető rendszerként működjön. A GRC keretrendszer alkalmazása továbbá lehetővé teszi érettségi modellek kialakítását, amelyek révén a szervezetek objektív módon értékelhetik saját biztonsági szintjüket, valamint meghatározhatják a fejlesztési irányokat.

1.6.3 Az iparbiztonsági hatósági munka hatékonyságának növelése

Megállapítható, hogy a GRC meta keretrendszer alkalmazása a veszélyes anyagokkal foglalkozó üzemekben közvetlen módon támogatja a katasztrófavédelmi hatóság felügyeleti és ellenőrzési tevékenységét. Az integrált irányítási, kockázatkezelési és megfelelőségi struktúra révén a hatóság átfogóbb és strukturáltabb képet kap az üzem működéséről, beleértve a kritikus folyamatokat, a kulcsbeszállítói függőségeket, a kockázati kitettséget, valamint az alkalmazott védelmi intézkedések teljeskörű rendszerét.

A GRC-alapú megközelítés lehetővé teszi a kockázatkezelési intézkedések és azok végrehajtásának nyomon követését, ezáltal nem csupán a dokumentált megfelelőség, hanem a tényleges működés is értékelhetővé válik. Az indikátoralapú működés (KPI–KRI–KCI) révén a hatóság képes azonosítani a kockázati trendeket, valamint a kontrollok hatékonyságának változásait, ami megalapoz egy pontosabb adatszolgáltatást és preventív beavatkozást, amennyiben szükséges.

További előny, hogy a belső és független auditok eredményei strukturált formában integrálhatók a rendszerbe, így a hatósági ellenőrzések célzottabbá válhatnak. Ennek eredményeként az iparbiztonsági szempontból releváns hiányosságok hatékonyabban azonosíthatók és ellenőrizhetők, ami növeli az ellenőrzések hatékonyságát és csökkenti az adminisztratív terhelést.

A GRC alkalmazása emellett elősegíti a kockázatalapú hatósági felügyelet megvalósítását is, mivel lehetőséget biztosít arra, hogy az ellenőrzési erőforrások a legnagyobb kockázatot jelentő

területekre koncentrálódjanak. Ez összhangban áll a modern katasztrófavédelmi megközelítéssel, amely a megelőzésre, a reziliencia növelésére és a rendszerszintű kockázatok kezelésére helyezi a hangsúlyt. Az érintett szervezet korábbi belső vagy független auditjai során feltárt üzembiztonsággal kapcsolatos hiányosságokat a hatóság célzottan tud visszaellenőrizni.

A GRC meta keretrendszer nem biztosít közvetlen, folyamatos információáramlást a hatóság számára, ugyanakkor jelentősen növeli az ellenőrzések hatékonyságát azáltal, hogy a szervezeti működéshez kapcsolódó kockázatok, kontrollok és teljesítménymutatók strukturált és átlátható formában állnak rendelkezésre. Ennek eredményeként a hatóság a helyszíni ellenőrzések és dokumentációvizsgálatok során célzottabban képes azonosítani a kritikus területeket, valamint kockázatalapú módon priorizálni felügyeleti tevékenységét.

Azon üzemek, melyek GRC meta keretet alkalmaznak, azok a hatóság számára nem több adatot, hanem jobb minőségű, strukturált és kockázatalapúan értelmezhető információt képesek biztosítani.

1.7 Fejezet részkövetkeztetései

1. A hipotézisben megfogalmazott állítás, miszerint a szabályozási rendszerek összehasonlítása és a nemzetközi irányítási modellek alkalmazása növeli az üzemeltetés biztonságát és csökkenti a baleseti kockázatokat, a GRC-alapú megközelítés keretében igazolható. A GRC nem csupán támogatja, hanem strukturált, transzparens és mérhető módon biztosítja ezen célok megvalósulását.

2. Megállapítható, hogy a 219/2011. (X.20.) Korm. rendelet által előírt biztonsági irányítási rendszer a veszélyes anyagokkal foglalkozó üzemek esetében megfelelő alapot biztosít a súlyos ipari balesetek megelőzéséhez, azonban működése alapvetően safety- és compliance-orientált. Ennek következtében a BIR önmagában nem minden esetben alkalmas a modern, digitalizált ipari környezetben megjelenő kiber-fizikai kockázatok teljes körű kezelésére.

3. A vizsgálat alapján igazolható, hogy a GRC keretrendszer alkalmas lehet a BIR továbbfejlesztésére, mivel az irányítási, kockázatkezelési és megfelelőségi dimenziókat egységes rendszerbe rendezi. Ez különösen fontos a veszélyes üzemek esetében, ahol az életvédelmi, folyamatbiztonsági, információbiztonsági, OT-biztonsági, üzemeltetési és lakosságvédelmi szempontok egymástól explicit módon nem választhatók el.

4. A NIS2 és CER irányelvek, valamint azok hazai implementációja rámutat arra, hogy a reziliencia és a kockázatalapú működés mára az európai biztonságpolitikai és iparbiztonsági gondolkodás központi elemévé vált. Ugyanakkor azonosítható olyan szabályozási hiátus, amelyben egyes küszöbérték alatti vagy kisebb méretű, de kockázatos veszélyes üzemek kiberbiztonsági szempontból nem, vagy csak korlátozottan kerülnek lefedésre.

5. Megállapítást nyert, hogy a STAMP és a GRC nem azonos rendeltetésű modellek, azonban egymást kiegészítő módon alkalmazhatók a veszélyes üzemek biztonságirányításának értelmezésében. A STAMP a biztonság rendszerszintű, kontrollalapú magyarázatát adja, míg a GRC ennek szervezeti irányítási, kockázatkezelési és megfelelőségi keretbe illesztését támogatja. Ezáltal a GRC-alapú modell elméleti megalapozása erősíthető a STAMP rendszerszemléletével.

6. A KPI–KRI–KCI indikátorrendszer alkalmazása lehetőséget biztosít arra, hogy a biztonságirányítás ne kizárólag utólagos eseményértékelésen alapuljon, hanem preventív, kontrollorientált és fejlesztésközpontú működéssé váljon. Ezáltal a veszélyes üzemek biztonsági teljesítménye nemcsak auditálható, hanem objektív mutatók alapján folyamatosan fejleszthető is.

7. Továbbá megállapítható, hogy a szervezeti integritás, a biztonsági kultúra és az etikus működés nem kiegészítő jellegű tényezők, hanem a biztonságirányítás alapvető feltételei. A veszélyes anyagokkal foglalkozó üzemek esetében a lakosság bizalma, a transzparens kommunikáció és a vállalt kötelezettségek következetes teljesítése közvetlenül hozzájárul a társadalmi elfogadottsághoz és a működési legitimitáshoz.

2. IPARI BALESETEK KEZELÉSE, KÜLÖNÖS TEKINTETTEL A BEAVATKOZÓ ÁLLOMÁNY ÉS AZ ÉRINTETT LAKOSSÁG VÉDELMÉRE

A 21. században a fejlett világ országaiban, köztünk hazánkban is az ipari balesetek száma, noha csökkenő tendenciát mutat, számuk sosem lesz nulla. A kockázat folyamatosan jelen van, a fenyegetés bekövetkezésének valószínűsége kisebb, mint a korábbi évszázadban. Ezt az állítást hivatott alátámasztani az Európai Unió Minerva online felületén megtalálható statisztika is. [4]

Az ipari balesetek kezelésére számos módszer és eszköz áll rendelkezésre, valamint a beavatkozó állomány is naprakész ismeretekkel rendelkezik egy esetleges baleset elhárításának operatív végrehajtását tekintve. Ma, a digitális valós idejű kapcsolatok és digitális eszközök számos megoldási lehetőséget kínálnak a beavatkozó állomány és a lakosság egészségének megőrzése érdekében. Azonban a digitalizációnak vannak árnyoldalai, melyek leginkább a kibertérből érkező fenyegetések formájában manifesztálódnak. Nemcsak akkor kell körültekintően eljárni, mikor a balesetek kezelését támogató - és a lakosság és beavatkozó állomány védelmét biztosító rendszereket és eszközöket tervezik és üzemeltetik, hanem mikor ipari létesítményekben kibertámadásra utaló incidens alakul ki. Napjainkban a hálózati forgalomba becsatornázott kiber-fizikai rendszerek is közvetetten ipari balesetek kialakulásának kockázati tényezőjévé váltak.

A lakosság életének és egészségének megóvása minden állam felelősége és egyben kötelezettsége.

2.1 Lakosságvédelem a 21. században

A lakosságvédelem a 21. században különösen felértékelődött, mivel a klasszikus természeti és ipari kockázatok mellett egyre összetettebb, egymással relációban álló veszélyforrások jelentek meg, mint például a klímaváltozás hatásai, a kritikus infrastruktúrák sérülékenysége, a kiberfenyegetések, valamint a geopolitikai konfliktusok következményei. Utóbbiak, akár közvetlen, akár közvetett módon, szintén lakosságvédelmi intézkedéseket tesznek szükségessé, ideértve a tömeges migráció kezelését, az ellátási láncok zavaraiból eredő kockázatokat, vagy a hibrid fenyegetések hatásainak mérséklését. A globalizáció és az urbanizáció következtében a kockázatok hatása gyorsabban és szélesebb körben érvényesül, így egy-egy esemény rövid idő alatt jelentős lakossági érintettséget eredményezhet. Mindezek

alapján a lakosságvédelem nemcsak folyamatosan aktuális téma, hanem napjainkban komplexebb és nagyobb jelentőségű, mint korábban bármikor.

A 21. századi lakosságvédelem eszközrendszere alapvető strukturális átalakuláson ment keresztül, amelynek középpontjában a digitalizáció, a valós idejű adatfeldolgozás, valamint a hálózatba kapcsolt érzékelő- és döntéstámogató rendszerek állnak. A hagyományos, reaktív védekezési modelleket egyre inkább felváltják a prediktív, integrált és interoperábilis megoldások, amelyek a komplex kockázati környezetben, mint például a CBRN[11] események is képesek a gyors helyzetfelismerésre és az azonnali beavatkozási döntések támogatására. A modern lakosságvédelmi rendszerek így nem csupán riasztási és reagálási funkciókat látnak el, hanem kiterjedt adatgyűjtési, modellezési és kockázatbecslési kapacitásokkal is rendelkeznek, valamint prediktív képességek segítségével kockázatcsökkentő vagy elkerülő képességeket is biztosítanak. A detektálási és atmoszferikus terjedésmodellezési rendszerek képesek a veszélyes anyagok kibocsátását követően a hatások tér- és időbeli előrejelzésére, valamint a lakosságvédelmi intézkedések megalapozására.

A veszélyhelyzetek kezelése napjainkban már elválaszthatatlan az informatikai, távfelügyeleti és szimulációs technológiák alkalmazásától. Fontos hangsúlyozni, hogy a CBRN-kockázatok nem kizárólag ipari balesetek következményeként jelentkezhetnek, hanem szándékos emberi tevékenység eredményeként is. [37] A balesetek kezelését pedig már sokszor döntéstámogató rendszerek segítségével hajtják végre. Az utóbbi időben a mesterséges intelligencia a döntéstámogatási mechanizmusokban is fokozatosan megjelent.

Az Egyesült Államokban az United States Environmental Protection Agency (a továbbiakban: EPA) és más szövetségi szervek több, egymást kiegészítő technológiát alkalmaznak a veszélyes anyagok légköri kibocsátásának észlelésére és modellezésére. Az egyik kiemelt eszköz az ASPECT (Airborne Spectral Photometric Environmental Collection Technology), amely az EPA egyedülálló, repülőgép-fedélzeti mérőrendszere. Az egy hajtóműves turbólégcsavaros repülőgépre telepített szenzor- és szoftverrendszer valós időben képes veszélyes vegyi anyagok és radiológiai ágensek detektálására, továbbá infravörös és légi képalkotási funkciókkal is rendelkezik. A rendszer tudományosan validált adatokat akár öt percen belül képes szolgáltatni, térképi megjelenítéssel együtt. Az Egyesült Államok területén legfeljebb kilenc órán belül

[11] a vegyi, biológiai, radiológiai és nukleáris eredetű veszélyekhez kapcsolódó fenyegetések, kockázatok és védelmi intézkedések összefoglaló megnevezése

bárhol bevethető, így kulcsszerepet tölt be ipari balesetek és egyéb rendkívüli események gyors felderítésében. [38]

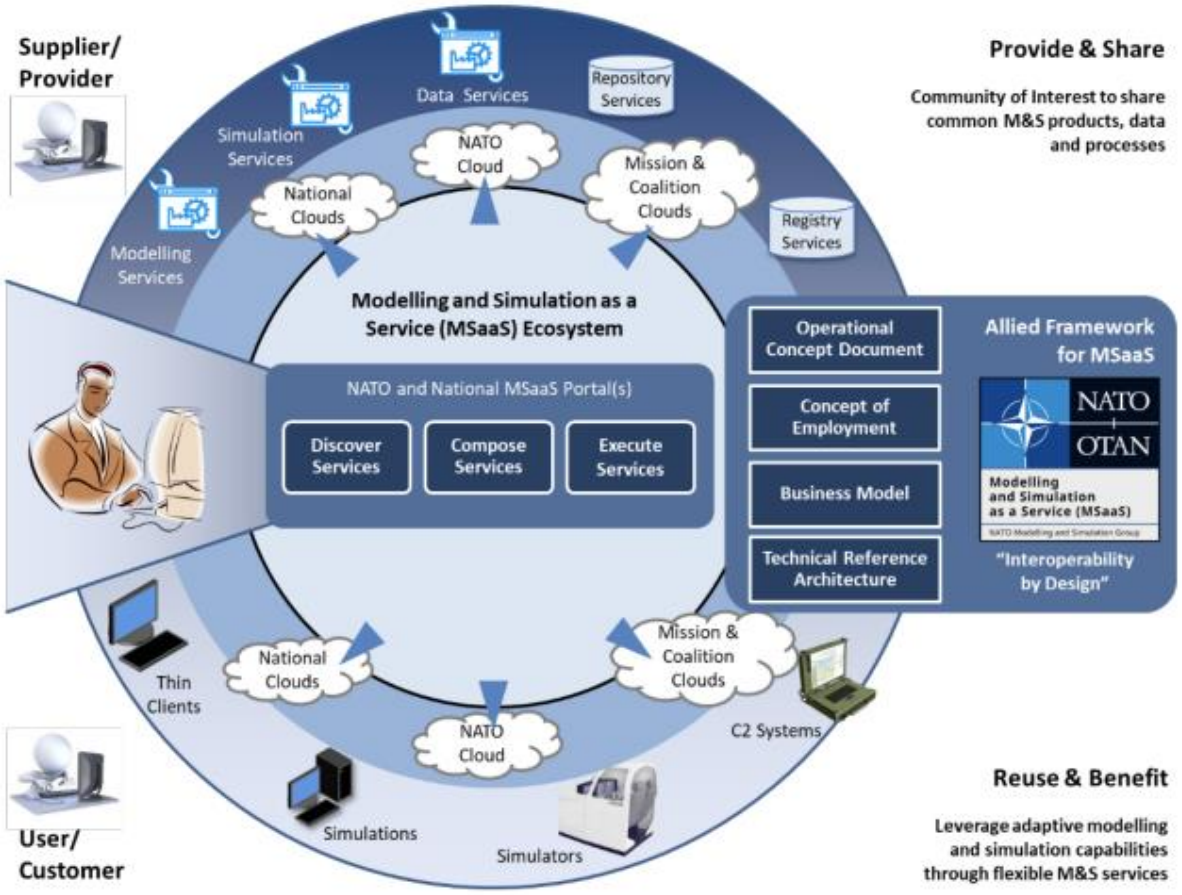
A modellezési és előrejelzési képességek terén meghatározó szerepet játszik a National Atmospheric Release Advisory Center (NARAC), amelyet a Lawrence Livermore National Laboratory (LLNL) működtet. A NARAC egy zárt, kormányzati célú rendszer, így nem található róla részletes publikus információ, amely különböző léptékű (lokális, regionális és globális) légköri terjedési modellek futtatására alkalmas. A rendszer integrálja a valós idejű meteorológiai adatokat, a földrajzi és népességi adatbázisokat, valamint az egészségügyi kockázati paramétereket (például dóziskonverziós tényezőket és védelmi határértékeket). Főbb jellemzői közé tartozik az időjárás-előrejelzés, a rugalmas térbeli felbontás, az ülepedési és csapadékképződési folyamatok modellezése, továbbá speciális algoritmusok alkalmazása robbanások vagy akár nukleáris detonációk hatásainak szimulálására. [39]

Az Európai Unió jelenleg nem rendelkezik a NARAC-hoz hasonló, teljes mértékben centralizált rendszerrel, ugyanakkor több tagállam szintű megoldás működik a CBRN-kockázatok kezelésére és a vészhelyzeti reagálás támogatására. Németország 2017-ben fejlesztett a Katasztrófavédelmi szervezete számára egy CBRN MLK nevű szoftvert, melyet 111 járműben rendszeresített. A szoftvert főleg CBRN-események operatív kezelésére, különösen veszélyes anyagok kibocsátásának modellezésére és a mérési tevékenységek koordinálására alkalmazzák. [40] A radioaktív kibocsátások légköri terjedésének modellezésére Európában több döntéstámogató rendszert alkalmaznak. A legelterjedtebbek közé tartoznak a RODOS és az ARGOS rendszerek, amelyeket számos európai ország sugárvédelmi és katasztrófavédelmi hatóságai alkalmaznak nukleáris balesetek következményeinek becslésére, a lakosságvédelmi intézkedések tervezésére és döntéstámogatásra. [41] [42]

E strukturális hiányosságok mérséklése érdekében az Európai Unió Védelmi Együttműködési Keretrendszerében, a Permanent Structured Cooperation (PESCO) égisze alatt átfogó fejlesztési program indult egy egységes, moduláris, skálázható és rugalmas CBRN-detektálási - és kockázatkezelési rendszer létrehozására. A CBRN SaaS (Surveillance as a Service) elnevezésű kezdeményezés célja, hogy szolgáltatásalapú formában biztosítson CBRN-megfigyelési és adatgyűjtési képességeket az Európai Unión belül és azon kívül végrehajtott műveletek támogatására, a rendszer csak a tagállamok számára lesz elérhető. A projektet Ausztria vezeti, Magyarország pedig aktív résztvevője a fejlesztésnek. A rendszer elsődleges célja a valós idejű helyzetkép biztosítása CBRN-események során, beleértve az azonosítást,

mintavételt és analitikai feldolgozást, így biztosítva az egységes európai szintű helyzetértékelést és döntéshozatalt. [43]

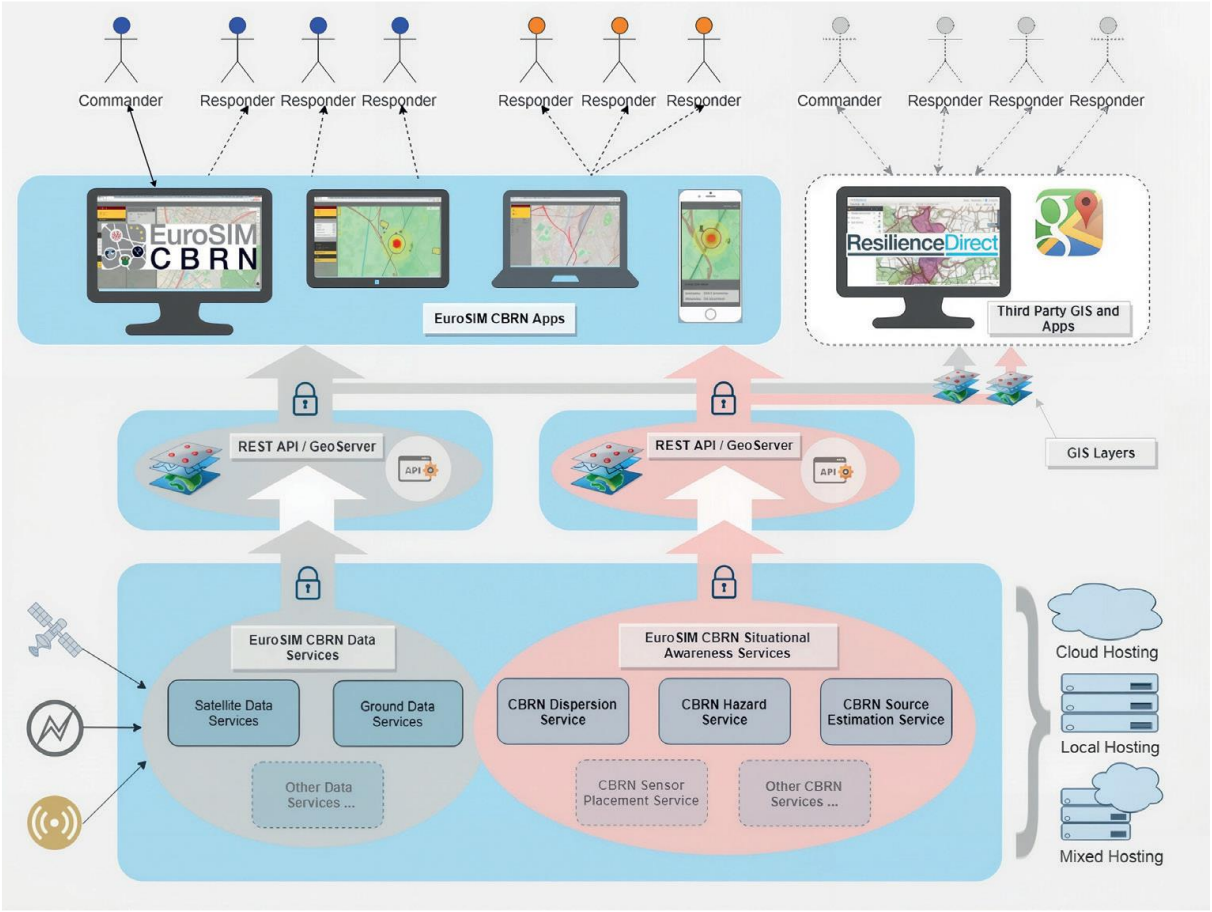
Ezzel párhuzamosan elindult az EUROSIM projekt, amely kifejezetten a képzési és szimulációs kapacitásfejlesztésre fókuszál egy közös európai szimulációs központ létrehozását tűzte ki célul Magyarországon. A kezdeményezés lehetőséget biztosít a katonai, rendvédelmi, terror-elhárító, egészségügyi és kiberbiztonsági szervezetek, valamint a civil szereplők számára, hogy integrált módon gyakorolják a válságkezelési feladatokat. Az EUROSIM informatikai architektúrája felhőalapú infrastruktúrára épül, amelyet edge computing megoldások egészítenek ki, lehetővé téve a számítási feladatok megosztását a helyi csomópontok és a központi felhő között. Ez alacsonyabb késleltetést és gyorsabb válaszidőt biztosít, ami a valós idejű szimulációk esetében kiemelt jelentőségű. [44]



5. ábra A NATO által biztosított MSaaS szolgáltatás működési architektúrája, forrás: [45]

Az EuroSIM rendszer a MSaaS (Modelling and Simulation as a Service) elvét követi, amelynek értelmében a modellezési és szimulációs képességek szolgáltatásként érhetők el a felhasználók számára. A rendszer „mesh” architektúrán alapul, amely lehetővé teszi a nemzeti

központok közvetlen, központi szervertől független kommunikációját, ezáltal magas szintű üzembiztonságot és hibatűrést biztosít. Az EuroSIM CBRN-alrendszer automatikusan gyűjti, feldolgozza és értelmezi a meteorológiai adatokat, szenzorinformációkat, űralapú megfigyelési adatokat, valamint térinformatikai rétegeket, például a népsűrűségi adatokat. A rendszer kulcseleme az UrbanAware modul, amely kifejezetten városi környezetben modellezi és szimulálja a CBRN-veszélyeket. [46] A modul képes előre jelezni a veszélyes anyagok terjedését, kijelölni a védelmi zónákat, és valós idejű döntéstámogatást nyújtani mind a mobilalkalmazáson keresztül dolgozó beavatkozók, mind a parancsnoki munkaállomások számára. A rendszer globálisan telepíthető felhőszolgáltatásként, illetve helyi vastag kliensként[12] is alkalmazható. [47]



6. ábra A rendszer magas szintű architektúra ábrája; forrás: [48]

[12] Lokálisan telepített, saját erőforrásokra támaszkodó alkalmazás, amely a feldolgozási logika jelentős részét kliens oldalon valósítja meg.

2.1.1 Lakosság katasztrófavédelmi felkészítése

Mindezek alapján a technológiai támogatás mellett kiemelt jelentőséggel bír a lakosság megfelelő felkészítése és tájékoztatása is. A lakosság katasztrófavédelmi felkészítésének célja, a helyben jellemző veszélyeztető hatások ismertetése és valós veszélyhelyzet esetén követendő magatartási szabályok megismertetése. A hatóság, valamint a vonatkozó jogszabályok a cél elérése érdekében két megközelítést alkalmaznak az aktív és passzív lakosságtájékoztatást, mindkét megközelítés alapvetően preventív jellegű védelmi intézkedések közé sorolható. [49] [50] [51]

Az aktív tájékoztatás Magyarországon a vármegyei katasztrófavédelmi igazgatóság szervezésében valósul meg a kirendeltség által. Azon települések esetén melyek I. katasztrófavédelmi osztályba kerültek besorolásra évente legalább egyszer. Budapest esetén 23 kerületből 15 kerület I. katasztrófavédelmi osztályba került besorolásra a vonatkozó jogszabály értelmében. Az aktív lakosságtájékoztatás megvalósítása több módszer és eszközrendszer alkalmazásával is lehetséges, a legelterjedtebb megoldások közé tartozik a lakossági tájékoztató kiadványok kibocsátása, melyet a katasztrófavédelem helyi szerve az érintett önkormányzat bevonásával valósít meg jellemzően. A helyi szintű médiumok segítségével is eljuttatható az érintett lakosság felé a tájékoztatás közlemények és internetes tájékoztató felületek által. Az aktív lakosságtájékoztatás megvalósulhat lakossági fórumok szervezésével, vagy egyéb nyilvános rendezvény során, mint például város- vagy falunap keretében.

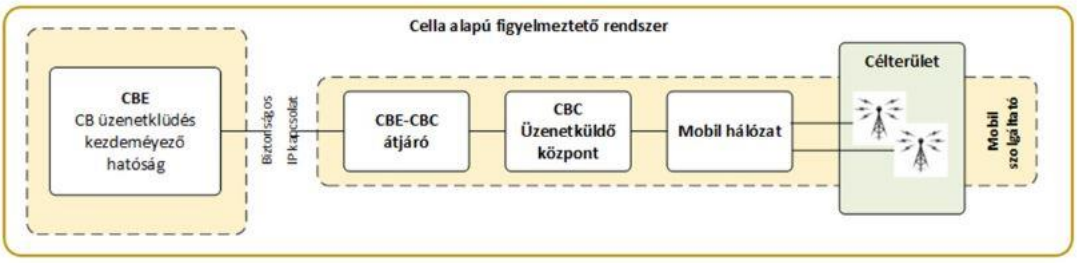
Ezzel szemben a passzív lakosságtájékoztatás nem közvetlen, azonnali elérésre épülő kommunikációs mechanizmus, hanem az információk elérhetővé tételén keresztül a lakosság önkéntes és tudatos információigényére alapoz. Az érdeklődők számára a kirendeltség legalább évente egyszer nyílt napot tart, ahol az érdeklődők információt kapnak a katasztrófavédelem rendszeréről, a kirendeltség feladatairól és felszereléséről, a települést veszélyeztető tényezőkről és hatásokról, a felkészülési - és megelőzési lehetőségekről, a bekövetkezett veszély során követendő magatartási és védelmi szabályokról. A másik formája a passzív tájékoztatásnak, hogy az érdeklődő lakosság számára tájékoztató nyomtatványokat biztosítanak, vagy elektronikusan hozzáférhető kiadványokat tesznek elérhetővé.

A lakosságvédelem egyik fontos sarokköve bekövetkezett katasztrófa esetén a hiteles és időben történő tájékoztatás, melynek eszközrendszere kiterjedt Európában.

2.1.2 Digitális lakosságtájékoztatás

Az aktív lakosság tájékoztatási módszerek közé tartozik az egyik leghatékonyabb tájékoztatási forma a cell-broadcast alapú riasztás. Az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló, az Európai Parlament és a Tanács (EU) 2018/1972 irányelve irányozza elő valamennyi tagállam részére, hogy 2022 június 21-ig vezessen be egy olyan lakossági riasztási rendszert, amely földrajzilag célzottan, mobilhálózaton keresztül képes értesíteni a lakosságot. Az irányelv technológiailag semleges álláspontot képvisel, azonban a teljesítendő követelményekre a teljeskörű megoldást leginkább a cell-broadcast technológia biztosítja. A legtöbb tagállam már működtet EU-Alert kompatibilis rendszert. A túlnyomó többség cell-broadcast alapú vagy azt is tartalmazó megoldást alkalmaz. [52] Néhány tagállam kezdetben SMS-alapú rendszert vezetett be, majd később tért át a cell-broadcast technológiára. Legalább 15 uniós tagállam aktívan használja a saját cell-broadcast technológián alapú veszélyhelyzet riasztási rendszerét. [53] Azon tagállamok, amelyek nem cell-broadcast megoldást vezettek be, SMS vagy applikációs megoldásokat alkalmaznak, vagy ezek kombinációját. Az SMS-alapú és alkalmazás-alapú riasztási megoldások eltérő hálózati architektúrára épülnek, és megbízhatósági, skálázhatósági, valamint lefedettségi szempontból nem tekinthetők egyenértékűnek a cell-broadcast technológiával.

A Cell-Broadcast technológia az alábbi ábra szerint épül fel:



7. ábra Cellbroadcast működési elve, forrás: [54]

A riasztási folyamat négy fő fázisból áll:

1. az illetékes hatóság (például a BM Országos Katasztrófavédelmi Főigazgatóság) meghatározza a riasztással érintett földrajzi területet, amely lehet egy város, járás, településrész, illetve egy ipari vagy környezeti baleset közvetlen környezete;
2. a mobilhálózati szolgáltatók azonosítják azokat GSM cellákat, amelyek lefedik a kijelölt területet;

3. a riasztási üzenetet valamennyi érintett cella egyidejűleg sugározza;
4. minden, az adott cellák hatósugarán belül tartózkodó, kompatibilis mobilkészülék automatikusan megkapja és megjeleníti az üzenetet, előzetes regisztráció vagy személyes adatkezelés nélkül. [54]

A Cell Broadcast technológia egyik legnagyobb előnye, hogy nem terheli túl a mobilhálózatot, nem igényel visszirányú kommunikációt, és nagymértékben ellenálló a hálózati torlódásokkal szemben, amelyek tömeges SMS- vagy hanghívás-alapú riasztások esetén gyakran jelentkeznek. E tulajdonságai miatt a technológia különösen alkalmas ipari balesetek, természeti katasztrófák és egyéb gyors lefolyású veszélyhelyzetek során a lakosság hatékony tájékoztatására.

A Cell Broadcast egy hálózatalapú, pont–többpont (one-to-many) elven működő riasztási technológia, amely már a 2G, 3G és 4G mobilhálózatokban is szabványosított formában elérhető, és az 5G rendszerekben továbbfejlesztett képességekkel rendelkezik. A technológia sajátossága, hogy a riasztási üzeneteket nem egyéni előfizetőkhöz címezik, hanem a mobilhálózat bázisállomásai sugározzák azokat egy adott földrajzi területet lefedő cellákon keresztül. Ennek eredményeként az üzenet automatikusan megjelenik minden olyan mobilkészüléken, amely a riasztás időpontjában az érintett cellák által lefedett földrajzi területen található. [54]

Hazánkban egy másik lakosság riasztási megközelítés veszélyhelyzet esetén a veszélyes anyagokkal foglalkozó üzemek környezetében telepített MoLARi rendszer, mely országszerte 768 végponttal rendelkezik és az üzemek környezetében élő lakosság gyors és hatékony riasztását teszi lehetővé. Jelenleg a MoLaRi rendszer segítségével mintegy 517 ezer ember riasztható. A lakosság által követendő magatartási utasítások pedig a riasztási szirénákon túl élő szövegként is átadásra kerülhet, ami csökkenteni tudja a pánik helyzetet és a lakosságvédelmi intézkedések hatékonyságát növelni. A riasztó végpontok mellett, monitoring funkciót is ellátnak ezek az eszközök, melynek köszönhetően a veszélyes anyagok és keverékek levegőbe jutása esetén folyamatos koncentráció mérhető és ezen értékek megjelennek a Katasztrófavédelem ügyeleti rendszerében, ahonnan a riasztást le lehet adni a lakosság irányába. [55] Települési szinten a polgármester felel a riasztó-tájékoztató végpontok üzemképességéért és karbantartásáért, míg a gazdálkodó szervezetek vezetői kötelesek saját területükön biztosítani a riasztási és tájékoztatási rendszer kiépítését és működtetését.

A hatályos szabályozás a lakosság riasztását és veszélyhelyzeti tájékoztatását egységes, többcsatornás kommunikációs rendszerként határozza meg. A riasztás eszközei között kiemelt szerepet kapnak a klasszikus értelembe vett tájékoztatási platformok, a lakossági riasztó rendszereken felül, a közérdekű közlemény közzététele a médiaszolgáltatókon keresztül, az elektronikus hírközlési szolgáltatások igénybevétele, továbbá a helyben szokásos módon történő információ közlése és egyéb technikai eszközök használata. A jogalkotó lehetőséget biztosít e csatornák egyidejű alkalmazására, amely a redundancia és az elérési biztonság elvének érvényesülését szolgálja.

A közérdekű közlemény tartalmát a hivatásos katasztrófavédelmi szerv központi szerve határozza meg, biztosítva az információk hitelességét és egységességét. A szöveges tájékoztatásnak tartalmaznia kell különösen az esemény helyét és idejét, várható hatásait és kiterjedését, időtartamát, valamint a követendő magatartási szabályokat és a további információforrásokat. A riasztás elrendelése a veszély és annak hatásainak területi kiterjedéséhez igazodó, differenciált hatásköri rendben történik, amely országos, területi, települési és gazdálkodó szervezeti szinteken is meghatározza a felelős döntéshozót.

A redundáns lakossági vészhelyzeti riasztás rendszeréhez szervesen illeszkednek a lakosság részére fejlesztett lakosságvédelmi mobil applikációk. Már több uniós tagállam is bevezetett veszélyhelyzet-kezelő és/vagy -értesítő okostelefon-alkalmazást. Németországban a lakosság számára elérhető egy ingyenes mobilapplikáció, amely széles körű funkcionalitással bír. A Német Szövetségi Polgári Védelmi és Katasztrófa-védelmi Hivatal (BBK) által fejlesztett NINA (Notfall-Informations- und Nachrichten-App) nevű alkalmazás lehetőséget biztosít arra, hogy a felhasználók az aktuális tartózkodási helyük alapján figyelmeztetéseket és riasztásokat kapjanak telefonjukra hang- és fényjelzésekkel egybekötve, miközben nem tárolja a felhasználó helyadatait. A NINA célja, hogy megbízható és gyors információkat nyújtson a lakosságnak a veszélyhelyzetek kezeléséhez, és elősegítse a megfelelő felkészülést és magatartási formákat különböző katasztrófahelyzetekben. A felhasználóknak lehetőségük van vészhelyzeti tippeket olvasniuk, amelyek kategorizálva vannak a természeti és ipari katasztrófatípusoknak megfelelően. Az eseményleírás mellett cselekvési ajánlásokat is megfogalmaztak számukra. Továbbá az adott veszély kezeléséében hatáskörrel rendelkező hatóság elérhetőségét és hivatalos honlapját is feltünteti az alkalmazás az esetek leírásánál. [56]

Olaszországban ezzel szemben nincs egységes központi felügyelet alatt álló lakosságvédelmi mobilalkalmazás, hanem régiónként vagy városonként tudnak a felhasználók alkalmazást letölteni, ezek fejlesztése jellemzően közigazgatási megrendelésre történik: a szakmai

tartalomért és az operatív működtetésért a regionális polgári védelmi szervek felelnek, míg a technológiai fejlesztést és rendszerüzemeltetést szerződött informatikai szolgáltatók vagy regionális állami informatikai vállalatok végzik. A hivatalos nemzeti riasztási és veszélyhelyzeti tájékoztatást az IT-Alert cell-broadcast rendszer biztosítja. A regionális vagy helyi polgári védelmi mobilalkalmazások elsősorban kiegészítő funkciókat látnak el, kockázati információkat, meteorológiai riasztásokat és lakossági bejelentési lehetőségeket biztosítanak. A Szicíliában használatos Pronti all'azione („*Készen az akcióra*") alkalmazás lehetőséget biztosít a felhasználók részére az események bejelentésére, de emellett a funkció mellett a felhasználók olvashatnak az adott régióra jellemző kockázatokról és hasznos tippeket is kapnak az alkalmazáson keresztül. [57]

Hazánkban jelenleg okostelefonokra az Országos Katasztrófavédelmi Főigazgatóság (BM OKF) által fejlesztett ingyenes mobilalkalmazás érhető el iOS és Android operációs rendszerű eszközökre, az alkalmazás neve VÉSZ (Veszélyhelyzeti Értesítési Szolgáltatás). Az applikáció segítségével a felhasználók képesek valós időben tájékozódni veszélyhelyzetekről, például közlekedési balesetekről, tűzesetekről vagy időjárási riasztásokról. Az alkalmazás olyan kiegészítő funkciókkal rendelkezik, mint a felolvasási lehetőség és a nagykontrasztos mód. Valamint lehetőséget biztosít a helyalapú értesítések beállítására, így a felhasználók a tartózkodási helyükhöz kapcsolódó riasztásokat is megkaphatják. A VÉSZ célja, hogy megbízható, gyors és pontos információkkal segítse a lakosságot a veszélyhelyzetek elkerülésében és kezelésében. Azonban az applikáció a lakosság felkészítését jelen formájában nem támogatja, nincsenek felkészítéssel kapcsolatos funkciói. [58]

2.1.3 A lakosságvédelem nemzetbiztonsági aspektusai

Napjaink információs társadalmában már elengedhetetlen, hogy a lakosságvédelmi tájékoztató kiadványok és a lakosságfelkészítő anyagok ne csak nyomtatott formában létezzenek, hanem széles körben, online is elérhetők legyenek. A lakosság médiafogyasztási szokásai az elmúlt évtizedekben gyökeresen átalakult és a digitális tartalmak fogyasztása vált meghatározóvá a hagyományos médiumokkal szemben. Ezért elengedhetetlenné vált a lakosság digitális platformokon keresztül történő, hiteles információkon alapuló, felkészítése a válsághelyzetekre, ez csökkenti a nemzetbiztonsági kockázatokat, mert minimalizálhatja a pánik és a dezinformáció okozta bizonytalanság kialakulásának valószínűségét. Mindez elősegíti az állami erőforrások hatékonyabb felhasználását, lehetővé téve azok célzottabb alkalmazását preventív intézkedésekben és válságkezelésben. Azonban napjainkban a

lakosságot a természeti és civilizációs katasztrófák, valamint azok hatásai mellett fel kell készíteni az álhírek kiszűrésére is, ki kell alakítani a lakosság megfelelő médiaműveltségét. A médiaműveltségi programok segítségével a lakosság kellő rezilienciát tud kialakítani a dezinformációs kampányok és a digitális médián keresztül terjedő álhírek hatásaival szemben. Az Európai Unió 2022-ben kiadta a megerősített Dezinformációs Gyakorlati Kódexét, amelynek célja a dezinformáció elleni fellépés és az átláthatóság fokozása; ez egy önszabályzó keretrendszer, a benne foglaltakat az azt aláíró online platformok önként vállalják. Ennek a kódexnek részét képezi a felhasználói tudatosság növelése, valamint független tényellenőrző szervezetek működtetésének (fact-checkers) a lehetősége. [59] Ma a dezinformációs kampányok súlyos nemzetbiztonsági kihívást jelentenek valamennyi állam számára. Ezek ellen a leghatásosabb védelem a lakossági médiaműveltségi programok elindítása. Néhány uniós tagállam ezeket már középiskolás kortól, a közoktatás infrastruktúráját is felhasználva alkalmazza. Jelenleg Magyarországon még nem elterjedtek ezek a médiaműveltségi programok, azonban az Európai Unió honlapján számos magyar nyelvű oktatóanyag és videó is elérhető a témával kapcsolatban. [60]Az EU Külügyi Szolgálata (EEAS) létrehozta az East StratCom Task Force-t, amelynek fő feladata a hamis információk azonosítása, elemzése és cáfolata elsődlegesen a kelet európai régióra fókuszálva. Az East StratCom Task Force együttműködik a tagállamok kormányaival, kutatóintézetekkel és médiapartnerekkel dezinformáció elleni fellépés érdekében, eddig változó eredménnyel. [61] A Task Force 2015-ben létrehozott zászlóshajó projektje az EUvsDisinfo, ami cáfolt, hamis állításokat tartalmazó cikkek adatbázisa, sajnos elsődlegesen csak angol nyelven elérhető, így a magyar lakosság szélesebb körében történő népszerűsítése nem biztosított. [62]

Az álhírek generálásához és kampányszerű terjesztéséhez napjainkban nélkülözhetetlen eszközzé vált a mesterséges intelligencia (MI). Ez jelenleg az egyik legmeghatározóbb technológiai eszköz, amely egyszerre jelent jelentős társadalmi és gazdasági lehetőséget, valamint új típusú kockázatokat. Az információs térben a generatív MI-rendszerek megjelenése alapvetően alakította át az álhírek és a szervezett dezinformációs kampányok előállításának és terjesztésének mechanizmusait. A lakosság a közösségi médián, valamint különböző online felületeken keresztül fokozott mértékben ki van téve manipulált vagy valótlan tartalmaknak, amelyeket az MI-eszközök elterjedése tovább erősít. A generatív mesterséges intelligencia alkalmazásával ma már rendkívül valósághű képi, hang- és videótartalmak (*deepfake* anyagok) hozhatók létre alacsony költséggel és rövid idő alatt. Ennek következtében az álhírek nem csupán elszigetelt információs torzulásként jelennek meg, hanem kampányszerűen,

összehangolt módon képesek terjedni, gyakran automatizált fiókhálózatok és algoritmikus ajánlórendszerek támogatásával. A jelenség különösen veszélyes válsághelyzetekben, választási időszakokban vagy társadalmi feszültségek idején, amikor a lakosság információigénye megnövekszik, miközben a forráskritika csökkenhet. Erre reagálva párhuzamosan jelentek meg az MI-alapú detektáló és ellenőrző rendszerek is, amelyek célja a mesterségesen generált tartalmak azonosítása és kiszűrése. Azonban ez csak a probléma „tüneti kezelésére" elegendő, mivel a generatív és a detektáló technológiák fejlődése folyamatos „versenyhelyzetben" áll egymással. [63]

Az Európai Unió az álhírek és a generatív MI kérdéskörét összetetten kezeli és ezen kockázatok leküzdésére 2025 végén létrehozásra került a European Democracy Shield. Ez az EU stratégiai keretrendszere, amely a demokratikus fenyegetések elleni egységes uniós fellépést hivatott megerősíteni. A kezdeményezés nem váltja ki az egységes digitális szolgáltatási piacról és a 2000/31/EK irányelv módosításáról szóló az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (DSA) vagy a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról szóló az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (AI Act) előírásait, hanem ezekre építve kívánja erősíteni a kockázatelemzést, az előrejelzést és a gyors reagálást. Ezzel a hangsúly az utólagos tartalomkezelésről/cáfolásról fokozatosan a megelőzés, a korai felismerés és a rendszerszintű kockázatcsökkentés irányába tolódik el. Az Európai Bizottság Közös Kutatóközpontja (JRC) tudományos módszerek alapján elemzi a manipulációs mintázatokat, az MI-alapú tartalomgenerálás kockázatait, valamint a detektálási és mérséklési megoldások hatékonyságát. [64]

Az MI ugyanakkor nem kizárólag kockázati tényezőként értelmezhető, megfelelő keretek között alkalmazva a lakosság tájékoztatásának és ellenálló képességének növelését is szolgálhatja. Például az AI Agent-ek segítségével létrehozható reaktív információszolgáltató platformok (tudásbázis alapú agent (RAG)), amelyek képesek strukturált, hiteles és azonnali válaszokat adni a lakosság kérdéseire veszélyhelyzetek, rendkívüli események vagy bizonytalan információs környezet esetén. A reaktív agentek gyakorlatilag a környezeti ingerekre (trigger) reagálnak történeti kontextus nélkül, egyszerű feltétel – akció logika szerint működnek. [65] Egy hatósági felügyelet alatt működő, mesterséges intelligenciával támogatott tájékoztató felület lehetőséget teremt arra, hogy a lakosság valós időben jusson ellenőrzött információkhoz, lakosságvédelmi tanácsokhoz és cselekvési útmutatáshoz, különösen akkor, amikor a közösségi médiában és nem hiteles forrásokon keresztül terjedő álhírek fokozzák a

bizonytalanságot. Rövid távon a reaktív megközelítés bizonyul a leghatékonyabbnak: az agent a feltett kérdésekre hatóság által felügyelt adatbázisokból válaszolva képes csökkenteni az információs vákuumot, amely az álhírek egyik elsődleges táptalaja. Az ilyen rendszerek létrehozása hatósági oldalon viszonylag alacsony költséggel megvalósítható, mivel a nagy nyelvi modellek (LLM) jól integrálhatók meglévő digitális infrastruktúrákba, és egy megfelelően karbantartott, hatóság által validált adatbázishoz való hozzáférés révén releváns, konzisztens válaszokat tudnak biztosítani minimális humán erőforrás-igény mellett. További előnye a technológiának, hogy képes az adott ipari vagy természeti katasztrófához kapcsolódó, hatóságok által közzétett hiteles információk folyamatos monitorozására, és az aktuálisan elérhető, ellenőrzött adatok alapján a korábbi tudásbázist kiegészítve, dinamikusan válaszolni. [65]

A mai folyamat-automatizációs környezetben népszerűnek számító nyílt forráskódú n8n workflow-automatizációs platform lehetővé teszi, hogy a felhasználók alacsony kódigényű (low-code) környezetben, grafikus felhasználói felületen keresztül hozzanak létre strukturált automatizált folyamatokat. A rendszer node-alapú architektúrája támogatja külső szolgáltatások és API-k integrációját, valamint mesterségesintelligencia-alapú elemek (AI agentek) beépítését, ezáltal komplex, kommunikációs feladatok automatizált megvalósítását. Lehetőség van saját szerveren futtatni, így az adatok felhasználói felügyelet alatt maradnak, mely fokozottan előnyös, ha egy hatóság saját, zárt környezetben akarja tartani az adatait. Az n8n elnevezés a „node” szó rövidített formájából származik, utalva arra, hogy a rendszer működési alapegysége a node (csomópont), a folyamatokat alapvetően node-okból lehet felépíteni, ezek a folyamat egyértelműen elkülöníthető funkcionális egységeit jelölik, gyakorlatilag a folyamatok „építőkövei”. A node-ok együtt biztosítják a hiteles információfeldolgozást, a döntéstámogatást és a kontrollált válaszgenerálást. Az n8n automatizációs folyamat platform a legtöbb nagy nyelvi modell agentjeit támogatja, AI node-ok által. Ezeket az agent node-okat pedig a legoptimálisabb feladat végrehajtás érdekében promtolni szükséges. Az ilyen munkafolyamatokba javasolt az automatizáción kívüli humán interakciót is beépíteni olyan jellegű esetekre, amikor az agentek nem tudnak megfelelő választ adni, vagy ellentmondásokba ütköznek az adatbázisban tárolt információk tekintetében.

Szintén figyelembe szükséges venni, hogy információbiztonsági szempontból a platform jól teljesít, minden évben auditálásra kerül független auditori szervezet által, éves szinten penetrációstesztelést is végeztetnek független szakértőkkel, valamint sérülékenység scannelést. A platform rendelkezik legalább 12 hónapra visszamenő naplózással, szerepkör alapú

hozzáférés-kezelést (RBAC) is ki lehet alakítani benne, valamint a többfaktoros azonosítás is beállítható. A platform mind átviteli titkosítást (HTTPS/SSL/TLS), mind pedig adatok „at rest" titkosítását támogatja, beleértve az AES-256 szintű adattárolást és FIPS[13]-nek megfelelő kulcskezelést felhő környezetben. Saját host esetén az SSO[14] megvalósítható LDAP vagy SAML hitelesítési mechanizmusok alkalmazásával. A szolgáltatás napi adatmentést és replikációt biztosít, valamint az üzemeltető kidolgozott katasztrófa-helyreállítási tervet (DRP) is a rendszer kapcsán. A felhőben hosztolt N8N esetén tűzfalak, (WAF) és behatolás érzékelő rendszer (IDS) szolgálják a futó szolgáltatások védelmét. [66]

A mesterséges intelligenciával támogatott, munkafolyamat-automatizációs környezetbe integrált információszolgáltató rendszerek új lehetőségeket teremtenek a lakosságvédelmi kommunikáció hatékonyságának növelésére. A hiteles adatforrásokra épülő, hatósági felügyelet mellett működtetett AI-agent alapú megoldások képesek csökkenteni az információs bizonytalanságot, gyors és strukturált válaszokat biztosítani a lakosság számára, valamint hozzájárulni a társadalmi ellenálló képesség erősítéséhez. A megfelelő információbiztonsági és irányítási keretek alkalmazása mellett az ilyen rendszerek a jövőben a digitális lakosságvédelmi infrastruktúra fontos kiegészítő elemeivé válhatnak.

2.2 A Rouen-i Lubrizol ipari baleset tanulságai

Az ipari balesetek és veszélyes anyagokkal kapcsolatos események jelentős kockázatot hordoznak a környező lakosság egészségére és anyagi biztonságára, ezért a lakosságvédelem egyik kiemelt feladata az ilyen események során alkalmazandó tájékoztatási és kommunikációs mechanizmusok hatékony működtetése a megfelelő lakosságvédelmi intézkedések foganatosítása mellett. A megfelelő és naprakész válságkommunikáció alapvető szerepet játszik a lakosság biztonságának megőrzésében, mivel a hiteles, gyors és egyértelmű információk hozzájárulnak a pánik megelőzéséhez és az információsvákuum kialakulásának minimalizálásához, továbbá a szükséges lakosságvédelmi intézkedések elfogadásához és betartásához. Az ipari balesetekkel összefüggő kommunikációs gyakorlatok vizsgálata ezért fontos tapasztalatokat nyújt a lakosságvédelmi rendszerek működésének értékeléséhez.

[13] Egyesült Államok szövetségi kormánya által meghatározott információbiztonsági és adatfeldolgozási szabványok
[14] Single Sing On: A felhasználó egyszeri azonosítás és hitelesítést követően a további alkalmazásokhoz ismételt bejelentkezés nélkül fér hozzá.

A következőkben bemutatott Lubrizol-eset jól szemlélteti, hogy egy jelentős ipari tűzeset során milyen kihívások jelentkezhetnek a veszélyhelyzet kezelésén túl, a lakosság tájékoztatása, a kockázati információk közvetítése és a társadalmi bizalom fenntartása terén, valamint rámutat arra is, hogy a válságkommunikáció minősége miként befolyásolhatja a lakosság percepcióját és együttműködési hajlandóságát.

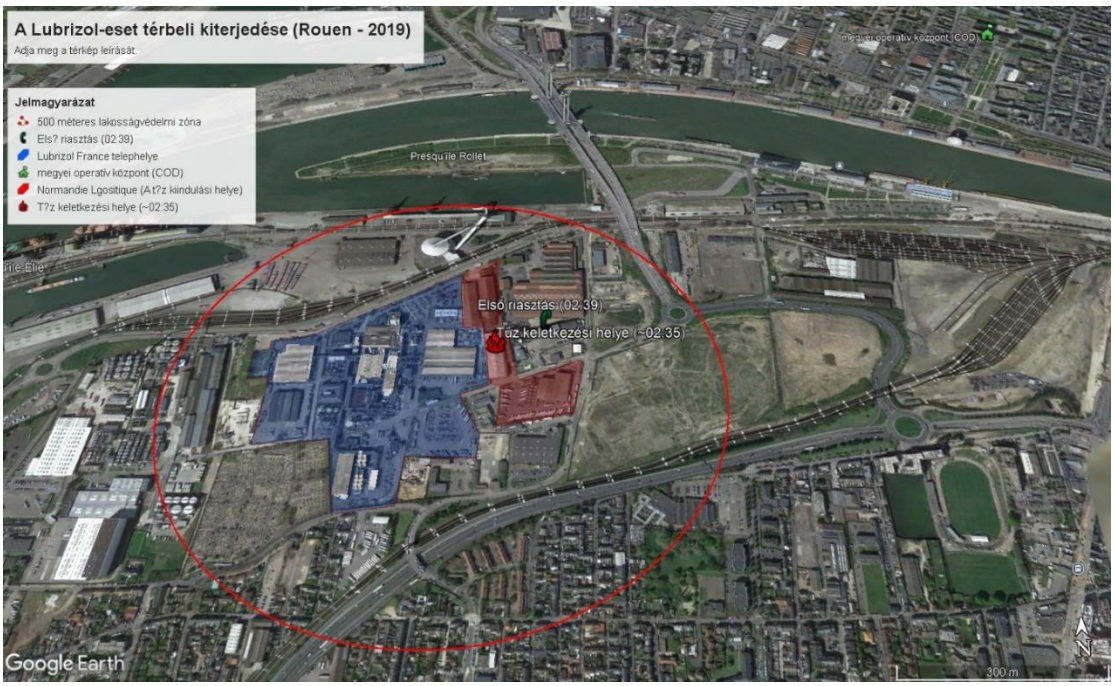
Az amerikai hátterű vegyipari vállalat francia leányvállalatának Rouen-melletti telephelye kenőanyag-adalékanyagok és más speciális vegyi anyagok gyártásával és raktározásával foglalkozik. A telephelyen nyersanyagok és késztermékek tárolására szolgáló területek, valamint gyártó- és keverőegységek találhatók. A vállalat francia telephelye SEVESO felső küszöbértékű besorolású veszélyes anyagokkal foglalkozó üzemként működött.

2019. szeptember 26-án hajnalban tűz ütött ki a szervezet Rouen melletti telepehelyén, a tűzfészek a közvetlen mellette levő Normandie Logistique raktár komplexuma volt. A részletes jelentés szerint két telephelyen összesen mintegy 9 500 tonna vegyi anyag égett el. A tűz nagyon gyorsan terjedt, nagymennyiségű füst- és koromfelhőt emelt a légkörbe, a fekete füst több tíz kilométeres területen volt észlelhető. A balesetkor fellépő szélmozgások a füstfelhőt észak-kelet felé vitték, aminek köszönhetően több településen korom és szennyeződés lerakódás jelent meg. A hivatalos vizsgálatok szerint a levegő- és talajmintavételek során a legtöbb komponens koncentrációja nem haladta meg azon értékeket, amelyek azonnali toxikus hatást jelentenének.

A francia Társadalmi Ügyek Főfelügyelősége (Inspection Générale des Affaires Sociales, továbbiakban: IGAS) 2020-ban kiadott jelentése részletesen értékeli a Lubrizol-tűzeset kezelését és a hatósági intézkedéseket, az esettanulmány alapja erre a 135 oldalas jelentésre épül.

A kialakult tüzet elsőként szomszédos Triadis vállalat biztonsági szolgálata észlelte, akik 02:39-kor értesítették a hatóságokat. A káresemény elhárításában az operatív beavatkozást a SDIS 76 (Seine-Maritime) tűzoltóság végezte, mintegy 240 tűzoltó bevonásával. Az ő felelőségi körükbe tartozott a tűz közvetlen oltása, a veszélyes anyagok terjedésének megakadályozása és a műszaki mentés. A jelentés kiemeli, hogy a tűzoltás és a környezetvédelmi beavatkozások összességében sikeresek voltak, mivel a tűz nem terjedt tovább, és nem követelt halálos áldozatot. A dokumentum szerint több önkéntes egység csatlakozott a hivatásos állományhoz az oltásban való közreműködés céljából. A tűzoltás

megkezdésével szinte egyidőben az üzemeltető biztonságba helyezte a foszfor-pentaszulfid[15] készleteit, ezzel megelőzve egy súlyos robbanást és aktiválta a belső védelmi tervet. Ekkor került kijelölésre a hivatásos tűzoltók által egy 300 méteres biztonsági zóna. A prefektúra 03:45-kor aktiválta az operatív központját (COD), valamint a biztonsági zóna 500 méteres sugarúra bővült, a törmelék- és robbanásveszély, valamint a mérgező és irritatív égéstermékek kockázata miatt. Hajnali 4 óra után a megyei operatív központ a kárhelyen zajló műveletek koordinálására válságstábot állított fel (cellule de crise). 5 órakor a prefektus elrendelte a lakosság elzárkóztatását a korábban kijelölt 500 m-es zónában. Később a külső védelmi terv is életbe lépett, aminek részeként a lakosság elzárkóztatását rendelték el Rouenben és a környező településeken.



8. ábra A baleset térképes kiterjedése - 2019.09.26. Rouen, Franciaország, készítette: a szerző [67]

A következő órákban a megyei operatív központ és annak válságstábja összehangolta az egészségügyi kockázatelemzést. Az elemzés szerint a füstfelhő hidrokarbon-alapú[16], nagy magasságban haladt, és nem okozott azonnali toxikus hatást. Ezért nem rendelték el a lakosság evakuálását, az akut mérgezés veszélye kizárható volt.

[15] sárgás színű, jellegzetes szagú, kristályos szilárd anyag, amely vízzel hevesen reagálva mérgező és gyúlékony gázokat fejleszt, ezért kezelése fokozott kémiai és munkabiztonsági intézkedéseket igényel. [123]
[16] főként szénhidrogén-eredetű részecskéket és illékony szerves vegyületeket tartalmaz, ezért sűrű, fekete, irritáló szagú, és hosszú ideig képes a levegőben lebegni.

A COD első ülésén, reggel 6 óra magasságában, meghatározta a közegészségügyi utasításokat, melyek kiterjedtek a szabadban történő tartózkodás tiltására, az épületek nyílászáróinak zárt állapotban történő tartására és kikapcsolt szellőzőrendszerekre. 13 településen az iskolák és óvodák átmeneti bezárását rendelték el, valamint az idősotthonokban és egészségügyi intézményekben tartózkodóknak az intézményeken belül kellett maradniuk.

Reggel 8:00-kor az oltás defenzív fázisa végett ért. 9:30-kor a francia megyei tűzoltóság és polgári védelem alkalmazásában álló VDIP egységek[17] megkezdték a levegő és a környező anyagok toxikológiai értékeinek mérését, valamint koromlerakódások feltérképezését, hogy pontosítsák a veszélyzónát. Ezzel párhuzamosan megkezdődött a habképző anyagok előállítása a szomszédos vállalatok közreműködésével. Délelőtt 11 órakor a tűzoltók úszógátakat telepítenek a Szajna védelmére és megkezdték a haboltást (top mousse), azért ezt a módszert alkalmazták, mert nagy mennyiségű égő vegyi anyag (olajok, adalékok) elfojtására a víz önmagában nem lett volna hatékony és további szennyezést is okozhatott volna.

13 órakor a tűz körülhatárolásra került. 15:00 -kor hivatalosan bejelentették, hogy a tűz eloltásra került. Az első nap végére a hatóságok megerősítették, hogy nincsenek súlyos egészségügyi esetek, a kórházak csak enyhe tünetekkel, mint fejfájás, hányinger és irritáció fogadtak betegeket. [68]

A baleset utókezelése során a dioxin és azbeszt koncentráció mérésére nagy hangsúlyt fektetett a prefektúra, valamint a francia Nemzeti Élelmiszer-, Környezetbiztonsági és Munkaegészségügyi Ügynökség (ANSES) és az Ipari és Környezeti Kockázatok Kezelésével foglalkozó Nemzeti Intézet is (INERIS). Az eredmények a tűzeset közelében a határértékhez közeli koncentrációt mutattak, később más pontokon és településeken is vettek mintákat, melyekben a dioxin és azbeszt szint a megengedett határérték alatt volt. [69]

Már szeptember 26-án az Élelmiszerügyi, Mezőgazdasági és Erdészeti Regionális Igazgatóság (Draaf Normandie) és a Terület- és Partvidékgazdálkodásáért felelős Állami Hivatal (DDTM) elkezdte az agrárkárok felmérését. Az első intézkedés során a termények betakarítása és az állatok legeltetése megtiltásra került a korommal szennyezett területeken. A káresetet követő napokban a mintavételezték a tej-, tojás-, zöldség- és takarmánytermékeket, aminek hatására a prefektúra szeptember 28-án elrendelte a helyi élelmiszerek és takarmányok forgalmazásának

[17] A francia VDIP egységek funkcionálisan a hazai Katasztrófavédelmi Mobil Laborok (KML) képességeihez hasonlíthatók, mivel elsődleges feladatuk a veszélyes anyagok helyszíni felderítése, azonosítása és mintavétele. [124]

felfüggesztését 112 településen. 2019 október 14-én tejtermékekre vonatkozó korlátozások feloldásra kerültek, majd október 18-án valamennyi mezőgazdasági termék korlátozása is eltörlésre került. A mezőgazdaságot érintő gazdasági veszteség becslések szerint körülbelül 65 millió euro nagyságú volt.

A balesetet követően a lakossági ivóvíz szennyezettségét még az év végéig monitorozták, valamint kibővítették az érintett vízkinyerő kutak számát és a vizsgált szerves vegyületek körét pl. dioxinok, furánok és egyes peszticid-maradványokra, A mérések arra a következtetésre jutottak, hogy az ivóvíz-források szennyezettsége sehol sem haladta meg az egészségügyi határértéket. Egy 2025-ös publikáció megerősíti a közegészségügyi hatóság (ARS Normandie) vízminőségi ellenőrzéséről készült jelentéseit. A kutatás nem csak szabályozott anyagokat vizsgált, hanem próbálta kimutatni az egészségre és környezetre káros hatású, égésből származó anyagok jelenlétét is nagyfelbontású tömegspektrometriás módszerekkel. Összesen 5 vízforrást (3 folyót és 2 vízbázist) monitoroztak 2022–2023 között.

A fő megállapítások között szerepelt, hogy 3 év után is 7 ismert Lubrizol termékhez köthető vegyület (pl. 4-tert-butylfenol, 2,6-di-tert-butylfenol, diphenilamin, BHT) kimutatható a felszíni és talajvizekben. A 4-tert-butylfenol és a BHT a későbbi, csapadékos időszakokat követő mintavételekben ismét kimutatható volt, ami a vegyületek másodlagos mobilizációjára, azaz a talajból vagy az üledékből történő kimosódásra utal.

A vizekből kimutatott nehézfém-koncentrációk (pl. Zn, Pb, Cu) az első, balesethez kronológiailag közelebbi mintákban voltak a legmagasabbak, majd fokozatosan csökkentek, ami hosszú távú helyreállásra utaló mintázat. További érdekesség, hogy néhány PAH[18] (fenantrén, antracén) a mintákból kimutatható volt, azonban a mért koncentrációk nem haladták meg MAC-EQS-határértékeket. Indokolt lehet a térség vizeinek további, hosszú távú vizsgálata, mert a balesetből visszamaradt vegyületek jelenléte 3–4 év múltán is igazolható. [70]

2.2.1 A Lurbizol baleset kezelésének hiányosságai

A lakosságvédelmi intézkedések hatékonysága ipari balesetek esetén nem kizárólag a technikai beavatkozások sikerességén múlik, hanem alapvetően meghatározza azt a lakosság felé irányuló tájékoztatás szervezettsége és hitelessége is. Ambrusz József és Beke Zoltán

[18] policiklusos aromás szénhidrogének, több összekapcsolt aromás gyűrűből álló szerves vegyületek, főleg szénhidrogének tökéletlen égésekor keletkeznek, toxikusak, perzisztensek és bioakkumulatívak.

szerint a lakossági tájékoztatás a katasztrófavédelemben előre tervezett, strukturált tevékenység, amelynek célja a bizonytalanság csökkentése és a társadalmi bizalom fenntartása. Az IGAS által készített jelentés több fejezetben is rámutat arra, hogy a Lubrizol-incidens kezelése során a kommunikáció és a lakosság felé irányuló tájékoztatás területén jelentős hiányosságok mutatkoztak, amelyek a helyreállítás folyamatát is kedvezőtlenül befolyásolták. [16]

A jelentés szerint a válságkommunikáció több ponton is hiányos volt. A kommunikáció egyirányú és túlzottan központosított maradt, nem tette lehetővé a gyors visszacsatolást. A prefektúrának nem volt elegendő kapacitása a közösségi média folyamatos monitorozására, csak a Twitter-en jelentek meg posztok, amik sokszor csupán a hivatalos honlapra mutató linket tartalmazták, nem biztosítottak valós idejű információkat és nem voltak interaktívak. Ezenfelül a helyi polgármesterek és civil szervezetek bevonása elmaradt, pedig hiteles közvetítőként növelhették volna a lakosság bizalmát és együttműködését.

A SAIP (Lakossági Riasztási és Információs Rendszer) által adott riasztás félreérthető volt, sok lakos nem tudta, mit kell tenni, amikor a szirénák megszólaltak. A SAIP lakosság riasztó rendszerhez fejlesztett mobil applikáció baleset idején nem üzemelt. Az érintett lakosság cell-broadcast technológia alkalmazásával sem került értesítésre. Az esetről az első hivatalos tájékoztatás a prefektúra honlapján és Twitterén jelent meg, valamint a radio France Bleu Normandie-n. Ezek a platformok nem voltak összhangban az emberek mindennapi média és hírfogyasztási szokásaikkal, ezért a kezdeti időszakban sokan nem értesültek az információkról és követendő magatartási szabályokról. A Lubrizol-eset után a francia kormány meggyorsította az új riasztási rendszer (FR-ALERT) fejlesztését, amely a cell broadcast technológián alapul és 2022-ben került bevezetésre. [71] További hiányosság, hogy nem készült azonnali, egységes térkép a füstterjedésről, ami akadályozta a teljeskörű tájékoztatást. A helyi orvosok is csak 15 nappal később kaptak részletes útmutatást az egészségügyi következményekről.

A laboratóriumi vizsgálatok nem kerültek központilag egységesen koordinálásra, így különböző adatformátumokat használtak, ami megnehezítette az azonnali kiértékelést. A védelmi zónák (agrár) kijelölése túl lassú volt, mivel nem állt rendelkezésre gyors térinformatikai elemzés. Az ANSES értékelése a tejfogyasztási tilalom ügyében késve és hiányosan érkezett, ami bizalomvesztést okozott. Az élelmiszerlánc-monitoring és a talajmintavételek nem voltak kellően integráltak. A döntéshozók, mint a prefektúra és az ARS nem ugyanabból a forrásból dolgoztak, ami napokkal késleltette az élelmiszer-fogyasztási

korlátozások és feloldások meghozatalát. Ezért kettős kommunikáció alakult ki országos és helyi szinten eltérő üzenetekkel, ami a lakosságot összezavarta és bizalmatlanná vált.

A válságkommunikáción felül hiányosságként került értékelésre, hogy az ipari telep nem rendelkezett saját létesítményi tűzoltósággal. A telephely vízbetáplálása nem redundánsan került kialakításra, így az oltás első óráiban nem volt elegendő oltóvíz és az oltóhab készlet sem volt elégséges. Ez legalább kétórás késedelmet okozott a tűz eloltásában. Az üzem belső védelmi terve nem tartalmazott elegendő információt az ilyen kiterjedésű tűz kezelésére. A védekezés irányítása túlságosan a prefektus[19] központú volt, kevés decentralizált döntési lehetőséggel.

A szervezettségi hiányokra vezethetők vissza, hogy az utólagos koordinációs egység (cellule post-accidentelle) nem állt fel időben a COD-ban, így az adatáramlás és döntéshozatal akadozott. Csak két nappal a tűz után jött létre hivatalosan, miközben már a krízis kezdetétől szükség lett volna rá. Ez Franciaország esetén egy fontos koordinációs egység, ami a baleseteket követő egészségügyi, környezeti, gazdasági feladatokat határozza meg és koordinálja azok végrehajtását.

A Lubrizol által létrehozott kártalanítási rendszer, átláthatatlan volt és döntően privát piaci szereplők által vezérelt, a gazdákat érintő maximális támogatás 10.000 euro volt. Javaslatként született meg, hogy az állami szereplők és mezőgazdasági kamarák a jövőben szorosabban kerüljenek bevonásba a mezőgazdasági kártalanítási döntéshozatalba. [68]

A fenti tapasztalatok jól szemléltetik, hogy egy ipari baleset kezelése során a lakosság riasztásának és veszélyhelyzeti tájékoztatásának szervezettsége alapvetően meghatározza a védekezés társadalmi elfogadottságát és hatékonyságát. A lakosok azonnali és szinte teljeskörű tájékoztatására jelenleg a leghatékonyabb megoldás a cell broadcast technológia alkalmazása. A Lubrizol-eset rámutat arra, hogy a késedelmes, fragmentált, egymásnak akár ellentmondó kommunikáció vagy nem megfelelő csatornákon történő kommunikáció információs vákuumot hozhat létre, amely a bizonytalanságot és a bizalomvesztést erősíti és kedvez az álhírek kialakulásának és terjedésének. Mindez alátámasztja a korszerű, többcsatornás riasztási rendszerek, digitális kommunikációs platformok, valamint egy központilag koordinált hatósági

[19] központi államhatalom képviselője (prefektúra vezetője), katasztrófák esetén egyszemélyi irányítást gyakorol a műveletek felett.

információs központ kialakításának jelentőségét, amely képes a lakosság gyors, hiteles és folyamatos tájékoztatására veszélyhelyzetek vagy krízisek idején.

2.3 Magyarország baleset elhárítási – és lakosságvédelmi képességei

2.3.1 Elhárítás és helyreállítás

Magyarországon a lakosságvédelem a katasztrófavédelem azon funkcionális területe, amelynek célja az emberi élet, az egészség, az alapvető létfeltételek és az alapvető szolgáltatást nyújtó infrastruktúrák védelme veszélyhelyzetek, katasztrófák és egyéb rendkívüli események esetén. 2011. évi CXXVIII. törvény értelmében a hazai lakosságvédelmi feladatok végrehajtásáért elsődlegesen a polgári védelem felel. A polgári védelem „*olyan össztársadalmi feladat-, eszköz- és intézkedési rendszer, amelynek célja katasztrófa, illetve fegyveres összeütközés esetén a lakosság életének megóvása, az életben maradás feltételeinek biztosítása, valamint a lakosság felkészítése azok hatásainak leküzdése és a túlélés feltételeinek megteremtése érdekében.”*[20]

A releváns jogszabályok nem rendelnek egyértelmű definíciót a lakosságvédelemhez mint fogalomhoz. A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény és annak végrehajtásáról szóló 234/2011. (XI.10.) Korm. rendelet a lakosságvédelmet módszertani szempontból közelíti meg és reaktív tevékenységként definiálja. Ha tágabban értelmezzük a lakosságvédelem fogalmát, akkor ide szükséges sorolni a lakosság katasztrófavédelmi felkészítését, a lakosság riasztását, tájékoztatását, valamint a lakosság egyéni védőeszközökkel történő ellátását is, ezzel pedig a lakosságvédelem komplexebb értelmezést nyer, preventív és reaktív módszerek, eljárások, protokollok és intézkedések összessége. A felkészítéssel és tájékoztatással kapcsolatos feladatokat bővebben a katasztrófák elleni védekezés egyes szabályairól szóló 62/2011. (XII.29.) BM rendelet részletezi.

A polgári védelem alapvető céljai közé tartozik a lakosság és az anyagi javak megóvása katasztrófák és fegyveres konfliktusok során, valamint a lakosság ezekre az esetekre történő felkészítése. 2012. januárjától a katasztrófavédelmi törvény hatályba lépésének köszönhetően, átalakításra került a polgári védelem szervezete és feladatai. Az új jogszabály a polgári

[20] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzákapcsolódó egyes törvények módosításáról 3.§ 20.

védelmet az össztársadalmi feladatok és eszközrendszer részévé tette, prioritásként kezelve a katasztrófa- és fegyveres összeütközés esetén történő védelmet. [72]

A polgári védelem Hazánkban egy jól definiálható vertikális intézményi struktúrával rendelkezik, az irányítási és végrehajtási rendszere többszintű. A hierarchikus struktúra fentről lefelé haladva, a központi (országos), területi (megyei) és helyi (települési) szintű szervezeteket tömörít, kiegészülve a munkahelyi szervezetekkel. A központi polgári védelmi szervezet felett a szakmai felügyeletet a BM Országos Katasztrófavédelmi Főigazgatóság, Országos Polgári Védelmi Főfelügyelőség biztosítja.

A települési polgári védelmi szervezetbe tartozhatnak:

- önkéntes polgári védelmi szervezetek,
- köteles polgári védelmi szervezetek,
- kijelölt gazdálkodó szervezetek eszköz- és erőforrás-kapacitásai.

Helyi szinten a polgármester határozattal osztja be a kijelölt lakosokat a települési polgári védelembe és gondoskodik a hivatásos katasztrófavédelmi szervek általi felkészítésükről. Az állampolgárok közreműködésére csak a nagy kiterjedésű káresemények felszámolásában van szükség, a hivatásos állomány tehermentesítése céljából.

A törvény a polgári védelem feladat és hatáskörébe utalja a lakosságvédelmi feladatokon túl a létfenntartáshoz szükséges anyagi javakról (különösen víz-, élelmiszer-, takarmány- és gyógyszerkészletek, állatállomány) és a kritikus infrastruktúrák védelméről történő gondoskodást, a közszolgáltatás ellátásának kiesésekor az, emberi életben, egészségben és az anyagi javakban esett kár megelőzése céljából a közszolgáltatás ideiglenes ellátásáról történő gondoskodás is feladatkörét képezi. További feladata lehet a kárterület felderítése, a mentés, az elsősegélynyújtás, a mentesítés és a fertőtlenítés, és az ezekkel összefüggő ideiglenes helyreállítás elvégzése (továbbá a halálos áldozatokkal kapcsolatos halaszthatatlan intézkedések).

Meg kell említeni a teljeség érdekében, hogy a polgári védelem feladatai közé tartozik a lakosság védelmét szolgáló létesítményekkel kapcsolatos feladatok ellátása, különösen azok nyilvántartása, fenntartása és a védekezés során történő igénybevételének biztosítása. Hazánk óvóhelyi infrastruktúrája napjainkban korlátozott szerepet tölt be, amely összefüggésben áll a hidegháborús időszakot követő védelmi szemlélet átalakulásával és a fejlesztési prioritások

átrendeződésével. A szakirodalom rámutat arra, hogy az óvóhelyek állapota és hasznosíthatósága heterogén képet mutat, ugyanakkor egyes meglévő létesítmények, például a mélyvezetésű közlekedési infrastruktúrák, potenciálisan bevonhatók a lakosságvédelmi feladatokba. [73] Az életvédelmi létesítmények létesítéséről, fenntartásáról és békeidőszaki hasznosításáról szóló 22/1992 (XII.29.) KTM rendelet alapvető keretet biztosít, azonban a jelenkori komplex kockázati környezetben az óvóhelyi képességek fejlesztése inkább egy lehetséges fejlesztési irányként értelmezhető a lakosságvédelem rendszerében.

A lakosságvédelem egyik meghatározó alapját a települések kockázatértékelésen alapuló veszélyeztetettségének szisztematikus felmérése képezi, amely a megelőzés és a felkészülés kulcselemeként jelenik meg a hazai katasztrófavédelmi gyakorlatban. A kockázatalapú megközelítés lehetővé teszi a potenciális veszélyforrások azonosítását, azok hatásainak előzetes értékelését, valamint az ezekhez igazodó védelmi intézkedések kialakítását. Ennek eredményeként a lakosságvédelem nem csupán eseményvezérelt beavatkozásokra korlátozódik, hanem egy tudatosan felépített, előrelátó rendszerként működik, amely a veszélyhelyzetek bekövetkezési valószínűségének csökkentésére és hatásainak mérséklésére egyaránt törekszik.

A lakosság egészségének megóvása érdekében távolsági vagy helyi védelem rendelhető el. A helyi védelem az elzárkóztatást jelenti, így minimalizálva az emberi szervezetre gyakorolt káros környezeti hatások kialakulását. A távolsági védelem célja a lakosság kivonása a katasztrófa súlytotta területről, ezzel megelőzve a káros hatások bekövetkezési valószínűségét. Amennyiben kitelepítés helyett kimenekítésre van szükség, a lakosság részére is kiosztásra kerül egyéni védőeszköz, ami az adott káros hatás ellen a kimenekítés idejéig védelmet nyújt például nukleáris eredetű baleset esetén jód-profilaxis. A lakosság fizikai védelme érdekében alkalmazott intézkedések körét bővíti a létfenntartáshoz szükséges anyagi javak biztosítása (víz, élelmiszer, gyógyszerkészletek) is, ami a túlélési feltételek fenntartását garantálja. Ezzel összefüggésben a kritikus infrastruktúrák védelme is a lakosságvédelem szerves részét képezi.

A beavatkozó állomány egyéni védőeszközzel történő felszereléséért a BM OKF felel, igazodva a baleset által okozott káros szennyezéshez. Az egyik leghatékonyabb védelem megszervezése érdekében azonban szükség van adatokra, ami alapján megfelelő döntés hozható. A felderítés során a felderítést végzők fokozatosan ki vannak téve a kárhelyen jelenlevő veszélyes gőzöknek, gázoknak és anyagoknak. Ezért a KML megfelelő egyéni védőfelszereléssel van

ellátva, valamint olyan kézi és kihelyezett eszközökkel rendelkezik, amelyek hatékonyan azonosítják a jelenlévő vegyületeket és keverékeket.

Kiemelendő a katasztrófavédelmi tervezés alapelve, amelynek központi eleme az együttműködés és a koordináció. A katasztrófavédelem, az egészségügyi ellátórendszer, a rendvédelmi szervek, valamint az önkormányzati struktúrák, közötti összehangolt működés elengedhetetlen a hatékony lakosságvédelem biztosításához. A komplex veszélyhelyzetek kezelése ugyanis meghaladja az egyes szervezetek önálló képességeit, és integrált, több szereplős együttműködési rendszert igényel, amelyben a feladatok, hatáskörök és felelősségek egyértelműen meghatározottak. [74]

Mindezek alapján megállapítható, hogy a lakosságvédelem a hazai szabályozási és intézményi környezetben implicit módon egy komplex, többdimenziós rendszerként értelmezhető. Ez a rendszer magában foglalja a preventív jellegű tevékenységeket, mint a lakosság felkészítése és a kockázatértékelés, a közvetlen védelmi intézkedéseket, ideértve a riasztást, az elzárkóztatást és a kitelepítést, valamint a reaktív beavatkozásokat, így a mentést, mentesítést és helyreállítást. A lakosságvédelem ilyen értelmezése túlmutat a hagyományos, szűkebb értelemben vett védekezési tevékenységeken, és egy integrált, ciklikus működésű rendszert rajzol ki, amely a teljes katasztrófavédelmi életciklust lefedi.

2.3.2 A modern kockázatok kezelése

Jelen értekezés kiemelt figyelmet fordít a veszélyes anyagokkal foglalkozó üzemek és kritikus szervezetek kiberkitettségére, valamint a kibertérből érkező támadások által közvetetten vagy közvetlenül okozott lehetséges ipari balesetek megelőzésére és elhárítására. Ezért fontos kitérni azokra az esetekre, ahol kiber-fizikai rendszerek kompromittálódásából következne be súlyos ipari baleset. Ezen balesetek elhárítása komplex és több hatóság szoros koordinált együttműködését igényelheti. A résztvevő hatóságok a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete (NBSZ NKI) és BM OKF érintett területi és helyi szervei.

Az NBSZ NKI, mint nemzeti eseménykezelő központ az incidensek elhárításában alapvetően koordináló jellegű, technikai támogatást nyújt, valamint a válaszlépésekre javaslatokat fogalmaz meg az érintett szervezet incidenskezelésében résztvevők számára. A helyreállást követően az NKI ellenőrzi a helyreállított állapot megfelelőségét. Ha szükséges, a naplófájlok segítségével rekonstruálja az incidens kiváltó okait és az eredmények alapján javaslatot tesz a

szükséges védelmi intézkedések bevezetésére, amelyek csökkentik a hasonló biztonsági események jövőbeli bekövetkezésének valószínűségét. [75] A hatóságok közötti együttműködési keretet az Európai Unió CER direktívája is előirányozza, melyet a hazai jogrendbe a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény implementált. Ha a baleset hatása kiterjed a környező lakosságra, a Polgári Védelem oldalán lakosságvédelmi feladatok jelentkezhetnek. Az alapvető szolgáltatásokat nyújtó szervezetek kiemelt célpontjai lehetnek a kibertámadásoknak, amennyiben ezen szervezetek üzemfolytonossága megszakad, a lakosság kitettsége a kiesett szolgáltatás negatív hatásaival szemben jelentős lenne. A kritikus szervezetek esetén fontos figyelembe venni a residualis kockázati értékeket, melyek között a dominóhatás kialakulása kiemelkedő valószínűséggel következhet be. Például a villamosenergia-szolgáltatás kiesése számos más ágazatra is azonnali negatív hatással lehet. Ezt a problémát felismerve, az Európai Bizottság elfogadta 2024-ben a *Network Code on Cybersecurity (NCCS)* rendeletet. Az NCC paradigmaváltást jelent, mivel a villamosenergia-rendszert összekapcsolt kiber-fizikai rendszerként kezeli, ahol a kiberbiztonság már nem kizárólag informatikai, hanem rendszerbiztonsági és ellátásbiztonsági kérdés. [76] Az ivóvíz- vagy szennyvízkezelési szolgáltatást nyújtó szervezetek ellen is már számos kiberbiztonsági támadást hajtottak végre az elmúlt években, így szintén jelentős lakosságbiztonsági kockázatot hordozó ágazatról van szó.

Amennyiben alapvető szolgáltatást biztosító kritikus rendszert érő támadás történik a közszolgáltatás ellátásának kiesésekor az, emberi életben, egészségben és az anyagi javakban esett kár megelőzése céljából a közszolgáltatás ideiglenes ellátásáról történő gondoskodás a polgári védelem feladatai közé tartozik. Az ivóvízellátás kiesése esetén a fő feladat gondoskodni az ivóvízellátás fenntartásáról. A polgári védelem által biztosított alternatív ivóvízellátás történhet például mobil víztartályok, vízszállító járművek (tartálykocsik) vagy palackozott víz kiosztásával. A település vezetésével együttműködve a polgári védelem logisztikai támogatást nyújt a vízellátás helyreállításáig, beleértve a víz szállítását, az elosztási pontok kialakítását, és a segélyek koordinálását. Emellett a polgári védelem részt vesz a veszélyhelyzetek elhárításában is, például szennyezett területek izolálásában, ha olyan jellegű a kár, akár az adott terület, eszközök és tárgyak mentesítésében. A polgári védelem részt vesz a lakosság tájékoztatásában is, figyelmezteti az érintett lakosságot a veszélyekre, és ismerteti, milyen óvintézkedéseket kell tenniük a biztonságuk érdekében.

A kiberkockázatokból adódó tartós kiesések minél előbb történő felszámolása érdekében a polgári védelem infokommunikációs egységének személyi állományában javasolt lehet IT biztonság területén jártas szakembereket is beosztani. Így a kritikus infrastruktúra részét képző rendszereket és rendszerelemeket ért kibertámadások hatásainak elhárításában, csökkentésében vagy az okozott károk helyreállításában kompetens segítséget biztosíthatnának az érintett szervezet szakembereinek. [77]

A polgári védelem működésének szempontjából kiemelt jelentőséggel bírnak a vezetési, riasztási és lakosságtájékoztatási feladatokat támogató elektronikus információs rendszerek, amelyek működőképességének fenntartása veszélyhelyzeti időszakban is alapvető követelmény. Ezen kritikus fontosságú rendszereket és infrastruktúrájukat megfelelő kiberbiztonsági védelmi intézkedésekkel szükséges biztosítani, annak érdekében, hogy egy esetleges összehangolt kibertámadás ne akadályozhassa a vezetési, koordinációs és lakosságvédelmi feladatok hatékony végrehajtását. [78]

2.4 A kiber-incidensek kivizsgálásának lehetőségei

Napjainkban a kibertérben napi szinten több száz millió kibertámadást követnek el. [79] Ezen incidensek kivizsgálása digitális forensic módszerekkel történik. Ez az interdiszciplináris tudomány a bűncselekmények felderítésére, bizonyítására és megelőzésére törekszik, saját módszertanokat és eszközöket alkalmazva. [80] Kutatásom során egy hazai igazságügyi szakértővel folytattam félig strukturált interjút, melynek keretében mélyebb megértést sajátítottam el a digitális forensicről, valamint a vizsgálat során végrehajtott operatív lépések technikai hátteréről, ezen interjú keretében kapott válaszokat is igyekeztem a kutatásomban megjeleníteni. A digitális forensic egyik módszertani forrása az amerikai NIST SP 800-86 dokumentum, amely a biztonsági események szakszerű kivizsgálását négy fázisra osztja:

1. adatgyűjtés
2. vizsgálat
3. adatelemzés
4. jelentés [81]

Az adatgyűjtés során az írásvédelmet biztosítani kell, mert az megakadályozza, hogy az adatok véletlenül vagy szándékosan módosuljanak az eredeti médián, miközben továbbításra

kerülnek a vizsgálatot végző forensic számítógépre elemzés céljából például: Tableau Forensic Bridge használatával.

Az adatgyűjtést követően a vizsgálat során az első lépések között szerepelnek a hálózati forgalomfigyelő eszközök, szoftverek vizsgálata pl.: tűzfalak elemzése. Az ipari rendszerek esetén a SCADA rendszerek naplófájlait és a PLC-ket javasolt jobban megvizsgálni, milyen parancsok futottak le rajtuk az incidens bekövetkezésének ideje környékén. Az IP címek figyelése is része az eljárásnak. Fontos ezeket fenntartással kezelni, mert a támadók gyakran használnak különböző VPN-eket, Proxy szervereket, hogy elfedjék valós IP címük, ami által beazonosíthatóvá válhatnának. Ellenben árulkodó nyomokat rejthet a biztonsági esemény bekövetkezése előtti időszak vizsgálata, ugyanis sokszor a támadók a célpont hálózatán úgy néznek körben, mint egyszerű user-ek.
A szakemberek az incidens előtti elmúlt néhány hét naplófájlait elemzik, rendellenességek után kutatva, így a több száz IP-cím közül néhány gyanús azonosítható. Ha szükséges, hatósági közreműködéssel VPN szolgáltatóktól is kikérhetők naplók bűncselekmények felderítésére.

A támadók gyakran használnak a Darkweben elérhető hacker kit-eket, például ransomware, DDoS támadásokhoz, ezekkel könnyen végrehajthatóvá válnak meghatározott sérülékenységekre célzott támadások, mély technikai ismeretek nélkül is. A támadást megelőzően gyakran sérülékenység- és portszkenneléssel térképezik fel a célhálózatot, hogy növeljék támadásaik sikerességét. Számos Dark-Weben lévő ransomware „készlet” feloldó kulcsa elérhető nyilvános oldalakon. Az igazságügyi szakértővel folytatott interjú során megemlítésre került a GitHub, valamint a no more ransom nevű weboldal, ahol hatékony dekódolási eszközök érhetők el, így megelőzhető a váltságdíjak megfizetése. A szakértő hangsúlyozta, hogy minden ransomware támadást követően elsőként érdemes ezeket a forrásokat felkutatni, és megpróbálni ingyenesen visszaszerezni a titkosított adatokat.

A digitális forensic adatelemzési fázisa a vizsgálat eredményeit dokumentált módszerek és technikák segítségével elemzi. Előtérbe helyezi a támadási módszerek azonosítását, az összefüggések keresését más támadásokkal, az indítékok feltárását és a támadás kiinduló helyének behatárolását.

A jelentés készítés során a szakértők dokumentálják a támadás folyamatát, kitérnek rá, hogy hogyan történt a behatolás, milyen módszereket használt a támadó. A jelentés kitér a

vizsgálat során feltárt és azonosított hálózati gyenge pontokra és javaslatokat tesz a biztonság növelésére.

A fenti általános digitális forensic megközelítések az ipari kiber-fizikai rendszerek (OT) környezetében jelentős sajátosságokkal egészülnek ki, különösen veszélyes anyagokkal foglalkozó üzemek esetében. E létesítményekben a kiberincidensek kivizsgálása nem kizárólag információbiztonsági kérdés, hanem közvetlen összefüggésben áll az üzembiztonsággal és a lakosságvédelmi kockázatokkal is.

Az OT környezetben az incidenskezelés egyik kulcseleme a támadók laterális mozgásának (lateral movement) feltárása. A támadók gyakran az IT rendszereken keresztül jutnak be a szervezet hálózatába, majd fokozatosan haladnak az OT környezet irányába, kihasználva a nem megfelelően szegmentált hálózati architektúrát. A laterális mozgás során hitelesítési adatok megszerzése, jogosultságkiterjesztés, valamint rendszergazdák által használt eszközök (pl. PowerShell, RDP) alkalmazása figyelhető meg, amely jelentősen megnehezíti az észlelést. OT környezetben ez különösen kritikus, mivel a támadók végül elérhetik a SCADA rendszereket vagy közvetlenül a vezérlőberendezéseket (PLC-k), és fizikai folyamatokat befolyásolhatnak.

A kivizsgálást tovább nehezíti az OT rendszerekre jellemző magas fokú beszállítói függőség (vendor lock-in). Számos ipari berendezés, például gyártósorok, kazánok, gázmotorok vagy vegyipari reaktorok vezérlőrendszerei, zárt, gyártóspecifikus architektúrával rendelkeznek, amelyekhez az adott szervezetnek nincs közvetlen ráhatása, így a naplófájlokhoz való hozzáférés, a konfigurációk kezelése vagy akár egy rendszer újraindítása is kizárólag a beszállító által delegált szakértők bevonásával lehetséges. Ez nemcsak időbeli késedelmet okoz az incidens kivizsgálásában, hanem jelentős költségnövekedéssel is jár. Míg IT környezetben egy forensic vizsgálat viszonylag gyorsan és házon belül is elvégezhető, addig OT rendszerek esetében egy-egy kritikus berendezés vizsgálata vagy leállítása jelentős anyagi hátrányt képes okozni.

A veszélyes anyagokkal foglalkozó üzemek esetében további sajátosság, hogy a forensic tevékenységek nem veszélyeztethetik a technológiai folyamat stabilitását. Ennek következtében a „live forensics”[21] kiemelt jelentőséggel bír, azonban ennek végrehajtása korlátozott, mivel a rendszerbe történő beavatkozás maga is kockázatot hordozhat (pl. egy vezérlő újraindítása

[21] éles rendszereken történő adatgyűjtés és adatelemzés

folyamatleállást vagy akár veszélyhelyzetet idézhet elő). Emiatt a bizonyítékgyűjtés gyakran indirekt módon, például hálózati forgalomelemzés, historian rendszerek[22] adatainak vizsgálata, illetve biztonsági mentések elemzése útján történik. [82]

A támadások vizsgálata során külön figyelmet kell fordítani az ipari kommunikációs protokollokra (pl. Modbus, OPC, DNP3), amelyek gyakran nem rendelkeznek beépített hitelesítési és naplózási mechanizmusokkal. Ez megnehezíti a támadási események rekonstruálását és az attribúciót. Ezen túlmenően a veszélyes üzemekben a támadások célja nem feltétlenül az adatlopás, hanem a fizikai folyamatok manipulálása, így ipari baleset vagy üzemzavar okozása.

A veszélyes anyagokkal foglalkozó üzemekben bekövetkező események kivizsgálására vonatkozó 219/2011 (X.20.) Korm. rendelet alapvetően az ipari balesetekre és üzemzavarokra fókuszál, azonban közvetett módon lehetőséget biztosít implicit módon a kiberincidensek vizsgálatára is, amennyiben azok műszaki, szervezeti vagy irányítási rendszerhez kapcsolódó eseményként jelennek meg.

A vonatkozó előírások értelmében az üzemeltető köteles a veszélyes anyagokkal kapcsolatos súlyos baleset vagy esemény körülményeit kivizsgálni, és annak eredményéről az iparbiztonsági hatóságot meghatározott határidőn belül tájékoztatni. Ez a kötelezettség kiterjed minden olyan okfeltárásra, amely a baleset kialakulásában szerepet játszott, így értelmezhető módon magában foglalhatja a kiberbiztonsági incidensek vizsgálatát is, különösen abban az esetben, ha a technológiai folyamatokba történő illetéktelen beavatkozás feltételezhető.

A hatósági oldalról az iparbiztonsági hatóság a tudomásszerzést követően rövid határidőn belül helyszíni ellenőrzést folytat le, amely során feltárja a műszaki, vezetési és szervezeti hiányosságokat. E folyamat keretében, bár explicit módon nem nevesítve, lehetőség nyílik a kiberbiztonsági sérülékenységek, azonosítására is. Súlyos hiányosságok esetén az utóellenőrzési kötelezettség biztosítja, hogy a feltárt problémák ténylegesen megszüntetésre kerüljenek.

Fontos megemlíteni, hogy az OT környezetben egy biztonsági esemény következménye gyakran nem önálló „kiberincidensként”, hanem fizikai eseményként (pl. technológiai zavar,

[22] olyan ipari adatgyűjtő és archiváló rendszer, amely az ipari folyamatokból származó adatokat időbélyeggel ellátva naplózza és hosszú távon tárolja.

üzemfolytonosság kompromittálódása, vagy veszélyes anyag kibocsátás) manifesztálódik. Ennek következtében a kivizsgálási kötelezettség automatikusan aktiválódik, függetlenül attól, hogy az esemény kiváltó oka digitális vagy fizikai eredetű volt. Ez a szabályozási sajátosság lehetőséget teremt arra, hogy a digitális forensic módszerek integrálásra kerüljenek a hagyományos ipari balesetvizsgálati eljárásokba.

Mindazonáltal megállapítható, hogy a jelenlegi szabályozási környezet nem tartalmaz explicit előírásokat a kiberincidensek kivizsgálására vonatkozóan a veszélyes üzemek esetében. Ez különösen problémás lehet az OT rendszerek komplexitása, a beszállítói függőségek, valamint a magas költség- és kockázati szintek miatt.

2.5 A katasztrófavédelmi helyreállítás rendszere és kiterjesztésének szükségessége

A katasztrófavédelem feladat-ciklusának egyik meghatározó eleme a helyreállítás, amelynek célja a káreseményt követően a társadalmi és gazdasági működőképesség visszaállítása, valamint az alapvető életfeltételek biztosítása. A hazai szabályozási és intézményi struktúrában a helyreállítási feladatok döntően a polgári védelem és a katasztrófavédelem szervezetrendszeréhez kapcsolódnak, különös tekintettel a lakosságvédelmi intézkedésekre és a kritikus infrastruktúrák működésének helyreállítására.

A helyreállítási tevékenység részfolyamatait a veszélyhelyzeti és katasztrófavédelmi feladatok végrehajtásáról rendelkező 234/2011. (XI. 10.) Korm. rendelet strukturált módon határozza meg. A szabályozás értelmében a helyreállítás a káreseményt követően, a védekezési szakasz lezárását követően megkezdődő, több lépcsőben megvalósuló folyamat, amelynek elsődleges célja a károk felmérése és a helyreállítási intézkedések megalapozása. Ennek keretében kiemelt jelentőséggel bír a kárfelmérés, amelyet a jogszabályban meghatározott kárbecslő munkacsoportok végeznek egységes szakmai szempontok alapján. A kárfelmérés eredményei szolgálnak alapul a szükséges beavatkozások meghatározásához, valamint az esetleges állami támogatások, különösen a vis maior támogatás, önkormányzatok általi igénybevételéhez. A folyamat következő lépéseként a helyreállítási feladatok tervezése és priorizálása történik meg, amely során figyelembe kell venni a lakosság alapvető ellátásának biztosítását, a létfontosságú infrastruktúrák működőképességének helyreállítását, valamint a további károk megelőzésének szempontjait.

Ugyanakkor a 21. századi kockázati környezetben egyre hangsúlyosabbá válik az a kihívás, hogy a helyreállítás fogalma már nem értelmezhető kizárólag fizikai károk elhárításaként, hanem kiterjed az információs és gyártástechnológiai rendszerek működésének visszaállítására is.

A helyreállítás felelősségének kérdése kapcsán gyakran megjelenik az az implicit megközelítés, miszerint az incidensek kezelése és következményeinek felszámolása elsődlegesen az érintett gazdálkodó szervezet működési kockázati körébe tartozik. Ez a megközelítés a klasszikus üzletmenet-folytonossági és kockázatkezelési logikával összhangban áll, azonban a kritikus infrastruktúrák és veszélyes anyagokkal foglalkozó üzemek esetében nem tekinthető teljeskörűen alkalmazhatónak.

A korszerű biztonsági irányítási rendszerek, ideértve a kiberbiztonsági szabványokon és iparági legjobb gyakorlatokon alapuló kontrollmechanizmusokat, képesek a kockázatok jelentős részének csökkentésére, azonban nem garantálják az incidensek teljes körű megelőzését. Különösen igaz ez az úgynevezett államilag támogatott kibertámadások (nation sponsored) esetében, amelyek magas erőforrás- és szakértelem-szintjük révén képesek a fejlett, kockázatokkal arányosan kialakított védelmi rendszerek kompromitálására is.

Ambrusz József kutatásai rámutatnak arra, hogy a helyreállítás komplex, többszintű folyamat, amely magában foglalja a fizikai infrastruktúra rekonstrukcióját, a szolgáltatások újraindítását, valamint a társadalmi működés normalizálását. Megközelítésében a helyreállítás nem egyszerűen technikai feladat, hanem koordinációs és irányítási kihívás is, amelyben az állami, önkormányzati és gazdálkodó szervezetek együttműködése kulcsfontosságú. Továbbá hangsúlyozásra kerül, hogy a helyreállítás hatékonysága jelentős mértékben függ az előzetes felkészültségtől, a tervezési folyamatoktól, valamint a különböző szervezeti szereplők közötti felelősségi viszonyok egyértelmű meghatározásától.

E megállapítások különös jelentőséggel bírnak a veszélyes anyagokkal foglalkozó üzemek és a kritikus infrastruktúrák esetében, ahol a helyreállítás nem csupán gazdasági kérdés, hanem közvetlen lakosságvédelmi relevanciával is rendelkezik. A hagyományos megközelítés azonban alapvetően fizikai káreseményekből indul ki (pl. ipari balesetek, természeti katasztrófák), és kevésbé reflektál azokra az új típusú fenyegetésekre, amelyek az információs rendszereken keresztül érik az üzemeltető szervezeteket. A jelenlegi hazai jogszabályi

környezetben nincsenek egyértelműen definiálva egy ipari rendszereket is érintő helyreállítás felelőségi és feladatkörei. [17]

A kibertámadások, különösen az ipari szereplőket érintő zsarolóvírus (ransomware) típusú incidensek sajátossága, hogy elsődlegesen az információs és kiber-fizikai rendszereket érintik, ugyanakkor közvetett módon fizikai következményekkel is járhatnak, különösen az ipari vezérlőrendszerek (ICS/SCADA) kompromittálódása esetén. Egy kettős jogállású gazdálkodó szervezet, amely egyidejűleg minősül veszélyes üzemnek és kritikus infrastruktúrának, esetében egy ilyen támadás komplex, kiber-fizikai válsághelyzetet eredményezhet és az általa nyújtott alapvető szolgáltatás kompromittálódhat, ezzel pedig a lakosság is érintetté válik.

Ebben az összefüggésben a helyreállítás kérdése már nem egyértelműen illeszthető a jelenlegi intézményi és jogi keretek közé. Míg a kibervédelmi incidensek kezelése elsősorban a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) hatáskörébe tartozik, addig a fizikai következmények kezelése és a lakosságvédelem az Országos Katasztrófavédelmi Főigazgatóság (BM OKF) feladatkörében jelenik meg. A két terület közötti kapcsolódási pontok azonban a helyreállítás fázisában nem egyértelműen szabályozottak.

A jelenlegi gyakorlat alapján megállapítható, hogy az informatikai rendszerek és ipari vezérlőrendszerek tényleges helyreállítása döntően az üzemeltető gazdálkodó szervezet felelősségi körébe tartozik. Ez magában foglalja az adatvisszaállítást, a rendszerek újrakonfigurálását, valamint a működés biztonságos újraindítását. Az állami szervek szerepe ezzel szemben jellemzően korlátozott: a kibervédelmi szervezetek incidenskezelési támogatást és szakmai iránymutatást nyújtanak, míg a katasztrófavédelem a következmények kezelésére és a lakosságvédelmi intézkedésekre koncentrál. Azonban a kritikus rendszereket érintő kibertámadások nem értelmezhetők kizárólag egyedi szervezeti kockázatként, hanem olyan rendszerszintű fenyegetésként jelennek meg, amelyek kezelése és különösen a helyreállítás már túlmutat az egyes gazdálkodó szervezetek kompetenciáján. Ennek ellenére a jelenlegi szabályozási és intézményi keretek között a helyreállítás operatív felelőssége továbbra is elsődlegesen az üzemeltetőnél marad, ami feszültséget eredményez a kockázat jellege és a felelősségi rendszer között.

A hazai szabályozási környezetben a helyreállítás állami támogatásának egyik meghatározó eszköze a vis maior támogatási rendszer, amelynek részletes szabályait a vis maior támogatás felhasználásának részletes szabályairól szóló 9/2011. (II. 15.) Korm. rendelet

tartalmazza. A rendszer alapvetően a helyi önkormányzatok által ellátott közfeladatokhoz kapcsolódó, előre nem látható, jellemzően természeti eredetű káresemények kezelésére került kialakításra, és elsődlegesen fizikai infrastruktúrában, illetve lakóingatlanokban keletkezett károk helyreállításának finanszírozását támogatja. A kárfelmérés és a támogatási igények megalapozása során az Országos Katasztrófavédelmi Főigazgatóság koordinációs és szakmai támogató szerepet tölt be, azonban a rendszer nem terjed ki a gazdálkodó szervezetek ingóságaiban, különösen az információs vagy ipari vezérlőrendszereiben, keletkezett károk kezelésére.

Ez a helyzet egyértelműen rámutat egy szabályozási és irányítási hiátusra, amely a kiber-fizikai rendszerek helyreállításának területén jelentkezik. Amíg a hagyományos helyreállítási modellek elsősorban fizikai károkból indulnak ki, addig a 21. századi, modern fenyegetési környezetben szükségessé válik a helyreállítás fogalmának kiterjesztése az információs rendszerekre is. Ennek hiányában a felelősségi viszonyok fragmentáltak maradnak, ami kritikus helyzetben a helyreállítás hatékonyságának csökkenéséhez vezethet.
A fragmentált felelősségi struktúra gyakorlati megjelenését jól szemlélteti a Jaguar Land Rover vállalatot érintő 2025 novemberi kibertámadás esete, amely a gyártási tevékenységben és az üzleti működésben is jelentős zavarokat okozott. Bár a Jaguar Land Rover nem alapvető szolgáltatást nyújt, az incidens rámutatott arra, hogy egy komplex ipari gyártási környezetben a kibertámadás túlmutat az informatikai területet érintő problémán, ezen támadások már közvetlen hatással lehetnek a fizikai termelési folyamatokra és az ellátási lánc működésére is.

A helyreállítás folyamata döntően a vállalati működés keretein belül zajlott, beleértve az informatikai rendszerek helyreállítását, a termelési kapacitások fokozatos újraindítását, valamint az üzletmenet stabilizálását. Az állam szerepvállalása túlmutatott a klasszikus kibervédelmi támogatáson: a brit kormányzat jelentős összegű, mintegy 1,5 milliárd font értékű gyorshitellel támogatta a vállalat működőképességének fenntartását, amely egyértelműen a gazdasági stabilizáció irányába mutató beavatkozásként értelmezhető. Fontos látni, hogy a mai modern nagy ipari vállalatok beszállítói láncai kiterjedtek és rengeteg kkv dolgozik egy-egy nagy gyártó vállalatnak. Éppen az ilyen szervezetek gyors és hatékony helyreállítása a beszállítói lánc működőképességének megőrzését is célozza. Ezek az esetek rávilágítanak arra, hogy egy mikrogazdasági szinten értelmezhető működési zavar a beszállítói láncokon keresztül makrogazdasági jellegű hatásokat is kiválthat, ebből az aspektusból vizsgálva is indokolt az állami beavatkozás. [83]

A fenti eset alapján megállapítható, hogy a helyreállítás nem egységesen értelmezett állami feladat, hanem több szinten megvalósuló tevékenység, amelyben a technológiai, gazdasági és társadalmi dimenziók eltérő intézményi szereplőkhöz kapcsolódnak. Ez a struktúra különösen problematikus lehet olyan kiber-fizikai rendszerek esetében, ahol a technológiai helyreállítás elmaradása közvetlen hatással lehet a társadalmi és gazdasági stabilitásra.

Indokoltnak tekinthető egy integrált, kiber-fizikai helyreállítási megközelítés kialakítása, amely egyértelműen definiálja az egyes szereplők feladatait, valamint biztosítja a különböző szakterületek és hatóságok közötti koordinációt. Egy ilyen modellben a gazdálkodó szervezetek üzletmenet-folytonossági és katasztrófa-helyreállítási tervei (BCP/DRP) szorosabban kapcsolódnának az állami incidenskezelési és katasztrófavédelmi mechanizmusokhoz, ezáltal csökkentve a jelenleg tapasztalható szabályozási „fehér foltot”.

2.6 Egy ingyenes terjedés-modellező szoftver fejlesztési lehetősége

A kutatásomhoz használt veszélyes anyag modellező eszköz kiválasztásánál kulcsfontosságú volt, hogy a szoftver széleskörű szakmai és oktatási közönség számára hozzáférhető legyen. A magyar honvédség és a BM Országos Katasztrófavédelmi Főigazgatóság által használt rendszerek fejlett, több paraméteres döntéstámogató rendszerek, nem elérhetők a nyilvánosság számára, valamint kutatási célokra sem, a rendszerek közötti közvetlen összehasonlításra nem volt lehetőségem, de jelen disszertációban sem lenne megengedett, és etikus sem ezen rendszerek műszaki tartalmainak közzététele. Ezen okokból kifolyólag a kutatás tárgyaként az Egyesült Államok Környezetvédelmi Ügynöksége (továbbiakban: EPA) és a Nemzeti Óceán- és Légkörkutató Hivatal (továbbiakban: NOAA) által kifejlesztett ALOHA® (Areal Locations of Hazardous Atmospheres) szoftvert választottam. Bár az ALOHA nem a legfejlettebb terjedésmodellező szoftver, ingyenes, nemzetközileg elismert és alacsony számítási kapacitással rendelkező info-kommunikációs eszközökön is alkalmazható. Az ALOHA modell elsősorban gyors, úgynevezett screening jellegű következményelemzésre szolgál, amely operatív katasztrófavédelmi döntéstámogatás esetén különösen fontos. Az ilyen modellek célja nem a komplex atmoszferikus folyamatok részletes szimulációja, hanem a veszélyeztetett területek gyors becslése a beavatkozás korai szakaszában vagy az ipari létesítmény üzemeltetői által készített elsődleges becslésre.

A kutatásom tudományos újdonsága abban rejlik, hogy bebizonyítja, hogy egy évtizedek óta létező, bevált szoftver „modernizálható” egy kortárs mikrovezérlő-alapú hardverrel, jelen esetben egy ESP32-alapú hordozható, digitális meteorológiai állomással történő integráció révén, ezáltal kiterjesztve funkcionalitását és javítva használhatóságát költséghatékony és hordozható formában. [84] A kutatás tárgyaként kiválasztott szoftvernek vannak limitációi is.

Alapvetően két matematikai modellt használ a terjedés kiszámításához: a Gauss-impulzus modellt és a nehéz gáz modellt (Dense Gas Dispersion, DEGADIS).

A Gauss-impulzus modell kiválóan alkalmas gyors számításokhoz, és jó közelítést ad a stabil légköri mozgásokhoz. Azonban csak sík terepen, állandó, homogén szélviszonyok esetén használható, így a városi környezet változó domborzata nem kerül figyelembevételre. A modell nem alkalmazható robbanásveszélyes, impulzus-szerű szivárgásokra. A DEGADIS modell a nehéz gázok terjedését veszi figyelembe, az ALOHA szoftver automatikusan átvált erre a számítási modellre, ha a levegőnél nehezebb anyagot választ ki a felhasználó, de egydimenziós megközelítést alkalmaz, és nem veszi figyelembe az időfüggő meteorológiai változásokat. A DEGADIS pontossága jelentősen csökken, ha a terep nem sima. Mindkét modell fontos korlátozása, hogy az ALOHA maximum 10 km-ig számol, ami nagy kibocsátások esetén nem elegendő. Ezenkívül sem a Gauss-modell, sem a DEGADIS-modell nem veszi figyelembe a kémiai reakciókat, a hőmérséklet hatását, a talaj nedvességtartalmát, a sugárzási hatásokat, vagy a robbanásszerű kibocsátásokat, ami eltéréseket okozhat. [85]

A szoftver úgy került kialakításra, hogy csatlakoztatható hozzá egy hordozható meteorológiai állomás (Station for Atmospheric Measurements, SAM), amelynek segítségével elkerülhető a kézi adatbevitel, és a legpontosabb, legfrissebb időjárási paraméterek tölthetők be automatikusan. A tudományos kutatásom elsődleges célja az ALOHA szoftver preventív-detektív képességének javítása volt egy olyan „digitális SAM” létrehozásával, amely az aktuális adatok mellett, illetve azokon túl előrejelzett meteorológiai adatokat is szolgáltat, így lehetővé téve egy időben jobban elhúzódó biztonsági incidens jobb nyomon követését és több jövőbeli időpontra vonatkozó terjedési szcenáriók készítését egy adott időpontban. Ennek az extra inputnak köszönhetően a szoftver funkcionalitása is javul. A fejlesztés során egy ESP32 energiahatékony mikrokontrollert használtam „digitális meteorológiai állomásként”. A külső hordozható fizikai eszköznek platformfüggetlennek kell lennie. Az ESP32 további előnye, hogy nagyon költséghatékony megoldás, Wi-Fi és Bluetooth képességekkel rendelkezik.

Az eszköz programozása az Arduino integrált fejlesztői környezet (IDE) segítségével történik, amely a C++ nyelv szintaxisán alapuló, mikrokontrollerekhez optimalizált programozási környezetet biztosít. Az ESP32 programozásakor figyelembevételre került a NOAA Emergency Response Division – Office of Response and Restoration által publikált, hordozható meteorológiai állomások tervezéséről szóló útmutató dokumentuma. [86]

A dokumentum célja, hogy meghatározza a hordozható meteorológiai állomások tervezési irányelveit, amelyek strukturált meteorológiai adatokat tudnak biztosítani a terjedés modellezéséhez. A dokumentumban szereplő ajánlások tartalmazzák a szükséges időjárási paraméterek, az adatrögzítés formátumát és a soros kommunikációs protokollok jellemzőinek részleteit.

A dokumentum alapján meghatározásra került a baudrate[23], az adatstruktúra és azok a minimális meteorológiai változók, amelyeket az ESP32-nek az ALOHA szoftver számára biztosítania kellett.

Az eszköz alapvető funkciói tekintetében az ESP32 egy beágyazott webszervert futtat, amely lehetővé teszi a felhasználó számára, hogy web böngészőn keresztül egy előre meghatározott helyi IP-címet elérve annak a grafikus felületét használva kiválassza a helyszínt, valamint azt, hogy aktuális vagy előrejelzett meteorológiai adatokat szeretne-e lekérni.

Az ESP32 a kiválasztott paraméterek alapján API-hívást kezdeményez a meteorológiai adatszolgáltató felé, mely ez esetben az openweathermap.org, majd a beérkező meteorológiai adatokat JavaScript Object Notation (JSON) formátumban fogadja. Végül ezeket az adatokat olyan struktúrába alakítja át, amelyet az ALOHA képes feldolgozni, és úgy érzékeli a kommunikációt, mintha egy fizikai hordozható meteorológiai állomásról kapná az adatokat soros porton keresztül. Az API-hívást követően a felhasználó a beágyazott webszerver felületén további meteorológiai paramétereket (relatív páratartalmat és felhőzetet) is megtekinthet és felhasználhat az ALOHA software-ben.

A sikeres működés érdekében meg kellett határozni bizonyos állandókat a szoftvernek elküldendő adatkészletben, például az eszköz akkumulátorának feszültségszintjét és az eszköz azonosítóját, amelyek kreált „nem valós” adatok. Az ALOHA szoftverrel való kommunikáció során a soros kapcsolat paramétereit 1200 baud átviteli sebességre és 8 adatbitre kellett beállítani.

[23] Adatátviteli sebességet meghatározó érték.

A rendszer emellett a szélirány szórását is kiszámítja. Mivel a szélirány ciklikus jellegű változó, a hagyományos szórásszámítási képletek alkalmazása helyett a programkódba a Yamartino-féle módszer került beépítésre. Ez az eljárás a legrosszabb esetben is ±2% eltérést eredményez, ami egy egyszerű és gyorsan számítható közelítő módszer esetében igen jó pontosságnak tekinthető.

A Yamartino-féle módszer a következőképpen írható fel:

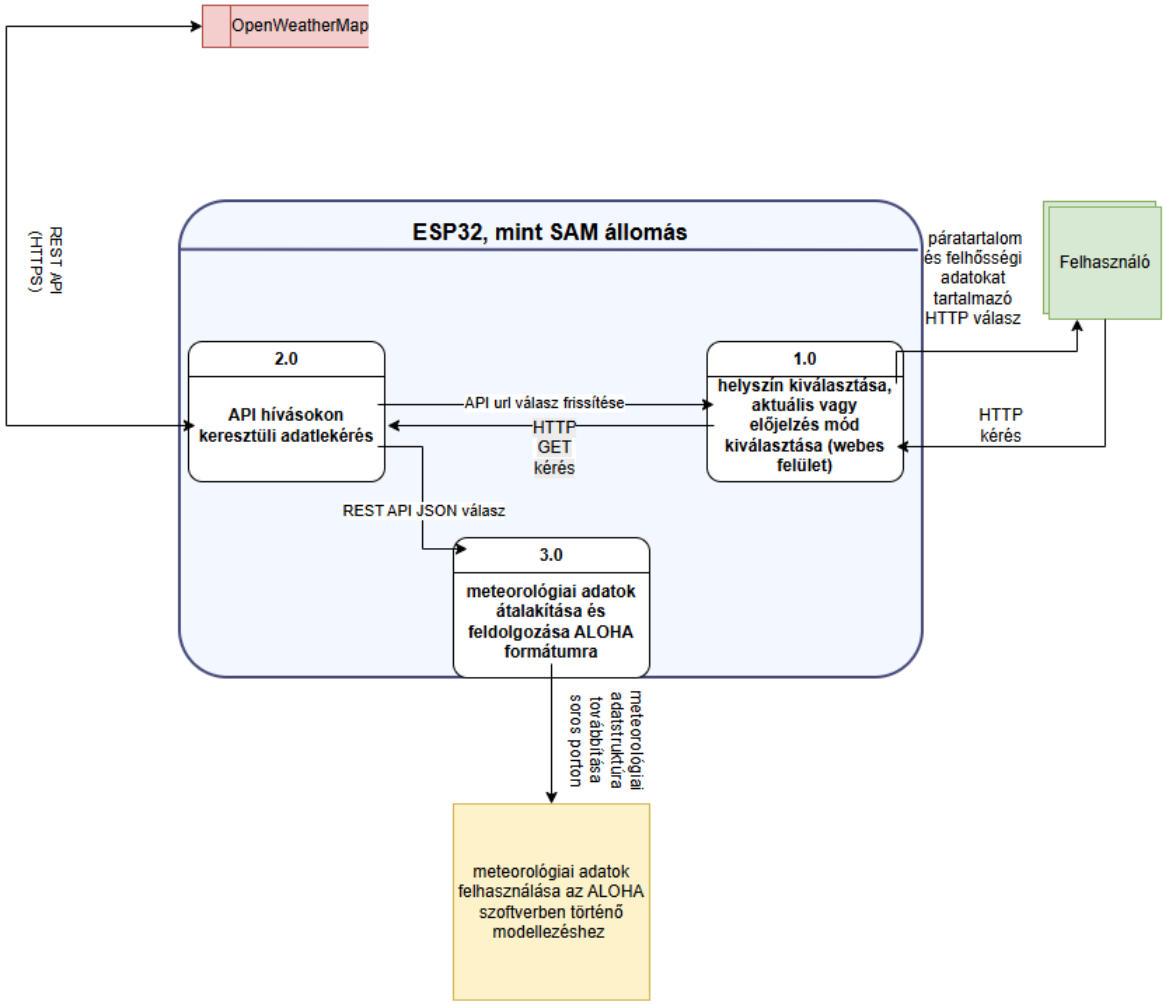
$S = \frac{1}{N}\sum_{i=1}^{N} sin\theta i\,;\; C = \frac{1}{N}\sum_{i=1}^{N} cos\theta i$

$\sigma_\theta = arcsin(\varepsilon)[1 + (\frac{2}{\sqrt{3}} - 1)\,\varepsilon^3]$ ahol $\varepsilon = \sqrt{1 - (S^2 + C^2)}$

$$\frac{2}{\sqrt{3}} - 1 = 0{,}1547$$

A Yamartino-módszer a szélirány ciklikus jellegét figyelembe véve a mért irányok szinusz- és koszinuszértékeinek átlagát használja. Az „n” a mérések számát jelenti, az θi az egyes mért szélirányértékeket jelöli, az $i$index pedig az adott mérési elem sorszámára utal. A képletben az „S” a szélirányok szinuszértékeinek átlaga, míg a „C” a koszinuszértékek átlaga, amelyekből meghatározható a szélirány cirkuláris szórása. [87]

A lenti ábra a fejlesztett rendszer működési folyamatát, valamint az egyes komponensek közötti kommunikációs kapcsolatokat szemlélteti. Az architektúra bemutatja a felhasználói webes interfész, az ESP32-alapú „digitális SAM” modul, a külső meteorológiai adatszolgáltató és az ALOHA szoftver közötti adatáramlást, illetve az alkalmazott kommunikációs protokollokat. Az ábrán nyomon követhető a meteorológiai adatok HTTP/REST API alapú lekérdezése, a JSON-formátumú válaszok feldolgozása, valamint az adatok ALOHA által értelmezhető struktúrává történő átalakítása és soros kommunikáción keresztüli továbbítása.



9. ábra Az ESP32 mikrovezérlő adatáramlási diagramja, készítette: a szerző

2.7 A rendszer gyakorlati használata

A következő alfejezet bemutatja az ALOHA® terjedésmodellező szoftverrel integráltan működő ESP32-alapú meteorológiai adatgyűjtő rendszer működési folyamatának főbb lépéseit. A fejlesztés során fontos szempontként került megfogalmazásra az egyszerű kezelhetőség, az ALOHA szoftverhez történő könnyű csatlakoztathatóság, valamint az egyszerű felhasználói felület.

2.7.1 Rendszerkapcsolatok és adatbevitel

Az integrált rendszer működésének megkezdésekor a felhasználó első lépésként az ESP32-alapú meteorológiai állomást egy laptop vagy asztali számítógép USB-portjához csatlakoztatja. Az operációs rendszer automatikusan felismeri az eszközt és a hozzárendelt COM-porton

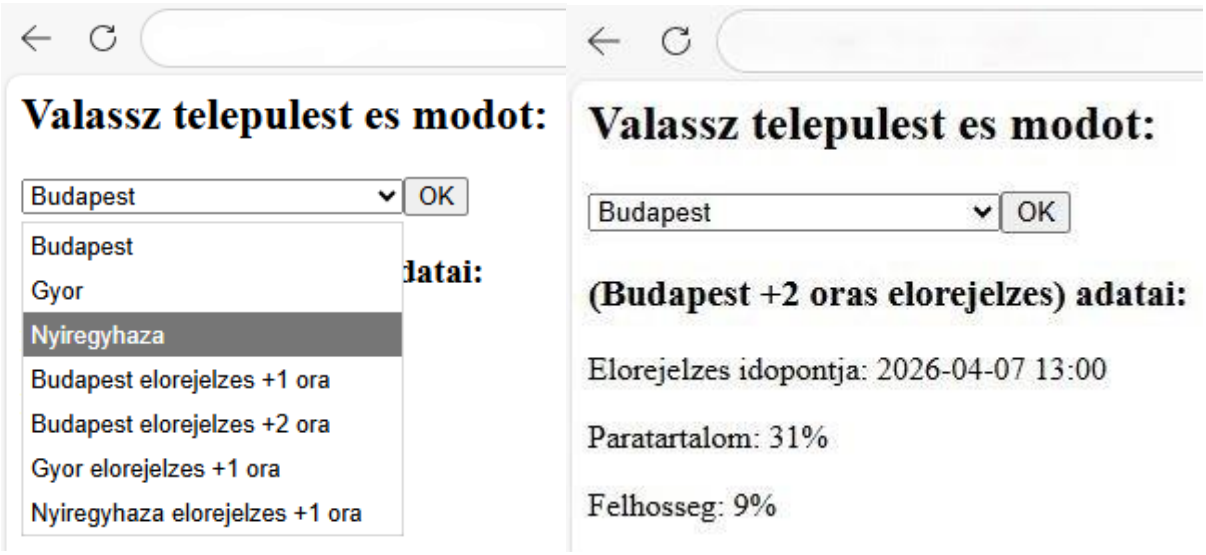
keresztül soros kommunikációs kapcsolatot létesít. Ez lehetővé teszi, hogy a felhasználó az ALOHA szoftvert ezzel párhuzamosan futtassa.

A következő lépésben a felhasználó az eszköz konfigurációs felületét egy szabványos webböngésző segítségével érheti el, amelyhez a böngésző címsorába be kell írnia az ESP32 helyi IP-címét. Ez előzetesen DHCP-n keresztül beállításra került, így az eszköz mindig ugyanazon az IP címmel érhető el. Miután a böngészőben beírtuk az IP-címet megnyílik a mikrokontroller által hosztolt beépített webes felület, amely lehetővé teszi a kívánt célterület kiválasztását, valamint a meteorológiai adatok lekérdezési módjának beállítását (aktuális vagy előrejelzett adatok).

A felhasználói felület kialakításakor elsődleges szempont volt az egyszerűség és az átláthatóság biztosítása, annak érdekében, hogy a rendszer működése ne terhelje aránytalan mértékben az ESP32 mikrokontroller számítási kapacitását.

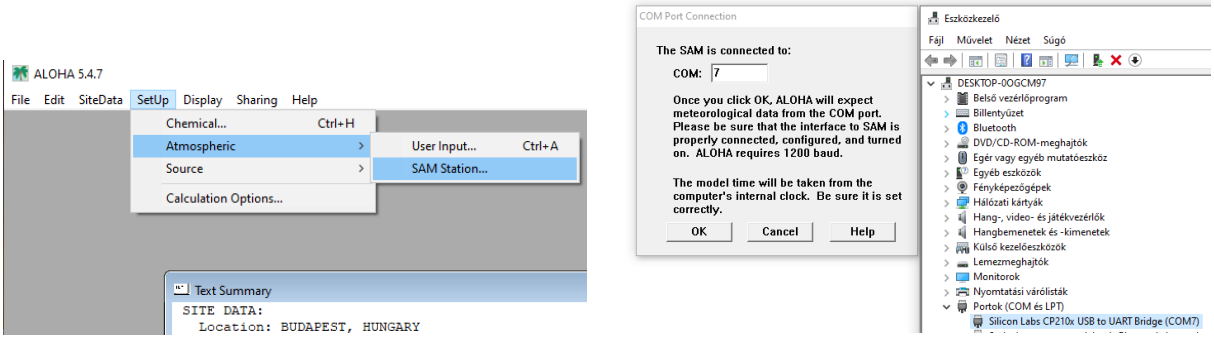
A felhasználói felületen egyértelmű visszajelzés jelenik meg, amint a felhasználó a legördülő menüből kiválasztja a kívánt települést, valamint az adatkérés típusát (aktuális vagy előrejelzési mód, előrejelzési mód esetén a lekérdezett értékekhez tartozó időpont is megjelenítésre kerül). Mivel az ALOHA szoftver a SAM Station használata esetén a relatív páratartalom és a felhőzet értékeinek manuális megadását igényli, az ESP32 által működtetett felhasználói felület ezeket az értékeket automatikusan megjeleníti a felhasználó számára, közvetlenül az API-lekérdezés válaszából kinyerve. Ez a megoldás jelentősen felgyorsítja az adatbevitel folyamatát és csökkenti az emberi hibázás valószínűségét.

A kutatás során reprezentációs célból Budapest tekintetében 1 és 2 órás előrejelzés is elérhető, a többi településnél csak 1 órás előrejelzés került implementálásra az előrejelzés módban, azonban az API hívásoknak köszönhetően lehetőség van az előrejelzési időközök rugalmas beállítására a forráskódban, így igény szerint rövidebb vagy hosszabb időtávra vonatkozó előrejelzések is lekérdezhetővé válhatnak. Különböző forgatókönyvek vizsgálatához akár több előrejelzési mód párhuzamosan is konfigurálható, például 1 órás előrejelzés, 3 órás előrejelzés, 6 órás előrejelzés. Az ESP32 firmware emellett az aktuális meteorológiai paraméterekre vonatkozóan 5 perces mozgóátlagot számít, és minden új API-lekérdezés során frissíti az átlagolt adatokat tartalmazó tömböt annak érdekében, hogy az ALOHA számára stabil és reprezentatív bemeneti értékeket biztosítson.



10. ábra Az ESP32 beágyazott webszerverének felhasználói felülete, készítette: a szerző

A megfelelő meteorológiai adatok és lokáció kiválasztását követően a felhasználónak az ALOHA szoftvert kell elindítania és miután megadta az érintett települést és az épülettípust, a kémiai anyag adatait ki kell választania a „SAM station” használatát. Annak érdekében, hogy az eszközt a szoftver felismerje, mint „hordozható meteorológiai állomás”, meg kell adni, melyik com-porton található. Ehhez érdemes az eszközkezelőből kiolvasni, mely com-porton van a mikrovezérlő.



11. ábra A digitális meteorológiai állomás kiválasztása az ALOHA szoftverben, készítette: szerző

Ezt követően a szoftver az ESP32-től kapott adatstruktúrát fél percenként beolvasva és az abban lévő meteorológiai értékek felhasználásával számítja ki a veszélyes anyag terjedési csóváját.

A továbbiakban még szükséges kiválasztani a kibocsátás forrását, majd az elkészült veszélyességi zóna kiexportálhatóvá válik, kml. vagy pas. fájlkiterjesztési formátumba. A PAS (Polygon Attribute Set) formátum kifejezetten térinformatikai elemzésekhez készült, és lehetővé teszi az eredmények integrálását GIS-környezetekbe, például az ArcMap

alkalmazásba. Ezzel szemben a KML. (Keyhole Markup Language) fájlformátum külső platformokon (pl. Google Earth Pro) történő vizualizációt tesz lehetővé.

2.7.2 Az eredmények vizualizált megjelenítése a Google Earth Pro-n keresztül

A Google Earth Pro alkalmazás került felhasználásra az ALOHA által generált AEGL-alapú veszélyességi zónák kml. formátumú fájlok vizualizálására. Ez a platform lehetővé teszi a georeferált, nagy felbontású térképi megjelenítést valós terep- és infrastruktúra-adatokon, ezáltal javítva a döntéshozók helyzetismeretét. Emellett támogatja több szcenárió (például aktuális és előrejelzett meteorológiai adatokon alapuló esetek) együttes megjelenítését, ami lehetővé teszi a terjedési folyamatok közvetlen összehasonlítását különböző környezeti feltételek mellett. Ez különösen hasznos mind operatív tervezési, mind képzési célokra.

Az ALOHA által generált veszélyzónák megjelenítése során a szélirány-bizonytalansági vonalak a terjedési tengely irányának bizonytalanságát jelölik, amely a modellezési időszakban mért szélirány-ingadozásokból adódik. A jelen vizsgálatban ezek a vonalak kizárólag a leghosszabb veszélyzónához, azaz az AEGL-1 (0,2 ppm) szinthez kapcsolódóan jelennek meg, és a veszélyeztetett terület oldalirányú eltérésének lehetséges mértékét szemléltetik. Fontos kiemelni, hogy ezek nem különálló veszélyzónák, ugyanakkor jelentős szerepet tölthetnek be a lakosságvédelmi tervezés során.

2.7.3 Alkalmazási lehetőségek

A fejlesztés elsődlegesen oktatási célú felhasználást támogat, például tűzoltói képzések, katasztrófavédelmi oktatás vagy vegyipari munkahelyi képzések során, szemléltetve a meteorológiai adatok valós idejű vagy előrejelzésen alapuló felhasználásának lehetőségeit. A rendszer lehetőséget biztosít a résztvevők számára annak megtapasztalására, hogy a veszélyes anyagok terjedési jellemzői miként változnak különböző időjárási körülmények között, valós idejű és előrejelzett meteorológiai adatok felhasználásával. Mindez összhangban áll a katasztrófavédelmi kutatások legújabb irányzataival, amelyek hangsúlyozzák a nemzetközi és hazai jó gyakorlatok, a műszaki innovációk, valamint az alkalmazott kutatási eredmények integrálásának fontosságát az iparbiztonsági oktatásban és a képességfejlesztésben, a veszélyes tevékenységekhez kapcsolódó kockázatok hatékony csökkentése érdekében. [88]

A rendszer további alkalmazási lehetőségeként szolgálhat másodlagos, tartalék megoldásként a hivatásos beavatkozó állomány számára az elsődleges rendszerek mellett, amennyiben azok

valamilyen okból kifolyólag nem állnak rendelkezésre. Emellett kisebb ipari szervezeteknél is alkalmazható mentési gyakorlatok szimulációjára vagy ipari balesetek kezelésének támogatására. Alternatív megoldásként alacsony költségű és könnyen alkalmazható eszközt biztosíthat harmadik országok ipari létesítményeinek üzemeltetéséhez, továbbá a katasztrófavédelmi, iparbiztonsági hatósági, illetve a Nemzeti Közszolgálati Egyetem Közös Közszolgálati gyakorlatán szcenáriók megjelenítésére. Ugyanakkor hangsúlyozni szükséges, hogy az ALOHA szoftver, még ezzel a hardverintegrációval együtt sem, helyettesíti a Magyar Honvédség és a hivatásos katasztrófavédelmi szervek által alkalmazott, nagy pontosságú, többváltozós veszélyesanyag-terjedési modellező és elemző rendszereket.

Összességében a fejlesztés kiegészítő funkcionalitást biztosít a meglévő szoftverhez, lehetővé téve, hogy gyakorlatilag bármely település esetében valós vagy előrejelzett meteorológiai adatok felhasználásával történjen modellezés, a lehető legköltséghatékonyabb módon. Ez különösen egy elhúzódó veszélyesanyag-kibocsátás esetén jelentős támogatást nyújthat a döntéshozatal számára. A kutatás értéke abban rejlik, hogy bemutat egy gyakorlati, alacsony költségű fejlesztési lehetőséget egy meglévő modellező eszköz továbbfejlesztésére, bizonyítva, hogy a valós idejű és előrejelzett meteorológiai adatok integrációja széles körben elérhető technológiák alkalmazásával is megvalósítható, ezáltal bővítve az ilyen modellezési megoldások alkalmazási lehetőségeit.

2.7.4 Veszélyes anyag terjedési modellezése és az MI kapcsolata

A fejlett technológiák térnyerésével a mesterséges intelligencia (MI) alkalmazása egyre nagyobb jelentőséggel bír az iparbiztonság és a veszélyhelyzet-kezelés területén. Ennek megfelelően a dolgozat olyan mesterséges intelligencián alapuló megközelítések alkalmazását javasolja, amelyek elősegíthetik a veszélyes anyagok terjedésének prediktív modellezését. A katasztrófavédelmi beavatkozó állomány munkakörülményeit figyelembe véve az elsődlegesen egy hordozható, ugyanakkor megfizethető, nagyobb számítási kapacitással rendelkező eszközt, például a Raspberry Pi 5 alkalmazását javaslom. A Rasberry Pi 5 további előnye, hogy a teljesítmény jól skálázható és mindenkori igényekhez szabható, valamint a nagy népszerűsége miatt rengeteg alkatrész és kiegészítő hardver elem könnyen beszerezhető hozzá.
Ez a hardverplatform már alkalmas egyszerűbb felügyelt tanulási algoritmusok, például regressziós modellek futtatására is. A modellek tanítására célszerű nagyobb számítási teljesítményű rendszereket vagy felhőalapú környezetet igénybe venni, míg az úgynevezett inferencia, azaz a betanított modell alkalmazása, a Raspberry Pi platformon is végrehajtható. A

Raspberry Pi által támogatott gépi tanulási keretrendszerek, mint például a TensorFlow Lite, az ONNX Runtime vagy a PyTorch Mobile, lehetővé teszik az optimalizált modellek futtatását korlátozott erőforrású környezetben is. [89]

A további kutatás célja lehet egy olyan prediktív rendszer kialakítása, amely képes az ALOHA szoftver által generált *.kml* formátumú terjedési térképek, illetve *.jpg* formátumú diszperziós képek, valamint a hozzájuk tartozó meteorológiai bemeneti adatok értelmezésére, és ezek alapján javaslatok megfogalmazására a védelmi zónák kijelölésére, valamint a lakosságvédelmi intézkedések meghatározására. Az ilyen rendszerek koncepciója összhangban áll az ipari és városi környezetben alkalmazott korszerű levegőszennyezés-előrejelző modellekkel, ahol az előrejelzés szenzoradatok és meteorológiai információk együttes felhasználásán alapul.

A konvolúciós és rekurzív neurális hálózatokat kombináló CNN–LSTM architektúrák különösen ígéretesnek tekinthetők a térbeli és időbeli mintázatok együttes kezelésében, mivel képesek egyaránt kezelni a térbeli jellemzők komplexitását (például a terjedési térképek esetében), valamint a meteorológiai változók időbeli dinamikáját. Számos kutatás igazolja, hogy az ilyen hibrid megoldások kifejezetten magas előrejelzési pontosságot biztosítanak környezeti rendszerek modellezése során, például a levegőminőség előrejelzésében. [90]

Ugyanakkor egyszerűbb regressziós modellek, például a Random Forest algoritmus is alkalmazható becslések készítésére a tényleges meteorológiai adatok alapján. Ezek az algoritmusok különösen előnyösek lehetnek alacsony erőforrásigényű eszközökön, mivel gyorsabban taníthatók és kisebb számítási kapacitást igényelnek. Számos kutatás rámutat arra, hogy bizonyos környezeti paraméterek becslése során a Random Forest alapú gépi tanulási módszerek meglepően pontos eredményeket adnak, gyakran felülmúlva a lineáris regresszió vagy az SVM (Support Vector Machine) modellek teljesítményét. [91]

Ezen gépi tanulási technikák előrejelzési pontossága, különösen az időbeli változások modellezése esetén, általában alacsonyabb a mély neurális hálózatokra épülő megközelítésekhez képest, mivel kevésbé képesek hatékonyan kezelni az időbeli vagy tér-időbeli mintázatokat. Ennek következtében a CNN–LSTM modellek magasabb prediktív teljesítményt biztosíthatnak a hosszabb távú előrejelzési feladatok során, míg a hagyományos modellek inkább a gyors döntéstámogatásban és forgatókönyv-alapú elemzésekben lehetnek előnyösek.

Fontos hangsúlyozni, hogy az ilyen rendszerek kizárólag döntéstámogató funkciót tölthetnek be, és a végső döntést minden esetben szakembernek kell meghoznia. A humán

validáció biztosítja, hogy a gépi előrejelzések és javaslatok értelmezése figyelembe vegye a helyi sajátosságokat, az operatív lehetőségeket és a társadalmi környezetet. Ez különösen fontos olyan helyzetekben, amikor a javasolt intézkedések közvetlen hatással lehetnek a lakosság biztonságára és életkörülményeire.

A rendszer komplexitását tovább lehet növelni a térképes megjelenítéshez kapcsolt népsűrűségen alapuló becslési lehetőségekkel. A lakosságvédelmi intézkedések meghatározásakor nemcsak a veszélyzóna földrajzi kiterjedése, hanem az érintett lakosság száma is kulcsfontosságú tényező. Az ALOHA által generált *.kml* fájlok lehetővé teszik a veszélyzónák koordinátaszintű meghatározását, amely megfelelő adatfeldolgozással összekapcsolható népsűrűségi és demográfiai adatbázisokkal. A kutatásom során egy Python programozási nyelven alapuló alkalmazást fejlesztettem, amely képes az ALOHA, illetve más veszélyesanyag-terjedési modellező szoftverek által generált terjedési csóvák geometriájának feldolgozására. A rendszer a modellezési eredményeket polygon-alapú reprezentációvá alakítja, majd a veszélyességi zónák (például AEGL gyűrűk) alapján meghatározza az érintett lakosság becsült számát, valamint egyéb demográfiai jellemzőit.

A népsűrűségi adatok számos nyílt forrású webes API-n keresztül elérhetők. Ezek az adatforrások jellemzően hivatalos népszámlálási (cenzus) adatokon alapulnak, amelyeket műholdas megfigyelések, földhasználati információk és éjszakai fényintenzitás-adatok felhasználásával bontanak le finomabb rácsfelbontásig, akár 30×30 méteres méretig. Az ilyen adatok felhasználása mesterséges intelligencia alapú módszerekkel egy adott terület (polygon), például egy veszélyzóna által érintett lakosság becslésére nem tekinthető új kutatási iránynak. Korábbi vizsgálatok sikeresen alkalmaztak Random Forest algoritmusokat [92], illetve mélytanulási modelleket a tartósan ott élő lakosság térbeli eloszlásának becslésére, jellemzően műholdfelvételek vagy távérzékelési adatok felhasználásával. [93]

Ezek a megközelítések jól adaptálhatók olyan döntéstámogató rendszerekben is, ahol a népsűrűségi adatok felhasználásával becslés adható arra vonatkozóan, hogy egy adott veszélyzóna mekkora lakosságot érinthet, adott időpillanatban.

Az általam fejlesztett alkalmazás ezt a logikát követve képes a terjedési modellek eredményeit népsűrűségi adatokkal összekapcsolni, és a veszélyzónák területén található lakosság becsült számát aggregációs módszerekkel meghatározni, azonban nélkülözi az adott pillanatban ténylegesen ott tartózkodók faktorát.

2.8 Lakossági kitettség becslése, a fejlesztett applikáció koncepciója

A 2019-es roueni Lubrizol-üzemi baleset is rámutatott arra, hogy egy ipari eredetű légszennyezés esetén a hatósági döntéshozatal egyik legkritikusabb eleme az érintett lakosság nagyságrendjének gyors és megbízható becslése, valamint ezen emberek értesítése, a válságkommunikáció ennek megfelelően történő kialakítása. A polgári védelem számára ezért kulcskérdés, hogy a modellezett veszélyességi zónák alapján milyen gyorsan tudja felmérni, hány embert kell arról a területről kitelepíteni vagy kimenekíteni, ahol a veszélyes anyag koncentrációja rövid idejű expozíció esetén is súlyos egészségkárosodást vagy halált okozhat.

A hazai ipari balesetek esetén is hangsúlyos a helyzetértékelés és döntéstámogatás digitális alapokra helyezése. Bár a BM OKF által alkalmazott térinformatikai és döntéstámogató rendszerek fejlett eszköztárat biztosítanak a hivatásos beavatkozó erőknek, azonban önkormányzati, vagy önkéntes szervezeteknek általában nincs közvetlen hozzáférése ezekhez. Ennek kezelésére indokolt olyan könnyen alkalmazható, autonóm eszközök fejlesztése, amelyek korlátozott informatikai háttérrel is képesek a lakossági kitettség gyors becslésére. [94]

2.8.1 A fejlesztett alkalmazás működése és alkalmazási lehetőségei

E célból készült egy önállóan futtatható applikáció, amely a légköri terjedést modellező szoftverek eredményeit automatikusan feldolgozza és megbecsüli a veszélyeztetett lakosság számát és demográfiai összetételét az egyes veszélyességi zónákra. A feldolgozásra kerülő terjedési poligonok tipikusan zónahatárokat leíró poligonok, amik gyűrűs szerkezetben, egymásra épülve képezik a terjedési csóvát. Az alkalmazás futtatható .exe fájl formátumú, így nem igényel installációt a munkaállomáson, vagy fejlesztői környezeten történő futtatást, és terepi körülmények között is egyszerűen használható.

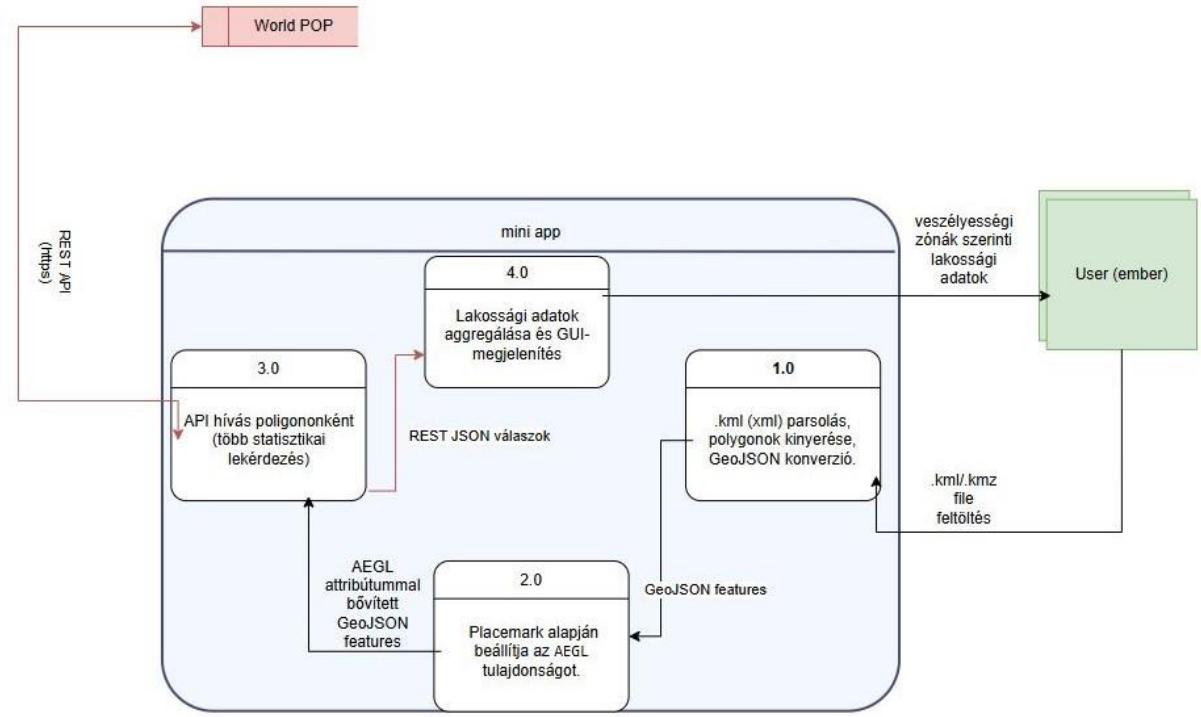
A terjedési minták feldolgozása nagymértékben automatizált: a modellkimenetből a szoftver önállóan konvertálja a veszélyzónákat poligonokká, ezt a betöltött kml. fájl xml[24](Extensible Markup Language) alapú feldolgozása révén végzi el. A kinyert poligonok GeoJSON formátumba kerülnek átalakításra, majd a Placemark metaadatok alapján AEGL[25] zónák szerint osztályozásra. Ezek REST-alapú API-hívások keretében kerülnek továbbításra a WorldPop által szolgáltatott nyílt demográfiai adatbázisokhoz, ahol ugyanazon geometriai bemenetre több

[24] Az XML esetében a címkék az adatok struktúráját és jelentését határozzák meg

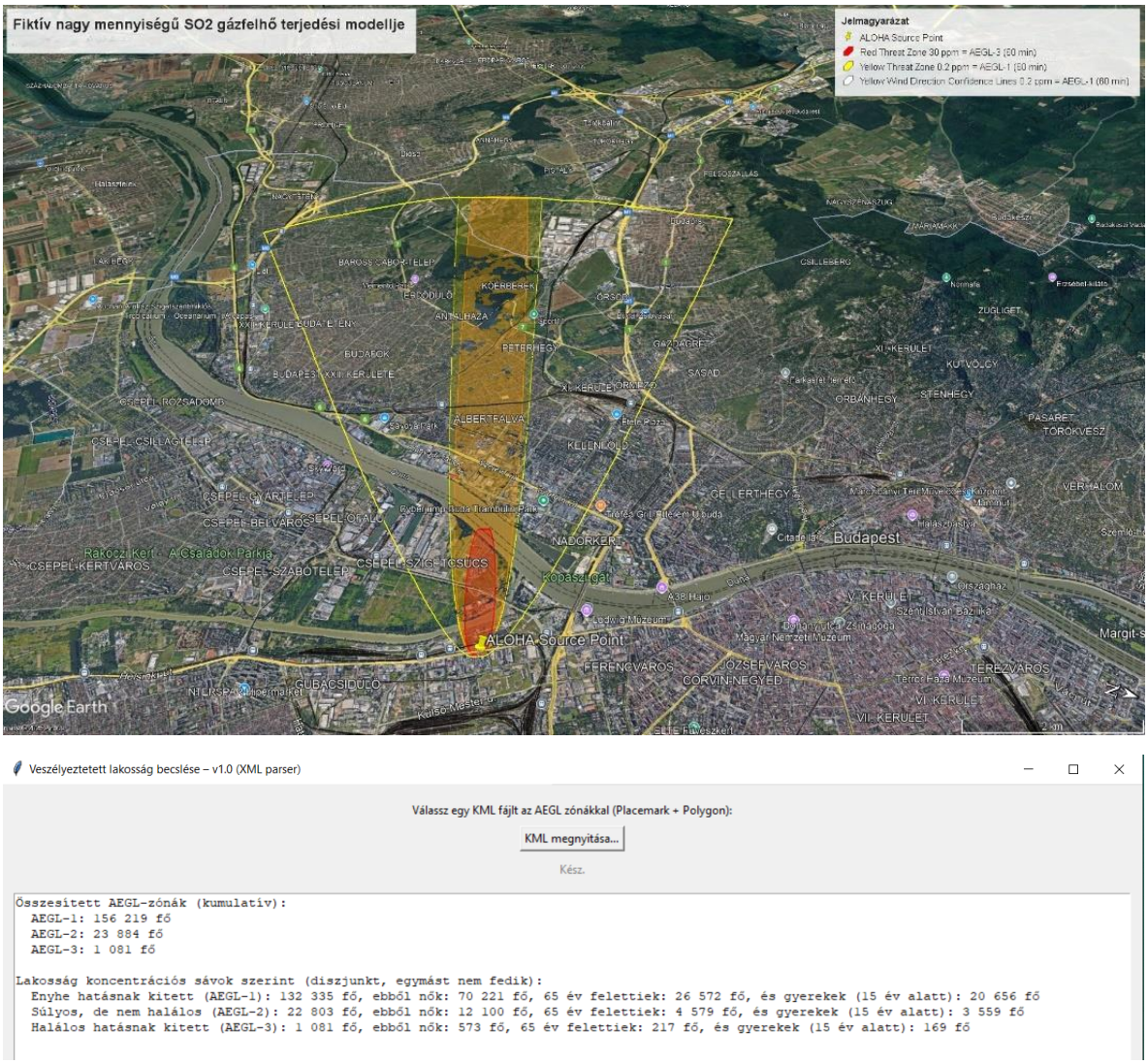
[25] Acute Exposure Guideline Levels egy nemzetközileg elfogadott referencia-rendszer, ami a veszélyes anyagok akut expozíciója során az enyhe tüneteket okozó (AEGL-1), a súlyos egészségkárosodást kiváltó (AEGL-2) és a halálos kimenetelű (AEGL-3) koncentrációzónákat írja le.

statisztikai lekérdezés fut le, beleértve az össznépességre, valamint a kor–nem szerinti megoszlásra vonatkozó becsléseket is. Majd az adott poligon által lefedett cellák népességadatai alapján szerver oldalon kiszámításra kerül az érintett lakosság, a raszteres cellaszintű adatok összegzésével. A WordPop szolgáltatás a poligonok által lefedett lakosság becsült létszámát és demográfiai adatait JSON formátumban adja vissza, amelyeket a kliensalkalmazás aggregál és grafikus felhasználói felületén (GUI) jelenít meg. A rendszer kialakítása tudatosan kerüli a helyi raszterfeldolgozást, így biztosítva az egyszerű futtatást és az alacsony számítási igényt.

Az alábbi adatáramlási diagram segítségével bemutatásra kerülnek a fejlesztett alkalmazás főbb folyamatai, valamint az egyes komponensek közötti adatkapcsolatok és kommunikációs mechanizmusok. Az ábra szemlélteti a bemeneti állományok feldolgozásának, a veszélyességi zónák polygon alapú kinyerésének, a GeoJSON konverziónak, továbbá a WorldPop szolgáltatás REST API interfészén keresztül végzett lakossági statisztikai lekérdezések és aggregációk folyamatát.:



12. ábra A lakosságbecslő applikáció adatáramlási diagramja, készítette: a szerző



13. ábra Az applikáció működés közben, a demográfiai csoportok demonstrációs jelleggel kerültek kiválasztása, készítette: a szerző

Az ilyen jellegű autonóm alkalmazások több szinten is illeszthetők a polgári védelem tevékenységébe. Oktatási környezetben jól használhatók a veszélyes anyagok légköri terjedésének, valamint a döntéstámogatási lánc kiindulási adatainak szemléltetésére. Gyakorlatok során segíthetik az állomány felkészítését arra, hogyan integrálható a modellezés és a lakossági adatbecslés egy beavatkozás korai döntéshozási szakaszába. A korábban bemutatott digitális meteorológiai állomásnak és ennek az alkalmazásnak az integrációja révén, egy hasznos eszközrendszert használhatnak a hallgatók akár a Közös Közszolgálati Gyakorlat során is. [95] A rendszer nagyfokú automatizáltsága lehetővé teszi, hogy akár alacsony sávszélesség mellett is gyorsan eredményt szolgáltasson, és így hasznos kiegészítője legyen a hivatalos rendszereknek, főként olyan esetekben, amikor azok átmenetileg nem elérhetők vagy valamilyen okból kifolyólag kompromittálódtak.

A fejlesztés célja nem egy komplex katasztrófavédelmi rendszer kiváltása, a jelentősége abban áll, hogy demonstrálja: nyílt adatokra és ingyenesen elérhető technológiákra építve is létrehozható olyan eszköz, amely képes térinformatikai modellezés alapján kvantifikálni a lakossági kitettséget. Ez a jövő polgári védelmi rendszereinek egyik fontos iránya is lehet, ahol a gyors, akár decentralizáltan is működni képes döntéstámogatás a hatékony reagálás alapfeltételévé válhat.

2.9 A fejlesztett rendszer-ökoszisztéma alkalmazásának bemutatása

Az általam fejlesztett ESP32 alapú rendszer komponens, valamint a lakosságkitettség becslését lehetővé tevő alkalmazás integrált megközelítésben történő hasznosíthatóságának bemutatásáról szól jelen alfejezet. Ennek érdekében egy fiktív szcenárión keresztül történik az eszközök alkalmazhatóságának bemutatása és igazolása.

A rendszer architektúrájának ilyen módon történő integrációja lehetővé teszi, hogy a veszélyesanyag-kibocsátás modellezése, a meteorológiai adatok automatikus integrációja, valamint a lakossági kitettség becslése egy egységes információs folyamatban valósuljon meg. Ez a megközelítés hozzájárulhat a veszélyes ipari események gyors következményelemzéséhez, valamint támogathatja az operatív lakosságvédelmi intézkedések döntéseinek, (például az elzárkóztatás, a kitelepítés vagy a lakossági riasztás), megalapozását.

14. ábra A fejlesztett rendszer architektúra működési folyamata, készítette: a szerző

2.9.1 Fiktív szcenárió

A kutatás keretében bemutatott fiktív eseménysor célja egy integrált, digitális döntéstámogató rendszer architektúrájának szemléltetése, amely veszélyes anyagok légköri kibocsátásának gyors következményelemzését és a potenciálisan érintett lakosság becslését támogatja. A rendszer alapvető célja, hogy a veszélyes ipari események során a meteorológiai adatok gyűjtését, a terjedési modellezést, valamint a lakosságvédelmi következmények értékelését egy egységes információs folyamatba integrálja. Egy feltételezett veszélyes anyag kibocsátási esemény modellezésére került sor budapesti városi környezetben. A fiktív esemény helyszíneként az Illatos úti ipari terület került kiválasztásra, amely Budapest délpesti részén helyezkedik el a IX., XX. és XIX. kerületek határvidékén elhelyezkedő ipari- és logisztikai zóna. A terület ipari múltja, valamint a közvetlen közelében található sűrűn lakott városi területek alkalmassá teszik arra, hogy egy veszélyes anyag kibocsátás potenciális következményeinek szemléltetésére szolgáljon, és az érintett lakosság is jól becsülhetővé válik. A helyszín kiválasztásának további indoka, hogy a modellezés eredményei térinformatikai környezetben, jelen esetben Google Earth-alapú megjelenítéssel, vizuálisan is jól

értelmezhetők, így a veszélyeztetett ipari és lakóterületek térbeli elhelyezkedése egyértelműen bemutatható.

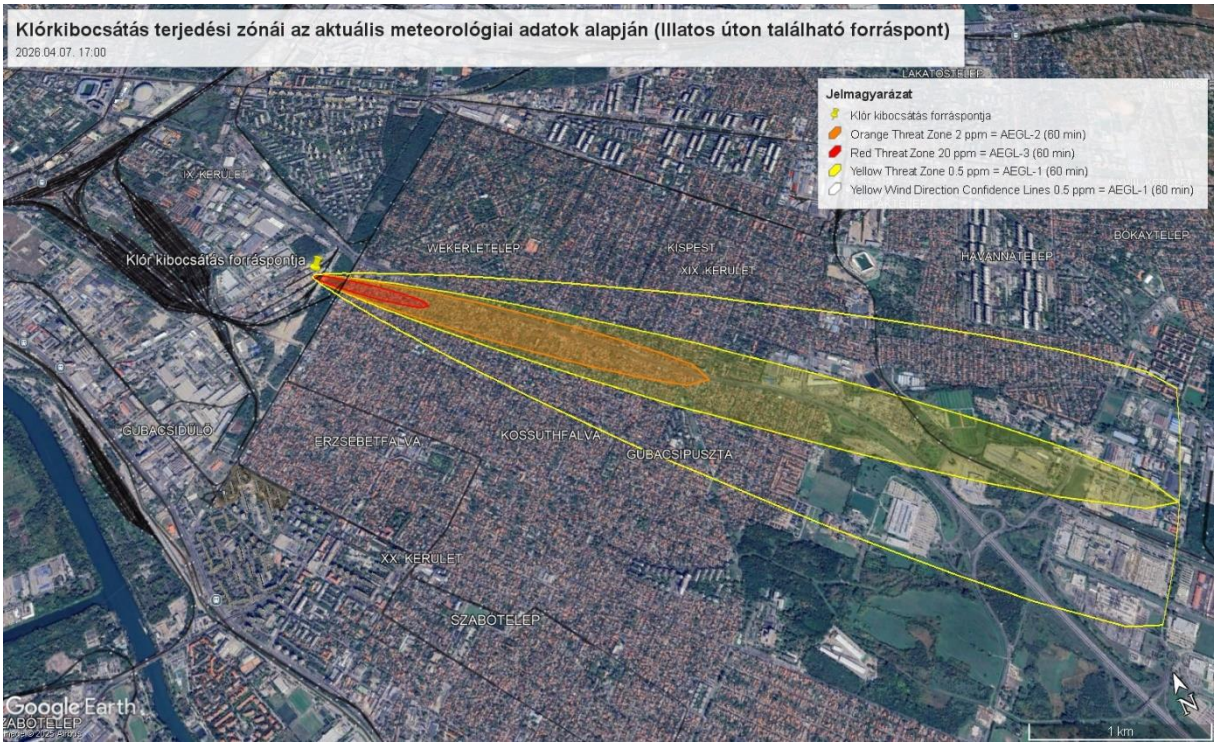
A modellezett esemény egy feltételezett klórgáz-kibocsátást ír le, amely egy ipari vegyianyag-tároló rendszer technológiai meghibásodásának következményeként alakul ki. A szcenárió szerint a telephelyen fertőtlenítési vagy technológiai célra alkalmazott klórt tartalmazó tárolótartály csatlakozóvezetékének tömítetlenné válása következtében mérgező klórgáz kerül a környezetbe. A modell egy 1 tonna névleges kapacitású klórtartály alkalmazását feltételezi, amely a baleset időpontjában hozzávetőlegesen 70%-os töltöttségi állapotban van. A csatlakozóvezeték sérülése következtében a klór gázfázisban, folyamatos szivárgás formájában jut a környezetbe. A kibocsátás időtartama a modellben 6 percben került meghatározásra, amely egy rövid idejű, de potenciálisan jelentős következményekkel járó mérgezőanyag-kibocsátási eseménynek tekinthető. A kibocsátási folyamat során cseppfolyósított klór nyomás alatti tartályból egy 2 cm átmérőjű nyíláson keresztül jut a környezetbe. Metastabil állapotból kerül atmoszférikus környezetbe, amely villanásszerű fázisátalakulást idéz elő. A keletkező kétfázisú áramlás és az intenzív párolgás következtében sűrű, hideg aeroszol–gáz keverék jön létre, amely a nehézgáz-terjedési mechanizmusoknak megfelelően viselkedik. Így a felszín közelében terjedő mérgező felhőt képezhet, amely a meteorológiai viszonyoktól függően a környező lakóterületek irányába sodródhat. Az ALOHA a klór, mint nehéz gáz miatt a DEGADIS modellt alkalmazta a terjedés számításakor.

A kibocsátás következményeinek becslésére az ALOHA atmoszférikus terjedési modellező szoftver került alkalmazásra, amely gyors, úgynevezett screening jellegű következményelemzésre szolgáló eszköz. A modellezéshez szükséges meteorológiai paraméterek egy ESP32 mikrokontrollerre épülő adatgyűjtő és megjelenítő rendszer segítségével kerülnek lekérésre egy meteorológiai adatokat szolgáltató külső alkalmazásprogramozási interfészből (API). A rendszer a lekért adatokat, beleértve a relatív páratartalmat és a felhőzeti viszonyokat, automatikusan megjeleníti a felhasználói felületen, ezáltal jelentősen csökkentve a manuális adatbevitel szükségességét és a paraméterezési hibák lehetőségét.

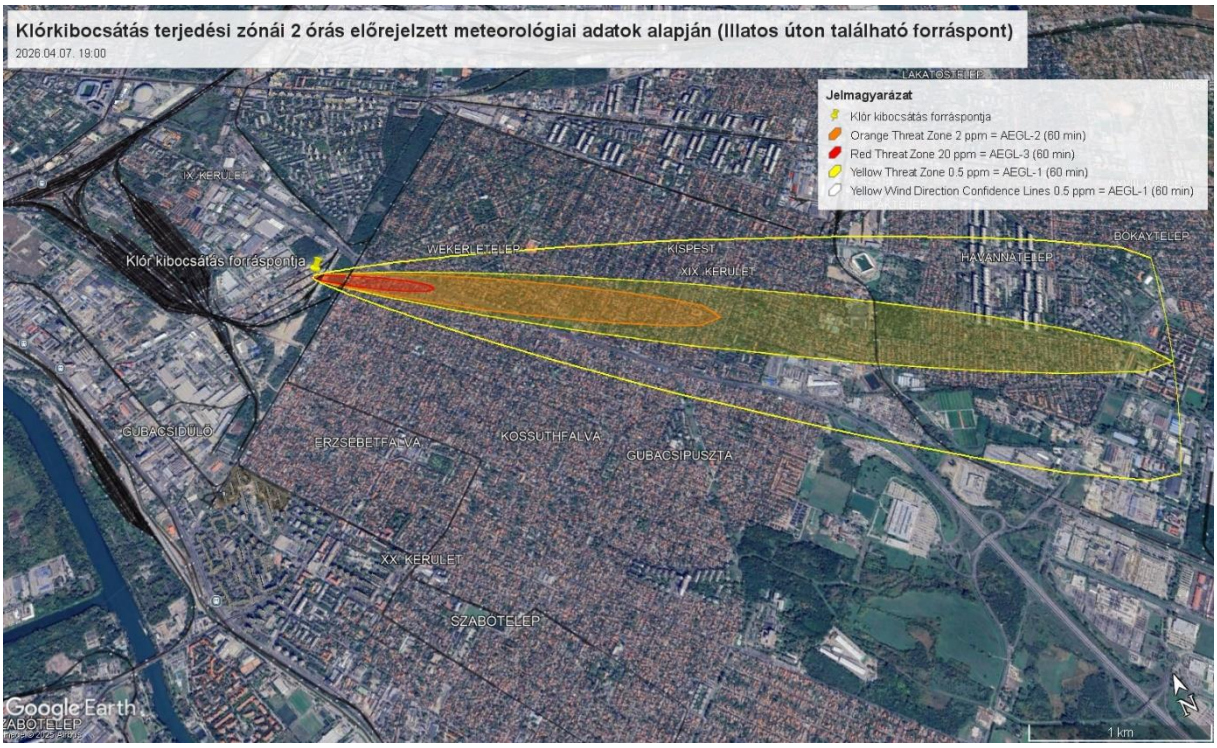
A rendszer architektúrájának fontos eleme, hogy az ESP32-alapú frontend nem csupán az aktuális meteorológiai adatokat képes megjeleníteni, hanem előrejelzési adatokat is integrál. A demonstráció során ezért a modellezés két eltérő meteorológiai állapot mellett kerül végrehajtásra: egyrészt az aktuális meteorológiai viszonyok alapján, másrészt egy két órával későbbi, előrejelzett meteorológiai állapot felhasználásával. Fontos hangsúlyozni, hogy az

előrejelzési mód nem a kibocsátás időtartamának meghosszabbítását jelenti; mindkét esetben ugyanaz a rövid idejű, hat perces kibocsátási esemény kerül modellezésre. Az eltérő meteorológiai feltételek alkalmazása lehetővé teszi annak vizsgálatát, hogy az atmoszférikus viszonyok változása miként befolyásolja a veszélyes anyag felhőjének terjedési irányát és kiterjedését.

Az ALOHA modell kimeneti eredményei térinformatikai formátumban kerültek exportálásra, majd Google Earth Pro alkalmazás segítségével kerülnek megjelenítésre, amely lehetővé teszi a veszélyeztetett területek térbeli vizualizációját.



15. ábra A klórgáz terjedési csóvája az aktuális meteorológiai adatok használatával, készítette: a szerző



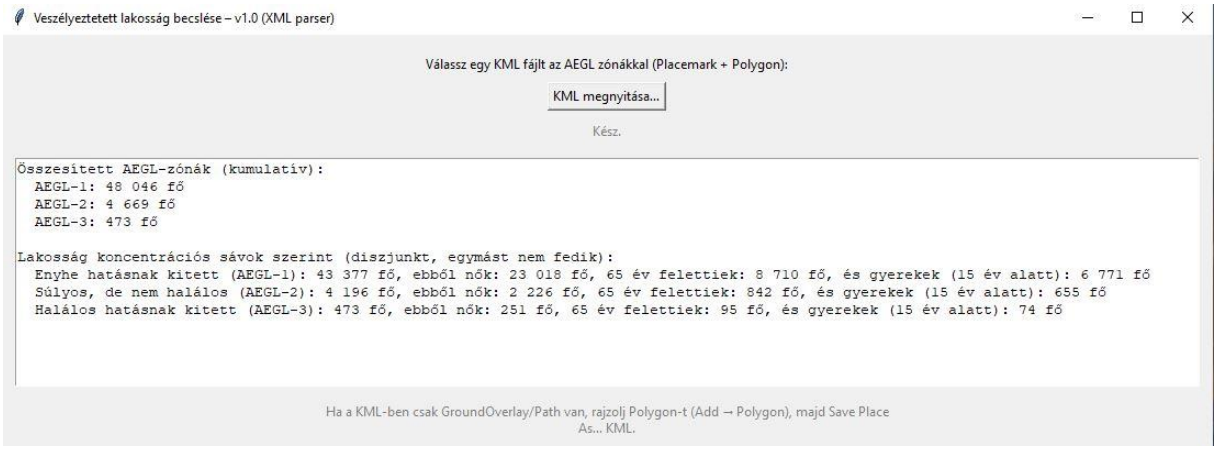
16. ábra A klórgáz terjedési csóvája 2 órás előrejelzett adatok felhasználása alapján, készítette: a szerző

A klórkibocsátás terjedési zónáinak általános iránya és geometriája alapvetően hasonló maradt az aktuális és a 2 órával későbbi meteorológiai adatok felhasználása esetén, ami arra utal, hogy a szélirány a vizsgált időintervallumban nem változott jelentős mértékben. Mindkét esetben a terjedés domináns iránya kelet–délkelet felé mutat.

Ugyanakkor a két modellfuttatás között lokális irányeltérés figyelhető meg, ez a veszélyeztetett területek eloszlásában is megjelenik. Az aktuális meteorológiai adatok alapján számított terjedési csóva elsősorban Pesterzsébet északi területeit érinti, míg a két órával későbbi előrejelzett adatok esetén a csóva tengelye Kispest irányába tolódik el, ezáltal eltérő lakóterületek kerülnek a potenciálisan veszélybe.

A rendszer architektúrájának következő eleme a kutatás keretében fejlesztett lakosságkitettség-becslő alkalmazás használata. Ez a modellezett veszélyzónák térbeli kiterjedését felhasználva becslést ad a potenciálisan érintett lakosság számáról és azok demográfiai adatairól. Az alkalmazás a veszélyzónák földrajzi kiterjedését összeveti a rendelkezésre álló települési és demográfiai adatokkal, így lehetővé válik annak gyors meghatározása, hogy egy adott kibocsátási esemény milyen nagyságrendű lakosságot érinthet. A vizualizáció során alkalmazott kml. fájlok betöltésre kerülnek a fejlesztett alkalmazásba,

majd az abban lévő polygonok-ra elkészülnek a lakossági kitettségre és demográfiai jellemzőkre vonatkozó becslések.



17. ábra Az első, aktuális meteorológiai adatok felhasználásával készült terjedési modell által érintett lakosság, készítette: a szerző

18. ábra A 2 órás előrejelzés meteorológiai adatai által készült terjedési modell által érintett lakosság, készítette: a szerző

Az aktuális és az előrejelzett meteorológiai adatok alapján végzett lakosságkitettség-becslés eredményei azt mutatják, hogy a veszélyeztetett lakosság nagysága és megoszlása a két esetben eltérően alakul. Az aktuális meteorológiai adatok alapján az AEGL-1 zónában mintegy 48 046 fő, míg az előrejelzett adatok esetén 52 953 fő érintett, ami növekedést jelez a tágabb, alacsonyabb koncentrációjú hatástartományban. Ezzel szemben a súlyosabb hatásokat reprezentáló zónákban ellentétes tendencia figyelhető meg: az AEGL-2 zónában az érintettek száma 4 669 főről 4 051 főre, míg az AEGL-3 esetében 473 főről 349 főre csökken.

Az eltérés a terjedési csóva irányának módosulásával magyarázható, amely az aktuális meteorológiai helyzetben inkább Pesterzsébet északi részének irányába tolódik, míg az előrejelzett állapot esetén nagyobb mértékben érinti a XIX. kerület területeit. Az eredmények rávilágítanak arra, hogy a rövid távú meteorológiai változások nemcsak a veszélyzónák geometriáját, hanem a különböző kockázati zónákhoz tartozó lakosság számát is érdemben befolyásolhatják, ami a lakosságvédelmi intézkedések tervezése szempontjából kiemelt jelentőségű lehet.

A szcenárióalapú modellezés eredményei alapján megállapítható, hogy egy rövid idejű, de intenzív klórkibocsátás esetén a kialakuló veszélyzónák kiterjedése és térbeli elhelyezkedése döntően a meteorológiai viszonyoktól, elsősorban a széliránytól és a szélsebességtől függ. A vizsgálat rámutatott, hogy még rövid távú meteorológiai változások is képesek a terjedési csóva irányát módosítani, amely eltérő lakóterületek érintettségét és jelentős különbségeket eredményezhet a különböző veszélyességi zónákhoz tartozó lakosság számában.

Az integrált rendszerarchitektúra megközelítés, ami a digitális meteorológiai állomást, az ALOHA alapú terjedésmodellezést, a térinformatikai megjelenítést és a fejlesztett lakosságkitettség-becslő alkalmazást egy rendszerben kezeli, lehetővé teszi a veszélyes anyagok kibocsátásának gyors, szemléletes és kvantitatív értékelését a veszélyeztetett terület és lakosság szempontjából is.

2.10 Fejezeti részkövetkeztetések

1. A modern ipari balesetek kezelésének hatékonyságát nem csak a beavatkozó erők technikai felkészültsége, hanem a gyors helyzetértékelés, az adatvezérelt döntéstámogatás és a lakosság irányába történő hiteles, időben megvalósuló válságkommunikáció együttesen határozza meg.

2. A lakosságvédelmi intézkedések társadalmi elfogadottsága szorosan összefügg a válságkommunikáció minőségével. A többcsatornás riasztási és tájékoztatási megoldások, valamint a digitális platformok tudatos alkalmazása elengedhetetlen a bizonytalanság és az álhírek mérsékléséhez. Ebben a környezetben a hatósági felügyelet mellett működő, mesterséges intelligencián alapuló reaktív információszolgáltató rendszerek valós, rövid távon is alkalmazható fejlesztési irányt jelentenek.

3. A jelenlegi hazai szabályozási környezet a veszélyes anyagokkal kapcsolatos események kivizsgálását kötelezővé teszi, azonban a kiberbiztonsági incidensek iparbiztonsági aspektusú vizsgálatára vonatkozó eljárások, felelősségi körök és módszertani követelmények nem

jelennek meg egyértelműen a szabályozásban. Ez a hiányosság különösen az ipari digitalizáció előrehaladásával válik jelentőssé, mivel ezen rendszerek ellen elkövetett kibertámadások potenciálisan hozzájárulhatnak veszélyes anyagokkal kapcsolatos súlyos balesetek kialakulásához is.

4. A veszélyes üzemeket és alapvető szolgáltatást nyújtó szervezeteket érintő kiberbiztonsági incidensek helyreállítása akár jelentős technológiai, üzemeltetési és gazdasági erőforrásokat igényelhet, különösen, ha fizikailag is sérülnek ipari vezérlőrendszerek és ipari berendezések. Az ilyen események által generált gazdasági és társadalmi hatások már túlmutathatnak az egyes gazdálkodó szervezetek működési kockázatain, és szükségessé válhat az állami szerepvállalás. Azonban a jelenlegi hazai vis maior és helyreállítási támogatási mechanizmusok elsősorban az önkormányzati és fizikai infrastruktúrában keletkezett károk kezelésére fókuszálnak. A harmadik fél által jogosulatlanul manipulált ipari rendszerekből eredő káresemények új szempontokat vethetnek fel a helyreállítási és vis maior támogatási mechanizmusok jövőbeni újraértelmezése során.

5. A bemutatott veszélyeztetett lakosságbecslő alkalmazás, mint koncepció azt szemlélteti, hogy nyílt adatokra és automatizált feldolgozásra építve is létrehozhatók olyan egyszerű, autonóm eszközök, amelyek érdemi támogatást nyújtanak a polgári védelem korai döntéshozatalában. Ezek az eszközök nem a komplex hatósági rendszerek kiváltását célozzák, hanem azok rugalmas kiegészítését, különösen időkritikus vagy decentralizált helyzetekben. A kutatás keretében bemutatott ESP32-alapú meteorológiai adatgyűjtő és -feldolgozó megoldás tovább bővíti ezt a koncepciót azáltal, hogy a veszélyesanyag-terjedési modellezéshez szükséges meteorológiai adatellátást is automatizált módon integrálja a rendszerbe. Az így kialakított architektúra már nem csupán egy önálló alkalmazásként értelmezhető, hanem egy olyan digitális rendszer-ökoszisztémaként, amely a veszélyhelyzeti modellezés teljes folyamatát képes lefedni az adatgyűjtéstől és feldolgozástól kezdve a modellezésen át egészen a lakosságvédelmi döntéstámogatásig.

6. Az ilyen, alacsony költségű és könnyen telepíthető megoldások különösen jól alkalmazhatók oktatási és gyakorlati környezetben is, mivel lehetővé teszik komplex veszélyhelyzeti szcenáriók valósághűbb szimulációját. Ennek köszönhetően a rendszer alkalmas lehet a hagyományos, úgynevezett *table-top exercise* gyakorlatok magasabb szintű, digitálisan támogatott kiváltására vagy kiegészítésére, ahol a résztvevők valós adatokon alapuló modellezési eredményekre támaszkodva hozhatnak döntéseket.

3. VESZÉLYES ANYAGOKKAL FOGLALKOZÓ ÜZEMEK 21. SZÁZADI KIHÍVÁSAI

3.1 A veszélyes üzemek fenyegetései

A modern társadalom fejlődésének egyik alapja volt az iparosodás. A vegyipar termékeinek is köszönhetően, a mai életszínvonal jelentősen magasabb, mint a korábbi évszázadokban volt. A vegyipar által előállított termékek a gazdaság szinte valamennyi ágazatában megjelennek, beleértve az energetikát, a gyógyszeripart, a mezőgazdaságot, az építőipart és a fogyasztási cikkek gyártását. A vegyipari termelés ezért kulcsszerepet játszik az európai gazdaság versenyképességének fenntartásában és az ipari értékláncok működésében

Ugyanakkor ezen létesítmények működése jelentős kockázatokat hordoz a lakosság, a környezet és a kritikus infrastruktúrák számára. A veszélyes anyagok tárolása, feldolgozása és szállítása során bekövetkező ipari balesetek súlyos következményekkel járhatnak, amint azt több múltban bekövetkezett esemény is alátámaszt, például a sevesoi (1976) vagy a bhopali (1984) ipari katasztrófák. Ezek az események jelentős hatást gyakoroltak az iparbiztonsági szabályozás fejlődésére, különösen Európában, ahol az ipari balesetek megelőzésére irányuló szabályozási keretek fokozatosan szigorodtak az elmúlt évtizedekben. [96]

A fenntartható fejlődés elvének előtérbe kerülésével a veszélyes üzemek működésének szabályozása nemcsak a balesetek megelőzésére, hanem a környezeti terhelés minimalizálására és az erőforrás-hatékonyság javítására is kiterjed. A fenntartható ipari működés a környezeti, gazdasági és társadalmi szempontok egyensúlyának megteremtését célozza, amely különösen fontos a túlnépesedéssel küzdő bolygónk és a nagy kockázatú iparágak esetében. Ennek megfelelően az ipari létesítmények egyre nagyobb hangsúlyt fektetnek az energiahatékonyság növelésére és a kibocsátások csökkentésére. [97]

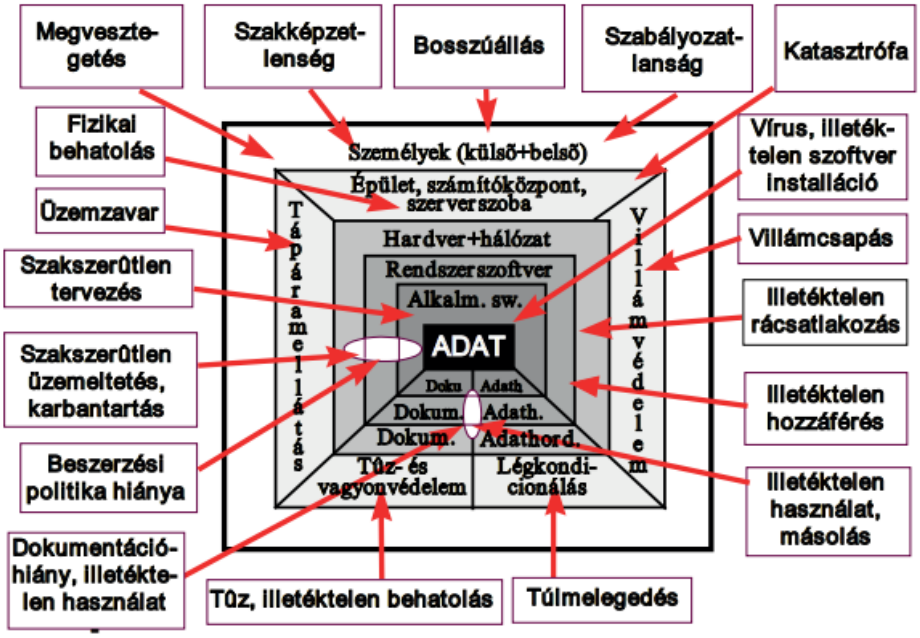
Az Európai Unió iparbiztonsági szabályozásának egyik központi eleme a Seveso irányelv**,** amely a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzésére és következményeik csökkentésére irányul. A jelenleg hatályos a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről szóló, az Európai Parlament és a Tanács 2012/18/EU irányelve (Seveso III irányelv) részletes követelményeket határoz meg többek között a kockázatértékelés, a biztonsági jelentések, a veszélyes anyagok nyilvántartása és a lakosság tájékoztatása tekintetében. Számos tagállam, köztük Magyarország, a nemzeti jogrendbe történő átültetés

során bizonyos területeken az uniós minimumkövetelményeknél szigorúbb szabályozást is alkalmaz, különösen a felügyeleti mechanizmusok és a hatósági ellenőrzések tekintetében. [98]

3.2 Az információbiztonság szerepe a veszélyes anyagokkal foglalkozó üzemek kiberkitettségének csökkentésében

A veszélyes anyagokkal foglalkozó ipari üzemek működése napjainkra szorosan összefonódott a digitalizált rendszerekkel, az automatizált irányítással és a hálózatba kapcsolt infrastruktúrával. Ezzel párhuzamosan az ilyen létesítmények kiberkitettsége is jelentősen megnövekedett, amely közvetlen hatással lehet nemcsak az üzembiztonságra, hanem a környezetre és a lakosság védelmére is. E kockázatok hatékony csökkentésének egyik legfontosabb eszköze az információbiztonság, amely megfelelően alkalmazva képes megelőzni, detektálni és kezelni a kibertámadásokból eredő incidenseket.

Az információbiztonság fogalma túlmutat a klasszikus informatikai rendszerek védelmén: olyan átfogó szemléletet jelent, amely az információk védelmét célozza függetlenül azok megjelenési formájától vagy tárolási módjától. Ennek megfelelően kiterjed a számítógépes rendszerekre, hálózatokra, kommunikációs csatornákra, valamint az analóg és digitális adathordozókon megjelenő információkra is. A szakirodalmi meghatározás szerint az információbiztonság „*a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt információk védelmére vonatkozik*” [99].



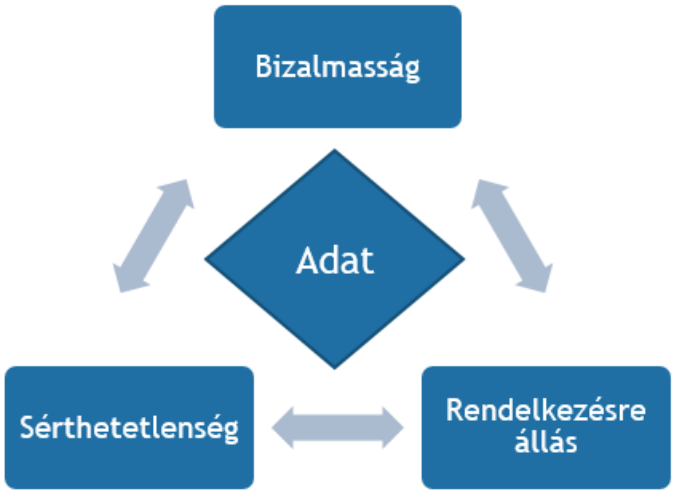
19. ábra Az adat több dimenziós védelme, forrás: [99]

A veszélyes üzemek esetében különösen fontos hangsúlyozni, hogy az információbiztonság alapvetően adatközpontú megközelítést alkalmaz. Ez azt jelenti, hogy nem csupán az informatikai (IT) rendszerek védelme a cél, hanem az ipari irányítási rendszerek (OT – Operational Technology) környezetében keletkező és kezelt adatok védelme is. Az OT rendszerek, például SCADA, DCS vagy PLC alapú irányítási megoldások, közvetlen kapcsolatban állnak a fizikai folyamatokkal, így egy sikeres kibertámadás nemcsak adatvesztést vagy szolgáltatáskiesést, hanem fizikai káreseményt, akár veszélyes anyag kibocsátást is eredményezhet.

Az információbiztonság egyik alapját a CIA (Confidentiality, Integrity, Availability), magyarul BSR (Bizalmasság, Sértetlenség, Rendelkezésre állás) elv képezi.

- **Bizalmasság** (Confidentiality): biztosítja, hogy az információkhoz csak jogosult személyek férhessenek hozzá;
- **Sértetlenség** (Integrity): garantálja, hogy az adatok nem módosulnak jogosulatlanul;

- **Rendelkezésre állás** (Availability): biztosítja, hogy az információk és rendszerek szükség esetén elérhetők legyenek.



20. ábra Információbiztonság három alapelve (BSR) készítette: a szerző

E három alapelv kiegészül további fontos tulajdonságokkal, mint a hitelesség, letagadhatatlanság és számonkérhetőség, amelyek az ipari környezetben is fontosak, ahol a folyamatok nyomon követhetősége és auditálhatósága alapvető követelmény. Minden információbiztonsági törekvés arra irányul, hogy a három biztonsági követelménynek való megfelelőséget minden időpillanatban biztosítsa az összes védendő információra és környezetükre egyaránt. Egy szervezet működése, akkor biztonságtudatos, ha munkavállalói akik, felhasználók és az egyéb szerepkörökben dolgoznak, tisztában vannak az alapvető és esetleg szervezetspecifikus fenyegetettségekkel, képesek ezeket azonosítani, valamint ismerik egy valószínűsíthető incidens esetén alkalmazandó szabályokat, eljárásrendeket, ami a gyakorlatban magába foglalja, hogy tudják, milyen csatorna segítségével jelenthetik be az incidenst és felhasználóként mi a követendő magatartás az egyes események kapcsán. Ezt az optimális szintet elérni sok időbe és költségbe kerül, de a szervezet biztonsági kultúráját meg kell teremteni. Felhasználóként tudnunk kell, hogy mi vagyunk az első és leginteligensebb védelmi vonala egy szervezetnek. [100]

A támadói oldal ezt a modellt a DAD (Disclosure, Alteration, Denial) logikával „tükrözi”, amely a bizalmasság megsértésére (adatkiszivárgás), az adatok módosítására, illetve a szolgáltatások megtagadására irányul. Egy veszélyes üzemben mindhárom támadási alapelv súlyos következményekkel járhat: például egy vezérlőrendszer paramétereinek módosítása

technológiai zavart vagy balesetet idézhet elő, míg a rendelkezésre állás megszüntetése (pl. DoS támadás) akadályozhatja a biztonsági (safety) rendszerek működését.

Az információbiztonság jelentősége az információs technológia fejlődésével párhuzamosan napról napra nő. Az adatvédelmi, valamint az elektronikus információs rendszereket érintő biztonsági incidensek, például a hackerek támadásai, malware-ek, rosszindulatú programok és az infokommunikációs rendszereket körbevevő fizikai környezeti tényezők (például tűz, árvíz) elleni védelem kiemelten fontos az információk védelme érdekében.

Az első jelentős kibertámadásokat csak az 1990-es években tapasztalta meg a világ, amikor az internet elterjedése és a számítógépes hálózatok növekedése lehetővé tette, hogy szélesebb tömegekhez és szervezetekhez is bevezetésre kerüljön, aminek hatására az emberek és gazdasági szervezetek egyre nagyobb mértékben kezdtek el függeni a digitális technológiától. Elég csak az 1990-es évek második felében zajló Moonlight Maze fedőnevet viselő támadás sorozatra gondolni, amit vélhetően orosz hackerek hajtottak végre az amerikai kormány és katonai szervezetek számítógépes rendszerein, ezres nagyságrendben tulajdonítottak el jogosulatlanul titkos katonai dokumentumokat. Amikor a számítógépes kémkedés jelei nyilvánvalóvá kezdtek válni, akkor már a támadók közel két éve figyelték belülről a rendszert. [101] Ez a támadás az APT-támadások[26] egyik korai példája volt, és világszinten felhívta a figyelmet az ilyen típusú fenyegetések komolyságára és veszélyeire, valamint arra, hogy a kormányzati és katonai szervek elektronikus információs rendszerei a kibertámadások potenciális célpontjaivá válhatnak. A kibertámadások hátterében húzódó célok a következők lehetnek:

- pénzügyi haszonszerzés,
- információ jogosulatlan megszerzése vagy azokban károkozás,
- politikai célok elérése,
- az adatok manipulálása/módosítása vagy megsemmisítése,
- a piaci versenytársakkal szembeni előny megszerzése, például azok információs rendszereinek meggyengítésével,

[26] APT-támadás (Advanced Persistent Threat): célja alapvetően nem a rongálás útján való károkozás, hanem az adatlopás. A támadó fejlett technikákkal és eszközökkel behatol egy célzottan kiválasztott hálózatba, ahol hosszabb időn keresztül észrevétlenül bent marad, és ezalatt értékes információkat szerez meg.

- alapvető szolgáltatások, kritikus infrastruktúrák elektronikus információs rendszereinek működésképtelenné tétele (terrorizmus). A kibertámadások áldozatai egyaránt lehetnek kormányok, vállalatok, szervezetek és egyének, a támadások módszerei, kiterjedtségük, hatásuk különbözőek lehetnek a céloktól, képességektől és az érintett rendszer védelmétől függően.

Az információbiztonsági kockázatok kezeléséhez komplex védelmi intézkedésrendszer szükséges, amely három fő kategóriába sorolható:

- *Adminisztratív intézkedések***:** szabályzatok, eljárásrendek, biztonságtudatossági képzések, incidenskezelési folyamatok kialakítása. Ezek képezik a kapcsolatot a technikai és fizikai védelem között, és meghatározzák a szervezeti működés biztonsági kereteit. A szervezetnek az operatív működésének tükröznie kell a dokumentumokban meghatározottakat.
- *Fizikai védelem:* Fizikai védelem fogalmába tartozik az elektronikus információs rendszerek hardver elemeinek, valamint az azok működését biztosító infrastruktúra elemeknek a védelme. A fizikai biztonság elsődleges feladata, hogy a jogosulatlan fizikai hozzáférést megakadályozza az érintett elektronikus információs rendszer(ek)hez, valamint azok helyét biztosító helyiségekhez. A másik fontos aspektusa, hogy a védeni kívánt rendszerek működési állapotát biztosító infrastrukturális elemek kompromittálódását (például elektromos hálózat zavarása, megsemmisítése) megelőzze, amennyiben szükséges hatékonyan és gyorsan elhárítsa (például redundancia biztosításával). A fizikai védelem eszközei közé sorolhatók a különböző behatolásjelzők, tűz- és füstjelző megoldások stb.
- *Logikai (informatikai) védelem*: Logikai védelemhez tartoznak mindazon szoftverkomponensek, amelyek az elektronikus rendszer védelme során felhasználhatók. A szervezet által kikényszerített jelszókezelési szabályok, jogosultságkezelés megvalósítása, a szervezet naplózási tevékenységei, a kriptográfiai megoldások, amik biztosítják az adatok titkosságát és hitelességét úgy, hogy a védtelen közegben elhelyezkedő adatokat titkosítják, illetve a védtelen közegen keresztüli kommunikációt biztosítják. A logikai védelmi pillér alapeszközei közé tartoznak: a szimmetrikus kulcsú és asszimetrikus kulcsú titkosítások, kriptográfiai hash függvények. Ide tartoznak a határvédelmi megoldások, például tűzfalak, IDS/IPS

megoldások stb. Gyakorlatilag ezt a pillért meg lehet feleltetni az informatikai védelem fogalmával.

A veszélyes üzemek esetében ezen intézkedéseknek integrált módon kell megjelenniük mind az IT, mind az OT környezetben. Külön kihívást jelent, hogy az OT rendszerek gyakran eltérő prioritások mentén működnek (pl. rendelkezésre állás elsődlegessége), valamint hosszabb életciklusú, nehezebben frissíthető komponensekből állnak, ami növeli a sérülékenységet.

Az információbiztonság gyakorlati megvalósítása során célszerű nemzetközi és hazai szabványokra és ajánlásokra támaszkodni. A jogszabály által megkövetelt megfelelés, valamint az önként vállalt nemzetközi keretrendszerek alkalmazása biztosítja, hogy a védelem egységes, auditálható, kockázat alapú megközelítést alkalmazzon, amit tükrözzenek az implementált védelmi intézkedések is, különös tekintettel a veszélyes anyagokkal foglalkozó üzemek komplex működési környezetére. Nemzetközi szinten az információbiztonság általános keretrendszerét az ISO/IEC 27001 szabványcsalád biztosítja, amely az információbiztonsági irányítási rendszerek (ISMS) kialakítására és működtetésére ad strukturált megközelítést. Ugyanakkor a veszélyes üzemek esetében az IT környezet mellett kiemelt jelentőséggel bír az ipari vezérlőrendszerek (OT) védelme, amely speciális megközelítést igényel. Ennek megfelelően célszerű alkalmazni az ipari kiberbiztonságra fókuszáló nemzetközi ajánlásokat is, különösen a NIST SP 800-82[27] útmutatót, amely kifejezetten az ICS/SCADA rendszerek biztonsági kihívásaira ad gyakorlati iránymutatást. Emellett az IEC 62443[28] szabványsorozat átfogó keretrendszert biztosít az ipari automatizálási és vezérlőrendszerek kiberbiztonságának kialakításához, lefedve mind a gyártói, mind az üzemeltetői oldal követelményeit. Végül kiemelendő az emberi tényező szerepe: a biztonságtudatos szervezeti kultúra kialakítása nélkül a technikai intézkedések önmagukban nem elegendők. A munkavállalók jelentik az első védelmi vonalat, ezért elengedhetetlen, hogy képesek legyenek felismerni a fenyegetéseket, és megfelelően reagáljanak egy esetleges incidens során.

A hazai szabályozási környezet az elmúlt években jelentős átalakuláson ment keresztül. A korábbi az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe

[27] Guide to Operational Technology (OT) Security
[28] Security for industrial automation and control systems

sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet helyét egy konzisztensebb és komplexebb jogi szabályozási keretrendszer vette át, részben az EU-s NIS2 hazai implementációja miatt, részben pedig a technológiai fejlődés lekövetése érdekében. Az új jogszabályi keret alapját a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény, valamint a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet képezi. Ezt a jogi környezet egészíti ki az implementálandó követelménykatalógust tartalmazó a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet. E jogszabályok összhangban az európai uniós NIS2 irányelvvel kockázatalapú megközelítést alkalmazva határozzák meg az a hatályuk alá tartozó szervezetek biztonsági követelményeit és kötelezettségeit.
Fontos kiemelni, hogy a kiberbiztonsági jogszabály hatálya számos veszélyes anyagokkal foglalkozó üzemre kiterjed, elsősorban az ágazati besorolás (pl. energia, vegyipar) és egyéb horizontális kritériumok (pl. méret, gazdasági bevétel) alapján. Ugyanakkor a lefedettség nem teljes: egyrészt bizonyos létesítmények a szabályozási küszöbértékek alatt maradnak, másrészt a veszélyes anyagokkal kapcsolatos kockázatok nem minden esetben esnek egybe a kiberbiztonsági szabályozás hatályával. Ez különösen igaz a kisebb kapacitású, úgynevezett küszöbérték alatti üzemek esetében, amelyek ugyan nem tartoznak a szigorúbb szabályozás alá, de potenciálisan jelentős kockázatot hordozhatnak.

Összességében megállapítható, hogy a veszélyes anyagokkal foglalkozó üzemek kiberkitettségi kockázatai jelentős mértékben csökkenthetők egy kockázatkezelésen alapuló adatközpontú, az IT és OT környezetet egyaránt lefedő, többrétegű információbiztonsági megközelítéssel. Ez nemcsak az információk védelmét szolgálja, hanem közvetetten hozzájárul az iparbiztonság és a lakosságvédelem magasabb szintű érvényesüléséhez is.

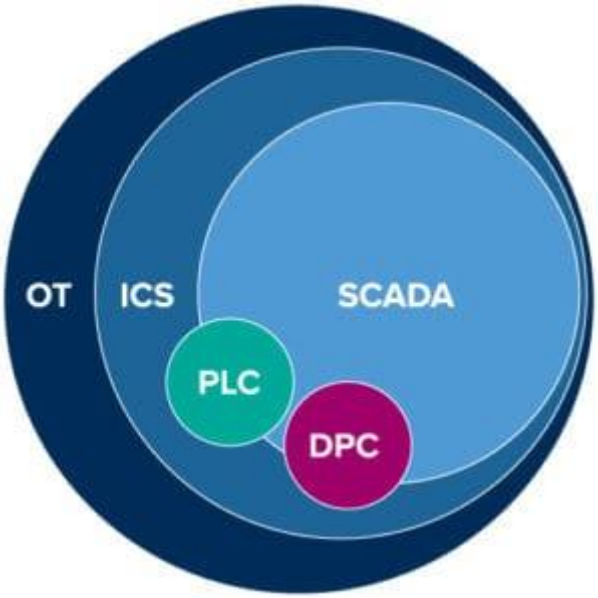
3.3 OT rendszerek és az ipari környezet

Az ipari digitalizáció előrehaladásával a fizikai folyamatokat irányító rendszerek egyre inkább hálózatba kapcsolt informatikai környezetben működnek. Az OT és IT közötti határvonal a gyakorlatban sokszor nehezen meghatározható. Az amerikai NIST az alábbi definiciót alkalmazza az OT rendszerek esetén: az OT olyan hardver- és szoftverrendszerek összessége, amelyek fizikai folyamatok monitorozását vagy vezérlését végzik, illetve fizikai bemeneteket és kimeneteket kezelnek. E definíció alapján minden olyan rendszer az OT

világába tartozik, amely fizikai környezetben változást okoz, vagy a fizikai környezetből származó jeleket érzékel. [102]

Számos olyan komponens létezik, amely informatikai technológiát használ, ugyanakkor az ipari vezérlési folyamatok működéséhez tartozik. Az OT környezetben tehát nem kizárólag a klasszikus ipari vezérlőberendezések tartoznak a kritikus elemek közé, hanem azok az informatikai komponensek is, amelyek a fizikai folyamatok felügyeletét vagy vezérlését támogatják.

Az OT környezet és annak rendszerei, rendszerelemei több nagy kategóriába sorolhatók, melyek a következők: Az ipari vezérlőrendszerek (Industrial Control Systems (ICS)) az OT rendszerek egy nagy részhalmazát alkotják. Az ICS rendszerek különböző technológiai komponensekből állnak, amelyek együtt biztosítják az ipari folyamatok irányítását. Ide tartoznak többek között a programozható logikai vezérlők (PLC), az elosztott vezérlőrendszerek (DCS), a felügyeleti irányítási rendszerek (SCADA), valamint ipari folyamatok esetén az emberi interakciót lehetővé tevő interfészek (HMI). Ezek a rendszerek együtt alkotják azt a technológiai környezetet, amely az ipari folyamatok automatizált működését biztosítja. A felügyeleti rétegben SCADA rendszerek és operátori állomások biztosítják a folyamatok megjelenítését és irányítását, míg a felsőbb szinten olyan alkalmazások találhatók, mint a Historian vagy a Manufacturing Execution System (MES), amelyek a gyártási folyamatok adatait gyűjtik és dolgozzák fel.



21. ábra Az OT környezetben alkalmazott rendszerek egymásba ágyazott struktúrája, forrás: [103]

A PLC-k az ipari automatizálás alapvető vezérlőelemei. Ezek speciális célú számítógépek, amelyek szenzorokból és más bemeneti eszközökből származó jeleket dolgoznak fel, majd ennek alapján vezérlési utasításokat adnak ki különböző berendezések számára. A PLC-k működése ciklikus jellegű: a rendszer meghatározott időközönként mintát vesz a bemeneti jelekből, feldolgozza azokat a programlogika alapján, majd vezérlési parancsokat küld a kimeneti eszközök felé. A bemeneti jelek lehetnek analóg vagy digitális jellegűek. Analóg jelek például a hőmérséklet, nyomás vagy áramerősség értékei, amelyek folyamatos változást mutatnak. Digitális jelek esetében a bemenetek bináris állapotot képviselnek, például egy kapcsoló vagy relé be- vagy kikapcsolt állapotát. A PLC-k megjelenése az 1960-as évek végére tehető, amikor az ipari folyamatok vezérlésében alkalmazott relés logikai rendszerek rugalmatlansága és karbantartási igénye egyre inkább korlátozó tényezővé vált. Az első PLC-k célja az volt, hogy szoftveresen újraprogramozható, megbízható és ipari környezet kihívásai ellenére is stabilan működő vezérlőegységeket biztosítsanak. [104] A veszélyes üzemekben a PLC-k különösen kritikus szerepet töltenek be, mivel közvetlenül befolyásolják a technológiai folyamatok biztonságát. Alkalmazásuk kiterjed például a nyomás-, hőmérséklet- és áramlásszabályozásra, a biztonsági reteszelések (interlock rendszerek) működtetésére, valamint a vészleállítási (Emergency Shutdown, ESD) rendszerek vezérlésére. A PLC-alapú vezérlés lehetővé teszi a folyamatok precíz szabályozását és a kritikus paraméterek folyamatos monitorozását, ezáltal jelentősen csökkentve az ipari balesetek kockázatát. [2]

Az Ipar 4.0 koncepciója miatt a klasszikus, izolált vezérlőegységekből mára hálózatba kapcsolt, kommunikációképes rendszerek váltak, amelyek integrálódnak a felügyeleti és adatgyűjtő rendszerekkel (SCADA), valamint a vállalatirányítási rendszerekkel (ERP). Azonban a PLC-k hálózati integrációja új kockázatokat is magában rejt. A korábban zárt rendszerek egyre inkább nyitottá válnak, ami növeli a kibertámadásokkal szembeni kitettséget. A PLC-k és az ipari vezérlőrendszerek (ICS) elleni támadások, például a Stuxnet incidens, rámutattak arra, hogy a kibertérben végrehajtott beavatkozások fizikai következményekkel is járhatnak. Ennek megfelelően a PLC-k biztonságának kérdése ma már nem csupán informatikai, hanem iparbiztonsági szempontból is kiemelt jelentőségű.

A PLC rendszerek mellett jelentős szerepet töltenek be az elosztott vezérlőrendszerek (Distributed Control Systems (DCS)) és felügyeleti vezérlő- és adatgyűjtő rendszer (Supervisory Control and Data Acquisition (SCADA)) rendszerek. Ezek elsősorban nagyobb ipari létesítményekben, például erőművekben vagy vegyipari üzemekben használatosak. A DCS rendszerek komplex ökoszisztémát alkotnak, amelyben a vezérlési intelligencia nem

egyetlen eszközben koncentrálódik, hanem több különböző vezérlőegység között oszlik meg. Tehát a DCS architektúra jellemzője a funkcionálisan elosztott, de logikailag egységes irányítás. A DCS rendszerek erősen támaszkodnak a redundanciára, mivel az ipari folyamatok folyamatos működése kritikus fontosságú. A redundáns vezérlők, kommunikációs csatornák és bemeneti-kimeneti modulok biztosítják, hogy egy rendszerelem meghibásodása ne vezessen az egész rendszer leállásához. A DCS közvetlenül részt vesz a technológiai folyamatok zárt hurkú (closed-loop) szabályozásában, addig a SCADA inkább felügyeleti jellegű, és jellemzően nem végez alacsony szintű, gyors ciklusidejű vezérlést. Emellett a DCS rendszerek általában egy adott létesítményen belül működnek, míg a SCADA rendszerek nagy kiterjedésű, gyakran heterogén hálózatokat fognak össze. A két rendszer közötti legfontosabb különbség tehát a vezérlés szintjében és integráltságában ragadható meg, a SCADA magasabb szintű vizualizációt, adatfeldolgozást és operátori beavatkozást támogat. A SCADA rendszerek tipikusan különböző terepi eszközöktől, például PLC-ktől és RTU-któl, származó adatokat integrálnak, lehetővé téve az operátorok számára a rendszer állapotának valós idejű nyomon követését. Ezen túlmenően a SCADA rendszerek támogatják a riasztáskezelést, az eseménynaplózást, valamint a történeti adatok (historian)[29] archiválását és elemzését is. A modern SCADA megoldások egyre inkább hálózatalapú architektúrákra épülnek, és integrálódnak más vállalati rendszerekkel, ami elősegíti az adatvezérelt döntéshozatalt, ugyanakkor jelentős kitettséget is jelent az OT környezetre nézve. [2]

A HMI (Human–Machine Interface) ezzel szemben az a felhasználói felület, amelyen keresztül az operátor közvetlen kapcsolatba lép az irányítórendszerrel. A HMI biztosítja a technológiai folyamatok vizuális megjelenítését folyamatábrák, trendek és állapotjelzések formájában, valamint lehetőséget ad a beavatkozásra, például paraméterek módosítására vagy vezérlési parancsok kiadására. A HMI rendszerek kialakítása során kiemelt szempont az ergonómia és az információk áttekinthető megjelenítése, mivel az operátori döntések közvetlenül befolyásolják a folyamatok biztonságának alakulását.

Az ipari vezérlőrendszerek működésében kulcsszerepet játszanak a terepi eszközök. Ide tartoznak például a szenzorok, szelepek, relék, motorok vagy robotikai berendezések. Ezek az eszközök közvetlen kapcsolatban állnak a fizikai környezettel, és a vezérlőrendszerek számára szolgáltatnak adatokat, illetve hajtják végre a vezérlési utasításokat. A terepi eszközök a kiber-

[29] A SCADA rendszerek a történeti adatok kezelését jellemzően dedikált *process historian* komponenseken keresztül valósítják meg, amelyek időbélyegzett folyamatadatok (pl. hőmérsékleti értékeket, nyomás, áramlás stb.) nagy mennyiségű tárolását és elemzését teszik lehetővé, míg az eseménynaplózás külön alrendszerben történik.

fizikai rendszerek legalsó rétegét alkotják, és egyben a fizikai folyamatok biztonságának utolsó védelmi vonalát jelentik. Amennyiben ezek az eszközök manipulálhatók vagy kompromittálhatók, a támadások közvetlen hatással lehetnek a fizikai környezetre. [105]

3.4 Ipari vezérlőrendszereket érintő esettanulmányok

Az ipari létesítmények elleni kibertámadások tudományos igényű elemzését jelentősen nehezíti, hogy az érintett szervezetek túlnyomó többsége nem hoz nyilvánosságra incidenseket, vagy azokat minimálisan dokumentálja. Ennek hátterében több, egymást erősítő tényező áll. Egyrészt egy kibertámadás nyilvánosságra kerülése súlyos reputációs veszteséggel jár, különösen az alapvető szolgáltatást nyújtó szervezetek esetén, ahol a társadalmi bizalom fenntartása alapvető üzleti és működési érdek, ezen túlmutatóan akár nemzetbiztonsági érdek is lehet. Másrészt az incidens részleteinek nyilvános közzététele paradox módon növeli a szervezet kiberbiztonsági kitettségét, valamint felhívja a szervezetre a figyelmet, ugyanis a feltárt sérülékenységek, támadási vektorok és rendszerarchitektúrára vonatkozó információk más, a kibertérben tevékenykedő rosszindulatú aktorok számára is hasznosítható hírszerzési értéket képviselnek, ezzel ténylegesen bővítve a támadási felületet. Harmadrészt, számos állam jogrendszerében, köztük az Európai Unió tagállamai esetén a NIS2 irányelv széles körű alkalmazása előtt, nem állt fenn általános kötelező incidensjelentési kötelezettség a kockázatos és kiemelten kockázatos ágazatokba tartozó szervezetek számára. Mindezek következtében a szakirodalom és a nyilvános esetadatbázisok erősen torzítottak: jellemzően csak az állami szervek által önként publikált (mint a német BSI 2014-es Lageberichtje), vagy a támadók által nyilvánosságra hozott esetek válnak széleskörben elérhetővé és kutathatóvá. Ez utóbbi forrástípus különösen problematikus, mivel a támadók kommunikációja stratégiai érdekeik által vezérelt, és megfigyelhető a műveletük által okozott negatív hatás eltúlzása. Az elemzett esetek ezért szükségképpen a jéghegy csúcsát reprezentálják, nem a bekövetkezett esetek teljes spektrumának valós képét tükrözik.

3.4.1 Ausztrál szennyvízkezelő elleni kibertámadás (2000)

Az ausztrál üzem SCADA rendszere ellen elkövetett kibertámadás, az első jegyzett SCADA elleni kibertámadásnak minősül, amit több, mint negyed évszázada követtek el. Az akkor 49 éves Vitek Boden által elkövetett támadás klasszikus példa az elbocsátott munkavállaló bosszújára. Vitek a Hunter Watertech cégnek dolgozott, akik ipari vezérlő

rendszerek telepítését és üzemeltetését végezték Maroochy Shire[30] Tanácsának megbízásából. Boden elbocsátása és a Tanácsnál elutasított jelentkezése után bosszút állt mindkettőn.

2000. február 28. és április 23. között Boden legalább 46 alkalommal támadta a szennyvízkezelő SCADA rendszerét rádióparancsokkal, ami akkoriban még analóg rádiófrekvenciás kommunikációt használt, ekkor még a legtöbb ipari vezérlő rendszer nem IP alapú kommunikációt folytatott. A szennyvízkezelőnek 142 darab szennyvízszivattyú telepe volt, melyekre a cég a saját fejlesztésű PDS Compact 500 nevű RTU-jait telepítette, így lehetővé vált, hogy a szennyvízkezelő üzem valamennyi vízszivattyú telepét monitorozza és adatokat gyűjtsön a SCADA rendszerén keresztül. A szivattyúállomások közötti, valamint a szivattyúállomás és a központi számítógép közötti kommunikáció egy saját analóg kétirányú rádiórendszer segítségével történt, amely átjátszó állomásokon keresztül működött. Minden átjátszóállomás más-más frekvencián sugárzott.
Az elkövető képes volt hozzáférni és megváltoztatni a szennyvízszivattyú állomások adatait, meghibásodásokat okozva azok működésében. Olyan anomáliák jelentkeztek mint, például a szivattyúk működésképtelenné válása, a központi számítógépen a biztonsági riasztások nem jelentek meg, továbbá megszakadt a kommunikáció a szivattyúállomások és a SCADA rendszer között. Gyakorlatilag a szervezet elvesztette a kontrollt az ipari folyamatainak egy része felett. Sokáig nem derült ki, hogy a fellépő „hibák" valójában szándékosan generáltak voltak. Szakértők által végrehajtott digitális forensic vizsgálatokra volt szükség annak megállapításához, hogy folyamatos támadás zajlik.
A helyzet kialakulásához az is hozzájárulhatott, hogy a kibervédelmi intézkedések rendszerszintű bevezetése még nem vált általánosan elfogadott gyakorlattá globális szinten, a szervezet nem rendelkezett egységes kiberbiztonsági szabályozási és kontroll rendszerrel.

A támadások következtében 800 000 liter kezeletlen szennyvíz ömlött ki a helyi parkokba, folyókba és még egy szálloda területére is. A tengeri élővilág egy része elpusztult, a patakok vize feketére színeződött, a bűz pedig elviselhetetlen volt a lakosok számára.

Vitek Boden „tökéletes bennfentes" volt, mert a teljes infrastruktúrát és annak elemeit ismerte, de soha nem volt alkalmazottja a célba vett szervezetnek. Egy olyan alvállalkozó alkalmazottja volt, amely a Maroochy Shire Tanács számára ipari rendszertechnológiát szállított. Emellett a szolgáltatási szerződés nem megfelelően került meghatározásra a Watertech felelősségét

[30] Ma Sunshine Coast régió.

illetően, nem tartalmazott információbiztonsági szempontokat és személyi biztonsági elvárásokat sem.
Az elkövetőt véletlenül fogták el közlekedési szabálysértés miatt. Az autójában az üzem RTU-jainak rádiófrekvenciájára hangolt rádiót találtak, továbbá a laptop és egyéb eszközök is bizonyították bűnösségét. A bíróság két év börtönbüntetésre ítélte, valamint kötelezte a helyreállítási költségek megtérítésére.

Az eset rámutat az ellátási láncbéli sebezhetőségekre és a szervezeten kívüli harmadik felektől származó kockázatok kezelésének fontosságára. Kiemelt figyelmet kell fordítani „belső" személy által végrehajtott támadások azonosítására is. [106]

3.4.2 Németországi acélmű elleni kibertámadás (2014)

A 2014-es németországi acélmű elleni kibertámadás az ipari létesítmények elleni célzott kibertámadások egyik legjelentősebb európai precedenseként tartható számon, és a német szövetségi hatóság által nyilvánosan dokumentált eset, amelyben kibertámadás közvetlen, mérhető fizikai infrastrukturális kárt okozott.
Az esetet a Német Szövetségi Információbiztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik, BSI) hozta nyilvánosságra 2014 decemberében megjelent éves IT-biztonsági jelentésében. A BSI az incidenst APT-típusú (Advanced Persistent Threat) támadásnak minősítette, azonban az érintett szervezet adatait nem hozták nyilvánosságra. A hivatal mindössze egyetlen bekezdésben foglalta össze az esetet, a SANS Institute ICS CP/PE elemzése, ugyanakkor hiteles, független szakértői rekonstrukciót készített az ismert adatok alapján.

A BSI leírása és a SANS elemzők rekonstrukciója alapján a támadás két jól elkülöníthető fázisra bontható. Az első fázisban a támadók kifinomult spear-phishing kampányt folytattak, amelynek célcsoportját kifejezetten ipari üzemi operátorok alkották. A megtévesztő elektronikus levelek nagy valószínűséggel rosszindulatú kódot végrehajtó dokumentumokat (pdf) tartalmaztak, amelyek megnyitásukkor rejtett hálózati kapcsolatot létesítettek a támadók számára a szervezet irodai hálózatához. Ezt követően a második fázisban az elkövetők, olyan rendszereket kompromittálhattak, mint a vállalati Active Directory. A megszerzett információk alapján már képesek voltak az irodai hálózatból az üzemi hálózatba (OT) laterális mozgással behatolni. A művelet pontos technikai hátteréről sajnos nem áll rendelkezésre semmilyen hivatalos információ.

A támadás eredményeként bizonyítottan sérültek a vezérlő rendszer egyes elemei, valamint maga a nagyolvasztó működése is, amelynek típusa ugyan nem ismert, de működésének zavara kritikus következményekkel járt. A PLC-alapú központi vezérlési funkciók érintettsége különösen valószínűsíthető, mivel ezek felelősek az ipari folyamatok automatizált szabályozásáért. Ezzel párhuzamosan a riasztórendszerek, valamint a SIS rendszerek működésének zavara tovább növelhette a kockázatokat, hiszen ezek feladata a veszélyes állapotok felismerése és a szükséges védelmi intézkedések aktiválása és a folyamatok biztonságos állapotba történő visszaállítása.
Az operátorok és a technológiai folyamat közötti kapcsolatot biztosító Human Machine Interface (HMI) rendszerek esetleges kompromittálódása szintén hozzájárulhatott ahhoz, hogy a beavatkozó személyzet nem rendelkezett megfelelő helyzetképpel a folyamat állapotáról. Funkcionális szinten mindez kihatással lehetett többek között az adagolási és anyageloszlási folyamatokra, a tömeg- és energiamérlegek egyensúlyára, a kinetikai modellek helyes működésére, valamint a forrólevegős rendszer szabályozására is. Ezen rendszerek és funkciók együttes sérülése végső soron az irányítás elvesztéséhez vezethetett, amely nemcsak az üzemi folyamatok instabilitását idézte elő, hanem közvetlen fizikai károsodást is eredményezhetett az ipari berendezésekben. A kritikus esemény eredményeként egy nagyolvasztó szabályozatlan leállítását kellett végrehajtani, ami a normál leállási folyamat megkerülése következtében az olvasztó nem definiált állapotba került, ami jelentős kárt okozott a berendezésben. Személyi sérülés nem történt, ami a SANS elemzők szerint a fizikai biztonsági rendszerek (SIS) megfelelő mérnöki kialakítását tükrözi. A potenciális következmények súlyosságát jól illusztrálja, hogy egy nem kibertámadáshoz kötődő, hasonló jellegű nagyolvasztó-robbanás, a 2001-es port talboti angliai üzemben két halálos áldozatot és tizenhárom sérültet követelt.

A SANS publikációja szerint az elkövető legvalószínűbb profilja egy APT-szereplő, azonban ezek a csoportok jellemzően a szellemi tulajdon megszerzését tűzik célul, nem pedig a károkozást. Ugyanakkor a BSI riportjában lévő leírás és a folyamatra vonatkozó részletes technikai tudás alapján a szerzők arra a következtetésre jutnak, hogy a fizikai károkozás szándékos volt. Az elkövetők kiléte és motivációja máig nem tisztázott nyilvánosan, az ipari szabotázstól az állami hírszerzési műveletig számos hipotézis felmerült.

Az eset számos strukturális sérülékenységet tárt fel. Kiemelten problémásnak bizonyultak a vállalati (irodai) és az üzemi hálózat közötti, implicit módon megbízhatónak tekintett kapcsolatok, amelyek megfelelő szegmentálás és folyamatos felügyelet hiányában elsődleges

támadási felületet jelentenek. A SANS elemzők kiemelik, hogy a légréses hálózatelkülönítés (*air gap*) az operatív igények miatt a legtöbb létesítményben nem fenntartható, ezért a hálózatok közötti kommunikáció szigorúan dokumentált, szabályozott és folyamatosan monitorozott DMZ-zónákon keresztül kell, hogy megvalósuljon. Az eset emellett egy fundamentális biztonsági paradoxont is exponál, a célpontértéket nem a védett szervezet önbesorolása, hanem egyedül a támadó szándéka és kalkulációja determinálja. Az acélmű formálisan nem minősült kritikus szervezetnek, mégis kiemelt célponttá vált.

Az eset tudományos értékét tovább növeli, hogy a BSI kormányzati szervként az incidens, ha szűkszavú formában is, nyilvános közzétételét vállalta, normatív precedenst teremtve az incidensmegosztás kultúrájának erősítéséhez egy olyan szektorban, amelyet strukturálisan az aluljelentés és információmegosztási zártság jellemez.

3.4.3 Olaszországi Vízkezelő Üzem Támadása (2023)

Egy dél-olaszi régióban ivóvizet biztosító szervezet ellen követtek el kibertámadást 2023 tavaszán. Az eset során a szervezet zsarolóvírus támadás áldozatává vált, amiért közel 500.000 ember tapasztalhatott meg technikai jellegű problémákat a szervezet ügyfélportálján. Az esetért a Medusa Ransomgang vállalta a felelőséget. A bűnszervezet egy hetet adott az áldozatának a váltságdíj megfizetésért, melynek értékét 100.000 dollárban határozta meg, amennyiben a víz ellátását biztosító szervezet határidőre fizet, az ellopott adatokat törli a Medusa, továbbá az adatok visszaszerzéséért ismételt 100.000 dollárt kell fizetnie a szervezetnek. Emellett lehetősége volt a vízkezelő üzemnek 10.000 dollárért egy nappal kitolni a váltságdíj megfizetésének határidejét. A csoport azt állította, hogy ügyféladatokat, szerződéseket, igazgatósági ülések jegyzőkönyveit, jelentéseket, csőhálózati információkat, és egyéb dokumentumokat szerzett meg. Az üzem működését sikerült megzavarniuk, bár a támadás nem okozott hosszú távú károkat a vízellátásban.
Nincs nyilvános információ arra vonatkozóan, hogy a vállalat végül kifizette-e a váltságdíjat, vagy milyen válaszlépéseket tett meg a támadás utáni helyreállítás érdekében. [107]

A Ransomware-as-a-Service (RaaS) modell keretében működő Medusa Ransomware csoport globális társszervezetekkel működik együtt, így a támadók műveleti területe és támadást követő hatás még szélesebb spektrumban mozog. A Medusa támadási stratégiájának megértése kulcsfontosságú a megfelelő válaszlépések megtételéhez. A zsarolóvírus elsősorban sebezhető Remote Desktop Protocolok (RDP) és megtévesztő adathalász (phishing) kampányok révén fér

hozzá a rendszerekhez. Miután egy rendszert sikeresen feltört, a támadók PowerShell-t használnak a parancsok végrehajtásához, és módszeresen törlésre kerülnek a "shadow copy" biztonsági mentések, ezzel megakadályozva az adatok későbbi visszaállíthatóságát. A támadás nem áll meg itt; a ransomware kiemelt jogosultságokat szerez, kikapcsolja a védelmi mechanizmusokat, és szétterjed a hálózaton. A támadás csúcspontja az adatok titkosítása és egy váltságdíjat követelő üzenet megjelenítése, amelyben az adatok visszafejtéséért jelentős összeget követelnek.

A Medusa Ransomware megjelenése jól szemlélteti a támadási módszerek és technikák folyamatosan változó természetét. A Medusa által alkalmazott kifinomult támadási vektorok, valamint a Ransomware-as-a-Service (RaaS) modellben való működésük jelentős fenyegetést jelent a vállalatok számára. A Medusa RaaS modellje lehetővé teszi, hogy több támadó együttműködve terjessze a ransomware-t és osztozzanak a bevételen, ami növeli a támadások gyakoriságát és sikerességi indexét. [108]
Ez a támadó csoport 2023 augusztus 21-én a Nemzetközi Polgári Védelmi Szervezet webszerverét is megtámadta. A bűnszervezet ebben az esetben is a kettős zsarolási technikáját alkalmazta. [109]

3.4.4 Libanoni vízkezelő rendszerek ellen elkövetett Izraeli kibertámadás (2024)

Izraelt támogató WeRedEvil nevű hacktivista csoport hajtott végre támadás sorozatot 14 libanoni vízkezelő üzem ellen 2024. szeptember végén. A csoport a saját telegram és X csatornáinak leírása szerint célul tűzte ki, hogy megsemmisít mindenkit, aki izraeliek életére tör. Jellemzően az ellenséges államok kritikus infrastruktúráit veszi célpontba. A csoport az általa célba vett rendszerek potenciális sebezhetőségeinek kihasználására egyedi, rosszindulatú szoftvereket fejleszt és alkalmaz, ez kifinomult technikai képességekről árulkodik.

A WeRedEvils social engineering technikákat alkalmazva érzékeny információkat gyűjt a célpontjaitól. Ezt az információt aztán támadásaik fokozására használják fel, vagy átadják ezeket az izraeli biztonsági erőknek. Pszichikai hadviselés céljából a csoport gyakran ad ki közvetlen fenyegetéseket magánszemélyeknek és szervezeteknek, például a Hezbollahnak és iráni tisztviselőknek, olyan titkosított csatornákon keresztül, mint a Telegram.
A kibertámadások kihasználásával Izrael jelentős nyomást gyakorolhat ellenfeleire anélkül, hogy közvetlen fegyveres konfrontációhoz folyamodna. Ez stratégiai előnyt jelent, mivel lehetővé teszi Izrael számára, hogy csökkentse ellenfelei műveleti képességeit és morálját.

A WeRedEvils jól példázza a nem állami szereplők szerepét a kiberhadviselésben. Miközben a hivatalos állami kiberegységektől függetlenül működnek, tevékenységük összhangban van a nemzeti stratégiai célokkal, és Izrael számára kiskaput és operatív rugalmasságot biztosít. [110]

A támadók azt állították, hogy átvették az irányítást dél-libanoni és bejrúti vízügyi létesítményhez kapcsolódó SCADA rendszerek felett, és sikerült megváltoztatni a klórszintet, ami arra utalhat, hogy a Hezbollah tagjainak harcképtelenné tétele volt a cél. Bár sok esetben a hackerek valóban hozzáférnek az ilyen típusú kiber-fizikai rendszerelemekhez, nem ritka, hogy eltúlozzák a támadásaik hatását. Szakértők szerint ez történt ebben az esetben, valamint hangsúlyozták, hogy amennyiben sikeres is volt a támadás a vízkezelő üzemek esetén lehetőség van fizikailag is beavatkozni a folyamatokba, így megakadályozható a kemikáliák drasztikus koncentrációjának módosítása. A támadás tényleges hatása inkább pszichológiai és dezinformációs jellegű lehetett. [111]

3.5 Kiberbiztonsági mutatók, trendek

Számos nemzetközileg ismert és szakmailag hiteles informatikai és kiberbiztonsággal foglalkozó szervezet ad ki rendszeres időnként kiberbiztonsági jelentést. E riportok adatbázisai, statisztikai kimutatásai és következtetései jellemzően az adott szervezet saját telemetriai adataira, incidenskezelési tapasztalataira, valamint ügyfélköréből származó megfigyelésekre épülnek. Ennek következtében ezen jelentések értékes betekintést nyújtanak a valós támadási trendekbe, ugyanakkor értelmezésük során figyelembe kell venni az adatforrásából fakadó esetleges torzításokat is.

3.5.1 Az IT rendszerek sérülékenységei

A szervezetek, így a veszélyes anyagokkal foglalkozó üzemek informatikai hálózatainak, rendszereinek és rendszerelmeinek kiberkockázata évről évre növekszik, és jelentős kihívást jelent ezen kockázatok megfelelő kezelése minden szervezetnek. A legtöbb informatikai infrastruktúra számos olyan sérülékenységgel rendelkezik, melyek kihasználása esetén a támadók rosszindulatú tevékenységeket hajthatnak végre távolról. Jelen kutatás alapvető adatforrását a CISCO Talos 2025-ös évről készült átfogó kiberbiztonsági jelentése adta.

A Cisco Talos jelentése rámutat arra, hogy a leggyakrabban kihasznált sérülékenységek listája egyszerre tartalmaz újonnan publikált sebezhetőségeket és több mint 10 éves CVE-

azonosítóval[31] rendelkező sebezhetőségeket. Kiemelendő, hogy a vizsgált sérülékenységek mintegy 32%-a legalább egy évtizede ismert, ami strukturális problémákra utal a patchmanagement és az eszköznyilvántartás területén. Ezek alapvető komponenseket érintenek, amelyek széles körben elterjedtek pl. PHP[32], web szerverek és sok esetben közvetlen kezdeti hozzáférést biztosítanak a támadók számára.

A Cisco Talos jelentése kiemeli, hogy a kritikus, széles körben használt nyílt forráskódú komponensek sérülékenységei több éves, akár ökoszisztéma-szintű kitettséget eredményezhetnek. Még intenzív patchmanagement tevékenység mellett sem lehetséges a sebezhető felület teljes megszüntetése, mivel ezek a komponensek mélyen beágyazódnak a szoftverellátási láncba. Ez rámutat a függőségek hosszú távú biztonsági hatására, valamint arra, hogy az egyszerűen kihasználható sérülékenységek tartós és nehezen eliminálható kockázatot jelentenek. Ezzel szemben a leginkább kihasznált sérülékenység 2025-ben publikált React2Shell volt. A sérülékenység azt demonstrálja, hogy az alkalmazásréteg esetében a sérülékenységek kihasználása szinte azonnal megkezdődik, minimális reakcióidőt hagyva a védekező oldalon.
A mostani kiberfenyegetési környezet egyik meghatározó jellemzője, hogy a támadók egyre inkább az informatikai infrastruktúra azon elemeit célozzák, amelyek központi szerepet töltenek be a hálózati kommunikáció, az autentikáció és a hozzáférés szabályozásában. A Cisco Talos elemzése alapján a hálózati infrastruktúrák sebezhetőségeinek kihasználása kiemelt jelentőségűvé vált, különösen azon rendszerek esetében, amelyek azonosítási vagy hozzáférés-ellenőrzési funkciókat látnak el.

A támadók elsődlegesen olyan rendszerelemeket céloznak, mint a VPN gateway-ek, tűzfalak, ADC[33]-k, valamint hálózatmenedzsment platformok. Ezek kompromittálása lehetővé teszi a hitelesítési mechanizmusok megkerülését, valid felhasználóként azonosítva magukat, valamint a hálózaton belüli laterális mozgást. Mivel ezen eszközök gyakran az infrastruktúra peremén helyezkednek el és közvetlen internetes kitettséggel rendelkeznek, sérülékenységeik kihasználása gyors és hatékony belépési pontot biztosít a támadók számára. A jelentés rámutat

[31] CVE (Common Vulnerabilities and Exposures) MITRE szervezet által nyilvántartott publikus katalógusa az információbiztonsági sérülékenységeknek.
[32] Programozási nyelv, elsődlegesen webalkalmazások fejlesztésére alkalmazzák.
[33] Application Delivery Controller olyan, az alkalmazási rétegben működő új generációs hálózati komponens, amely a backend szerverek erőforrás elosztását végzi, valamint autentikációs, titkosítási és session-kezelési funkciókat is ellát.

arra is, hogy a támadók számára nem a sérülékenységek száma, hanem azok kihasználhatósága és súlyossága a döntő tényező.

22. ábra A támadói művelet technikai lépései, készítette: a szerző

A Cisco Talos elemzése alapján azonban az ADC jelentősége elsősorban nem önmagában, hanem a támadási láncban betöltött szerepében ragadható meg: kompromittálása lehetővé teszi a támadó számára, hogy az alkalmazási réteg feletti kontroll megszerzésével több, egymástól független rendszerhez is hozzáférjen, és legitim felhasználóként jelenjen meg. Az ilyen típusú támadások jól illusztrálják, hogy a modern kiberfenyegetések nem izolált sérülékenységek kihasználására, hanem egymásra épülő infrastruktúra-elemek láncolatán keresztül megvalósított, hosszú távú hozzáférés-szerzésre irányulnak.

A zsarolóvírus-támadások továbbra is a legjelentősebb kiberfenyegetések közé tartoznak, amelyek folyamatosan fejlődő taktikákkal és üzleti modellekkel (ransomware-as-a-

service) operálnak. A Cisco Talos jelentése szerint 2025-ben a gyártóipar (manufacturing) volt a leginkább célzott szektor.

Ennek hátterében több tényező áll:

- alacsony tolerancia az üzemfolytonossággal szemben,
- IT és OT rendszerek összekapcsoltsága,
- komplex és gyakran elavult infrastruktúra,
- korlátozott kiberbiztonsági erőforrások.

Bár a Cisco Talos jelentés elsősorban a támadási trendeket mutatja be, ezek a tényezők jól magyarázzák az iparág fokozott kitettségét.
A második leginkább érintett szektor a tudományos, műszaki és szakmai szolgáltatások területe, amely magában foglalja az IT tanácsadást, mérnöki tevékenységeket és kutatási intézményeket. E szervezetek különösen vonzó célpontot jelentenek, mivel gyakran kritikus infrastruktúrák beszállítói, illetve magas hozzáadottértéket képviselnek, így az általuk kezelt adatok is fontosak, melynek köszönhetően a zsarolóvírusok kiemelt célpontjává vált ez a szektor.
A ransomware támadások során megfigyelhető egy egyértelmű trend az azonosítás- és hitelesítés-kezelési rendszereket célzó támadások irányába: a támadók jellemzően hiteles felhasználói fiókok megszerzésére és kihasználására törekednek, amely lehetővé teszi számukra a hálózaton belüli észrevétlen mozgást és a támadás kiterjesztését. a ransomware támadások során alkalmazott eszközök között egyértelmű dominancia figyelhető meg olyan technológiák esetében, amelyek legitim rendszergazdai vagy távoli hozzáférési funkciókat biztosítanak.

A leggyakrabban használt eszközök közé tartoznak:

- RDP (Remote Desktop Protocol),
- PsExec,
- PowerShell.

Ezek közös jellemzője, hogy:

- legitim adminisztrátori eszközök,
- működésükhöz érvényes hitelesítési adatok szükségesek,

- lehetővé teszik a rendszeren belüli észrevétlen mozgást.

Ezen túlmenően számos távoli elérést biztosító eszköz (pl. AnyDesk, TeamViewer) és speciális támadási eszköz (pl. Mimikatz, Impacket) is megjelenik a listán, amelyek a hitelesítési adatok megszerzését, valamint a laterális mozgást támogatják. Ez a tendencia tovább erősíti azt a megállapítást, hogy a hatékony védekezéshez nem elegendő a hagyományos technikai védelem, hanem kiemelt figyelmet kell fordítani a jogosultság- és hozzáféréskezelésre, valamint a felhasználói viselkedés monitorozására.

A Cisco Talos jelentés ugyan nem részletezi a távoli hozzáférési eszközök konkrét támadási mechanizmusait, azonban egyértelműen rámutat arra, hogy az olyan technológiák, mint az RDP, valamint a legitim távoli menedzsment eszközök (pl. TeamViewer, AnyDesk) kiemelt szerepet játszanak a zsarolóvírus-támadások során. A gyakorlatban ezek kihasználása jellemzően érvényes hitelesítési adatok megszerzésén alapul, amelyet követően a támadók interaktív módon, legitim felhasználóként férnek hozzá a rendszerekhez, lehetővé téve a laterális mozgást és a támadás kiterjesztését. Ezeket a legitim eszközöket felhasználó támadásokat szokás „living off the land” támadásnak nevezni.
A többfaktoros hitelesítés (MFA) az elmúlt években az egyik legfontosabb védelmi mechanizmussá vált a felhasználók azonosítása és hitelesítése terén. Ennek ellenére a kiberfenyegetési trendek azt mutatják, hogy a támadók egyre kifinomultabb módszereket alkalmaznak az MFA megkerülésére, illetve kijátszására. A Cisco Talos 2025-ös elemzése alapján az MFA elleni támadások jelentős növekedést mutatnak, különösen az azonosítási és hozzáféréskezelési rendszerek (IAM) esetében, amelyek a támadások mintegy 30%-át teszik ki. Ezek a rendszerek kulcsfontosságúak, mivel közvetlen hozzáférést biztosítanak üzleti alkalmazásokhoz, API-khoz és kritikus infrastruktúrákhoz. Sikeres kompromittálásuk esetén a támadó nem csupán egy rendszert ér el, hanem az egész szervezeti környezet felett szerezhet felügyeletet.

Az MFA elleni támadások egyik leggyakoribb formája az úgynevezett MFA spray támadás, amely során a támadók nagyszámú felhasználói fiókot céloznak meg, és korlátozott számú, gyakran használt jelszót próbálnak ki. E támadási módszer hatékonysága abban rejlik, hogy nagy volumenben, alacsony zajszint mellett képes működni, így nehezebben észlelhető. A cél nem egy konkrét felhasználó kompromittálása, hanem egy „gyenge láncszem” megtalálása, amelyen keresztül a támadó beléphet a rendszerbe. Sokszor botnetek követik el automatizáltan a támadásokat, és jellemzően M365 vagy hitelesítési portálokat támadnak, a támadás megkerüli a többfaktoros hitelesítést (MFA), mivel a nem interaktív bejelentkezési

folyamatokat használja, amelyeket sok szervezet nem monitoroz megfelelően. A támadások elosztott módon zajlanak, hogy minimalizálják a fiókzárolásokat és maximalizálják a kompromittálás esélyét.

Ezzel szemben az MFA fatigue (vagy MFA bombing) támadások egyetlen felhasználóra koncentrálnak. A támadó folyamatos hitelesítési kérelmekkel árasztja el az áldozatot, abban bízva, hogy az végül, figyelmetlenségből vagy kimerültségből jóváhagy egy jogosulatlan belépést. A két támadási forma közötti alapvető különbség tehát a hatókörben rejlik: míg a spray támadás széles körben próbálkozik, addig a fatigue támadás célzott és intenzív.
Az MFA elleni támadások egyre jelentősebb formája az úgynevezett eszközkompromittálás (device compromise), amely során a támadó nem a hitelesítési folyamatot támadja direktben, hanem magát a hitelesítési faktorként használt eszközt. Ennek egyik tipikus módja a hamis eszközregisztráció, amely során a támadó saját eszközét regisztrálja a felhasználó autentikációs rendszerében.

Az elemzések szerint a rosszindulatú eszközregisztrációs események száma jelentős növekedést mutatott, mintegy 178%-kal emelkedve egy év alatt, ami arra utal, hogy a támadók egyre inkább az egyszerűbb, tartós hozzáférést biztosító módszereket részesítik előnyben. Amennyiben a támadó sikeresen regisztrál egy eszközt, az a rendszer számára legitim hitelesítési faktorként jelenik meg, így a későbbiekben az MFA védelmi mechanizmus lényegében megkerülhetővé válik.

Az eszközkompromittálás különösen veszélyes, mivel:

- tartós hozzáférést biztosít,
- magas szintű bizalmi szintet eredményez, széleskörű hozzáférés,
- nehezen észlelhető a hagyományos biztonsági eszközökkel.

A támadások gyakran manipulációval (pl. vishing[34]), session-eltérítéssel vagy hitelesítési tokenek megszerzésével valósulnak meg.

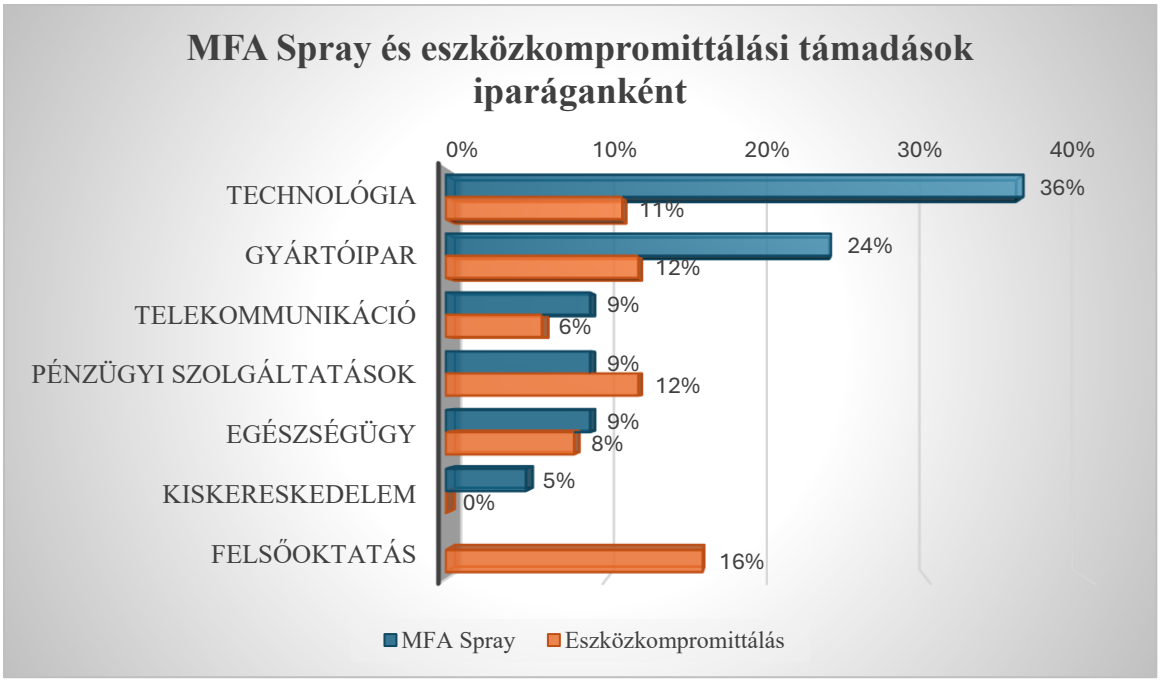
Az MFA elleni támadások és az eszközkompromittálási technikák alkalmazása szektoronként eltérő mintázatot mutat. A jelentésben a rendelkezésre álló adatok alapján a technológiai szektor a leginkább célzott, az MFA spray támadások mintegy 36%-át érintve. Ennek oka elsősorban

[34] hangalapú adathalászat, célja a bizalom kihasználása, ami pénz- vagy identitáslopáshoz vezethet pszichológiai manipuláció révén.

az, hogy ezek a szervezetek magas szintű IAM érettséggel, nagyméretű felhasználói bázissal és egységes autentikációs rendszerekkel rendelkeznek, amelyek ideális célpontot jelentenek a skálázható támadások számára.

Ezzel szemben a gyártóipar (köztük a veszélyes üzemek is) szintén kiemelt célpont, azonban eltérő okokból. Ebben a szektorban a heterogén, gyakran nem menedzselt eszközökből álló környezet, valamint az IT és OT rendszerek összekapcsoltsága kedvez az eszközkompromittálási támadásoknak. Az ipari környezetekben gyakoriak a megosztott munkaállomások, legacy rendszerek és kevésbé szigorú eszközkezelési folyamatok, amelyek növelik a támadási felületet.

További megfigyelés, hogy a magas eszközdiverzitással rendelkező környezetek, például felsőoktatási intézmények szintén különösen érzékenyek az eszközalapú támadásokra, mivel a nem menedzselt vagy részben kontrollált eszközök megnehezítik a hatékony védekezést.



22. ábra MFA elleni támadások megoszlása technika és ágazatok szerint, készítette: a szerző [27]

A Cisco Talos elemzése alapján az adathalászat továbbra is a kezdeti hozzáférés egyik legmeghatározóbb eszköze, amely a szervezeteket érintő biztonsági események mintegy 40%-ában szerepet játszik. A támadók elsődleges célja változatlanul a hitelesítési adatok megszerzése, amelyet gyakran már kompromittált fiókokból indított támadásokkal érnek el, növelve a hitelességet és sikerességet.

A phishing kampányok manapság már egyre kevésbé hasonlítanak a klasszikus spam-jellegű támadásokra, és sokkal inkább mindennapi üzleti kommunikációba ágyazott formában jelennek meg. A leggyakoribb témák közé tartoznak:

- számlák és kifizetések (invoice, payment),
- e-mailek és üzenetek továbbítása (fwd, message),
- jelentések és dokumentumok (report),
- értekezletek és belső kommunikáció.

Ez a tendencia azt mutatja, hogy a támadók tudatosan a szervezeti működés operatív folyamatait célozzák.

2025-ben jelentős növekedés volt megfigyelhető az utazással és logisztikával kapcsolatos témákban, ami arra utal, hogy a támadók a vállalati utazási és költségelszámolási folyamatokat használják ki. Ezen támadások célja jellemzően:

- hitelesítési adatok megszerzése,
- pénzügyi információk ellopása,
- MFA tokenek megszerzése hamis SSO oldalak segítségével.

Ezzel párhuzamosan csökkent a politikai témájú phishing, míg az IT és technikai jellegű tartalmak hangsúlyosabbá váltak, különösen az IT munkakörben dolgozókkal szembeni célzott támadások esetén.
A phishing nemcsak a kezdeti hozzáférés megszerzésében játszik szerepet, hanem akár a támadási lánc későbbi szakaszaiban is. Lehetővé teszi a laterális mozgást és a támadás kiterjesztését, miközben a tevékenység valódinak és hitelesnek tűnik.

Kiemelt fenyegetést jelentenek az úgynevezett Direct Send támadások, amelyek során a támadók Microsoft 365 környezetben belső feladónak tűnő e-maileket küldenek anélkül, hogy valódi felhasználói fiókot kompromittálnának, megkerülve bizonyos e-mail hitelesítési ellenőrzéseket. A Direct Send funkció lehetővé teszi a belső eszközök (pl. nyomtatók, szkennerek) részére, hogy autentikáció nélkül a szervezet domainjével egyező feladóval küldjenek e-mailt.

Az ilyen jellegű támadások különösen veszélyesek, mert az e-mailek belső forrásból származónak tűnnek, nagyobb bizalmat keltenek és gyakran vezetői vagy pénzügyi témákat céloznak (pl. bónuszok, kifizetések, jóváhagyások).

A bemutatott trendek alapján a veszélyes anyagokkal foglalkozó üzemek szempontjából is több fontos következtetés vonható le:

- Az ipari környezetekben gyakori üzleti és logisztikai folyamatok (pl. szállítás, beszerzés, raktározás) ideális célpontot jelentenek a phishing kampányok számára.
- A támadók által használt témák (pl. „shipment", „invoice", „booking") jól illeszkednek a gyártást végző szervezetek működéséhez.
- A kompromittált fiókokból indított belső phishing különösen veszélyes lehet olyan környezetekben, ahol az ellátási lánc és a belső kommunikáció erősen összekapcsolt.

Ez alapján megállapítható, hogy a veszélyes üzemek nemcsak közvetlen technikai támadásoknak, hanem üzleti folyamatokat célzó social engineering támadásoknak is kitettek.

Az államilag támogatott kiberműveletek sajátossága, hogy jellemzően magas, szinte korlátlan erőforrásokkal rendelkező szereplők hajtják végre őket, és hosszú távú, célzott hozzáférés megszerzésére törekednek. E műveletek elsődleges célpontjai gyakran a kritikus infrastruktúrákhoz vagy valamilyen stratégiailag fontos szervezethez kapcsolódó informatikai rendszerek és ipari vezérlőrendszerek (OT/ICS), amelyek kompromittálása nemcsak információbiztonsági, hanem fizikai és társadalmi következményekkel is járhat.

A vizsgált esetek alapján megfigyelhető, hogy a támadók előszeretettel használják ki mind az újonnan felfedezett (zero-day), mind a hosszabb ideje ismert, de nem javított (n-day) sérülékenységeket, különösen a hálózati eszközök és peremrendszerek esetében. Ezek a komponensek, például VPN-ek, routerek és ipari kommunikációs eszközök, gyakran biztosítanak belépési pontot a belső hálózatok felé.
Kiemelendő továbbá, hogy a támadások jelentős része nem azonnali károkozást tűzi ki célul, hanem rejtett, tartós jelenlét kialakítására törekszik, amely lehetővé teszi az információgyűjtést, valamint szükség esetén az üzemi működés befolyásolását. Ez a megközelítés különösen releváns az ipari környezetekben, ahol az IT és OT rendszerek integrációja új támadási felületeket hoz létre.
Az orosz – ukrán konfliktus során az orosz államhoz köthető kibertevékenység szintje szorosan korrelált a geopolitikai fejleményekkel, különösen az USA és az EU által bejelentett szankciókkal. Legmarkánsabban ez május hónapban mutatkozott meg, amikor a szankciók bevezetése egy négyszeres növekedést hozott a megfigyelt orosz kibertevékenységben.

Hasonló összefüggés volt látható októberben és decemberben is. Ez a minta arra utal, hogy a geopolitikai fordulópontok előre jelezhetik a fokozott kiberkockázatot.

23. ábra A nyugati szankciók és az orosz kiberműveletek közti összefüggések, készítette: a szerző [27]

A CISCO jelentése mesterséges intelligencia (MI) kérdésével is mélyrehatóbban foglalkozik, megállapításra került, hogy az MI megjelenése és gyors fejlődése alapvetően alakítja át a kibertérben végrehajtásra kerülő műveletek dinamikáját. Az MI nem csupán új támadási lehetőségeket teremt, hanem jelentősen növeli a meglévő támadási módszerek hatékonyságát, automatizálhatóságát és skálázhatóságát. Megállapítható, hogy a mesterséges intelligencia nem önálló fenyegetési kategóriát jelent, hanem egy olyan erősítő tényezőt, amely a teljes támadási spektrum mentén növeli a kockázatokat.

Az MI alkalmazása különösen jól nyomon követhető a teljes támadási életciklus mentén. A felderítési fázisban az MI képes nagy mennyiségű nyilvánosan elérhető és kompromittált adat gyors elemzésére, lehetővé téve a célpontok, szervezeti struktúrák és felhasználók azonosítását. A „fegyverkezési" szakaszában műveleteknek a támadók MI-alapú eszközöket használhatnak rosszindulatú kódok generálására, illetve azok obfuszkációjára[35], ami megnehezíti a detektálást és a későbbi elemzést.

[35]Az obfuszkáció célja, hogy a programkód szándékosan értelmezhetetlenné váljon miközben a működése változatlan marad. Ennek köszönhetően a vírusirtók és a kutatók nem képesek megérteni és visszafejteni a program működését rövid idő alatt. [122, 122]

A támadások kézbesítési fázisában a generatív MI különösen jelentős szerepet játszik. Lehetővé teszi rendkívül meggyőző adathalász (phishing) e-mailek, hamis weboldalak és kommunikációk létrehozását, amelyek gyakran nehezen különböztethetők meg a legitim, valós tartalmaktól. Ez különösen a hitelesítési mechanizmusokat célzó támadások, valamint az MFA-mechanizmusok megkerülése szempontjából jelent kritikus kockázatot.
A sérülékenységek kihasználása során az MI támogathatja a sebezhetőségek azonosítását és a kihasználási technikák fejlesztését, csökkentve az ehhez szükséges szakértelmet és időráfordítást. Az installáció és perzisztencia kialakítása során az MI-alapú komponensek lehetővé tehetik a rosszindulatú kód rejtettebb működését, például jogtiszta alkalmazásokba vagy pluginekbe ágyazva.
Az irányítási és vezérlési (command and control) fázisban az MI képes az emberi utasításokat végrehajtható parancsokká alakítani, ami növeli a támadások rugalmasságát és adaptivitását. Végül, a célok elérésének és a nyomeltüntetés során az MI támogatja az adatlopás automatizálását, valamint a rosszindulatú tevékenységek legitim forgalomként történő álcázását.
Kiemelendő, hogy az MI kettős hatást fejt ki a fenyegetési környezetre. Egyrészt csökkenti a belépési küszöböt, lehetővé téve kevésbé képzett támadók számára is a komplex támadások végrehajtását, másrészt fokozza a támadások hatékonyságát és gyorsaságát.
A Cisco Talos jelentése alapján a 2025. évi kiberfenyegetési környezetet az azonosítási és hozzáférés-kezelési rendszereket célzó támadások erősödése, a ransomware dominanciája, valamint a régi és új sérülékenységek széles körű kihasználása jellemezte. A támadók egyre gyakrabban legitim eszközökre és hozzáférési mechanizmusokra támaszkodnak, különös tekintettel a hálózati peremeszközökre és azonosításkezelési pontokra, lehetővé téve a tartós, rejtett jelenlét kialakítását. Ezt tovább erősíti az MFA-mechanizmusok megkerülése és a mesterséges intelligencia alkalmazása, amely a támadások automatizáltságát és hatékonyságát növeli. [27]

E trendek a veszélyes anyagokkal foglalkozó ipari létesítmények esetében kiemelt kockázatot jelentenek, mivel az IT–OT rendszerek konvergenciája révén a támadások potenciálisan elérhetik az ipari vezérlőrendszereket is. Egy ilyen környezetben a kibertámadás következménye nemcsak információvesztés lehet, hanem üzemzavar, veszélyes anyagok kontrollvesztett kibocsátása vagy akár súlyos ipari baleset is, ami rámutat a kiberbiztonság és az üzembiztonság szoros összefüggésére.

3.5.2 Az ipari rendszerek kitettsége

Az ipari szervezeteknek, így a veszélyes anyagokkal foglalkozó üzemeknek is az IT környezetük mellett van gyártási környezetük is, melynek digitális architektúrája és rendszerei, rendszerelemei az IT-tól eltérő sérülékenységekkel is rendelkeznek, és az utóbbi időben az IT-OT konvergencia, valamint az internet felé kiforgatott eszközöknek köszönhetően a gyártási (OT) környezet is kibertámadások célpontjaivá vált. Jelen alfejezetben ismert kiberbiztonsággal foglalkozó nemzetközi vállalatok által publikált aktuális ipari rendszereket érintő biztonsági jelentések kerülnek bemutatásra, valamint azokból globális és regionális következtetések levonása. Ennek érdekében, valamint az empirikus kutatás alátámasztása miatt, kvalitatív megközelítés került alkalmazásra. Ezzel az eljárással mélyebb összefüggések megfigyelését kívánom elvégezni. A kutatás során olyan dokumentumok kerültek kiválasztásra, melyek szakmailag megbízható forrásoknak tekinthetők, és az azokban található számadatok, statiszták dekódolását és összevetését követően reprezentatív mintának minősülnek. Három nagy kiberbiztonsági szervezet biztonsági riportja került elemzésre, minden esetben szempont volt, hogy az IT relevanciájú mutatók és számadatok mellett, OT rendszerek is képezzék a jelentés tárgyát.

A kifejezetten OT környezetek védelmére specializálódott amerikai székhelyű Dragos éves kiberbiztonsági jelentése átfogó képet ad az OT/ICS környezetet érintő aktuális fenyegetésekről és több olyan kulcsfontosságú megállapítást fogalmaz meg, melyek veszélyes anyagokkal foglalkozó üzemek esetén is relevánsak.

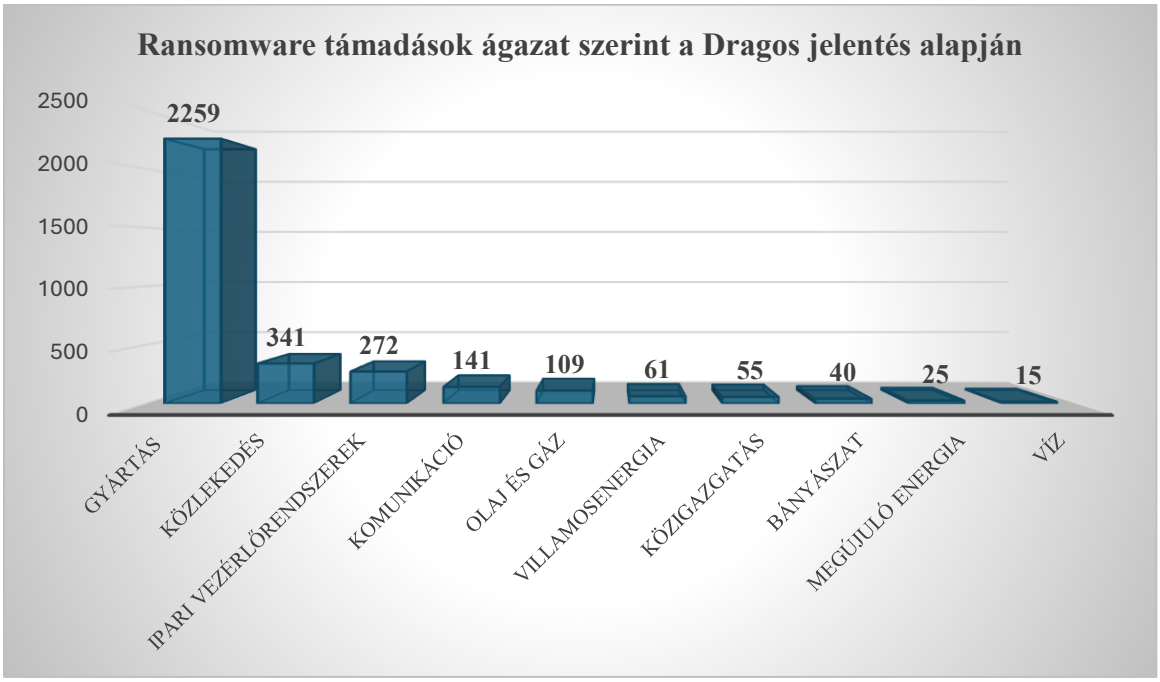
A jelentés szerint a támadók operatív tempója és technikai felkészültsége már meghaladja a legtöbb üzem detektálási képességeit, miközben az OT környezetek jelentős részében még mindig hiányzik az alapvető hálózati monitoring képesség. A Dragos becslése szerint világszinten az OT hálózatok kevesebb mint 10%-ában áll rendelkezésre megfelelő monitoring, ami alapvetően korlátozza az incidensek felismerését és kivizsgálását. A beszámoló kitér arra, hogy a kiber-fizikai rendszerekre az egyik legmeghatározóbb fenyegetés még mindig a ransomware támadás. A Dragos 119 aktív ipari rendszereket támadó zsarolóvírus csoportot azonosított. A jelentés arra is kitért, hogy a ransomware támadásokat jellemzően IT rendszereket érintő támadásként szokták kezelni, mert általában Windows-alapú rendszereket érintenek, azonban a legtöbb mérnöki munkaállomás, valamint SCADA-k és HMI-k windows alapú operációs rendszeren futnak.

A jelentés a támadási mintázatok tekintetében megállapítja, hogy legtöbb esetben nem OT specifikus kártékony kódokat alkalmaznak, hanem az IT esetén alkalmazott malware-ek kerülnek felhasználásra OT rendszerek kompromittálásában. Különösen kritikus, hogy a támadások gyakran nem közvetlenül a PLC-ket vagy terepi eszközöket célozzák, hanem azokat a támogató rendszereket (pl. SCADA szerverek, historian, hypervisorok), amelyek kiesése esetén az üzem elveszíti a folyamatok feletti kontrollt és valós idejű nyomon követést. További probléma, hogy az OT rendszerek, rendszerelemek patch managementje általában nem megfelelően szabályozott, az üzemfolytonosság és a magas rendelkezésre állás miatt, pedig mellőzött, így a közismert sérülékenységek sem kerülnek sokszor kijavításra.

Kiemelendő, hogy a támadások túlnyomó többsége a gyártóipart érinti, amely a jelentés szerint az összes azonosított áldozat több mint kétharmadát teszi ki. nemcsak gazdasági, hanem geopolitikai szempontból is fokozott kitettséggel rendelkeznek. A jelentés rámutat arra, hogy a RaaS ökoszisztéma erősen specializált és többszereplős modellként működik. A támadási lánc különböző szakaszai, például a kezdeti hozzáférés megszerzése, a laterális mozgás, valamint a végrehajtás, gyakran eltérő szereplők között oszlanak meg. Ebben a modellben kiemelt szerepet játszanak az úgynevezett initial access broker (IAB) szereplők, akik a kompromittált rendszerekhez való hozzáférést értékesítik a zsarolóvírust használni kívánóknak. Az OT környezeteket érő támadásokban megfigyelhető felderítési és támadási fázisok szétválása. . Kiemelt példát szolgáltat erre az ELECTRUM csoport aktivitása, amely korábban az ukrán villamosenergia-hálózat elleni támadásokkal volt összefüggésbe hozható, és a jelentés szerint jelenleg is aktív, különösen az európai, például lengyelországi, energetikai infrastruktúrák elleni műveletekben. Az ilyen típusú műveletek alapján feltételezhető, hogy az ELECTRUM mögött állami támogatottságú (nation-state sponsored) szereplő áll, amely stratégiai célpontokat választ. Az európai veszélyes üzemek és kritikus infrastruktúrák tehát nemcsak gazdasági, hanem geopolitikai szempontból is fokozott kitettséggel rendelkeznek. [112]

A Dragos hangsúlyozza, hogy a RaaS támadások többsége nem közvetlenül az ipari vezérlőeszközöket célozza, hanem azokat az IT-alapú rendszereket, amelyek az OT működéséhez kapcsolódnak, például a SCADA szervereket, vagy a virtualizációs infrastruktúrát. Ennek következtében a támadások elsődleges hatása gyakran nem fizikai károkozás, hanem az operatív működés megszakítása. A jelentés ezt „denial of view” és „denial of control” jelenségként írja le, amely során az üzem operátorai elveszítik a folyamat feletti felügyeletet és irányítást.

A jelentés egyik fontos megállapítása, hogy a zsarolóvírus-támadások egyre inkább a működéskiesés maximalizálására irányulnak, nem csupán az adatok titkosítására. Az ipari szervezetek, különösen a gyártóipar és az energetikai szektor esetén a termelés leállása közvetlen gazdasági veszteséget okoz, ami növeli a váltságdíj kifizetési hajlandóságot. A támadók ezt a kényszert tudatosan használják ki, és egyre inkább az üzletmenet-folytonosság megszakítására optimalizálják műveleteiket.



24. ábra Ágazatokat ért ransomware támadások a Dragos által gyűjtött adatok alapján, készítette: a szerző [113]

A Dragos jelentés továbbá kiemeli, hogy a RaaS támadások sikerességét nagymértékben elősegítik az alapvető biztonsági hiányosságok, különösen a gyenge hitelesítési mechanizmusok, a nem megfelelően védett távoli hozzáférési pontok és a hiányos hálózati szegmentáció. A támadók gyakran legitim hitelesítő adatokkal férnek hozzá a rendszerekhez, majd laterális mozgással érik el az OT környezetet kiszolgáló rendszereket.

A Dragos továbbá ismertette, hogy a 2025 ös évben az OT kiberbiztonsági incidensek jelentős része nem előre meghatározott indikátorok alapján került azonosításra, hanem üzemeltetésbeli rendellenességek hívták rájuk fel a figyelmet. Az ilyen esetek az összes vizsgált incidens mintegy 30%-át tették ki, ami rámutat arra, hogy az OT környezetekben a kiberbiztonsági események gyakran a fizikai folyamatok szintjén manifesztálódnak.

A klasszikus indikátorok közül a malware és a ransomware továbbra is meghatározó szerepet játszottak, egyaránt körülbelül 23%-os arányban jelenve meg az incidenskezelési esetek kiváltó okaként. Ugyanakkor a jelentés hangsúlyozza, hogy az incidensek felismerését jelentősen

hátráltatja a megfelelő adatgyűjtési és monitoring képességek hiánya. Számos esetben a szervezetek nem rendelkeztek elegendő objektív adattal a kiváltó ok pontos meghatározásához, ami késleltette az incidensek diagnosztizálását és kezelését.

Az ipari környezetben gyakran hiányos az eszközleltár, korlátozott a naplózás és a hálózati forgalom monitorozása, valamint nem áll rendelkezésre ICS-specifikus detektálási képesség. Ennek köszönhetően a támadók képesek hosszabb ideig észrevétlenül jelen lenni az ipari hálózatban, kihasználva a natív ipari protokollokat és a legitim működésbe ágyazott kommunikációt.

A Dragos jelentés rámutat arra, hogy a támadók egyre gyakrabban célozzák a központi infrastruktúra-elemeket, különösen a hypervisorokat[36], amelyek több OT-funkciót kiszolgáló rendszerek működését támogatják. E rendszerek kompromittálása lehetővé teszi a támadók számára, hogy egyszerre több kritikus komponens felett szerezzenek kontrollt, ezáltal növelve a támadások hatását és hatékonyságát. A hypervisor által kezelt megosztott erőforrásmodell következtében egyetlen rendszer túlterhelése több, kritikus ipari funkciót kiszolgáló virtuális környezet működésére is hatással lehet.
A Dragos jelentés a terepi tapasztalatok alapján az OT környezetek védelméhez öt kulcsfontosságú biztonsági kontrollt határoz meg, ami egy OT környezet megfelelő védelmének az alapját kell, hogy képezze. [113]

A jelentés az OT környezetek védelmének öt kiemelt kontrollterületét azonosítja. Az első az OT-specifikus incidenskezelési terv kialakítása, amelynek figyelembe kell vennie a folyamatbiztonsági és üzemfolytonossági követelményeket is. A második a védhető architektúra kialakítása, különös tekintettel az IT és OT hálózatok megfelelő szegmentációjára és a jogosultságkezelésre, mivel ezek hiányosságai elősegíthetik a támadók laterális mozgását. Harmadik elemként a jelentés kiemeli az OT hálózatok láthatóságának és monitorozásának fontosságát, amely alapvető feltétele a fenyegetések korai felismerésének. Negyedikként a biztonságos távoli hozzáférés jelenik meg, beleértve a multifaktoros hitelesítést, a hozzáférések szigorú kontrollját és a távoli műveletek monitorozását. Az ötödik kontrollterület a kockázatalapú sérülékenységkezelés, amely az OT környezetek sajátosságai miatt a

[36] A hypervisor olyan virtualizációs réteg, amely lehetővé teszi több virtuális gép egyidejű futtatását egyetlen fizikai hardveren. A virtuális gépek egymástól logikailag szeparált környezetben működnek, saját erőforrás-hozzárendeléssel rendelkeznek

sérülékenységek valós kihasználhatóságán és az érintett rendszerek technológiai kritikalitásán alapuló prioritásképzést helyezi előtérbe.

A második biztonsági riport az IBM X-Force Threat Intelligence Index 2026 jelentése, ami nem különíti el explicit módon az ipari kiberbiztonságot a klasszikus IT kiberbiztonságtól, hanem iparági bontásban vizsgálja a kiberfenyegetéseket. Ennek megfelelően az ipari kiberbiztonság elsősorban a gyártóipar és az energetikai szektor elemzésén keresztül jelenik meg, ahol az IT és OT rendszerek konvergenciája miatt a támadások hatása közvetlenül az operatív folyamatokban jelentkezik. A jelentés rámutat arra, hogy a támadók egyre gyakrabban céloznak olyan szervezeteket, amelyek működése kritikus infrastruktúrákhoz vagy ipari termeléshez kapcsolódik, mivel ezek esetében a működéskiesés közvetlen gazdasági és társadalmi hatásokkal jár.

Az IBM X-Force is arra a következtetésre jutott, amire a Dragos is, az ő adatbázisuk alapján is a zsarolóvírus-alapú támadások dominálták a fenyegetési térképet, azonban ezek jellege jelentősen átalakult. A klasszikus titkosításon alapuló támadások mellett egyre nagyobb szerepet kap az adatszivárgással kombinált zsarolás (double extortion). A gyakorlatban ez gyakran külön váltságdíjak formájában jelenik meg, ahol az egyik a rendszerek helyreállításáért, míg a másik az adatok nyilvánosságra hozatalának elkerüléséért kerül meghatározásra (lásd *dél-olasz vízkezelő elleni támadás*). Továbbá olyan kiberműveletek jelentek meg, amelyek célja nem feltétlenül az adatmegsemmisítés, hanem az üzletmenet megzavarása. Ez különösen releváns az OT környezetekben, ahol már a rendszerek rendelkezésre állásának megszűnése is kritikus hatásokat eredményezhet. Az IBM jelentés kiemeli, hogy a kritikus infrastruktúrák és a gyártóipar továbbra is a leginkább érintett szektorok közé tartoznak. A gyártóipar esetében a magas fokú automatizáltság és az ellátási láncok összekapcsoltsága miatt a támadások gyorsan láncreakciós hatásokat válthatnak ki. A támadók számára ezek a szervezetek különösen vonzó célpontok, mivel az leállások jelentős pénzügyi veszteségekkel járnak, így a zsarolási potenciál is magasabb.

Külön figyelmet érdemel, hogy az IBM X-Force jelentése szerint a sérülékenységek kihasználása egyre meghatározóbb kezdeti behatolási vektorrá válik, amelyhez jelentősen hozzájárulnak az automatizált exploit-eszközök és a nyilvánosan elérhető sérülékenységi információk. Ez az OT környezetekben különösen jelentős kockázatot hordoz, mivel az ipari rendszerek frissítése és javítása az üzemfolytonossági követelmények miatt sok esetben korlátozottan hajtható végre.

A jelentés egyik stratégiai jelentőségű megállapítása, hogy a szervezetek jelentős része továbbra sem rendelkezik megfelelő monitorozási és incidensdetektálási képességekkel, különösen az OT környezetekben. Ez összhangban áll más iparági elemzésekkel, amelyek szerint a támadások jelentős része hosszabb ideig észrevétlen marad, ami növeli a potenciális károkat.

A jelentés kitér arra is, hogy az elmúlt öt évben közel négyszeresére nőtt a jelentős ellátási láncot vagy harmadik feleket érintő incidensek száma. A támadók egyre gyakrabban használják ki a fejlesztői bizalmi kapcsolatokat és az azonosítás-alapú integrációkat, pl.: SSO, hitelesítő adatok megszerzésére, majd ezek segítségével belépnek felhőalapú környezetekbe, és tartós jelenlétet építenek ki az egymással összekapcsolt rendszerekben.

A kiterjedt, több szereplőt magában foglaló beszállítói függőségek olyan támadási felületeket hoznak létre, amelyek nehezen védhetők, és ahol egyetlen gyenge láncszem is számos szervezetet tehet sebezhetővé. Bár az ellátási lánc támadások elsődlegesen az informatikai környezetekben kerültek azonosításra, azok az OT környezet esetében is kiemelt relevanciával bírnak. Az ipari környezetekben jellemző az erős beszállítói függőség, különösen a gyártói szoftverek, firmware-ek és távoli karbantartási hozzáférések, olyan kritikus támadási felületeket jelentenek, amelyek kompromittálása közvetlen hatással lehet akár több üzem folyamat- és üzembiztonságára is. [114]

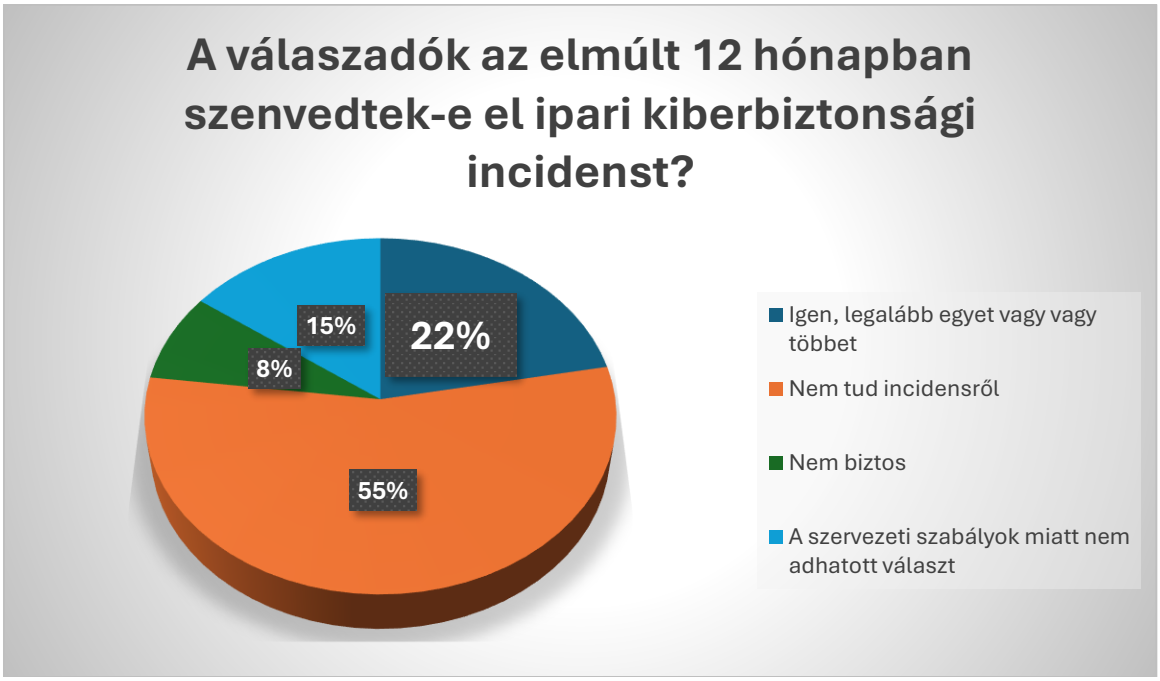
A harmadik biztonsági jelentés az Egyesült Államokbeli SANS Institute publikációja, ami a 2025-ös év ICS és OT biztonsági állapotát vette górcső alá. A biztonsági jelentés primer adatforrása egy kérdőíves felmérés, amelyet 330 ipari és kiberbiztonsági szakember körében végeztek, és ezt egészítették ki szakértői tapasztalatokon és iparági információkon alapuló elemzésekkel. Ennek megfelelően a jelentés inkább percepció-alapú iparági állapotfelmérésként értelmezhető, semmint teljes körű, empirikus incidensadatokon alapuló elemzésként.

A jelentés megállapította, hogy a vizsgált szervezetek mintegy 22%-a tapasztalt kiberincidenst az elmúlt évben, amelynek jelentős része jogosulatlan hozzáféréshez vagy zsarolóvírus-támadásokhoz kapcsolódott. Ezen incidensek közel 40%-a közvetlen működési zavart okozott az ICS/OT környezetben, ami jól mutatja, hogy a kiberbiztonsági események már nem csupán informatikai, hanem operatív, valós következményekkel is járnak.

Pozitívumként a jelentés kitér arra, hogy az ipari kiberbiztonságot két fő tényező alakítja: a fenyegetések növekvő komplexitása és a szabályozási környezet erősödése. A szervezetek egyre nagyobb mértékben támaszkodnak fenyegetési információkra (threat intelligence),

amelyet a válaszadók 67%-a már aktívan alkalmaz, míg további 16% tervezi annak bevezetését. Ez a tendencia arra utal, hogy a védekezési stratégiák egyre inkább adatvezérelt megközelítés felé mozdulnak el.

Ahogy a fenti két biztonsági ripot is kitért rá a SANS dokumentuma is megállapítja, hogy a szervezetek jelentős része nem rendelkezik megfelelő detektálási képességgel az OT környezet tekintetében, ami a gyakorlatban azt jelenti, hogy kiberbiztonsági incidensekről, támadásokról akár napokkal vagy hetekkel később szereznek csak tudomást, ami egy veszélyes üzem esetén akár fizikai következményeket is jelenthet.



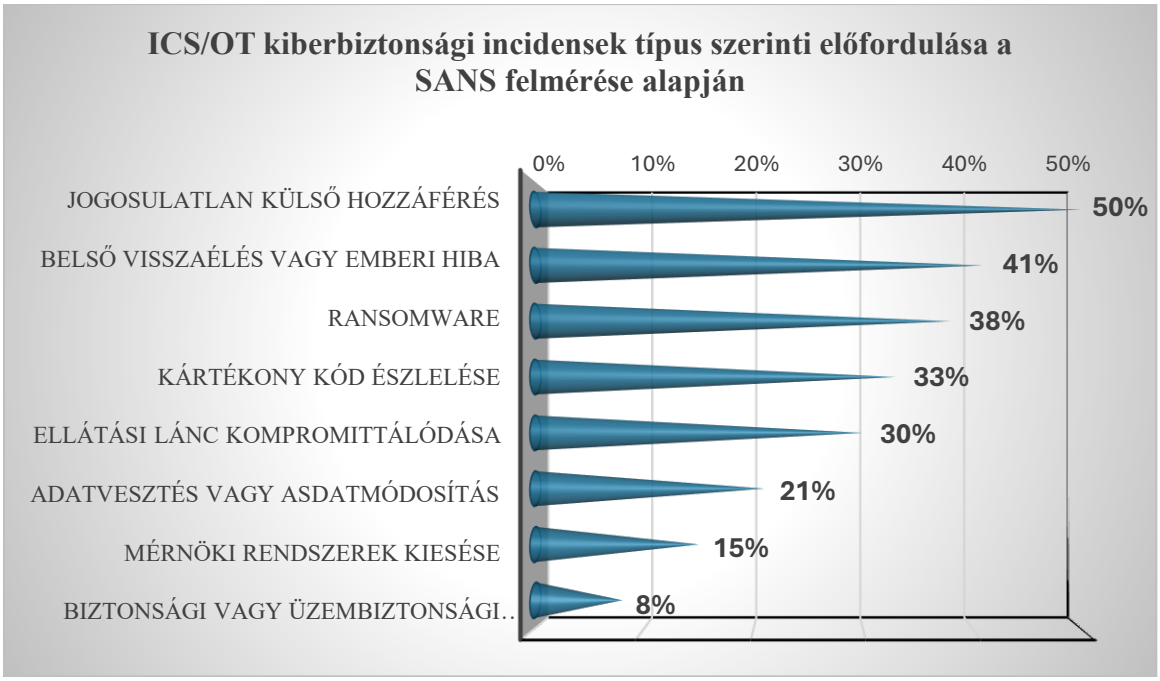
25. ábra A SANS kiber-fizikai környezetet érintő incidensekre vonatkozó felmérésének eredménye, készítette: a szerző [115]

A korábbi évekhez hasonlóan a válaszadók 22%-a számolt be arról, hogy szervezetük kiberbiztonsági incidenst szenvedett el. Ezek közül az esetek többsége jogosulatlan külső hozzáférésből származott (50%), illetve zsarolóvírus-támadásokhoz kapcsolódott (38%).

Ezek az incidensek valós, fizikai és gazdasági következményekkel járnak: az esetek 40%-a az ICS/OT rendszerek működésének megzavarását eredményezte, 13%-uk pénzügyi veszteséget vagy adatkompromittációt okozott.

A jelentés továbbá rámutat arra, hogy az OT környezetekben a támadások nem csupán adatvesztést vagy pénzügyi károkat okoznak, hanem egyre gyakrabban jelennek meg fizikai biztonsági kockázatok is. Bár ezek aránya alacsonyabb (kb. 8%), mégis kiemelt jelentőségű, mivel a veszélyes anyagokat kezelő üzemekben egy ilyen esemény akár súlyos ipari balesethez is vezethet.

Figyelemre méltó, hogy azon létesítményekben, melyeknek valamilyen kiberbiztonsági szabályozási keretrendszernek meg kell felelniük, nagyjából azonos számú ICS/OT incidens fordult elő, azonban mind a pénzügyi veszteségek, mind a fizikai biztonságot érintő kockázatok mintegy 50%-kal alacsonyabbak voltak a nem szabályozott létesítményekhez képest.



26. ábra A kiber-fizikai rendszereket érő incidenstípusok megoszlási aránya, készítette: a szerző [115]

A bemutatott kategóriák nem kizáró jellegűek, hanem többválaszos felmérésen alapulnak, így egyetlen incidens több kategóriában is megjelenhet. Ennek megfelelően az egyes arányok nem összegezhetők 100%-ra, mivel azok az egyes eseménytípusok előfordulási gyakoriságát jelzik a válaszadók körében.

A biztonsági jelentés egyértelműen rámutat arra, hogy a helyreállítási fázis továbbra is jelentős kihívást jelent. Az incidensek felszámolása és a normál működés visszaállítása átlagosan több napot vesz igénybe, az esetek 22%-ában 2–7 nap közötti időtartamot, míg 19%-ában akár egy hónapot meghaladó helyreállítási időt figyeltek meg. Különösen kritikus, hogy egyes esetekben a teljes helyreállítás akár egy évnél is tovább tarthat. Ez a megállapítás közvetlen összefüggésben áll az üzletmenet-folytonossági (Business Continuity Planning, BCP) és katasztrófa-helyreállítási (Disaster Recovery Planning, DRP) tervek és az azokhoz kapcsolódó folyamatok és tesztek jelentőségével, mivel ezek célja éppen az üzemfolytonossági kiesés minimalizálása és a helyreállítási idők csökkentése.

A jelentés hangsúlyozza, hogy a megfelelő felkészültség kulcsfontosságú tényező az incidensek hatékony kezelésében. A válaszadók 57%-a rendelkezik dedikált ICS/OT-specifikus

eseménykezelési tervvel, amely arány 70%-ra emelkedik azon szervezetek esetében, amelyek jogszabályi megfelelés érdekében vagy más keretrendszerek miatt szabályozott környezetben működnek és fenyegetési információkat is alkalmaznak. Ez arra utal, hogy a szabályozási környezet és a threat intelligence integrációja jelentős mértékben hozzájárul a szervezeti reziliencia növeléséhez.

Az üzletmenet-folytonosság és a helyreállítás szempontjából kiemelendő a tesztelési gyakorlatok szerepe is. A szervezetek 39%-a évente, míg 25%-a már negyedévente teszteli incidenskezelési terveit. A gyakoribb tesztelés nemcsak a reagálási idő csökkentéséhez járul hozzá, hanem komplexebb és valósághűbb felkészülést is biztosít technikai szimulációk és szcenário alapú tesztek esetén. Ez közvetlenül kapcsolódik az üzletmenetfolytonossági és katasztrófahelyreállítási képesség hatékonyságához, mivel a rendszeresen tesztelt és frissített tervek jelentősen növelik a szervezetek helyreállítási képességét.

A jelentés további fontos megállapítása, hogy az incidenskezelési tervek folyamatos frissítése elengedhetetlen: a válaszadók közel 80%-a 2025-ben módosította ilyen terveit. A frissítések fő hajtóerői a fenyegetési információk (41%) és a szabályozási vagy audit követelmények (40%) voltak, ami jól mutatja, hogy az ipari kiberbiztonságot erőteljesen befolyásolják a külső környezeti tényezők. [115]

Megállapítható, hogy az ipari kiberbiztonságban a kizárólag megelőzésre épülő védelmi megközelítés önmagában már nem tekinthető elegendőnek, ezért a detektálási és reagálási képességek szerepe folyamatosan felértékelődik. Ezt jól összegzi a jelentésben megfogalmazott elv: „a védelem ideális, de a detektálás elengedhetetlen”. Ez a szemlélet különösen releváns a veszélyes üzemek esetében, ahol a komplex IT–OT környezetekben a teljes támadásmegelőzés nem garantálható, ugyanakkor a korai felismerés, az incidensek gyors izolálása és az időben végrehajtott beavatkozás jelentősen mérsékelheti a technológiai, gazdasági és akár lakosságvédelmi következményeket is.

3.6 A NIS2 irányelv és hazai implementációja

Az Európai Unió kiberbiztonsági szabályozásának egyik meghatározó eleme az Európai Parlament és a Tanács (EU) 2022/2555 irányelve, közismert nevén a NIS2 irányelv (Network and Information Security Directive 2), amely a digitális infrastruktúrák és szolgáltatások védelmének megerősítését célozza. Az irányelv a 2016-ban elfogadott NIS irányelv felülvizsgálatának és kibővítésének eredményeként jött létre, reagálva az elmúlt években jelentősen fokozódó és egyre komplexebbé váló kiberfenyegetésekre.

A NIS2 célja az Európai Unió tagállamaiban a kiberreziliencia egységes és magas szintjének biztosítása, különös tekintettel a kritikus és egyéb jelentős ágazatok működésére. Az irányelv hatálya jelentősen kibővült és új szektorokra is kiterjed, így többek között a postai és futárszolgáltatásokra, a hulladékgazdálkodásra, a vegyiparra, az élelmiszeriparra, a gyártóiparra, a digitális szolgáltatókra és a kutatási szektorra. Az érintett szervezetek két fő kategóriába sorolhatók: alapvető (essential) és fontos (important) szervezetek.

Hangsúlyozni szükséges, hogy a NIS2 irányelv szerinti „kiemelten kritikus" és „fontos" ágazatok nem azonosak a kritikus infrastruktúrák fogalmával, amelyek védelmét külön szabályozás, a CER irányelv rendezi. A NIS2 hatálya alá főszabály szerint azok a közép- és nagyvállalatok tartoznak, amelyek legalább 50 főt foglalkoztatnak vagy éves árbevételük meghaladja a 10 millió eurót, ugyanakkor egyes digitális infrastruktúra-szolgáltatók mérettől függetlenül is érintettek, például a minősített bizalmi szolgáltatást nyújtó szervezetek, DNS-szolgáltatók, legfelső szintű domainnév-nyilvántartók, valamint a digitális infrastruktúrák alapvető szolgáltatói.

A szabályozás egyik kulcseleme a kockázatalapú megközelítés alkalmazása, amely a teljes üzleti folyamatokra és az ellátási láncokra is kiterjed. Ez különösen releváns az ipari és veszélyes anyagokkal foglalkozó üzemek esetében, ahol a beszállítói lánc sérülékenysége közvetlen fizikai és környezeti kockázatokat is eredményezhet. Az irányelv hangsúlyt fektet továbbá a humán tényezőre, előírva a rendszeres biztonságtudatossági képzések bevezetését, amelyek a vezetői szintre is kiterjednek.

A NIS2 a modern kiberbiztonsági megközelítések közül kiemelten támogatja a zero trust modell alkalmazását, amely szerint a hálózaton belüli kommunikáció sem tekinthető automatikusan megbízhatónak, így minden hozzáférést folyamatosan ellenőrizni szükséges. Ezzel összhangban a legkisebb jogosultság elvének érvényesítése is alapkövetelménnyé válik.

Az irányelv jelentős hangsúlyt helyez az incidenskezelésre és a gyors reagálásra. Az érintett szervezetek számára kötelezővé teszi az események bejelentését és azok részletes dokumentálását. A tagállamoknak biztosítaniuk kell a megfelelő intézményi kereteket, így létre kell hozniuk vagy meg kell erősíteniük a nemzeti számítógépes biztonsági eseménykezelő központokat (CSIRT-eket), valamint elő kell segíteniük a nemzetközi együttműködést. E célt szolgálja többek között az EU CyCLONe hálózat, amely a nagyszabású kiberbiztonsági incidensek koordinált kezelését támogatja, valamint az ENISA által támogatott együttműködési mechanizmusok. A direktíva hatálya alá tartozó alapvető és fontos szervezetek jelentéstételi

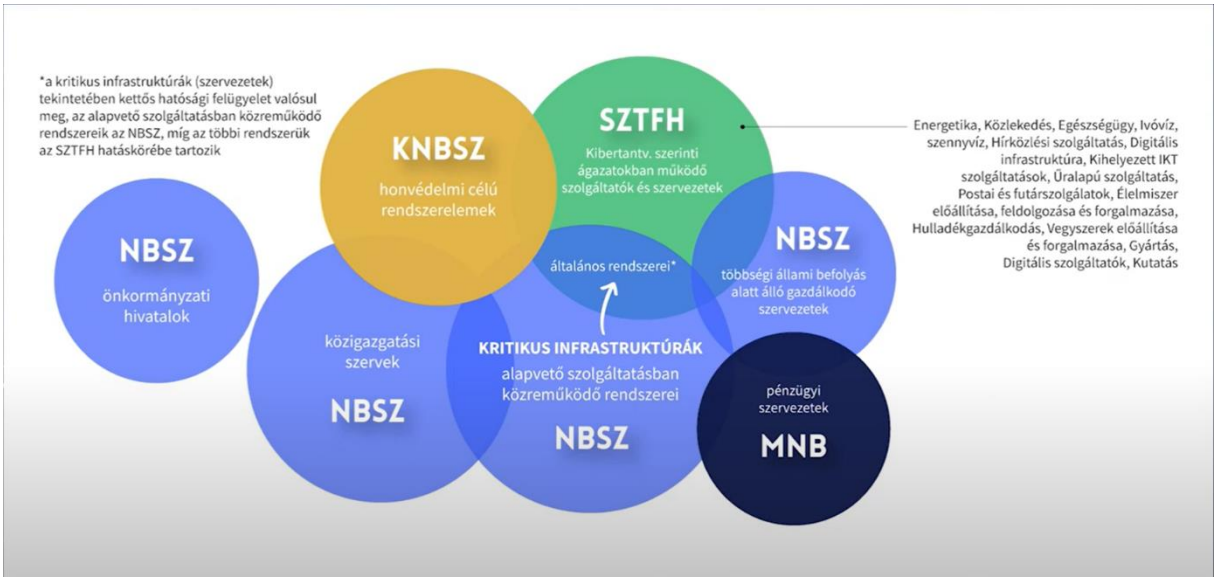
kötelezettséggel rendelkeznek az eseménybejelentés tekintetében, ideértve az esemény jelentését és értékelését, az esemény kezelésével kapcsolatos tájékoztatást, valamint az információk továbbítását a CSIRT-nek és az illetékes hatóságoknak. Emellett a direktíva kitér az érintett szervezetek és a CSIRT közötti kommunikációra, a határokon átnyúló eseményekre vonatkozó együttműködésre és az információk összegyűjtésére és megosztására vonatkozó rendelkezésekre.

A szabályozás végrehajtását szigorú felügyeleti és szankcionálási rendszer támogatja. Az alapvető szervezetek esetében a bírság mértéke elérheti akár a 10 millió eurót vagy az éves árbevétel 2%-át, amely jelentős ösztönzőt jelent a megfelelőség biztosítására.

Az ENISA a NIS2 irányelv alapján feladatul kapta egy európai szintű sérülékenység-adatbázis létrehozását és működtetését, amely az Európai Sérülékenység Adatbázis (European Vulnerability Database – EUVD) néven került kialakításra. Az adatbázis célja, hogy megbízható és időszerű információt biztosítson az információs és kommunikációs technológiai (IKT) termékeket és szolgáltatásokat érintő sérülékenységekről, ezáltal támogatva a kiberbiztonsági kockázatkezelési tevékenységeket.
A nyilvánosan elérhető sérülékenységi információk kulcsfontosságú erőforrást jelentenek mind a szolgáltatásokat igénybe vevő szervezetek, mind az illetékes hatóságok, valamint a szélesebb kiberbiztonsági közösség számára. Az EUVD egy központi európai sérülékenységi adatbázis, amely támogatja az új sérülékenységek önkéntes bejelentését, nyilvántartását és megosztását. Ez elősegíti, hogy a felhasználók időben megtehessék a szükséges kockázatcsökkentő intézkedéseket. A párhuzamosságok elkerülése és a nemzetközi együttműködés erősítése érdekében az ENISA szorosan együttműködik a MITRE Corporation szervezettel, valamint a Common Vulnerabilities and Exposures (CVE) rendszer európai és nemzetközi üzemeltetőivel. A sérülékenység-adatbázisban található sérülékenységekre vonatkozó információkhoz minden érdekelt fél számára szabad hozzáférést kell biztosítani, ezzel segítve valamennyi szervezetet és beszállítót. [116]
A kiberbiztonsági intézkedések gazdasági indokoltságát számos nemzetközi kutatás is alátámasztja. Az IBM 2023-as jelentése szerint az adatvédelmi incidensek átlagos költsége 4,45 millió amerikai dollárra emelkedett [117], míg a Sophos 2024-es felmérése alapján a zsarolóprogram-támadások helyreállítási költsége átlagosan 2,73 millió dollár. A jelentések rámutatnak arra is, hogy a proaktív biztonsági intézkedések, például a DevSecOps alkalmazása vagy a rendszeresen tesztelt incidenskezelési tervek jelentős költségcsökkentő hatással bírnak. [118]

Magyarország a NIS2 irányelvnek való megfelelés érdekében átfogó jogszabályi és intézményi reformot hajtott végre. A hazai követelmények, valamint az audit módszertan alapja az amerikai NIST SP 800-53 rev5-ös dokumentum. Ez azt eredményezte, hogy míg a legtöbb tagállam az ISO/IEC 27001 alapú követelményeket határozott meg, addig Magyarország egy sokkal mélyebb és részletesebb és a fenyegetésekkel szemben naprakészebb elvárásokat fogalmazott meg a direktíva hatálya alá tartozó szervezetek felé. [29] [28]

A hazai végrehajtás intézményi struktúrája több hatóság együttműködésén alapul. A felügyeleti feladatokat többek között a Szabályozott Tevékenységek Felügyeleti Hatósága, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, a Magyar Nemzeti Bank, valamint a Katonai Nemzetbiztonsági Szakszolgálat látják el. E modell sajátossága, hogy nem egyetlen központi „szuperhatóság” működik, hanem több, egymással együttműködő, szektor-specifikus hatóság biztosítja a szabályozás érvényesülését. A gazdálkodó szervezetek esetén alapvetően az SZTFH látja el a felügyeleti hatósági feladatokat és a kiberbiztonsági tanúsításukat ezen szereplőknek, külső auditori cégekkel együttműködve. Az állami és önkormányzati szervezetek, többségi állami tulajdonban lévő gazdálkodó szervezetek, valamint azon EIR-ek, melyek kritikus infrastruktúrának lettek kijelölve, az NBSZ NKI hatáskörébe tartoznak. [119]



27. ábra A hazai kiberbiztonsági felügyeletet ellátó hatóságok, forrás: [120]

Az MNB a pénzügyi szervezetek információbiztonságának felügyeletét és irányítását végzi. A pénzügyi ágazat digitális működési rezilienciájáról szóló (EU) 2022/2554 rendelet (DORA rendelet) alapján. A rendelet hatálya 20-féle pénzügyi szervezetre és nekik IT szolgáltatást nyújtó külső szolgáltatókra terjed ki, függetlenül attól, hogy kiszervezés keretében, vagy egyéb

módon nyújtják ezen szolgáltatásaikat. A rendelet fő célja, hogy a NIS2 irányelv „lex specialis”-aként, a teljes pénzügyi szektorra vonatkozó, uniós szintű, egységes rezilienciára vonatkozó előírásokat fogalmazzon meg.

A körülbelül 3000 magyarországi székhellyel rendelkező gazdálkodó szervezetet érintő első kiberbiztonsági auditoknak legkésőbb 2026. június 30-ig le kell zárulniuk. Azon szervezetek, melyek az első audit során nem feleltek meg a jogszabály által előírt 70%-os SZEKI[37]-nek, cselekvési tervet kell készíteniük és az abban foglaltak megvalósításának előrehaladásáról az SZTFH felé három havonta riportálniuk kell. Az empirikus kutatásom alapján megállapítható, hogy a NIS2 irányelv eredeti célkitűzése a kockázatarányos védelem kialakításának elősegítése volt, azonban a hazai implementáció során megjelenő követelményrendszer komplexitása és adminisztratív terhelése a magyar középvállalati környezetben számos esetben nehezen alkalmazható. Ennek következtében a szervezetek jelentős része nem elsődlegesen a tényleges kiberkockázatok kezelésére és a reziliencia növelésére fókuszál, hanem az audit megfelelőség teljesítésére történő felkészülést helyezi előtérbe. A kutatás során szerzett tapasztalataim alapján a hazai gazdálkodó szervezetek a kiberbiztonsági követelménykatalógust számos esetben szó szerinti értelmezés alapján alkalmazzák, miközben korlátozott mértékben élnek azokkal a kockázatarányos testreszabási lehetőségekkel, amelyeket a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI.24.) MK rendelet is biztosít. A rendelet ugyanis explicit módon lehetőséget biztosít a védelmi intézkedések kockázatelemzésen alapuló testreszabására, eltérő vagy helyettesítő kontrollok alkalmazására, valamint a szervezetspecifikus biztonsági követelmények meghatározására. Megállapítottam továbbá, hogy a testreszabás korlátozott alkalmazása hosszabb távon a formális megfelelőség előtérbe kerülését és akár hamis biztonságérzet kialakulását is eredményezheti, különösen sikeres auditot követően, miközben a szervezet tényleges kiberrezilienciája nem minden esetben tükrözi az elért megfelelőségi szintet. Emellett megállapítottam, hogy az elektronikus információs rendszerek (EIR-ek) lehatárolása és értelmezése az érintett szervezetek között jelentős eltéréseket mutat, amely megnehezítheti az egységes megfelelőségértékelést és a kockázatarányos védelem következetes érvényesülését.

Azonban fentebb elemzett nemzetközi trendek azt igazolják, hogy azon szervezetek, melyeknek valamilyen kiberbiztonsági jogszabály vagy szabvány követelményeinek meg kell

[37] Szervezeti Ellenállóképességi Index

felelniük és rendszeres ellenőrzés alá vannak vetve, sokkal magasabb kiberrezilienciát képesek kialakítani, mint azon szervezetek, amelyeknek nincs ilyen jellegű kötelezettségeik.

3.7 Veszélyes üzemek kiberrezilienciájának kialakítási lehetőségei

Magyarországon a veszélyes anyagokkal foglalkozó üzemek működését alapvetően a katasztrófavédelmi és iparbiztonsági szabályozási jogi környezet határozza meg. Ehhez érkezett meg a kiberbiztonsági hazai jogszabályi keret, melynek hatálya számos magyar veszélyes anyagokkal foglalkozó üzem informatikai infrastruktúráját is érinti. A szabályozási lefedettség tekintetében fontos kiemelni a „fehér foltok" problémáját is. Számos kisebb, küszöbérték alatti vagy alsó küszöbös üzem nem tartozik a NIS2 irányelv hatálya alá, miközben működésük lokális vagy regionális szinten jelentős kockázatot hordozhat. A hatályos jogszabályi keretet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 211/2019. (IX. 5.) Korm. rendelet biztosítja, amely az úgynevezett alsó és felső küszöbértékű üzemek számára kötelezővé teszi biztonsági dokumentációk: biztonsági elemzés (BE), illetve biztonsági jelentés (BJ), valamint a küszöbérték alatti üzemek esetén a súlyos káresemény elhárítási terv (SKET) elkészítését. E dokumentumok szerves részét képezi a Biztonsági Irányítási Rendszer (BIR), amely alapvetően a technológiai és természeti kockázatok kezelésére fókuszál.

A jelenlegi szabályozási és gyakorlati megközelítés ugyanakkor elsősorban a fizikai és technológiai biztonságra koncentrál, miközben az ipari vezérlőrendszerek és az ipari környezet kiberbiztonsági kitettsége egyre jelentősebbé válik. Ebből következően indokolt a BIR kiterjesztése oly módon, hogy az ne kizárólag a hagyományos üzembiztonsági (safety) aspektusokat, hanem az ipari környezet kiberbiztonsági (security) fenyegetései ellen is kockázatokkal arányos védekezés kialakítása szükséges és az ehhez szükséges védelmi intézkedéseket a BIR-ben javasolt integrált módon kezelni. Ez a megközelítés összhangban áll a modern „safety–security convergence" elvével, amely a működési, fizikai és kiberkockázatok egységes kezelését hangsúlyozza.

A hazai kiberbiztonsági szabályozási környezet, különösen a 7/2024. (VI.24.) MK rendelet, alapvetően az amerikai NIST SP 800-53 Rev.5 kontrollkatalógus logikáját követi. Ez a megközelítés azonban elsősorban informatikai (IT) rendszerekre lett kialakítva, és csak korlátozottan alkalmazható az ipari vezérlőrendszerek sajátos környezetében. Az OT rendszerek esetében ugyanis a rendelkezésre állás (availability) elsődlegessége, a hosszú

életciklusok, a gyártói (vendor) függőség, valamint az üzemfolytonosság kritikus jellege jelentősen eltér az IT rendszerek működési paradigmájától.

Különösen problémás terület a sérülékenységkezelés és a javításkezelés (patch management), ahol a hagyományos IT megközelítések, például az azonnali frissítési kötelezettség, nem alkalmazhatók közvetlenül, mivel egy nem megfelelően tesztelt beavatkozás az ipari folyamatok leállását vagy akár súlyos balesetet is eredményezhet. Hasonló kihívást jelent a magas szintű beszállítói kitettség, ahol a rendszerek jelentős része külső gyártók által fejlesztett és karbantartott komponensekből áll, korlátozva az üzemeltető szervezetek ráhatását a biztonsági beállításokra, valamint a rendszerelemeknek is abban a szegmensben homogénnek kell lenniük, hiszen minden nagyobb beszállító saját kommunikációs protokollt alkalmaz.

A fentiek alapján indokolt egy olyan, kifejezetten veszélyes üzemekre szabott kiberreziliencia-keretrendszer kialakítása, amely a BIR szerves részét képezi, és figyelembe veszi az OT rendszerek sajátosságait. E keretrendszer kialakítása során célszerű a nemzetközi ipari kiberbiztonsági ajánlásokra támaszkodni, különösen a NIST SP 800-82 és az IEC 62443 szabványsorozat követelményeire, mert ezen dokumentumok specifikusan az ipari vezérlőrendszerek kiberbiztonsági követelményeit és azok megvalósítási lépéseit határozza meg. [2] [3]

Az IT-OT konvergencia miatt, valamint a teljeskörű digitális reziliencia megvalósítása érdekében, a kutatás nem csak az OT rendszerek szabályozására törekszik. Az üzembiztonság felől közelítve azokra az informatikai kontrollokra fókuszál, amelyek közvetlen hatással vannak az emberi élet és az üzem biztonságára. Ez a megközelítés korrelál a katasztrófavédelem alapelveivel.

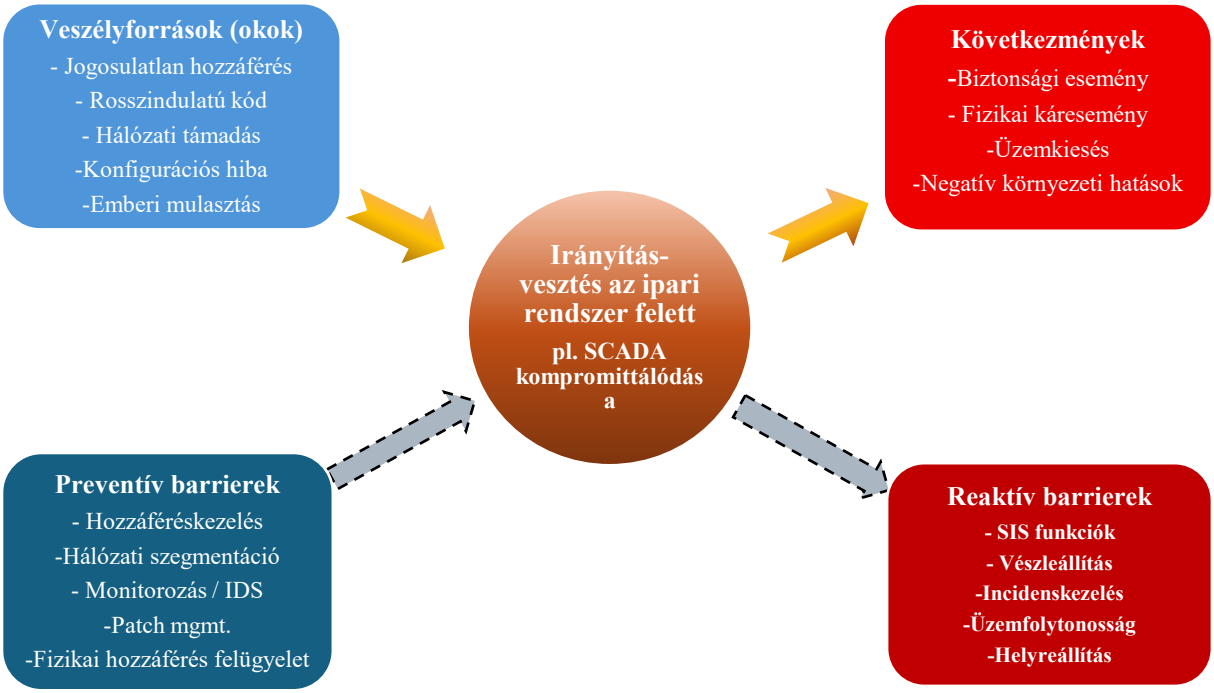
A kockázatalapú megközelítés a hatékony és arányos védelem kialakításának egyik meghatározó alapelve, amelyet a NIS2 irányelv mellett a veszélyes üzemekre vonatkozó hazai szabályozási környezet is hangsúlyosan megjelenít. A veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011 (X.10.) Korm. rendelet 3. melléklete meghatározza a biztonsági jelentés (BJ), biztonsági elemzés (BE), valamint a súlyos káresemény elhárítási terv (SKET) tartalmi és formai követelményeit, és egyértelműen rögzíti, hogy ezen dokumentumok szerves részét kell képezze a veszélyes anyagokkal kapcsolatos súlyos balesetek által okozott veszélyeztetés értékelése. Ennek keretében az üzemeltető köteles olyan módszert alkalmazni, amely együttesen veszi figyelembe a veszélyeztetést, a kockázatot és a lehetséges következményeket.

A rendelet 3. mellékletének 1.6.1. pontja szerint: *„az üzemeltető a veszélyes anyagokkal foglalkozó üzem által okozott veszélyeztetést, a kockázatot és a következmények értékelését együttesen figyelembe vevő módszerrel értékeli.”* E követelmény implicit módon olyan komplex, integrált kockázatelemzési megközelítések alkalmazását indokolja, amelyek képesek a különböző veszélyforrások, így a kiberfenyegetések, együttes kezelésére.

A hagyományosan alkalmazott módszertanok (pl. HAZOP, LOPA) elsősorban technológiai és folyamatbiztonsági eltérések vizsgálatára fókuszálnak, azonban a digitalizált ipari környezetben indokolttá válik ezen elemzések kiberbiztonsági kiterjesztése. Ezen a ponton illeszthető be a Cyber PHA módszertan, amely megfelel a rendelet által megkövetelt komplex értékelési szemléletnek, mivel a kockázatot a fenyegetések, a sérülékenységek és a következmények együttes figyelembevételével vizsgálja. A Cyber PHA módszertan jellemzően több lépésben valósul meg, amely magában foglalja az érintett rendszerek és eszközök feltérképezését, a sérülékenységek azonosítását, a fenyegetési forgatókönyvek kidolgozását, valamint a következmények és kockázatok értékelését. A folyamat során a klasszikus folyamatbiztonsági elemzések (pl. HAZOP) eredményei kiindulási alapként szolgálnak a potenciális kibereredetű baleseti események azonosításához. A módszer egyik kulcseleme, hogy a kockázatot nem önmagában a sérülékenységek szintjén értelmezi, hanem a következmények (pl. egészségkárosodás, környezeti kár, üzemzavar) szempontjából vizsgálja. A sikeres Cyber PHA megvalósítása érdekében, elengedhetetlen, hogy különböző szervezeti egységek meghatározott szerepkörei összehangoltan, megfelelő workshop tool-ok felhasználásával (pl. Cyber PHA Worksheet) együtt dolgozzák ki a kockázatok elemzését.

A Cyber PHA alkalmazásával lehetőség nyílik annak elemzésére, hogy egy adott ipari folyamatban milyen kibereredetű események vezethetnek súlyos baleseti következményekhez, továbbá azonosíthatók azok a védelmi intézkedések, amelyek képesek ezen kockázatok csökkentésére. A módszer a klasszikus folyamatbiztonsági elemzések eredményeire épít, és azokat kiegészítve tárja fel a potenciális kiberfenyegetések által kiváltott eltéréseket és következményeket.

A Cyber PHA módszertan eredményeinek strukturált megjelenítésére és a kockázati összefüggések szemléltetésére jól alkalmazható a bow-tie modell. A megközelítés lehetővé teszi a veszélyforrásokból kiinduló eseményláncok, a kiváltó okok (beleértve a kiberfenyegetéseket), valamint a megelőző és következménycsökkentő védelmi intézkedések egységes ábrázolását. [121]



28. ábra Kiber bow-tie modellre példa, készítette: a szerző

A Cyber PHA továbbá támogatja a kockázatarányos védelem kialakítását is, mivel lehetőséget biztosít a védelmi intézkedések priorizálására és testreszabására. Ez különösen fontos a veszélyes anyagokkal foglalkozó üzemek esetében, ahol a biztonsági rendszerek redundanciája és megbízhatósága kritikus jelentőségű. A módszer eredményeként olyan integrált kockázatalapú intézkedési terv állítható össze, amely figyelembe veszi mind a technológiai, mind a kiberbiztonsági aspektusokat.

3.7.1 A kiberbiztonsági keretrendszer módszertani háttere

Az általam megalkotott kontrollkatalógus és a mögötte lévő módszertan az alábbi néven került meghatározásra: „*Safety-Driven Indusrtrial Cybersecurity Filtering Model*”.

A kontrollrendszer kialakítási módszertana során fokozott figyelmet fektettem a kritikus szervezetek ellenállóképességéről szóló 2024. évi LXXXIV. törvény és a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról szóló 474/2024. (XII.30.) Korm. rendeletre, amely három ellenállóképességi szintet határoz meg, összesen 44 követelménnyel. Ebből 17 követelmény minden szervezet számára kötelező, amelyeket az alapszintű védelem minimumkövetelményeiként lehet értelmezni. Mivel ez a kontrollkatalógus a BM OKF által került elkészítésre, a hatályos kiberbiztonsági kontrollkatalógus követelményszámához viszonyítva, kevés követelményt tartalmazó baseline kialakítását tűztem ki célul, mely nem ró aránytalanul nagy adminisztratív és erőforrásbeli terheket a veszélyes üzemek üzemeltetőire, és figyelembevételre került a hazai középvállalatok működési és érettségi sajátosságai is.

E logika mentén két lehetséges megközelítés volt körvonalazható a veszélyes üzemek kiberrezilienciájának fejlesztésére:

1. Szintalapú modell alkalmazása, amely a CER szabályozáshoz hasonlóan differenciált követelményrendszert határoz meg;
2. Baseline alapú megközelítés, amely egy viszonylag kis számú, kötelező minimumkövetelményeket tartalmazó kontrollkészletet definiál.

A kutatásban végül egy hibrid megközelítés került kialakításra, ami a baseline alapú modellre épül, ugyanakkor egy magasabb érettségi szintet biztosító kiterjesztett kontrollréteget (overlay) is tartalmaz. Ennek az egyik oka, hogy feltehetően számos olyan veszélyes anyagokkal foglalkozó szervezet működik ma Magyarországon, melyek eddig nem tartoztak semmilyen kiberbiztonsági elvárásnak hatálya alá és ebből kifolyólag az ilyen jellegű ellenállóképességük sem alakult még ki. A megfelelő érettségi szint eléréséhez pedig sokszor évek kellenek. A kiterjesztett kontrollszett alkalmazása elsődlegesen azon üzemek esetén releváns, amelyek a NIS2 hatály alá tartoznak, felső küszöbértékű veszélyes üzemnek minősülnek, vagy magasabb digitalizációs / OT-integrációs érettséggel rendelkeznek.

A javasolt baseline modell nem kívánja kiváltani a NIS2 irányelvhez kapcsolódó kiberbiztonsági követelményrendszert, hanem azt kiegészítve vagy attól függetlenül, kifejezetten a veszélyes üzemek iparbiztonsági és üzembiztonsági szempontjaira fókuszál. A kutatás során arra a következtetésre jutottam, hogy a veszélyes üzemek kiberrezilienciájának fejlesztése érdekében nem indokolt a rendszerspecifikus vagy rendszerelem-alapú követelményrendszerek közvetlen alkalmazása (IEC 62443). Ehelyett egy egységes, funkcionális alapú baseline megközelítés szükséges, amely a NIS2-alapú hazai szabályozási környezethez illeszkedik és az OT rendszerek sajátosságait figyelembe véve biztosítja a gyakorlati megvalósíthatóságot és a hatósági ellenőrizhetőséget. Ennek érdekében a NIST SP 800-53 Rev.5 és NIST SP 800-82 Rev.3 OT overlay lett a kiindulási pontja a keretrendszernek, azonban számos olyan IEC 62443 követelmény is beválogatásra került, mely az NIST kontrollszettben közvetlenül nem található meg önálló követelményként.

A baseline követelmények kialakításához a Secure Controls Framework (SCF) módszertanát alkalmaztam, amely lehetőséget biztosít a kontrollok kockázatalapú súlyozására. Megközelítésem szerint azon követelmények kerültek első körben a keretrendszerhez kiválasztásra, melyek a kellően magas súlyozással szerepelnek. Így a „8”-as súlyozású és attól

nagyobb értékű kontrollok kerültek kiválasztásra. Ezen védelmi intézkedések megléte a kritikus területek egyik legfontosabb kockázatmitigáló eszköze.

A kontrollok kiválasztása nem bináris módon történt, hanem többkritériumos értékelési modell alkalmazásával, amely a fizikai következmények súlyosságát, az üzemeltetési realitásokat és a szabályozási illeszkedést együttesen veszi figyelembe.

Miután kiválasztásra kerültek a fent említett keretrendszerek kellő súlyossággal rendelkező követelményei, ezek további szűrése érdekében meghatározásra került egy kétlépcsős döntési logika. Első lépésben kizárásra kerültek azok a kontrollok, amelyek nem rendelkeznek legalább közvetett safety hatással, vagy OT környezetben nem megvalósíthatók. Ezt követően a kontrollok összpontszám alapján kerültek besorolásra, ahol a magas pontszámú elemek a kötelező baseline részét képezik, míg a közepes értékű kontrollok a magasabb érettségi szintű kontrollrétegbe sorolódtak.

Az alábbi értékelési mátrixok kerültek meghatározásra a követelménykatalógus kialakítása érdekében:

Safety dimenzió		
pontszám	**jelentés**	**Értelmezés**
0	nincs hatás	A kontroll hiánya nem hozható összefüggésbe olyan eseménnyel, amely az emberi életet, egészséget vagy a környezetet veszélyeztetné.
1	gyenge, indirekt	A kontroll hiánya csak közvetett, alacsony valószínűségű eseményláncon keresztül vezethet olyan helyzethez, amely safety kockázatot jelenthet.
2	közvetett safety hatás	A kontroll hiánya reális forgatókönyvben lehetővé teheti olyan esemény bekövetkezését, amely további lépések révén fizikai következményekhez vezethet (láncolt hatás).
3	közvetlen safety hatás	A kontroll hiánya közvetlenül olyan működési zavart vagy kontrollvesztést idézhet elő, amely azonnali veszélyt jelenthet az emberi életre vagy a környezetre.

1. táblázat A klasszikus iparbiztonsági dimenzió értékelési módszertana, készítette: a szerző

OT megvalósíthatóság dimenzió		
pontszám	**jelentés**	**Értelmezés**
0	Nem megvalósítható	OT környezetben nem alkalmazható (pl. folyamatos patch kötelezettség)
1	Erősen korlátozott	Csak jelentős kockázattal / leállással / vendor módosítással
2	Korlátozottan megvalósítható	Kompenzáló intézkedésekkel (pl. izoláció, workaround)
3	Jól megvalósítható	Natívan alkalmazható OT környezetben, leállás nélkül

2. táblázat A kiber-fizikai környezetben történő kontroll megvalósíthatósági dimenzió, készítette: a szerző

Üzemfolytonosság dimenzió		
pontszám	**jelentés**	**Értelmezés**
0	nincs hatás	A kontroll hiánya nem befolyásolja az ipari folyamatok működését, kiesés vagy zavar nem várható.
1	marginális	A kontroll hiánya kisebb működési zavarokat okozhat, azonban ezek nem eredményeznek jelentős termeléskiesést vagy biztonsági kockázatot.
2	működést befolyásolja	A kontroll hiánya érzékelhető hatással van a működésre, például termeléscsökkenést, folyamatinstabilitást vagy ideiglenes kiesést okozhat.
3	kritikus működéshez szükséges	A kontroll hiánya a működés leállását, súlyos zavart vagy kontrollvesztést eredményezhet, amely közvetlenül veszélyezteti az ipari folyamatok biztonságos fenntartását.

3. táblázat Az üzemfolytonosság dimenziójára történő hatása a kontrollnak, készítette: a szerző

Összpontszám szerinti besorolási küszöbök:	
Tartomány	**Besorolás**
7-9	**Az alapkövetelmény keretrendszer része**
5-6	**Kiterjesztett - ajánlott**
0-4	**Hatókörön kívüli**

4. táblázat Az egyes követelmények besorolási kategóriái, készítette: a szerző

Az értékelési mátrixok kialakítása során a cél az volt, hogy olyan következményalapú értelmezési keretrendszer kerüljön létrehozásra, amely biztosítja a kontrollok konzisztens, reprodukálható és az ipari környezet sajátosságait figyelembe vevő értékelését.

Egyes kontrollok közvetlen OT/safety szempontból nem tekinthetők kritikusnak, ugyanakkor integrált vállalati kiberbiztonsági és szabályozási környezetben, különösen NIS2-alapú működés esetén nélkülözhetetlenek az egységes governance és kockázatkezelési működés

biztosításához. Ebből kifolyólag a kiterjesztett követelménykatalógushoz lett rendelve, melyet akkor kell alkalmazni a szervezetnek, ha többek között NIS2 érintett is.

Az általam megalkotott szűrési módszertannak köszönhetően 85 darab olyan követelmény került azonosításra, melyek abszolút nélkülözhetetlenek annak érdekében, hogy az üzembiztonságot fenyegető kiberkockázatokkal szemben hatékony védelmi képességet alakítson ki egy hazai veszélyes üzem, ezzel tovább növelve az ellenállóképeségét.

A javasolt kontrollkatalógus és a mögötte lévő üzembiztonsági szemlélet lehetőséget biztosíthat arra, hogy a veszélyes üzemek technológiai és kiber-fizikai rendszereinek ellenőrzése az iparbiztonsági szakterület bevonásával történjen meg, míg a klasszikus vállalati informatikai és NIS2 megfelelőségi követelmények ellenőrzése továbbra is a kijelölt kiberbiztonsági hatósági struktúrában maradjon. Ez csökkentheti a párhuzamos auditálási és adminisztratív terheket, miközben jobban érvényesülhetnek az iparbiztonsági és safety-specifikus szempontok. A megközelítés további előnye lehet, hogy a kiber-fizikai rendszerek értékelése és felkészítése a technológiai folyamatok, valamint az üzembiztonsági következmények figyelembevételével, iparbiztonsági szakmai támogatás mellett valósulhatna meg.

3.8 Fejezetbéli részkövetkeztetések

1. A fejezetben bemutatott nemzetközi kiberbiztonsági jelentések, így különösen a Cisco Talos és az IBM X-Force elemzései egyértelműen rámutatnak arra, hogy a gyártóipar és a kritikus infrastruktúrák ellen irányuló kibertámadások száma az elmúlt években folyamatos növekedést mutat. Ez a két ágazat közel teljeskörűen lefedi a hazai jogszabályok által nevesített veszélyes anyagokkal foglalkozó üzemeket. Ezen ágazatok évek óta a támadások célpontjai között kiemelt helyet foglalnak el, amelyek potenciális következményei túlmutatnak az információbiztonság keretein és közvetlen hatással lehetnek a fizikai biztonságra, a környezetre és az emberi életre.

2. Az informatikai (IT) és a kiber-fizikai (OT) rendszerek közötti konvergencia következtében a hagyományos biztonsági megközelítések már nem tekinthetők elegendőnek. Az OT környezet sajátosságai, mint például a magas rendelkezésre állási követelmények, a hosszú életciklusú rendszerek, továbbá a nagyfokú ellátási lánctól való függőség, és a fizikai folyamatokhoz való közvetlen kapcsolódás indokolttá teszik egy specifikus, az ipari működéshez illeszkedő kiberbiztonsági szemlélet alkalmazását.

3. A veszélyes anyagokkal foglalkozó üzemek teljes körű rezilienciájának biztosítása érdekében elengedhetetlen, hogy a kockázatértékelési folyamatok kiterjedjenek a kiberfenyegetésekre is. Ennek megfelelően indokolt a hagyományos folyamatbiztonsági elemzések, különösen a HAZOP kiegészítése Cyber PHA (Process Hazard Analysis) megközelítéssel, amely lehetővé teszi az ipari folyamatbiztonságot érintő kiber fenyegetések - és a kiber-fizikai rendszerekből eredő kockázatok strukturált azonosítását és értékelését.

4. A veszélyes üzemekre alkalmazható kiberbiztonsági keretrendszer kialakítása során indokolt egy olyan módszertan alkalmazása, amely nem választja el élesen az IT és OT környezeteket, hanem integrált módon kezeli azokat. A javasolt megközelítés alapját a safety és iparbiztonsági szemlélet képezi, amely az üzembiztonság és az emberi élet védelme szempontjából legkritikusabb követelmények azonosítására és priorizálására törekszik, egy dedikált szűrési módszertan alkalmazásával, melynek a „*Safety-Driven Indusrtrial Cybersecurity Filtering Model"* nevet adtam.

5. A szabályozói és hatósági oldal szerepe kulcsfontosságú a fenti követelmények érvényesítésében. Ennek keretében indokolt a BM Országos Katasztrófavédelmi Főigazgatóság iparbiztonsági szakterületének digitális iparbiztonsági képességekkel történő megerősítése, amely biztosítja a kiberbiztonsági követelmények szakszerű ellenőrzését és felügyeletét. A hatáskör és illetékesség szempontjából a kiber-fizikai rendszerek biztonságának felügyelete indokoltan illeszkedik a BM OKF iparbiztonsági feladatai közé, tekintettel arra, hogy ezen rendszerek közvetlen hatással vannak a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzésére és következményeinek kezelésére. Ezen feladatkör más hatóságokhoz történő kijelölése kevésbé lenne hatékony, figyelembe véve azok meglévő leterheltségét és eltérő szakterületi fókuszát.

6. A digitális iparbiztonsági kompetenciák fejlesztése nemcsak hazai szinten járul hozzá az üzembiztonság növeléséhez, hanem nemzetközi szinten is erősítheti a hatóság szakmai elismertségét és az ipari kiberbiztonság fontosságát. Ez az innovatív, kiberbiztonsági aspektusokat is integráló iparbiztonsági megközelítés különösen releváns a jelenlegi geopolitikai és digitalizált környezetben, ahol a kibertérből érkező fenyegetések egyre többször irányulnak az ipari vezérlőrendszerek ellen, és egyre többször cél a digitális károkozáson felül a fizikai környezetben történő negatív hatás kiváltása, ezzel pedig az üzemfolytonosság kompromittálása is.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A kutatás célja annak vizsgálata volt, hogy a veszélyes anyagokkal foglalkozó üzemek biztonsága a 21. századi digitalizált környezetben milyen módon fejleszthető tovább integrált iparbiztonsági, kiberbiztonsági és lakosságvédelmi megközelítések alkalmazásával. A vizsgálatok kiterjedtek a veszélyes üzemek biztonsági irányítási rendszereinek elemzésére, a nemzetközi és hazai szabályozási környezet értékelésére, az OT-környezetek sajátosságainak vizsgálatára, valamint olyan digitális döntéstámogatási és lakosságvédelmi megoldások kutatására, amelyek hozzájárulhatnak a veszélyhelyzeti reziliencia növeléséhez.

A kutatás eredményei alapján megállapítható, hogy a veszélyes anyagokkal foglalkozó üzemek biztonsága már nem értelmezhető kizárólag hagyományos safety vagy információbiztonsági keretrendszerek mentén. Az ipari digitalizáció, az IT–OT konvergencia, valamint a kiber-fizikai fenyegetések növekvő szerepe indokolttá teszi olyan integrált megközelítések alkalmazását, amelyek egységes rendszerben kezelik az üzembiztonsági, kiberbiztonsági, üzemfolytonossági és lakosságvédelmi szempontokat. A kutatás során vizsgált GRC-alapú biztonságirányítási megközelítés, a safety-központú OT-kiberbiztonsági szemlélet, valamint a digitális lakosságvédelmi döntéstámogatási és kommunikációs megoldások együttesen hozzájárulhatnak a veszélyes üzemek rezilienciájának növeléséhez, a veszélyhelyzeti eseményekre történő hatékonyabb felkészüléshez, valamint a lakosság kockázattudatosságának és médiaműveltségének erősítéséhez.

I. Iparbiztonságot szolgáló irányítási rendszerek hatékonyságának fejlesztési lehetőségei

1. Vizsgálataim során részletesen elemeztem a veszélyes anyagokkal foglalkozó üzemekre vonatkozó hazai és nemzetközi szabályozási környezetet, különös tekintettel a Seveso III irányelv, a NIS2 irányelv, a CER irányelv, valamint a kapcsolódó hazai iparbiztonsági és kiberbiztonsági szabályozások összefüggéseire. Megállapítottam, hogy a hagyományos biztonsági irányítási rendszerek elsődlegesen safety- és compliance-orientált megközelítést alkalmaznak, miközben a modern ipari környezetben megjelenő kiberkockázatok integrált kezelése egyre hangsúlyosabbá válik.

2. Kutatásaim során elemeztem a Governance, Risk and Compliance (GRC) meta-keret alkalmazhatóságát veszélyes anyagokkal foglalkozó üzemekkel kapcsolatban. Megállapítottam, hogy a GRC alkalmas az irányítási, kockázatkezelési és megfelelőségi

folyamatok integrálására, valamint összekapcsolni az üzembiztonsági, információbiztonsági, OT-biztonsági és lakosságvédelmi szempontokat.

3. Megállapítottam, hogy a jelenlegi szabályozási környezetben az iparbiztonsági és kiberbiztonsági követelmények, részben elkülönülten jelennek meg, valamint bizonyos üzemek esetén nem teljeskörűen jelennek meg a kiberbiztonsági szempontok. Miközben a veszélyes üzemek esetében a kiber-fizikai rendszerek biztonsága közvetlen hatással lehet a súlyos ipari balesetek megelőzésére és következményeinek kezelésére. Ennek következtében indokolt olyan integrált megközelítések alkalmazása, amelyek egységes rendszerben kezelik az üzemek teljeskörű rezilienciájának kialakítását.

4. Megállapítottam, hogy a KPI–KRI–KCI alapú integrált indikátorrendszer alkalmazása lehetőséget biztosíthat a veszélyes üzemek biztonsági teljesítményének objektív, mérhető és fejlesztésorientált értékelésére, ezáltal támogatva a preventív és reziliencia-központú biztonságirányítási működést.

5. Kutatásaim során arra a következtetésre jutottam, hogy a szervezeti integritás, az etikus működés és a biztonsági kultúra a veszélyes anyagokkal foglalkozó üzemek esetében nem kizárólag támogatói elemek, hanem a hosszú távú üzembiztonság és társadalmi elfogadottság alapvető tényezői.

Az előzőekben leírtak alapján igazoltnak tekintem az 1. hipotézisben foglaltakat, valamint megalapoztam az 1. számú tudományos eredményt.

II. Ipari balesetek kezelése, különös tekintettel a beavatkozó állomány és az érintett lakosság védelmére

1. Vizsgálataim során megállapítottam, hogy a modern ipari veszélyhelyzetek kezelése során a gyors helyzetértékelés, az adatvezérelt döntéstámogatás és a hiteles, többcsatornás válságkommunikáció együttesen meghatározó szerepet tölt be a lakosságvédelmi intézkedések hatékonyságában.

2. Elemzéseim alapján megállapítottam, hogy a lakosságvédelmi intézkedések társadalmi elfogadottsága és eredményessége szoros összefüggésben áll a hivatalos kommunikáció hitelességével, gyorsaságával és egységességével, aminek következtében a digitális platformokon megjelenő dezinformáció hatása csökken.

3. Vizsgálataim során megállapítottam, hogy a jelenlegi hazai helyreállítási és vis maior támogatási mechanizmusok elsősorban az önkormányzati és fizikai infrastruktúrában keletkezett károk kezelésére fókuszálnak, miközben a nemzetközi példák igazolják, hogy a kiber incidensek által kiváltott balesetek vagy üzemzavarok akár olyan következményekkel járhatnak, amelyek túlmutatnak a gazdálkodó szervezet helyreállítási képességein és szükségessé válhat az állami szerepvállalás. Megállapítottam továbbá, hogy a kibertérből kiinduló, de fizikai következményekkel járó káresemények új szempontokat vethetnek fel a jövőbeni helyreállítási és támogatási mechanizmusok kialakítása során, különösen a makrogazdasági és társadalmi válsághelyzetek megelőzése érdekében.

4. Kutatásaim során egy veszélyes anyagok terjedésének modellezésére alkalmas, ingyenesen elérhető szoftver funkcionalitását ESP32-alapú meteorológiai adatgyűjtő rendszerelemmel egészítettem ki a modellezéshez szükséges meteorológiai adatellátás támogatása érdekében. A rendszer lakosságvédelmi funkcionalitásának bővítése érdekében veszélyeztetett lakosságbecslő szoftvert fejlesztettem, amely lehetővé teszi a modellezett veszélyzónák által érintett lakosság gyors becslését. Megállapítottam, hogy a minimális költségű, nyílt és ingyenesen elérhető adatokra épülő digitális rendszerarchitektúrák különösen hatékonyan alkalmazhatók oktatási környezetben, digitálisan támogatott veszélyhelyzeti gyakorlatok és polgári védelmi felkészítések során.

Az előzőekben leírtak alapján igazoltnak látom a 2. hipotézisemben foglaltak teljesülését, valamint megalapoztam a 2. számú tudományos eredményt.

III. Veszélyes anyagokkal foglalkozó üzemek 21. századi kihívásai

1. A nemzetközi kiberbiztonsági jelentések és esettanulmányok elemzése során megállapítottam, hogy a gyártóipar és a kritikus infrastruktúrák globálisan a leginkább támadott ágazatok közé tartoznak, a gyártóipar közé sorolandó a veszélyes üzemek döntő hányada is. Megállapítottam továbbá, hogy az ezen ágazatokat érő kibertámadások következményei túlmutathatnak az információbiztonság keretein, és közvetlen hatással lehetnek az emberi életre, a környezetre, az üzembiztonságra és az üzemfolytonosságra is.

2. Vizsgálataim során elemeztem az IT–OT konvergencia hatásait és az OT-környezetek sajátosságait, melyet összevetettem a jelenlegi iparbiztonsági szabályozással. Megállapítottam, hogy az ipari rendszerek magas rendelkezésre állási követelményei, hosszú életciklusai és fizikai folyamatokhoz való közvetlen kapcsolódása indokolttá teszik egy olyan kiberbiztonsági megközelítés alkalmazását, amely elsődlegesen az üzembiztonsági és üzemfolytonossági szempontokat helyezi előtérbe és szakit a rendszerek kategórikus besorolásával.

3. Kutatásaim során elemeztem a hagyományos iparbiztonsági kockázatelemzéseket és a Cyber PHA megközelítés kapcsolatát. Megállapítottam, hogy a veszélyes anyagokkal foglalkozó üzemek teljes körű rezilienciája érdekében indokolt a kiberfenyegetések strukturált integrálása az iparbiztonsági kockázatértékelési folyamatokba.

4. Kidolgoztam egy safety-központú, veszélyes üzemek környezetére optimalizált kiberbiztonsági szűrési és priorizálási megközelítést „*Safety-Driven Industrial Cybersecurity Filtering Model*” néven. Megállapítottam, hogy a biztonsági kontrollok értékelése során szükséges üzembiztonsági hatás, az üzemfolytonossági relevancia és az OT-megvalósíthatóság együttes figyelembevétele.

5. Vizsgálataim során megállapítottam, hogy a veszélyes üzemeket érintő kiber-fizikai rendszerek biztonságának felügyelete indokoltan kapcsolható az iparbiztonsági hatósági feladatokhoz, tekintettel arra, hogy ezen rendszerek közvetlen hatással lehetnek a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzésére és következményeinek kezelésére.

Az előzőekben leírtak alapján igazoltnak látom a 3. hipotézisemben foglaltak teljesülését, valamint megalapoztam a 3. számú tudományos eredményt.

ÚJ TUDOMÁNYOS EREDMÉNYEK

1. A veszélyes anyagokkal foglalkozó üzemek biztonsági irányítási és kockázatkezelési rendszereinek tudományos vizsgálata alapján **megállapítottam**, hogy a hagyományos, üzembiztonsági és követelményrendszereknek történő megfelelőségi megközelítések önmagukban már nem képesek teljeskörűen kezelni a modern ipari környezetben megjelenő kockázatokat. Ennek megfelelően **kialakítottam** egy olyan integrált megközelítést, amely a Governance, Risk and Compliance (GRC) szemléletet alkalmazva egységes keretben kezeli az üzembiztonsági, kockázatkezelési, megfelelőségi, OT-kiberbiztonsági és lakosságvédelmi szempontokat. **Meghatároztam** továbbá azokat az integrációs és irányítási szempontokat, amelyek lehetővé teszik az üzembiztonsági, kiberbiztonsági, megfelelőségi és lakosságvédelmi követelmények egységes, reziliencia-központú kezelését a veszélyes üzemek súlyos ipari baleseteinek megelőzése érdekében.

2. A veszélyes anyagokkal foglalkozó üzemek veszélyhelyzeteinek elemzésére és értékelésére építve **megállapítottam**, hogy azok kezelése során a gyors helyzetértékelés, az adatvezérelt döntéstámogatás és a hiteles lakosságtájékoztatás együttesen meghatározó szerepet töltenek be a lakosságvédelem feladatrendszerében. Ennek figyelembevételével **kidolgoztam** egy digitális lakosságvédelmi döntéstámogatási rendszert, amely egységes architektúrában integrálja a meteorológiai adatgyűjtést, a veszélyesanyag-terjedési modellezést, a térinformatikai megjelenítést és a veszélyeztetett lakosság becslését, ezáltal biztosítva a hatékony lakosságvédelmi intézkedések végrehajtását.

3. A nemzetközi és hazai kiberbiztonsági jelentések és OT-specifikus esettanulmányok elemzése alapján **megállapítottam**, hogy a gyártóipar és a kritikus infrastruktúrák a kibertámadásokkal leginkább érintett ágazatok közé tartoznak, amelyek halmazába a veszélyes anyagokkal foglalkozó üzemek jelentős része is beletartozik. Továbbá a folyamatbiztonsági és kiberbiztonsági megközelítések elemzése alapján **megállapítottam**, hogy az IT-orientált kiberbiztonsági szemlélet korlátozottan alkalmazható a veszélyes anyagokkal foglalkozó üzemek ipari környezetében. **Ennek megfelelően kidolgoztam** egy üzembiztonsági központú, veszélyes üzemekre optimalizált kiberbiztonsági módszertani keretrendszert, valamint **igazoltam,** hogy a

Cyber PHA szemlélet integrálása alkalmas lehet a kiber-fizikai veszélyek strukturált azonosítására és az iparbiztonsági kockázatértékelési folyamatok kibővítésére.

AZ ÉRTEKEZÉS AJÁNLÁSAI

Az értekezésem következtetéseinek és tudományos eredményeinek felhasználására az üzemeltetőknek, jogalkotóknak és az iparbiztonsági szereplőknek az alábbi ajánlásokat teszem:

1. Indokolt a veszélyes anyagokkal foglalkozó üzemek biztonsági irányítási rendszereinek olyan irányú továbbfejlesztése, amely integrált módon kezeli az iparbiztonsági, kiberbiztonsági, OT-biztonsági, compliance és lakosságvédelmi szempontokat. Ennek keretében javasolt a GRC-alapú szemlélet alkalmazása, amely támogatja az irányítási, kockázatkezelési és megfelelőségi folyamatok összehangolását.

2. Javasolt a veszélyes anyagokkal foglalkozó üzemek kiberrezilienciájának növelése érdekében olyan integrált kiberbiztonsági követelményrendszer kialakítása, amely a védelmi intézkedések meghatározását elsődlegesen az üzembiztonsági, üzemfolytonossági és fizikai következménykockázati szempontok figyelembevételével végzi. Ez a megközelítés lehetőséget biztosíthat arra, hogy a biztonsági kontrollok priorizálása közvetlenül a technológiai folyamatok kritikalitásához és a potenciális safety-hatásokhoz igazodjon.

3. Indokolt a BM Országos Katasztrófavédelmi Főigazgatóság iparbiztonsági szakterületének digitális iparbiztonsági kompetenciákkal történő megerősítése, továbbá olyan módszertani és szabályozási környezet kialakítása, amely egyértelműen meghatározza a veszélyes üzemeket érintő kiberbiztonsági incidensek iparbiztonsági aspektusú vizsgálatának szakmai kereteit.

4. Javasolt a helyreállítási és vis maior támogatási mechanizmusok felülvizsgálata annak érdekében, hogy azok a jövőben kezelni tudják a kiber-fizikai rendszereket érintő, fizikai következményekkel járó káreseményeket és azok társadalmi-gazdasági hatásait is.

5. Indokolt a digitális lakosságtájékoztatási rendszerek továbbfejlesztése, különös tekintettel a hivatalos, többcsatornás válságkommunikációs megoldások kialakítására, valamint az egységes üzenetközvetítést támogató kommunikációs protokollok alkalmazására. Emellett javasolt a lakosság kockázattudatosságának és médiaműveltségének fejlesztését célzó edukációs programok erősítése, amelyek hozzájárulhatnak az álhírek és dezinformációs kampányok hatásainak csökkentéséhez és a lakossági együttműködés növeléséhez veszélyhelyzet esetén.

6. Javasolt a digitális döntéstámogatási rendszerek oktatási környezetben történő szélesebb körű alkalmazása, különösen a veszélyhelyzeti gyakorlatok, a table-top exercise szimulációk kiegészítése, valamint a polgári védelmi felkészítések korszerűsítése érdekében.

A KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGA

A kutatómunka eredményeit az alábbiak szerint javaslom felhasználni:

1. A kutatás eredményei támogatást nyújthatnak a veszélyes anyagokkal foglalkozó üzemek biztonsági irányítási rendszereinek továbbfejlesztéséhez, különösen az iparbiztonsági, kiberbiztonsági és fizikai reziliencia szempontok integrált kezelésében.

2. A kidolgozott, üzembiztonság-központú megközelítés alkalmazható lehet olyan ipari kiberbiztonsági követelményrendszer kialakításához, amely a kiberbiztonsági kontrollokat az iparbiztonsági szabályozási környezet üzembiztonsági és üzemfolytonossági célrendszeréhez igazított módon kezeli, ezáltal támogatva az iparbiztonsági hatósági felügyelet hatékonyabb érvényesítését.

3. A kutatás eredményei hozzájárulhatnak a veszélyes üzemeket érintő kiberbiztonsági ellenőrzési, felügyeleti és incidensvizsgálati módszertanok fejlesztéséhez, különösen az iparbiztonsági hatósági feladatok digitális kompetenciáinak erősítése területén.

4. A kutatásban ismertetett digitális lakosságtájékoztatási és többcsatornás válságkommunikációs megközelítések és technológiai eszközök növelhetik a hatósági kommunikáció hatékonyságát, valamint hozzájárulhatnak az álhírek és dezinformációs kampányok hatásainak mérsékléséhez.

5. A kutatás során bemutatott digitális döntéstámogatási architektúra eredményesen alkalmazható oktatási és gyakorlati környezetben, különösen digitálisan támogatott veszélyhelyzeti gyakorlatok, szimulációs környezetek és polgári védelmi felkészítések fejlesztése során. A rendszer emellett támogatást nyújthat veszélyesanyag-terjedési modellezési, lakosságvédelmi és korai helyzetértékelési feladatok végrehajtásához is.

HIVATKOZOTT IRODALOM JEGYZÉKE

[1] A. Toffler, *Future Schock*, New York, USA: Random House, 1970.

[2] K. Stouffer , M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule és M. Thompson, „Guide to Operational Technology (OT) Security," NIST SP 800-82 Rev. 3, 09 2023.. [Online]. Elérhető: https://csrc.nist.gov/pubs/sp/800/82/r3/final.

[3] International Society of Automation (ISA), „ISA-62443-1-1 Seurity for indusrtial automation and control systems, Part 1-1: Terminology, concepts, and models," ISA, 2007.

[4] European Commission, „European Commission - Minerva Portal," [Online]. Elérhető: https://emars.jrc.ec.europa.eu/en/emars/statistics/statistics.

[5] Cybersecurity & Infrastructure Security Agency (CISA), „Cybersecurity Alerts & Advisories". [Online] Elérhető: https://www.cisa.gov/news-events/cybersecurity-advisories

[6] MItre ATT&CK, „ATT&CK Matrix for Enterprise," [Online]. Elérhető: https://attack.mitre.org/.

[7] OCEG, *GRC Capability Model,* OCEG, 2024.

[8] Secure Controls Framework, „What Is The Secure Controls Framework®?," [Online]. Elérhető: https://securecontrolsframework.com/start-here.

[9] United Nations Office for Disaster Risk Reduction, „*Sendai Framework for Disaster Risk Reduction 2015 - 2030*," United Nations, Geneva, Switzerland, 2015.

[10] World Health Organization (WHO), „*WHO competency framework, risk communication and community engagement*," World Health Organization, Geneva, Switzerland, 2024.

[11] J. Dobor és R. Szendi, „Vegyi felderítés és mentesítés a veszélyes üzemek belső védelmi terveiben: a belső védelmi tervekkel kapcsolatban felmerülő problémák," *Hadtudományi Szemle,* 7. évfolyam, 1. szám, pp. 1-12, 2014. [Online] Elérhető: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/10617/2014_1_hm_dobor_szendi.pdf?sequence=2&isAllowed=y

[12] Z. Mesics és L. Kátai-Urbán, „Veszélyes üzemi biztonsági irányítási rendszer működtetése," *Hadmérnök,* X. évfolyam, 1. szám, pp. 99-107, 2015. [Online] Elérhető: http://hadmernok.hu/151_09_mesicsz_kul_1.pdf

[13] Gy. Vass, „*A településrendezési tervezés helye és szerepe a veszélyes anyagokkal kapcsolatos súlyos ipari balesetek megelőzésében,*” Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Kar, Katonai Műszaki Doktori Iskola, Budapest, 2006.

[14] Zs. Cimer, L. Kátai-Urbán és Gy. Vass, „A veszélyes üzemeket érintő településrendezési szabályozás értékelése az Európai Unióban,” *Bolyai Szemle,* XXIV. évfolyam, 4. szám, pp. 100-111, 2015.

[15] J. Kovács és L. Halász, „Az emberi tényező szerepe a katasztrófavédelmi helyzetértékelés folyamatban, különös tekintettel a helyzetértékelő csoport felépítésére,” *Hadmérnök,* III. évfolyam, 4. szám, pp. 4-14, 2008. [Online] Elérhető: http://hadmernok.hu/archivum/2008/4/2008_4_kovacsj.pdf

[16] J. Ambrusz és Z. Beke, „V. fejezet a lakossági tájékoztatás feladatai,” in *A katasztrófavédelem lakosságfelkészítési feladatai*, Budapest, Pytheas Könyvmanufaktúra, 2023, pp. 637-638. ISBN 978-615-5741-71-5

[17] J. Ambrusz, *Katasztrófák következményeinek felszámolása, valamint a helyreállítás, újjáépítés vezetési-irányítási, műszaki feladatainak lehetséges megoldásai*, Budapest: Doktoranduszok Országos Szövetsége, 2019. DOI: 10.23715/SDA.2022.1

[18] I. Kátai-Urbán, „Veszélyes anyagokkal foglalkozó telephelyek riasztási és terület kiürítési hatékonyságának vizsgálata,” *Műszaki Katonai Közlöny,* XXVIII. évfolyam, 1. szám, pp. 76-102, 2018. [Online] Elérhető: https://folyoirat.ludovika.hu/index.php/mkk/article/view/1726/1033

[19] N. G. Leveson, *Engineering a Safer World Systems Thinking Applied to Safety*, Cambridge, Massachusetts: Massachusetts Institute of Technology Press, 2011.

[20] Z. Wang, J. Wang, Z. Wei, W. Ye és L. Zhang, „Safety integrity level assessment for safety instrumented system in oil and gas station with cyber threat,” *Reliability Engineering & System Safety,*265. szám Part B, 01 2026. https://doi.org/10.1016/j.ress.2025.111614

[21] Az Európai Parlament és a Tanács (EU), „2022/2557 Irányelv: a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről,” 14. 12. 2022. [Online]. Elérhető: https://eur-lex.europa.eu/legalcontent/HU/TXT/PDF/?uri=CELEX:32022L2557.

[22] Szabályzott Tevékenységek Felügyeleti Hatósága, „Az SZTFH kiberbiztonsági felügyeleti tevékenységének bemutatása,” 2025.

[23] L. Pók, „Megjelent a magas szintű uniós kiberbiztonságot biztosító intézkedésekről szóló irányelv (NIS 2),” 2023. [Online]. Elérhető: https://gdpr.blog.hu/2023/01/02/megjelent_a_nis_2_iranyelv

[24] D. Márky, „Kötelező IT biztonság az EU-ban, NIS2 irányelv összefoglaló,” 2023. [Online]. Elérhető: https://www.dunaelektronika.com/nis2-megfeleles

[25] Az Európai Parlament és a Tanács (EU), „2022/2555 Irányelv: az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/ 1148 irányelv hatályon kívül helyezéséről (NIS 2),” 14. 12. 2022. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32022L2555&qid=1700772235586

[26] L. Kátai-Urbán és H. Horváth, „Assessment of the Implementation Practice of Emergency Planning Regulations Dedicated to the Rail Transportation of Dangerous Goods,” *Academic and Applied Research in Military Science ,* Vol. 12, 1. szám., pp. 73-82, 2013. https://doi.org/10.32565/aarms.2013.1.9

[27] CISCO Talos, „2025 year in review,” CISCO, Online, 2025.

[28] ISO/IEC, 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Geneva, CH: ISO copyright office, 2022.

[29] National Institute of Standards and Technology, „NIST Special Publication 800-53 Revision 5 Security and privacy controls for information systems and organizations,” U.S. Department of Commerce, 2020.

[30] ISO, 45001:2018(en) occupational health and safety management systems — Requirements with guidance for use, 2018.

[31] CMMI Institute, „CMMI Model V2.0,” CMMI Institute, https://cmmiinstitute.com, 2018.

[32] B. Day és L. Holznierkemper, „What Is A KPI? Definitions And Examples,” Forbes, 11. 09. 2025. [Online]. Elérhető: https://www.forbes.com/advisor/business/what-is-a-kpi-definition-examples/

[33] P. Guevara, „Understanding the Importance of Key Risk Indicators to Organizations,” Safety Culture, 25. 09. 2025. [Online]. Elérhető: https://safetyculture.com/topics/risk-management/key-risk-indicators

[34] H. Parkkinen, „KPI, KRI, & KCI – MODELED & EXPLAINED,” 09. 12. 2023. [Online]. Elérhető: https://henrikparkkinen.com/2023/12/19/kpi-kri-kci-modeled-explained/.

[35] ISO/IEC, „ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation,” International Organization for Standardization / International Electrotechnical Commission, Geneva, 2016.

[36] ISO, 37001:2025 Anti-bribery management systems - Requirements with guidance for use, 2025.

[37] J. Dobor, B. Barina és G. Pátzay, „A CBRN eseményekből adódó kihívások napjainkban,” *Polgári Védelmi Szemle,* XVI. évfolyam, Különszám, pp. 217-234, 2024. [Online] Elérhető: https://mpvsz.hu/pv_szemlek/pvszemle2024/index.html

[38] United States Environmental Protection Agency, „Airborne Spectral Photometric Environmental Collection Technology (ASPECT),” EPA, 30. 09. 2025. [Online]. Elérhető: https://www.epa.gov/emergency-response/aspect

[39] Lawrence Livermore National Laboratory, „LAWRENCE LIVERMORE NATIONAL LABORATORY,” [Online]. Elérhető: https://narac.llnl.gov/tools/operational-modeling

[40] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, „Infoseite Zukunft der CBRN-Erkundung,” BBK, 13. 08. 2025. [Online]. Elérhető: https://www.bbk.bund.de/DE/Themen/CBRN-Schutz/CBRN-Faehigkeiten/CBRN-Erkundung/cbrn-erkundung_node.html#vt-sprg-2

[41] BM Országos Katasztrófavédelmi Főigazgatóság, „Nukleárisbaleset-elhárítási döntéstámogató rendszer,” Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság, [Online]. Elérhető: https://www.katasztrofavedelem.hu/95/nuklearisbaleset-elharitasi-dontestamogato-rendszer

[42] PDC-ARGOS, „ARGOS User Group Members,” PDC-ARGOS CBRN Crisis Management, [Online]. Elérhető: https://www.pdc-argos.com/members.html

[43] Eurpean Defence Agency, „Permanent Structured Cooperation (PESCO),” [Online]. Elérhető: https://www.pesco.europa.eu/project/integrated-european-joint-training-and-simulation-centre-eurosim/

[44] European Defense Agency, „Pesco Projects,” [Online]. Elérhető: https://www.pesco.europa.eu/project/chemical-biological-radiological-and-nuclear-cbrn-surveillance-as-a-service-cbrn-saas/

[45] T. van den Berg, „Overview of M&S as a Service,” NATO Science and Technology Organization, 3. 12. 2024. [Online]. Elérhető: https://publications.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-MSG-211/EN-MSG-211-1.6.pdf

[46] ESA, „The European Space Ageny,” [Online]. Elérhető: https://business.esa.int/projects/european-space-based-information-management-system-for-cbrn-eurosim-cbrn

[47] Riskaware, „Riskaware,” [Online]. Elérhető: https://www.riskaware.co.uk/what-we-do/urbanaware/

[48] ESA, „The European Space Agency,” [Online]. Elérhető: https://business.esa.int/projects/european-space-based-information-management-system-for-cbrn-eurosim-cbrn

[49] 234/2011. (XI. 10.) Korm. rendelet *a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról.*

[50] 44/2021. (XII. 16.) BM rendelet *a települések katasztrófavédelmi besorolásáról.*

[51] 62/2011. (XII. 29.) BM rendelet *a katasztrófák elleni védekezés egyes szabályairól.*

[52] ETSI, „Technical Specification Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service," ETSI TS 102 900 V1.4.1 , 06 2023. [Online]. Elérhető: https://www.etsi.org/deliver/etsi_ts/102900_102999/102900/01.04.01_60/ts_102900v010401p.pdf#:~:text=European%20Public%20Warning%20System%20(EU-ALERT)%20using%20the%20Cell%20Broadcast%20Service&text=The%20generic%20name%20for%20the%20European%20Public%20Wa

[53] BEREC, „Public Warning Systems Database," BEREC, [Online]. Elérhető: https://www.berec.europa.eu/en/pws?field_vas_country_target_id=All&field_type_of_pws_value=Cell%20Broadcast&field_link_to_pws_description_value=&page=0

[54] T. Koi, „Jövő nyáron indulhat itthon a cella alapú védelmi riasztás," 16. 06. 2025. [Online]. Elérhető: https://www.hwsw.hu/hirek/69242/vedelmi-riasztas-cell-broadcast-sms-uzenet-cella-mobilcella-mobilszolgaltato-hivatal-hatosag-nmhh.html

[55] BM OKF, „MoLaRi-rendszer," [Online]. Elérhető: https://www.katasztrofavedelem.hu/49/molari-rendszer

[56] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, „Warn-App NINA," [Online]. Elérhető: https://www.bbk.bund.de/DE/Warnung-Vorsorge/Warn-App-NINA/warn-app-nina_node.html

[57] ETT S.p.A., *Pronti all' Azione,* Dipartimento della Protezione Civile - Presidenza della Regione Siciliana, 2023. https://apps.apple.com/lb/app/pronti-allazione/id6467635573

[58] BM OKF, „VÉSZ," [Online]. Elérhető: https://www.katasztrofavedelem.hu/37/vesz

[59] European Commission, „The Strengthened Code of Practice on Disinformation 2022," 2022. [Online]. Elérhető: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

[60] Európai Bizottság, „Médiaműveltség," 15. 10. 2024. [Online]. Elérhető: https://digital-strategy.ec.europa.eu/hu/policies/media-literacy

[61] Európai Unió Külügyi Szolgálat Stratégiai kommunikáció Szerkesztősége, „Countering Disinformation - Questions and Answers about the East StratCom Task Force," 27. 10. 2021. [Online]. Elérhető: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11234

[62] European External Action Service, „EUvsDisinfo," East StratCom Task Force, [Online]. Elérhető: https://euvsdisinfo.eu/about/

[63] A. M. Elkhatat, K. Elsaid és S. Almeer, „Evaluating the efficacy of AI content detection tools in differentiating between human and AI-generated text," *International Journal for Educational Integrity,* vol 19, issue17, pp. 1-16., 2023. https://doi.org/10.1007/s40979-023-00140-5

[64] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, „European Democracy Shield: Empowering Strong and Resilient Democracies," 12. 11. 2025. [Online]. Elérhető: https://commission.europa.eu/publications/european-democracy-shield-documents_en.

[65] A. Gutowska, „What are AI agents?," [Online]. Elérhető: https://www.ibm.com/think/topics/ai-agents

[66] n8n, „Security at n8n,", [Online]. Elérhető: https://n8n.io/legal/security/#compliance

[67] Ö. Vásárhelyi és Z. Mesics, „Nemzetközi esettanulmány rendszerszintű tanulságai és fejlesztési irányok az ipari katasztrófák lakosságvédelmi kezelésében," *Polgári Védelmi Szemle,* 18. évfolyam, Különszám, pp. 422-436, 2026. [Online] Elérhető: https://mpvsz.hu/pv_szemlek/pvszemle2026/index.html

[68] Inspection Générale des Affaires Sociales, „Retour d'expérience après l'incendie d'un site industriel à Rouen en septembre 2019 – Analyses et propositions sur la gestion de crise," 08. 07. 2020. [Online]. Elérhető: https://igas.gouv.fr/Retour-d-experience-apres-l-incendie-d-un-site-industriel-a-Rouen-en-septembre.

[69] Préfet de la Seine-Maritime, „Chronologie des publications," 26. 09. 2024. [Online]. Elérhető: https://www.seine-maritime.gouv.fr/Actions-de-l-Etat/Securite-et-Defense/Securite-civile/Risques-naturels-et-technologiques/Risque-industriel/Post-accidentel/Incendie-Lubrizol-et-NL-Logistique-du-26-septembre-2019/Chronologie-des-publications/Chronologie-

[70] L. Moufarrej, G. Limousin, C. Castilla, T. Legeard, J. Vievard, M. Mignot, I. Schmitz, S. Tisse, P. Cardinael, M. Fournier és F. Portet-Koltalo, „Identification of industrial fire-related chemical markers in French rivers and underground water using chromatography hyphenated to high-resolution mass spectrometry systems for nontarget screening," *Environmental Science and Pollution Research,* vol 32, p. 20971–20990, 2025. https://doi.org/10.1007/s11356-025-36882-7

[71] C. Paylor, „FR-Alert: What is France's Emergency Alert System," 11. 10. 2024. [Online]. Elérhető: https://www.frenchentree.com/living-in-france/healthcare/fr-alert-what-is-frances-emergency-alert-system/.

[72] Á. Muhoray, „A polgári védelem helye a modern katasztrófavédelemben," *Hadmérnők,* XII. évfolyam, 2. szám, pp. 188-200, 06. 2017. [Online] Elérhető: http://hadmernok.hu/172_15_muhoray.pdf

[73] A. Kasza, „Az óvóhelyekre és a metróra, mint védelmi létesítményekre vonatkozó hazai szabályozás áttekintése," *Műszaki Katonai Közlöny,* XXV. évfolyam, 1. szám, pp. 67-73, 2015.

[Online] Elérhető: https://mkk.uni-nke.hu/document/mkk-uni-nke-hu/2015_1_04_Az%20ovohelyyekre%20es%20a%20metrora.pdf

[74] D. Baumstark és Z. Szelid, „*Rendvédelmi szervek és alapfeladatok,*” 2023. ISBN 978-963-9208-89-6

[75] NBSZ Nemzeti Kibervédelmi Intézet, „Incidenskezelés,” Nemzeti Kibervédelmi Intézet, [Online]. Elérhető: https://nki.gov.hu/szolgaltatasok/tartalom/incidenskezeles/

[76] Európai Bizottság, „A BIZOTTSÁG (EU) 2024/1366 FELHATALMAZÁSON ALAPULÓ RENDELETE az (EU) 2019/943 európai parlamenti és tanácsi rendeletnek a határkeresztező villamosenergia- áramlás kiberbiztonsági szempontjaira vonatkozó ágazatspecifikus szabályokról szóló üzemi és kereske,” Az Európai Unió Hivatalos Lapja, 11. 03. 2024. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=OJ:L_202401366.

[77] Ö. Vásárhelyi, „A vízkezeléssel foglalkozó üzemek elleni kibertámadások és azok lehetséges következményeinek lakosságvédelmi feladatai,” *Polgári Védelmi Szemle,* XVII. évfolyam, Különszám, pp. 472-487, 2025. [Online] Elérhető: https://mpvsz.hu/pv_szemlek/pvszemle2025/index.html

[78] Cs. Krasznay, „A polgárok védelme egy kiberkonfliktusban,” *Hadmérnők,* VII. évfolyam, 4. szám, pp. 142-151, 12. 2012. [Online] Elérhető: http://hadmernok.hu/2012_4_krasznay.pdf

[79] Microsoft, „Microsoft Digital Defense Report 2024,” 10. 2024. [Online]. Elérhető: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf.

[80] Cs. Fenyvesi, „Nyitott Egyetem - Fenyvesi Csaba: A kriminalisztika elmélete és gyakorlata,” 09. 02. 2021. [Online előadás]. Elérhető: https://www.youtube.com/watch?v=yBC4Ght7nNk.

[81] K. Kent, S. Chevalier, T. Grance és H. Dang, „Guide to Integrating Forensic Techniques into Incident Respons,” National Institute of Standards and Technology (NIST), 08. 2006. [Online]. Elérhető: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

[82] 4Geeks, „Live vs Dead Acquisition in Digital Forensics,” 4Geeks, [Online]. Elérhető: https://4geeks.com/lesson/live-vs-dead-acquisition-in-digital-forensics.

[83] G. Topham és J. Jolly, „Jaguar Land Rover slides to loss of almost £500m after cyber-attack,” The Guardian, 14. 11. 2025. [Online]. Elérhető: https://www.theguardian.com/business/2025/nov/14/jaguar-land-rover-loss-cyber-attack.

[84] Office of Response and Restoration - NOAA, „Office of Response and Restoration National Oceanic and Atmospheric Administration,” [Online]. Elérhető: https://response.restoration.noaa.gov/alohadevhistory.

[85] U.S Environmental Protection Agency; National Oceanic and Atmospheric Administartion, „ALOHA User's Manual,” February 2007. [Online]. Elérhető: https://nepis.epa.gov/Exe/ZyPDF.cgi/P1003UZB.PDF?Dockey=P1003UZB.PDF.

[86] Emergency Response Division Office of Response and Restoration National Oceanic and Atmospheric Administration, „Designing a portable weather station for use with ALOHA,” Seattle, 2011.

[87] R. J. Yamartino, „A Comparison of Several “Single-Pass” Estimators of the Standard Deviation of Wind Direction,” *Journal of Climate and Applied Meteorology,* 23. évfolyam, pp. 1362–1366, 1984.

[88] Gy. Vass, J. Ambrusz, Á. Restás, F. Varga és L. Kátai-Urbán, „A katasztrófavédelmi kutatások eredményei és fejlesztése a rendészettudomány rendszerében,” *Academic Journal of Internal Affairs,* vol 72, 5. szám, pp. 815-833, 2024. [Online] Elérthető: 10.38146/BSZ-AJIA.2024.v72.i5.pp815-833

[89] A. S. Tigadi és K. Rodrigues, „Study on Building a Raspberry Pi AI system: Tools and Techniques,” *International Journal of Research and Analytical Reviews (IJRAR),* vol. 10, Issue 2, pp. 476-482, 2023. [Online] Elérhető: https://www.researchgate.net/publication/370519865_Study_on_Building_a_Raspberry_Pi_AI_system_Tools_and_Techniques

[90] A. Bekkar, B. Hssina, S. Douzi és K. Douzi, „Air-pollution prediction in smart city, deep learning approach,” *Journal of Big Data,* vol 8, 161. szám, 2021. [Online] Elérhető: https://doi.org/10.1186/s40537-021-00548-1

[91] R. Meenal, P. Angel, D. Pamela és E. Rajasekaran, „Weather prediction using random forest machine learning model,” *Indonesian Journal of Electrical Engineering and Computer Science,* 22. évfolyam, 2. szám, pp. 1208-1215, 2021. [Online] Elérhető: 10.11591/ijeecs.v22.i2.pp1208-1215

[92] F. R. Stevens, A. E. Caughan, C. Linard és A. J. Tatem, „Disaggregating Census Data for Population Mapping Using Random Forests with Remotely-Sensed and Ancillary Data,” *PLOS One,* vol 10, 2. szám., 2015. [Online] Elérhető: https://doi.org/10.1371/journal.pone.0107042

[93] P. Doupe, E. Bruzelius, J. Faghmous és S. G. Ruchman, „Equitable development through deep learning: The case of sub-national population density estimation,” Naioroby, Kenya, 2016. ISBN: 978-1-4503-4649-8, https://doi.org/10.1145/3001913.3001921

[94] BM OKF, „Megújult a katasztrófavédelem döntéstámogató rendszere,” 12. 05. 2022. [Online]. Elérhető: https://katasztrofavedelem.hu/611/szechenyi-2020/21/264307/megujult-a-katasztrofavedelem-dontestamogato-rendszere.

[95] Ö. Vásárhelyi, „The Role of Integrated Data Sources for Advanced Modelling of the Spread of Hazardous Substances,” *Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata,* 153. évfolyam, Special Issue 2, pp. 66-81, 2025. [Online] Elérhető: 10.35926/HDR.2025.2.5

[96] M. Christou, Z. Gyenes és M. Struckl, „Risk assessment in support to land-use planning in Europe: Towards more consistent decisions?,” *Journal of Loss Prevention in the Process Industries,* 24 vol. 3. szám, pp. 219-226, 2011. [Online] Elérhető: https://doi.org/10.1016/j.jlp.2010.10.001

[97] United Nation General Assembly, „Transforming our world: the 2030 Agenda for,” Resolution adopted by the General Assembly on 25 September 2015 , 21. 10. 2015. [Online]. Elérhető: https://docs.un.org/en/A/RES/70/1.

[98] Az Európai Parlament és a Tanács, „a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK,” 2012/18/EU Irányelve, 24. 07. 2012. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32012L0018. [Hozzáférés dátuma: 01 04 2024.].

[99] L. Muha és Cs. Krasznay, „Az elektronikus információs rendszerek biztonságáról vezetőknek,” Nemzeti Közszolgálati Egyetem, Budapest, 2014. ISBN 978-615-5491-65-8

[100] NIST Computer Security Division, „NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001,” 2020. [Online]. Elérhető: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fcsrc.nist.gov%2FCSRC%2Fmedia%2FPublications%2Fsp%2F800-53%2Frev-5%2Ffinal%2Fdocuments%2Fsp800-53r5-to-iso-27001-mapping.docx&wdOrigin=BROWSELINK. [Hozzáférés dátuma: 14. 10. 2022.].

[101] Z. Haig és L. Kovács, „Fenyegetések a cybertérből,” *Védelempolitika,* 1. évfolyam, 5. szám, pp. 61-69, 2008. [Online] Elérhető: https://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf

[102] National Institute of Standards and Technology U.S. Department of Commerce, „Risk Management Framework for Information Systems and Organisations,” NIST Special Publication 800-37 Rev. 2, 2018. [Online]. Elérhető: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[103] K. Gast, „What is ICS Security? How to Defend Against Attacks,” 30 12 2020. [Online]. Elérhető: https://securityboulevard.com/2020/12/what-is-ics-security-how-to-defend-against-attacks/.

[104] W. Bolton, Programmable Logic Controllers, Burlington, Massachusetts: Newnes, 2015.

[105] K. Tamás, Szerző, *ICS/OT kiberbiztonság Bevezetés az OT csodálatos világába.* [Előadás]. 2026.

[106] M. Abrams és J. Weiss, „Malicious Control System Cyber Security Attack Case Study,” The MITRE Corporation, 23. 07. 2008. [Online]. Elérhető: https://www.mitre.org/sites/default/files/pdf/08_1145.pdf.

[107] A. Khaitan, „Medusa Ransomware Group Claims Alto Calore Cyber Attack,” The CyberExpress, 02. 05. 2023. [Online]. Elérhető: https://thecyberexpress.com/alto-calore-cyber-attack-medusa-ransomware/.

[108] SOCRadar, „Dark Web Profile: Medusa Ransomware (MedusaLocker),” SOCRadar Your Eyes Beyond, 5. 09. 2023. [Online]. Elérhető: https://socradar.io/dark-web-profile-medusa-ransomware-medusalocker/.

[109] V. Pandagle, „International Civil Defense Organization, Novi Pazar-Put and Sartrouville Listed by Medusa,” The Cyber Express, 22. 08. 2023. [Online]. Elérhető: https://thecyberexpress.com/medusa-group-claims-icdo-cyber-attack/.

[110] B. Anthonny, „Analysis of WeRedEvils' Operations and Geopolitical Context,” Linkedin, 02. 08. 2024. [Online]. Elérhető: https://www.linkedin.com/pulse/analysis-weredevils-operations-geopolitical-context-anthony-burgess-k5yje/.

[111] E. Kovacs, „Israeli Group Claims Lebanon Water Hack as CISA Reiterates Warning on Simple ICS Attacks,” Security Week, 26. 09. 2024. [Online]. Elérhető: https://www.securityweek.com/israeli-group-claims-lebanon-water-hack-as-cisa-reiterates-warning-on-simple-ics-attacks/.

[112] Kaspersky, „Ransomware-as-a-service (RaaS),” [Online]. Elérhető: https://encyclopedia.kaspersky.com/glossary/ransomware-as-a-service-raas/.

[113] Dragos, „YEAR IN REVIEW OT/ICS Cybersecurity report,” Dragos Inc., 2026.

[141] IBM X-Force, „X-Force Threat Intelligence Index 2026,” IBM Corporation, 25. 02. 2026. [Online]. Elérhető: https://www.ibm.com/reports/threat-intelligence.

[115] J. D. Christopher, „2025 Survey - State of ICS/OT Security 2025,” SANS Research Program, online, 2025.

[116] ENISA, „About,” European Union Vulnerability Database, 2025. [Online]. Elérhető: https://euvd.enisa.europa.eu/about.

[117] IBM Security, „Cost of a Data Beach Report,” IBM Corporation, Armonk, NY, United States of America, 2023.

[118] Sophos, „The State of Ransomware,” Sophos Ltd., Abingdon, UK, 2024.

[119] N. NKI, Interviewee, *Indul a NIS2 tájékoztató kampány (2. rész).* [Interjú]. 24. 03. 2024.

[120] D. Orosházi, „A NIS2 közvetlen hatásai a kritikus infrastruktúrára és az állami szektorra,” IT Business Konferencia, 19. 03. 2023. [Online]. Elérhető: https://itbusiness.hu/wp-content/uploads/2024/03/6.-Oroshazi-David_prezi.pdf.

[121] J. Morella és J. A. Cusimano: *Cyber PHA A proven method to assess industrial control system.* [Előadás]. AE Solutions, 2019.

[122] NBSZ NKI, „Obfuszkáció - A láthatatlan háború,” Nemzeti Kiberbiztonsági Intézet, 05 05 2025.. [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/hirek/obfuszkacio-a-lathatatlan-haboru/.

[123] ILO & WHO, „Foszfor-pentaszulfid,” Európai Bizottság, 2018. [Online]. Elérhető: https://chemicalsafety.ilo.org/dyn/icsc/showcard.display?p_card_id=1407&p_version=2&p_lang=hu.

[124] Ministére des Armées et des Anciens Combattants, „Véhicule de Détection Identification et Prélèvements,” [Online]. Elérhető: https://www.terre.defense.gouv.fr/pompiers-paris/engins-bspp/moyens-nrbc/vehicule-detection-identification-prelevements.

A TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓIM

Vásárhelyi Örs, Dobor József, Ambrusz József (2023): Veszélyes üzemek XXI. századi fenyegetettségekkel szembeni védelmi képességeinek fejlesztési lehetőségei, *Polgári Védelmi Szemle,* 15. évfolyam, DAREnet projekt különszám, pp.325-339., 15p.

Ö. Vásárhelyi, J. Dobor, J. Ambrusz (2023): IoT as a tool in achieving Disaster Management purposes, In: László Bodnár, György Heizler (szerk.): *3rd Fire Engineering & Disaster Management Prerecorded International Scientific Conference : Book of extended abstracts,* Budapest, Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet, pp. 178-181, 4 p. ISBN: 978-615-01-8104-2

Ambrusz József, Dobor József, Vásárhelyi Örs (2024): Létfontosságú rendszerek,-rendszerelemek rezillienciájának fejlesztési lehetőségei az Európai Unió direktíváinak tükrében, Polgári Védelmi Szemle, 16. évfolyam, különszám, pp.57-69. , 13 p.

Vásárhelyi Örs (2024): A veszélyes üzemek információbiztonsági képességeinek fejlesztési lehetőségei napjaink kihívásainak tükrében, *Belügyi Szemle*, 72. évfolyam, 1. szám, pp.89-111., 23 p. https://doi.org/10.38146/BSZ.2024.1.6

Vásárhelyi Örs (2024): A vízkezelő üzemek 21. századi kihívásai, a

lakosságvédelem aspektusaiból *Védelem Tudomány*. különszám Természeti Katasztrófák Csökkentésének Világnapja Nemzeti Közszolgálati Egyetem nemzetközi tudományos konferencia Konferenciaközlemény pp. 166-172. 8 p.

Örs Vásárhelyi (2025):The Role of Integrated Data Sources for Advanced Modelling of the Spread of Hazardous Substances

Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata 153 évf.: Special Issue 2 pp. 66-81. , 16 p.

Vásárhelyi, Örs (2025): A vízkezeléssel foglalkozó üzemek elleni kibertámadások és azok lehetséges következményeinek lakosságvédelmi feladatai
Polgári Védelmi Szemle 17. évfolyam: Különszám pp. 472-487. , 16 p.

Vásárhelyi Örs, Mesics Zoltán (2026): Nemzetközi esettanulmány rendszerszintű tanulságai és fejlesztési irányok az ipari katasztrófák lakosságvédelmi kezelésében, Polgári Védelmi Szemle, 18. évfolyam, pp. 422-436. , 15 p

MELLÉKLETEK

1. Alkalmazott rövidítések és szakkifejezések jegyzéke

2. Témához kapcsolódó jogszabályok és belső szabályozó eszközök jegyzéke

3. Ábrák és táblázatok jegyzéke

4. „Safety driven” kontrollkatalógus

5. Kohéziós táblázat

1. sz. melléklet

Alkalmazott rövidítések és szakkifejezések jegyzéke

EIR	elektronikus információs rendszer
OT	kiber-fizikai rendszerek hálózata
BIR	biztonsági irányítási rendszer
ISO	Nemzetközi Szabványügyi Szervezet
NIST	Nemzeti Szabványügyi és Technológiai Intézet (USA)
AEGL	Acute Exposure Guideline Levels
API	Application Programming Interface
BCP	Üzletmenet-folytonossági terv
BIA	Üzleti hatáselemzés
BYOD	Bring Your Own Device
C2	Command and Control
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
Cyber PHA	Cyber Process Hazard Analysis
DMZ	Demilitarized Zone
ESP32	Mikrovezérlő-alapú IoT platform
GRC	Governance, Risk and Compliance
HAZOP	Hazard and Operability Study

HMI	Human–Machine Interface
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISA	International Society of Automation
KML	Keyhole Markup Language
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LAN	Local Area Network
NIS2	Network and Information Security Directive 2
NIST	National Institute of Standards and Technology
PHA	Process Hazard Analysis
PLC	Programmable Logic Controller
PV	Polgári Védelem
SCADA	Supervisory Control and Data Acquisition
SCF	Secure Controls Framework
Safety	Működésbiztonság, üzembiztonság
SIEM	Security Information and Event Management
SIS	Safety Instrumented System

SOC	Security Operations Center
SSO	Single Sign-On
STAMP	System-Theoretic Accident Model and Processes
VPN	Virtual Private Network
WAN	Wide Area Network
Zero Trust	Bizalommentes biztonsági modell
Zóna	Az IEC 62443 szerinti, azonos biztonsági követelményekkel rendelkező rendszerek logikai csoportja
Konduit	Az IEC 62443 szerinti, zónák közötti szabályozott kommunikációs kapcsolat
Reziduális kockázat	A kontrollintézkedések alkalmazását követően fennmaradó kockázat
Kompenzáló kontroll	Olyan alternatív védelmi intézkedés, amely egy hiányzó vagy nem alkalmazható kontroll hatását részben, vagy egészben kiváltja
Kritikus infrastruktúra	A társadalom és gazdaság működése szempontjából alapvető jelentőségű infrastruktúra
Veszélyes anyagokkal foglalkozó üzem	A vonatkozó jogszabályok alapján veszélyes anyag jelenléte miatt szabályozás alá tartozó üzem
Üzemfolytonosság	A szervezet képessége a kritikus működés fenntartására és helyreállítására
Lakosságvédelem	A lakosság életének és alapvető életfeltételeinek védelmét szolgáló intézkedések összessége
Védelmi létesítmény	A lakosság fizikai védelmét szolgáló építmény vagy infrastruktúra

2. sz. melléklet

Témához kapcsolódó jogszabályok és belső szabályozó eszközök jegyzéke

Nemzetközi és Európai Unió jogi szabályozás

1. Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról

2. Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (DORA rendelet)

3. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről

4. Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

5. Az Európai Parlament és a Tanács 2012/18/EU irányelve (2012. július 4.) a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/E

6. Az Európai Parlament és a Tanács (EU) 2016/425 rendelete (2016. március 9.) az egyéni védőeszközökről és a 89/686/EGK tanácsi irányelv hatályon kívül helyezéséről tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről

7. Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)

8. Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete az egységes digitális szolgáltatási piacról és a 2000/31/EK irányelv módosításáról (Digital Services Act – DSA)

9. Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint egyes uniós jogi aktusok módosításáról (Artificial Intelligence Act – AI Act)

10. A bizottság (EU) 2024/1366 felhatalmazáson alapuló rendelete (2024. március 11.) az (EU) 2019/943 európai parlamenti és tanácsi rendeletnek a határkeresztező

villamosenergia-áramlás kiberbiztonsági szempontjaira vonatkozó ágazatspecifikus szabályokról szóló üzemi és kereskedelmi szabályzat létrehozása révén történő kiegészítéséről

Hazai jogi szabályozás

11. Magyarország Alaptörvénye (2011. április 25.)

12. 22/1992 (XII.29.) KTM rendelet az életvédelmi létesítmények létesítéséről, fenntartásáról és békeidőszaki haszonosításáról

13. 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

14. 234/2011 (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

15. 9/2011 (II. 15.) Korm. rendelet a vis maior támogatás felhasználásának részletes szabályairól

16. 62/2011. (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól

17. 208/2011. (X. 12.) Korm. rendelet a katasztrófavédelmi bírság részletes szabályairól, a katasztrófavédelmi hozzájárulás befizetéséről és visszatérítéséről

18. 219/2011 (X.20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

19. 61/2012. (XII. 11.) BM rendelet a települések katasztrófavédelmi besorolásáról, valamint a katasztrófák elleni védekezés egyes szabályairól

20. 2013 L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (hatályon kívül)

21. 41/2015 (VII.15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (hatályon kívül)

22. 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

23. 2024. évi LXXXIV. törvény a kritikus szervezetek ellenállóképességéről

24. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

25. 1089/2025. (III. 31.) Korm. határozat Magyarország Kiberbiztonsági Stratégiájáról

26. 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

27. 44/2021. (XII. 16.) BM rendelet a települések katasztrófavédelmi besorolásáról

28. 7/2024. (VI.24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

29. 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

30. 474/2024. (XII.31.) Korm. rendelet a kritikus szervezetek ellenállóképességéről szóló törvény végrehajtásáról

31. 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról

Ábrák és táblázatok jegyzéke

Ábrák jegyzéke

1. ábra NIS 2 direktíva hatálya alá tartozó vállalatok méret szerint 38
2. ábra A keretrendszerek egymásra épült hierarchiája 47
3. ábra A kulcs kockázati indikátorok kialakításának lépései 54
4. ábra Az indikátorok egymásra hatása a GRC meta-keretben 56
5. ábra A NATO által biztosított MSaaS szolgáltatás működési architektúrája 66
6. ábra A rendszer magas szintű architektúra ábrája 67
7. ábra Cellbroadcast működési elve 69
8. ábra A baleset térképes kiterjedése - 2019.09.26. Rouen, Franciaország 78
9. ábra Az ESP32 mikrovezérlő adatáramlási diagramja 100
10. ábra Az ESP32 beágyazott webszerverének felhasználói felülete 102
11. ábra A digitális meteorológiai állomás kiválasztása az ALOHA szoftverben 102
12. ábra A lakosságbecslő applikáció adatáramlási diagramja 108
13. ábra Az applikáció működés közben, a demográfiai csoportok demonstrációs jelleggel kerültek kiválasztása 109
14. ábra A fejlesztett rendszer architektúra működési folyamata 111
15. ábra A klórgáz terjedési csóvája az aktuális meteorológiai adatok használatával 113
16. ábra A klórgáz terjedési csóvája 2 órás előrejelzett adatok felhasználása alapján 114
17. ábra Az első, aktuális meteorológiai adatok felhasználásával készült terjedési modell által érintett lakosság 115
18. ábra A 2 órás előrejelzés meteorológiai adatai által készült terjedési modell által érintett lakosság 115
19. ábra Az adat több dimenziós védelme 120
20. ábra Információbiztonság három alapelve (BSR) 121
21. ábra Az OT környezetben alkalmazott rendszerek egymásba ágyazott struktúrája 126
22. ábra MFA elleni támadások megoszlása technika és ágazatok szerint 141
24. ábra A nyugati szankciók és az orosz kiberműveletek közti összefüggések 144
25. ábra Ágazatokat ért ransomware támadások a Dragos által gyűjtött adatok alapján 148
26. ábra A SANS kiber-fizikai környezetet érintő incidensekre vonatkozó felmérésének eredménye 152
27. ábra A kiber-fizikai rendszereket érő incidenstípusok megoszlási aránya 153
28. ábra A hazai kiberbiztonsági felügyeletet ellátó hatóságok 157
29. ábra Kiber bow-tie modellre példa 162

Táblázatok jegyzéke

1. táblázat a klasszikus iparbiztonsági dimenzió értékelési módszertana 165
2. táblázat A kiber-fizikai környezetben történő kontroll megvalósíthatósági dimenzió 166
3. táblázat Az üzemfolytonosság dimenziójára történő hatása a kontrollnak 167
4. táblázat Az egyes követelmények besorolási kategóriái 167

4. számú melléklet

„Safety driven” kontrollkatalógus

#	Baseline kontroll név	Kontroll ID	Pont
1	Információbiztonsági szabályzat	**PM-1**	7
2	Intézkedési terv és mérföldkövei	**PM-4**	8
3	Elektronikus információs rendszerek nyilvántartása	**PM-5**	7
4	Hozzáférés-felügyelet szabályzat	**AC-1**	7
5	Fiókkezelés	**AC-2**	7
6	Hozzáférési szabályok érvényesítése	**AC-3**	7
7	Azonosítás és hitelesítés nélkül engedélyezett tevékenységek	**AC-14**	8
8	Távoli hozzáférés	**AC-17**	8
9	Vezeték nélküli hozzáférés	**AC-18**	8
10	biztonságtudatossági képzésre vonatkozó szabályzat és eljárásrend	**AT-1**	7
11	Biztonságtudatossági képzés	**AT-2**	8
12	Szerepkör alapú biztonsági képzés	**AT-3**	8
13	Naplózás és elszámoltathatóság szabályzat és eljárásrend	**AU-1**	7
14	Naplózható események	**AU-2**	7
15	Naplóbejegyzések tartalma	**AU3**	7
16	Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel	**AU-6**	7
17	Időbélyegek	**AU-8**	7
18	Értékelés, engedélyezés, monitorozás szabályzat és eljárásrend	**CA-1**	7
19	Biztonsági értékelések	**CA-2**	9
20	Információcsere	**CA-3**	7
21	Az intézkedési terv és mérföldkövei - rendszerszintű	**CA-5**	8
22	Engedélyezés	**CA-6**	7
23	Folyamatos felügyelet	**CA-7**	7
24	Konfigurációkezelési szabályzat	**CM-1**	7
25	Alapkonfiguráció	**CM-2**	7
26	A konfigurációváltozások felügyelete (változáskezelés)	**CM-3**	7
27	Biztonsági hatásvizsgálatok	**CM-4**	8
28	A szoftverhasználat korlátozásai	**CM-10**	8
29	Készenléti tervezés szabályzat és eljárásrend	**CP-1**	7
30	Üzletmenet-folytonossági terv	**CP-2**	7
31	EIR mentései	**CP-9**	7
32	EIR helyreállítás és újraindítás	**CP-10**	8
33	A kommunikáció integritása	**CR 3.1**	7
34	Network segmentaion	**CR 5.1**	7

35	Legkisebb jogosultság elve	**CCSC 3 (4.4)**	7
#	**Baseline kontroll név**	**Kontroll ID**	**Pont**
36	Azonosítás és hitelesítés szabályzat és eljárásrend	**IA-1**	7
37	Azonosítás és hitelesítés	**IA-2**	7
38	Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése	**IA-2(1)**	7
39	Azonosító kezelés	**IA-4**	7
40	A hitelesítésre szolgáló eszközök kezelése	**IA-5**	7
41	A hitelesítésre szolgáló eszközök kezelése A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés	**IA-5** **IA-5.1**	7
42	A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés	**IA-5(1)**	8
43	Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	**IA-8**	7
44	biztonsági eseménykezelési szabályzat	**IR-1**	7
45	Képzés a biztonsági események kezelésére	**IR-2**	8
46	Biztonsági események kezelése	**IR-4**	8
47	A biztonsági események nyomonkövetése	**IR-5**	8
48	A biztonsági események jelentése	**IR-6**	7
49	Biztonsági eseménykezelési terv	**IR-8**	9
50	karbantartási szabályzat	**MA-1**	8
51	Szabályozott karbantartás	**MA-2**	7
52	Távoli karbantartás	**MA-4**	8
53	Karbantartó személyek	**MA-5**	8
54	Adathordozók védelme szabályzat és eljárásrend	**MP-1**	7
55	Hozzáférés az adathordozókhoz	**MP-2**	7
56	Adathordozók használata	**MP-7**	8
57	Zone boundary protection	**NDR 5.2**	7
58	Fizikai és környezeti biztonsági szabály	**PE-1**	8
59	A fizikai belépés ellenőrzése	**PE-3**	7
60	Környezeti védelmi intézkedések	**PE-14**	8
61	Be- és kiszállítás	**PE-16**	7
62	Biztonságtervezési szabályzat	**PL-1**	7
63	Rendszerbiztonsági terv	**PL-2**	7
64	Viselkedési szabályok	**PL-4**	7
65	Biztonsági követelmények kiválasztása	**PL-10**	9
66	Személyi biztonságra vonatkozó szabályzat	**PS-1**	7
67	Munkakörök biztonsági szempontú besorolása	**PS-2**	7
68	Hozzáférési megállapodások	**PS-6**	8
69	Külső személyekhez kapcsolódó biztonsági követelmények	**PS-7**	7
70	Kockázatkezelés szabályzat és eljárásrend	**RA-1**	7
71	Kockázatelemzés – Ellátási lánc	**RA-3(1)**	8
72	Sérülékenységmenedzsment	**RA-5**	8

73	Sérülékenységmenedzsment – Sérülékenységi adatbázis frissítése	**RA-5(2)**	8
74	Kockázatokra adott válasz	**RA-7**	8
#	**Baseline kontroll név**	**Kontroll ID**	**Pont**
75	Rendszer és szolgáltatásberszerzés szabályzat/eljárásrend	**SA-1**	7
76	Támogatással nem rendelkező rendszerelemek	**SA-22**	7
77	rendszer- és kommunikációvédelmi szabályzat	**SC-1**	7
78	Szolgáltatásmegtagadással járó támadások elleni védelem	**SC-5**	8
79	Rendszer- és információsértetlenségi szabályzat	**SI-1**	7
80	Kártékony kódok elleni védelem	**SI-3**	7
81	Biztonsági riasztások és tájékoztatások	**SI-5**	8
82	Ellátási lánc kockázatkezelése szabályzat/eljárásrend	**SR-1**	7
83	Ellátási láncra vonatkozó kockázatmenedzsment szabályzat	**SR-2**	8
84	Ellátási láncra vonatkozó követelmények és folyamatok	**SR-3**	7
85	Értesítési megállapodások	**SR-8**	8

#	Recommended kontroll név	Kontroll ID	Pont
1	Sikertelen bejelentkezési kísérletek	**AC-7**	5
2	Rendszerhasználati jelzés	**AC-8**	5
3	Külső elektronikus információs rendszerek használata	**AC-20**	6
4	Biztonságtudatossági képzés – Belső fenyegetés	**AT-2(2)**	6
5	A biztonsági képzésre vonatkozó dokumentációk	**AT-4**	5
6	Naplózás tárkapacitása	**AU-4**	6
7	Naplózási hiba kezelése	**AU-5**	6
8	Letagadhatatlanság	**AU-10**	5
9	Naplóbejegyzés megőrzése	**AU-11**	5
10	Folyamatos felügyelet – Kockázatmonitorozás	**CA-7(4)**	6
11	A változtatásokra vonatkozó hozzáférés korlátozások	**CM-5**	5
12	Konfigurációs beállítások	**CM-6**	6
13	Legszűkebb funkcionalitás	**CM-7**	6
14	Rendszerelem leltár	**CM-8**	5
15	Felhasználó által telepített szoftver	**CM-11**	6
16	Üzletmenet-folytonossági terv tesztelése	**CP-4**	6
17	Mobilkód	**EDR 2.4**	5
18	Korlátozott adatfolyam	**FR-5**	6
19	Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – Visszajátszás elleni védelem	**IA-2(8)**	6
20	Adathordozók törlése	**MP-6**	5
21	Általános célú személyek közötti kommunikációs rendszer korlátozása	**NDR 5.3**	6
22	Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	**PE-15**	5

23	Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások	**PL-4(1)**	5
24	Személyek háttérellenőrzése	**PS-3**	6
#	**Recommended kontroll név**	**Kontroll ID**	**Pont**
25	Fegyelmi intézkedések	**PS-8**	5
26	Munkaköri leírások	**PS-9**	6
27	Biztonsági osztályba sorolás	**RA-2**	6
28	Kockázatelemzés	**RA-3**	6
29	Sérülékenységmenedzsment – A lefedettség szélessége és mélysége	**RA-5(11)**	5
30	Erőforrások rendelkezésre állása	**SA-2**	6
31	A rendszer fejlesztési életciklusa	**SA-3**	5
32	Beszerzések	**SA-4**	6
33	Biztonságtervezési elvek	**SA-8**	6
34	Kriptográfiai védelem	**SC-13**	6
35	Hibajavítás	**SI-2**	6
36	Az EIR monitorozása	**SI-4**	6
37	Rendszerek vagy rendszerelemek vizsgálata	**SR-10**	6
38	Rendszerelem hitelessége	**SR-11**	5

Kohéziós táblázat

5. számú melléklet

TUDOMÁNYOS PROBLÉMA	HIPOTÉZIS	CÉLKITŰZÉS	KUTATÁSI MÓDSZER	KÖVETKEZTETÉS	HIPOTÉZIS IGAZOLÁSA/ ELVETÉSE	ÚJ TUDOMÁNYOS EREDMÉNY
1. veszélyes anyagokkal foglalkozó üzemek működése napjainkban egyre összetettebb kihívások elé néz, különösen az információbiztonság és a kiberfenyegetések területén. Az Ipar 4.0 jelentősen átalakította az ipari folyamatokat, ugyanakkor új sebezhetőségeket és kockázatokat is hozott. A modern ipari környezetben a kockázatok azonosítása, értékelése és kezelése csak akkor lehet hatékony, ha integrált módon kezeli a technológiai, jogi, szervezeti és kiberbiztonsági szempontokat is. Ennek megfelelően további vizsgálatra érdemes a veszélyes üzemek üzembiztonságának fejlesztési lehetősége a GRC-szemlélet mentén, amely elősegítheti az üzemi biztonság holisztikus erősítését és a veszélyes üzemek teljes körű rezilienciájának növelését.	1. Megítélésem szerint a felső és alsó küszöbértékű veszélyes anyagokkal foglalkozó üzemekre vonatkozó előírások és azok alapján készült szabályrendszer összehasonlítása alapján a veszélyes anyagok és technológiák hatékonyabban meghatározhatóak. Az általános vezetési rendszer és biztonsági irányítási rendszer nemzetközi szabványok ajánlásaival, valamint a PDCA vagy a PDSA ciklussal való kibővítésével az üzemeltetés biztonsága növelhető, a balesetek kialakulásának kockázata csökkenthető.	Célul tűztem ki veszélyes anyagokkal foglalkozó üzemekre vonatkozó hazai és nemzetközi szabályozási, biztonságirányítási és kockázatkezelési megközelítések vizsgálatát annak érdekében, hogy meghatározhatók legyenek azok az integrált irányítási és reziliencia-központú módszertani elemek, amelyek hozzájárulhatnak az üzembiztonság növeléséhez, a modern kori kihívások hatékonyabb kezeléséhez és a súlyos ipari balesetek megelőzéséhez.	Szakirodalom- és dokumentumelemzés; összehasonlító szabályozási vizsgálat; kvalitatív rendszerszemléletű elemzés; empirikus tapasztalatok feldolgozása.	A vizsgálatok alapján megállapítható, hogy a veszélyes anyagokkal foglalkozó üzemek hagyományos üzembiztonság és compliance-orientált megközelítése a modern ipari környezetben megjelenő kiberkockázatok kezelésére önmagában már nem minden esetben elegendő. A GRC meta-keret alkalmas lehet az üzembiztonsági, információbiztonsági, OT-biztonsági és lakosságvédelmi szempontok integrált kezelésére, valamint a veszélyes üzemek teljes körű rezilienciájának támogatására.	A hipotézist elméleti szinten igazoltam, mivel a kutatás eredményei alátámasztották, hogy az integrált, reziliencia-központú biztonságirányítási megközelítések hozzájárulhatnak a veszélyes anyagokkal foglalkozó üzemek biztonságának növeléséhez és a modern kori kihívások hatékonyabb kezeléséhez.	A veszélyes anyagokkal foglalkozó üzemek biztonsági irányítási és kockázatkezelési rendszereinek tudományos vizsgálata alapján **megállapítottam**, hogy a hagyományos üzembiztonsági és követelményrendszereknek történő megfelelőségi megközelítések önmagukban már nem képesek teljeskörűen kezelni a modern ipari környezetben megjelenő kockázatokat. **Ennek megfelelően kialakítottam** egy GRC-alapú, integrált és reziliencia-központú módszertant, amely egységes keretben kezeli az üzembiztonsági, kockázatkezelési, megfelelőségi, OT-kiberbiztonsági és lakosságvédelmi szempontokat a veszélyes üzemek súlyos ipari baleseteinek megelőzése érdekében.

TUDOMÁNYOS PROBLÉMA	HIPOTÉZIS	CÉLKITŰZÉS	KUTATÁSI MÓDSZER	KÖVETKEZTETÉS	HIPOTÉZIS IGAZOLÁSA/ELVETÉSE	ÚJ TUDOMÁNYOS EREDMÉNY
2. A modern ipari környezet működéséből fakadóan azonosíthatóvá vált az a tudományos rés, hogy egy kiber-fizikai rendszer elleni célzott támadás következményeként akár lakosságvédelmi intézkedések végrehajtása is szükségessé válhat. Az ilyen események következményei túlmutathatnak az üzemi károkon, és veszélyeztethetik környezetet, a lakosság egészségét és a kritikus szervezetek működését. Az ilyen típusú incidensek kezelése megköveteli a veszélyhelyzet-értékelés, a veszélyesanyag-terjedési modellezés, a lakosságvédelmi intézkedések tervezésének és a hiteles lakosságtájékoztatás támogatásának, valamint a katasztrófavédelmi szervek és társhatóságok közötti együttműködés hatékony fejlesztését.	2. Feltételezem, hogy a valós idejű és előrejelzett meteorológiai adatokra épülő digitális anyagterjedés-modellezési és döntéstámogatási rendszerek alkalmazásával hatékonyabban támogatható a veszélyhelyzeti helyzetértékelés, valamint csökkenthető a beavatkozó állomány és a potenciálisan veszélyeztetett lakosság egészségkárosodásának kockázata. Feltételezem továbbá, hogy a digitálisan támogatott és hiteles lakosságtájékoztatás hozzájárulhat a lakosság együttműködési hajlandóságának növeléséhez a veszélyhelyzeti intézkedések végrehajtása során.	Célkitűzésem, hogy megvizsgáljam és bemutassam a felderítésben résztvevő állomány egészségi állapotának megőrzését és hatékonyabb felderítési és elemzési folyamatokat eredményező, a jelenleg rendelkezésre álló veszélyes anyag terjedését modellező szoftverek fejlesztési lehetőségeinek vizsgálata és bemutatása, különös tekintettel a lakosságvédelmi döntéstámogatás, a helyzetértékelés és a digitálisan támogatott lakosságtájékoztatás lehetőségeire.	Szakirodalom- és dokumentumelemzés; Design Science Research (DSR) módszertan; kísérleti rendszerfejlesztés és rendszerintegráció; szcenárió alapú veszélyes anyag-terjedési modellezés; összehasonlító elemzés; demonstrációs célú validáció.	A vizsgálatok alapján megállapítható, hogy a modern ipari veszélyhelyzetek kezelése során a gyors helyzetértékelés, az adatvezérelt döntéstámogatás és a hiteles lakosságtájékoztatás együttesen meghatározó szerepet töltenek be a lakosságvédelmi intézkedések hatékonyságában. Megállapítottam továbbá, hogy a digitális platformokon megjelenő dezinformáció elleni hatékony fellépés szoros összefüggésben áll a hivatalos kommunikáció gyorsaságával, hitelességével és egységességével.	A hipotézist igazoltam, mivel a szakirodalmi vizsgálatok és a kutatás eredményei alátámasztották, hogy a valós idejű és előrejelzett meteorológiai adatokra épülő digitális veszélyesanyag-terjedési modellezés alapvetően támogatja a veszélyhelyzeti helyzetértékelést és a lakosságvédelmi döntéshozatalt. A szakirodalomban különösen hatékony megközelítésként jelennek meg a Random Forest alapú, valamint a neurális hálózatokra épülő prediktív MI modellek. A fejlesztett digitális rendszerarchitektúra oktatási környezetben is alkalmazható lehet, különösen digitálisan támogatott gyakorlatok során.	A veszélyes anyagokkal foglalkozó üzemek veszélyhelyzeteinek elemzésére és értékelésére építve **megállapítottam**, hogy azok kezelése során a gyors helyzetértékelés, az adatvezérelt döntéstámogatás és a hiteles lakosságtájékoztatás együttesen meghatározó szerepet töltenek be a lakosságvédelem feladatrendszerében. Ennek figyelembevételével **kidolgoztam** egy digitális lakosságvédelmi döntéstámogatási rendszert, amely egységes architektúrában integrálja a meteorológiai adatgyűjtést, a veszélyesanyag-terjedési modellezést, a térinformatikai megjelenítést és a veszélyeztetett lakosság becslését, ezáltal biztosítva a hatékony lakosságvédelmi intézkedések végrehajtását.

TUDOMÁNYOS PROBLÉMA	HIPOTÉZIS	CÉLKITŰZÉS	KUTATÁSI MÓDSZER	KÖVETKEZTETÉS	HIPOTÉZIS IGAZOLÁSA/ELVETÉSE	ÚJ TUDOMÁNYOS EREDMÉNY
3. A modern ipari környezetben a kiber-fizikai rendszerek elleni támadások közvetlen hatással lehetnek az üzembiztonságra, az üzemfolytonosságra, valamint az emberi élet és a környezet biztonságára is. Ez indokolttá teszi olyan üzembiztonság-központú és kockázatarányos védelmi megközelítések vizsgálatát, amelyek figyelembe veszik az ipari vezérlőrendszerek sajátos működési követelményeit.	3. Feltételezem, hogy különösen az alsó és felső küszöbértékű veszélyes anyagokkal foglalkozó üzemek esetén a kibertérből érkező támadásokkal szembeni kitettség jelentős mértékű és ez a tendencia az elkövetkező években folyamatos növekedést fog mutatni.	Egy modern műszaki, technikai és adminisztratív keretrendszer és eljárásrend kidolgozását tűztem ki célul, amely a kiber-fizikai eszközök (OT) és azokkal párhuzamosan működő IT rendszerek magas szintű kibervédelmi képességeinek kialakításához szükséges.	Trend elemzés; kiberbiztonsági szervezetek primer adatainak összegyűjtése és analitikai elemzése; esettanulmányok vizsgálata. Releváns Uniós és hazai jogszabályok vizsgálata; nemzetközi szabványok vizsgálata.	A vizsgálatok alapján megállapítható, hogy a veszélyes anyagokkal foglalkozó üzemek a kibertámadásokkal leginkább érintett gyártóipari és kritikus infrastruktúra szektorokhoz kapcsolódnak, miközben a kiber-fizikai rendszereket érő támadások közvetlen hatással lehetnek az üzembiztonságra és az üzemfolytonosságra. Megállapítottam továbbá, hogy az OT-környezetek sajátosságai indokolttá teszik egy üzembiztonság-központú és kockázatarányos kiberbiztonsági megközelítés alkalmazását, amelynek metodikai alapjait kutatásaim során megalapoztam.	A hipotézist igazoltam, mivel a nemzetközi kiberbiztonsági jelentések és OT-specifikus esettanulmányok elemzése alapján megállapítható, hogy a veszélyes üzemek is olyan kritikus szervezetek és infrastruktúrák, amelyeknek a kibertámadásokkal kapcsolatos kitettsége jelentős. A kutatás eredményei továbbá megalapozták egy veszélyes üzemekre szabott, iparbiztonsági fókuszú kiberbiztonsági keretrendszer módszertani alapjait.	A nemzetközi és hazai kiberbiztonsági jelentések és OT-specifikus esettanulmányok elemzése alapján **megállapítottam**, hogy a veszélyes anyagokkal foglalkozó üzemek jelentős része a kibertámadásokkal leginkább érintett gyártóipari és kritikus infrastruktúra ágazatok részét képezi, miközben a kiber-fizikai rendszereket érő támadások közvetlen hatással lehetnek az üzembiztonságra és az üzemfolytonosságra, valamint az emberi élet és a környezet biztonságára is. **Ennek megfelelően kidolgoztam** egy üzembiztonsági központú, veszélyes üzemekre optimalizált kiberbiztonsági módszertani keretrendszert. Valamint igazoltam a Cyber PHA szemlélet alkalmazhatóságát az iparbiztonsági kockázatértékelési folyamatok kibővítésére.