Védelem Tudomány 11. évfolyam 2. szám, 2026 DOI: 10.61790/vt.2026.23374

Integrált biztonságirányítás és kiberreziliencia veszélyes üzemekben

Integrated Safety Management and Cybersecurity Resilience in Seveso Plants

Vásárhelyi Örs László
szerző
Szervezet, beosztás: NKE, HHK, KMDI doktorandusz
Email: vasarhelyi.ors.laszlo@stud.uni-nke.hu
ORCID: 0000-0002-6752-2546

Szabó Rafael
társszerző
Szervezet, beosztás ALTEO Group, CISO
Email: szabo.rafael@hirs.hu

Absztrakt:

A veszélyes anyagokkal foglalkozó üzemek erősödő digitalizációja és az IT–OT rendszerek fokozódó konvergenciája következtében a kiberbiztonsági kockázatok már nem kizárólag az információbiztonság területén jelentenek kihívást, hanem közvetlen hatással lehetnek az üzembiztonságra, az üzemfolytonosságra, valamint a környező lakosság és élővilág egészségére is. Miközben a Seveso-szabályozás hagyományosan a safety szemléletre épül, míg a NIS2 irányelv és az ahhoz kapcsolódó kiberbiztonsági követelmények elsősorban dominánsan IT-fókuszú szemléletet tükröznek, amely nem minden esetben illeszthető közvetlenül a safety-kritikus OT-környezetek működési sajátosságaihoz. A tanulmány egy olyan integrált biztonságirányítási megközelítést mutat be, amely az irányítási, kockázatkezelési és kötelezettségeknek való megfelelőségi (GRC) szemlélet alkalmazásával támogatja a kockázatarányos követelmények kialakítását a szervezet technológiai, operatív és irányítási területein egyaránt. A modell célja a teljes körű szervezeti reziliencia erősítése, valamint a biztonsági kockázatokra és működési kihívásokra való rugalmas reagálóképesség fejlesztése. A kutatás során a szerzők elemezték a hazai és nemzetközi szabályozási környezetet, a releváns irányítási rendszereket és kiberbiztonsági keretrendszereket, különös tekintettel, a kiber-fizikai környezet megfelelő védelmének kialakításáról szóló ajánlásokra. A tanulmány eredményeként egy olyan integrált megközelítés kerül bemutatásra, amely támogatja a veszélyes anyagokkal foglalkozó üzemek komplex rezilienciájának fejlesztését.

Kulcsszavak: biztonságirányítás, reziliencia, veszélyes üzemek

Abstract:

Due to the increasing digitalization of hazardous plants and the growing convergence of IT and OT systems, cybersecurity risks no longer pose a challenge solely in the realm of information security; they can also have a direct impact on operational safety, business continuity, and the health of the surrounding population and wildlife. While the Seveso regulations are traditionally based on a safety-oriented approach, the NIS2 Directive and its associated cybersecurity requirements primarily reflect a predominantly IT-focused approach, which does not always align directly with the operational characteristics of safety-critical OT environments. The study presents an integrated security management approach that supports the development of risk-proportionate requirements across the organization's technological, operational, and governance domains by applying a governance, risk management, and compliance (GRC) approach. The model aims to strengthen comprehensive organizational resilience and develop the ability to respond flexibly to security risks and operational challenges. During the research, the authors analyzed the domestic and international regulatory environment, relevant management systems, and cybersecurity frameworks, with particular attention to recommendations for establishing adequate protection of the cyber-physical environment. The study presents an integrated approach that supports the development of comprehensive resilience in Seveso establishments.

Keywords: safety management, resilience, Seveso plants

1. BEVEZETÉS – A FRAGMENTÁLT BIZTONSÁGI SZABÁLYOZÁS PROBLÉMÁJA

A veszélyes anyagokkal foglalkozó üzemek és a kritikus infrastruktúrák biztonságának kérdése az elmúlt években új dimenzióba lépett, amelyet elsősorban az ipari digitalizáció felgyorsulása, valamint a hagyományos informatikai (IT) és operatív technológiai (OT) rendszerek fokozódó konvergenciája eredményez. Az Ipar 4.0 megjelenését követően a korábban elszigetelt ipari vezérlőrendszerek és egyéb technológiai rendszerek egyre szorosabban kapcsolódnak a vállalati informatikai környezetekhez, valamint a távfelügyeleti, távoli karbantartási és adatgyűjtési funkciók megjelenése miatt egyre gyakrabban kapcsolódnak külső hálózatokhoz is. Ez a folyamat a korábban izolált rendszerek támadási felületének jelentős növekedését eredményezi, és fokozza a kibertérből érkező fenyegetéseknek való kitettséget. Különösen kritikus ez a tendencia a veszélyes anyagokkal foglalkozó üzemek esetében, ahol egy kiberbiztonsági esemény nem csupán gazdasági károkat, hanem közvetlen üzembiztonsági, környezeti és a lakosságra negatívan ható következményeket is eredményezhet. [1] [2]

Az ipari rendszerekben a safety és security dimenziók egyre szorosabban összekapcsolódnak. A technológiai folyamatokat felügyelő és védő biztonsági műszeres rendszerek (Safety Instrumented Systems - SIS) digitalizációja és hálózati integrációja új támadási felületeket hoz létre, miközben e rendszerek továbbra is a baleset-megelőzési hierarchia utolsó, kontrollált védelmi vonalát jelentik. Ennek következtében a biztonság értelmezése már nem korlátozható elkülönült safety vagy cybersecurity megközelítésekre, hanem integrált szemléletet igényel. [3] [1] [4]

A szabályozási környezet ugyanakkor továbbra is fragmentált. Számos veszélyes üzem nem tartozik a kiberbiztonsági szabályozások teljes hatálya alá, miközben működése jelentős kockázatokat hordozhat. A szabályozási környezet mellett a szervezeti működés szintjén is jelentős fragmentáció figyelhető meg. A biztonság különböző dimenziói, mint az iparbiztonság, a munkabiztonság, a fizikai biztonság, a kiberbiztonság, a megfelelőség (compliance) és a kockázatkezelés, jellemzően eltérő szervezeti egységekhez, felelősségi körökhöz és módszertani megközelítésekhez kapcsolódnak. A kiberbiztonságon belül további elkülönülés figyelhető meg az informatikai és az operatív technológiai környezetek között, miközben a kapcsolódó kockázatok a gyakorlatban egyre szorosabban összefonódnak. Ez a széttagolt működés akadályozza az egységes, kockázatarányos biztonságirányítás kialakítását, valamint a szervezeti reziliencia átfogó fejlesztését. [5] [6]

A tanulmány alapfeltevése, hogy a veszélyes üzemek teljes körű rezilienciájának fejlesztéséhez olyan integrált megközelítés szükséges, amely képes összehangolni a technológiai, szervezeti, irányítási és megfelelőségi követelményeket. Ennek elméleti keretét a Governance, Risk and Compliance (GRC) szemlélet biztosítja, amely a szervezeti célok, a kockázatok, a teljesítmény és a kötelezettségek kezelését egységes rendszerben értelmezi. A tanulmány célja egy olyan integrált biztonságirányítási modell bemutatása, amely képes összekapcsolni a jogszabályi, irányítási, technikai és szervezeti dimenziókat, és támogatja a biztonság mérhető, fejleszthető és adaptív megvalósítását. [7]

2. A VESZÉLYES ÜZEMEK HAZAI SZABÁLYOZÁSA

A veszélyes anyagokkal foglalkozó üzemek szabályozása az Európai Unióban egységes elveken alapul, amelyek kiindulópontját a Seveso-baleset tapasztalatai képezik. A veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről szóló 2012/18/EU Európai Parlamenti és Tanácsi Irányelv (továbbiakban Seveso III) 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 veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről 219/2011. (X.20.) Korm. rendelet révén kerültek átültetésre, amely meghatározza a veszélyes anyagokkal foglalkozó üzemek azonosításának, működésének és felügyeletének részletes szabályait.

2.1 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. A Seveso III direktíva ennek megfelelően két alapvető kategóriát különböztet meg: alsó küszöbértékű üzemek és 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 a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X.20.) Korm. rendelet alapján egy további kategóriát is bevezet: a küszöbérték alatti üzemeket. Ide azok a létesítmények tartoznak, ahol a jelenlévő veszélyes anyag mennyisége eléri az alsó küszöbérték 25%-át. Ezen üzemek működése indokolttá teheti egyes biztonsági követelmények alkalmazását. Ennek megfelelően rájuk is vonatkoznak előírások, elsősorban a veszélyazonosítás, az alapvető megelőző intézkedések, valamint a hatósági nyilvántartásba vétel és ellenőrzés területén.

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 a komplex ipari rendszerek és az ellátási láncok vizsgálata során, ahol a kisebb, de hálózatosan kapcsolódó üzemek is jelentős szerepet játszhatnak a rendszerszintű kockázatok alakulásában.

2.2 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.

2.2.1 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 audit és felülvizsgálati folyamatokat, jelentéstételi eljárásrendeket.

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

2.2.2 Veszélyazonosítás és kockázatelemzés

Az üzemeltető feladata a veszélyforrások azonosítása és a baleseti forgatókönyvek elemzése. A jogszabály nem ír elő konkrét módszert, de elvárja a technológiai folyamatok, a veszélyes anyagok tulajdonságainak, valamint a lehetséges hatások és érintett lakosság vizsgálatát.

Felső küszöbértékű üzemek esetén ezt biztonsági jelentésben kell dokumentálni, alsó küszöbértékű üzemek esetén ezt biztonsági elemzésben, míg küszöbérték alatti üzemek esetén hatósági mérlegelést követően.

2.2.3 Védelmi tervezés

A lakosságvédelem a szabályozás kiemelt eleme, amelyet a hatóság a külső védelmi terven keresztül biztosít. Ez meghatározza a veszélyeztetett területeket, a szükséges védelmi intézkedéseket, valamint a beavatkozó szervezetek együttműködését.
A hatóság biztosítja a riasztási és tájékoztatási rendszerek működését, valamint gondoskodik a lakosság előzetes tájékoztatásáról, beleértve a veszélyek jellegét és a követendő magatartási szabályokat. A tervek hatékonyságát rendszeres gyakorlatokkal ellenőrzik, és szükség esetén felülvizsgálják. A védelmi rendszer célja, hogy baleset esetén összehangolt, gyors és hatékony beavatkozás valósuljon meg, biztosítva a lakosság és a környezet védelmét.

2.3 A felügyeleti hatóság szerepe és eljárásai

A veszélyes üzemek felügyeletét az iparbiztonsági hatóság látja el, amely az üzemek azonosítását, engedélyezését és ellenőrzését végzi. Az ellenőrzések célja annak biztosítása, hogy a biztonsági rendszerek ténylegesen működjenek. Az ellenőrzések lehetnek rendszeresek vagy eseti jellegűek, és kiterjednek a BIR működésére, a kockázatelemzésekre, az üzemeltetési gyakorlatra és a védelmi tervek végrehajthatóságára. A felügyelet kockázatalapú, így a veszélyesebb üzemek esetében gyakoribb és részletesebb ellenőrzések történnek. Hiányosság esetén a hatóság korrekciós intézkedéseket rendelhet el, korlátozhatja az üzem működését, vagy bírságot szabhat ki a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezéssel összefüggő bírságokról szóló 208/2011. (X.12.) Korm. rendelet alapján.

2.3.1 Védelmi tervezés és lakosságvédelem

A veszélyes anyagokkal foglalkozó üzemekkel kapcsolatos védelmi tervezés és lakosságvédelem a hazai szabályozás egyik kiemelt területe, amely a súlyos ipari balesetek következményeinek mérséklését célozza. A hatóság egyik alapvető feladata a külső védelmi terv elkészítése és folyamatos karbantartása a felső küszöbértékű üzemek esetében, valamint azon üzemek esetén is, ahol indokolt. 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. Veszélyes üzemek esetén a lakosságvédelem egyik központi eleme a külső védelmi terv, amely meghatározza a veszélyeztetett területeket, a lakosságvédelmi intézkedéseket, a riasztási és tájékoztatási mechanizmusokat, valamint a beavatkozó szervezetek együttműködésének rendjét. A hatóság feladata a lakosság előzetes tájékoztatása, a tervek rendszeres gyakorlása és felülvizsgálata annak érdekében, hogy baleset esetén gyors és összehangolt beavatkozás valósuljon meg.

3. NIS2 HAZAI IMPLEMENTÁCIÓJA 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 az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (továbbiakban: NIS2). 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 Magyarország kiberbiztonságáról szóló 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 kiegészíti annak a végrehajtási rendelete 418/2024. (XII. 23.) Korm. rendelet, valamint a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI.24.) MK rendelet, ami gyakorlatilag az operatív követelménykatalógust biztosítja. A kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló 1/2025. (I.31.) SZTFH rendelet, ami a gazdálkodó szervezetekre és azok rendszereire vonatkozó kiberbiztonsági auditok módszertanát és részletszabályait tartalmazza.A hazai implementáció középpontjában a kiberbiztonsági kockázatok azonosítása, értékelése és kezelése áll. A követelményrendszer egy részletes technikai és szervezeti kontrollkatalógusra épül, amelynek kialakításában meghatározó szerepet játszott az amerikai NIST SP 800-53 Rev. 5 kontrollrendszere. A dokumentum azonban elsősorban informatikai környezetekre került meghatározásra. [8]

2.3.2 A szabályozási „fehér folt" problémája

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 és folyamatbiztonsági (safety) kockázatok szabályozottak, azonban a kiberbiztonsági dimenzió nem, vagy csak korlátozottan. A hazai NIS2 implementáció egyik sajátossága, hogy a kiberbiztonsági követelményrendszer eredendően informatikai környezetekre lett kialakítva. Ennek következtében az ipari vezérlőrendszerek és egyéb OT rendszerek is egységesen elektronikus információs rendszerként kerülnek kezelésre, és az auditok 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 kerültek 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. [9]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 és végső soron nem biztosít valamennyi hazai veszélyes üzem számára teljeskörű ellenállóképességet.

4. GRC, MINT INTEGRÁLÓ ELMÉLETI 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 alapú 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 figyelembevétele mellett valósul meg. 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 tényleges működésre, folyamatokra és rendszerekre. 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. Egy előre meghatározott követelménykatalógus hosszabb távon nem ösztönzi a legújabb trendeknek megfelelő vagy előremutató technológiai megoldások alkalmazását. Ez különösen igaz a kiber-fizikai rendszerek esetén, ahol a kockázatok gyakran nem lineáris módon, hanem 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. Az alkalmazandó védelmi intézkedések implementálását pedig mindig a kockázatelemzés eredményei függvényében hangolni. A modern ipari környezetekben a kockázatok gyakran a technológiai, szervezeti és humán tényezők kölcsönhatásából erednek, így kezelésük csak integrált megközelítésben lehetséges. [7]

5. A NEMZETKÖZI SZABVÁNYOK GRC-BE ILLESZTÉSE

A modern veszélyes anyagokkal foglalkozó üzemek esetén 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 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.

5.1 A nemzetközi szabványok integrációja GRC keretben

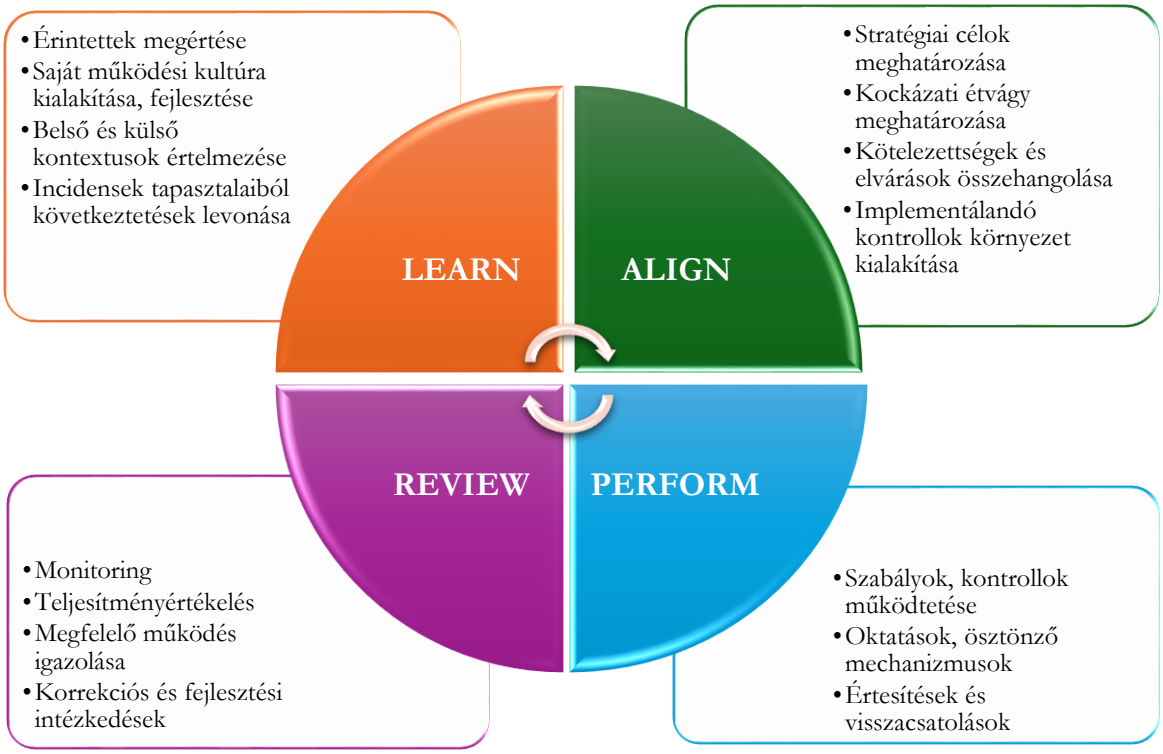
A biztonságirányítás gyakorlati megvalósítása során számos nemzetközi szabvány és ajánlás áll rendelkezésre, amelyek különböző aspektusait fedik le a biztonságnak. Ezek közül kiemelkedő jelentőségű az ISO/IEC 27001, amely a szervezeti szintű információbiztonsági irányítási rendszer kialakításához biztosít keretet. A szabvány kockázatalapú megközelítést alkalmaz, és meghatározza a szükséges irányítási struktúrákat, folyamatokat és felelősségeket, ezáltal elsősorban a governance és risk dimenziókat támogatja. [10] 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. [8]

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] [1] A safety 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, az ipari folyamatok elfogadható szélsőértékek között tartásáért és az élvédelemért felelő biztonsági műszeres rendszerek (SIS) szintén szigorú nemzetközi IEC 61511 szabványnak kell, hogy megfeleljenek. 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. [11] [4]

5.2 A LAPR ciklus

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" fázis célja a szervezet működési környezetének, kockázatainak, lehetőségeinek és érintetti elvárásainak folyamatos értelmezése, valamint a működés során keletkező tapasztalatok szervezeti tudássá alakítása. Ide sorolhatók a kockázatértékelési tevékenységek, a teljesítménymérések eredményeinek elemzése, a biztonságtudatossági képzések, a gyakorlatok és tesztelések tapasztalatainak feldolgozása, valamint a bekövetkezett incidensekből levont tanulságok rendszerszintű beépítése. E fázist olyan keretrendszerek támogatják, mint például az ISO 31000, NIST SP 800-37 kockázatkezelési szabványok vagy a NIST SP 800-137 folyamatos biztonsági monitorozási megközelítése. Az „Align" fázisban kerül sor a célok, politikák és irányítási keretek meghatározására, amelyben az ISO szabványok mellett az etikai dimenzió meghatározó szerepet játszik. E szakasz célja, hogy a szervezet stratégiai célkitűzései, kockázatkezelési elvárásai és megfelelőségi kötelezettségei összhangba kerüljenek egymással, valamint egyértelműen kijelölésre kerüljenek a felelősségi körök és a döntéshozatali mechanizmusok. A „Perform" fázis a kontrollok tényleges megvalósítását jelenti, ahol a NIST SP 800-53 kontrollkatalógusa, a NIST SP 800-82 és az IEC 62443 ipari biztonsági követelményei, valamint a jogszabály által nevesített biztonsági irányítási rendszer (BIR) elvárásai biztosítják a működési alapot. A „Review" fázisban a rendszer működésének értékelése történik auditok, hatósági ellenőrzések és visszacsatolási mechanizmusok révén. Az itt keletkező visszacsatolások és tapasztalatok egyúttal a „Learn" fázis bemeneteit is jelentik, támogatva a szervezeti tanulást, a kockázatok újraértékelését és a folyamatos fejlesztést, ezzel pedig a LAPR ciklikusságának folytonossága is biztosított.



1. ábra LAPR ciklus, készítette: A szerző (forrás: lsd: [7])

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

5.3 Az etikai és kulturális dimenzió szerepe

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. 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. 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:

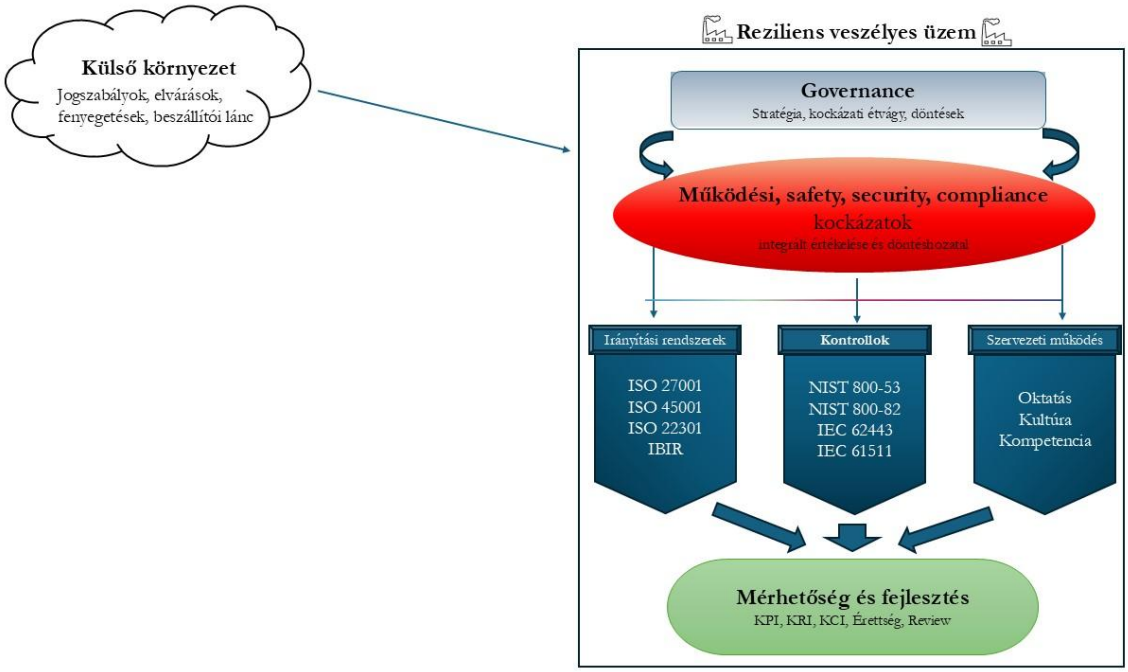
$$integritás = \frac{\text{betartott vállalások}}{tett\ vállalások}$$

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.

6. INTEGRÁLT GRC-ALAPÚ BIZTONSÁGI MODELL VESZÉLYES ÜZEMEKNEK

A veszélyes üzemek sajátossága, hogy a kockázatok következményei túlmutatnak az információbiztonság vagy az üzletmenet-folytonosság hagyományos dimenzióin. Egy ipari vezérlőrendszer vagy biztonsági PLC kompromittálódása közvetlen hatást gyakorolhat a technológiai folyamatokra, amely végső soron veszélyes anyag kibocsátásához vagy más súlyos ipari eseményhez vezethet. Ebből következően a kiberbiztonság nem értelmezhető pusztán támogató informatikai funkcióként, hanem az iparbiztonság integráns elemévé válik. Az ilyen jellegű kockázatok kezelése olyan integrált megközelítést igényel, amely a safety, security, compliance és governance dimenziókat egységes rendszerben értelmezi. A veszélyes üzemek esetében a biztonságirányítás elsődleges célja nem a jogszabályi megfelelés vagy az egyes védelmi intézkedések működtetése, hanem a súlyos következményekkel járó incidensek megelőzése és hatásainak csökkentése. Ennek megfelelően a modellben a safety szemlélet tölti be az integráló szerepet, amelyhez a kiberbiztonsági, megfelelőségi és irányítási követelmények kapcsolódnak.A modell a kockázatkezelést nem önálló szakterületként, hanem olyan összekötő mechanizmusként értelmezi,

amely biztosítja a különböző biztonsági dimenziók közötti kapcsolatot és támogatja a kockázatarányos döntéshozatalt. [12]



2. ábra A GRC meta-keret működése a veszélyes üzemek esetén, készítette: A szerző

Az integrált GRC-alapú modell lényege, hogy a biztonságirányítást nem különálló szabályozási és technikai elemek összességeként kezeli, hanem összekapcsolt irányítási struktúraként. Ebben a megközelítésben a jogszabályi környezet nem csupán megfelelési kötelezettségek halmaza, hanem a kockázatok értelmezésének kiindulópontja. A Seveso és a NIS2 szabályozás eltérő logikája – előbbi következményalapú, utóbbi szervezeti besorolásra épül – olyan szabályozási hiátust eredményezhet, amelynek következtében egy kiber-fizikai szempontból kritikus üzem kívül maradhat a kiberbiztonsági szabályozás hatályán. Az integrált modell ezt a problémát nem jogi, hanem kockázati összefüggésként kezeli, és lehetővé teszi, hogy a szervezet a formális kötelezettségeken túlmenően is kialakítsa a szükséges védelmi intézkedéseket. [7] [13] [14] A javasolt integrált GRC-alapú biztonsági modell a külső szabályozási követelményekre, az integrált irányítási rendszerekre és a technikai kontrollokra épül, amelyeket a vállalati governance és a kockázatkezelési folyamatok kapcsolnak össze egységes biztonságirányítási keretté. A négy elem nem hierarchikus értelemben különül el egymástól, hanem funkcionális szerepük alapján. A jogszabályi réteg határozza meg a kötelező minimumkövetelményeket, az irányítási réteg biztosítja a szervezeti működés és felelősségi rend kereteit, a technikai kontrollréteg valósítja meg a konkrét védelmi intézkedéseket, míg a vállalati governance réteg teremti meg azt a döntési, kockázatvállalási és erőforrás-allokációs környezetet, amelyben a biztonság ténylegesen működőképessé válik.

a. A jogszabályi réteg: Seveso és NIS2 kapcsolódása

A külső követelmények szintjén a modell alapját elsősorban a Seveso-szabályozás és a NIS2 irányelv hazai implementációja képezi. Bár a két szabályozási terület eltérő megközelítést alkalmaz, közös céljuk a szervezet működését veszélyeztető események megelőzése és következményeinek mérséklése.

A Seveso-rendszer elsősorban a veszélyes anyagokból eredő súlyos baleseti kockázatok kezelésére fókuszál, míg a NIS2 és a kapcsolódó hazai szabályozás a kiberbiztonsági kockázatok azonosítására, értékelésére és kezelésére helyezi a hangsúlyt. [7] [15] [16] A Seveso és a NIS2 közötti kapcsolatot nem formális hatályossági kérdésként, hanem kockázati összefüggésként szükséges értelmezni. Ennek alapján azon üzemek esetében is indokolt lehet kiberbiztonsági kontrollrendszer kialakítása, amelyek nem tartoznak a NIS2 hatálya alá, de technológiai folyamataik, veszélyesanyag-készletük, beszállítói kapcsolataik vagy ipari hálózati integrációjuk alapján rendszerszintű kockázatot hordoznak. [17] [7]

b. Az irányítási réteg: ISO-alapú menedzsmentrendszerek szerepe

Az irányítási dimenziót az ISO-alapú menedzsmentrendszerek biztosítják, amelyek lehetővé teszik a különböző biztonsági követelmények szervezeti folyamatokba történő integrálását. Kiemelt szerepet töltenek be az információbiztonsági, munkabiztonsági és üzletmenet-folytonossági követelményeket támogató szabványok, így különösen az ISO/IEC 27001, az ISO 45001 és az ISO 22301. Az irányítási réteg feladata, hogy a különböző szabványi megközelítéseket ne párhuzamos, egymástól független rendszerekként működtesse, hanem integrált menedzsmentrendszerként kapcsolja össze. [18] Az integrált modell ezért egységes kockázati és kontrollnyilvántartást feltételez, amelyben az egyes kockázatokhoz nem csupán informatikai vagy safety jellegű hatások rendelhetők, hanem azok kapcsolatai is megjelennek. [7] [13] [14] [19]

c. Technikai kontrollréteg

A harmadik pillért a technikai és szervezeti kontrollok alkotják, amelyek kialakításában meghatározó szerepet töltenek be az IEC 62443 szabványsorozat, a NIST SP 800-82 OT-biztonsági útmutatója és a NIST SP 800-53 kontrollkatalógusa. E keretrendszerek biztosítják azokat a védelmi intézkedéseket, amelyek támogatják az ipari rendszerek biztonságos működését. [20] [3] [21] [8] Az OT-környezetekben ugyanakkor a sérülékenységmenedzsment sajátos kihívásokat vet fel. Míg az informatikai rendszerek esetében az aktív sérülékenységvizsgálatok, az ügynökalapú végpontvédelem és a gyors hibajavítás általánosan elfogadott gyakorlatnak számítanak, addig az ipari környezetekben e tevékenységek önmagukban is kockázatot jelenthetnek a technológiai folyamatokra és a safety funkciókra nézve. Egy nem megfelelően végrehajtott szkennelés, frissítés vagy végpontvédelmi megoldás akár a rendszer validált állapotát is befolyásolhatja, ami jelentős üzemeltetési és biztonsági következményekkel járhat. [21] [5] A kérdés ezért nem pusztán technikai, hanem irányítási és kockázatkezelési probléma. Az integrált GRC-modell célja, hogy az IT-, OT-, safety- és megfelelőségi szempontok közös kockázatértékelési folyamatban kerüljenek mérlegelésre, és a döntések formális változáskezelés, safety-hatásvizsgálat és vezetői kockázatelfogadás alapján szülessenek meg. [22] Ennek megfelelően a sérülékenységmenedzsment nem kezelhető sem a hagyományos informatikai gyakorlatok mechanikus alkalmazásával, sem azok teljes elutasításával. A megfelelő megközelítést a kockázatarányos alkalmazás jelenti, amely figyelembe veszi az adott technológiai zóna kritikalitását, a safety követelményeket, valamint a rendelkezésre álló kompenzációs kontrollokat. [23] [21]

d. A vállalati governance réteg: döntéshozatal, felelősség és kockázati étvágy

A modell integráló elemét a vállalati governance jelenti, amely biztosítja, hogy a biztonság ne kizárólag technikai vagy megfelelőségi kérdésként jelenjen meg, hanem a szervezeti döntéshozatal részévé váljon. Veszélyes üzemek esetében ez különösen fontos, mivel a biztonsági döntések közvetlen hatással lehetnek a termelésre, a beruházásokra, az üzletmenet-folytonosságra és a külső érintettek bizalmára. [22] A governance réteg feladata a kockázati étvágy meghatározása, a felelősségi körök kijelölése, a biztonsági célok és teljesítménymutatók jóváhagyása, valamint a kritikus döntések vezetői szintű kezelése.

Ide tartozik annak eldöntése is, hogy a szervezet milyen mértékű reziduális kockázatot fogad el egy adott technológiai folyamat, beszállítói kapcsolat vagy távoli hozzáférési megoldás esetében. [11] Az integrált GRC-alapú biztonsági modell lényege tehát, hogy a veszélyes üzemek biztonságát nem különálló szabályozási, technikai vagy szervezeti dimenziók összességeként értelmezi, hanem összekapcsolt irányítási rendszerként. A modell összekapcsolja a szabályozási követelményeket, az irányítási rendszereket és a technikai kontrollokat, miközben a végső döntések a szervezet kockázati prioritásaihoz és biztonsági céljaihoz igazodnak. [17]

7. A GRC-ALAPÚ BIZTONSÁGIRÁNYÍTÁS MÉRHETŐSÉGE, ÉRETTSÉGI MODELLJE

Az integrált biztonságirányítási modell gyakorlati alkalmazhatóságának alapvető feltétele a mérhetőség és a folyamatos fejlesztés lehetősége. A veszélyes anyagokkal foglalkozó üzemek esetében a biztonsági teljesítmény értékelése különösen fontos, mivel a kockázatok következményei nem csupán információbiztonsági vagy üzletmenet-folytonossági problémákban, hanem súlyos ipari balesetekben, környezeti káreseményekben vagy lakosságvédelmi kihívásokban is megnyilvánulhatnak. A hagyományos megfelelőségi szemlélet ugyan alkalmas a jogszabályi és szabványi követelmények teljesülésének vizsgálatára, azonban önmagában nem ad kellően árnyalt képet a szervezet tényleges biztonsági képességeiről. A GRC megközelítés ezért a biztonságot nem statikus megfelelési állapotként, hanem folyamatosan fejleszthető szervezeti képességként értelmezi. A modell alapját egy ötszintű érettségi megközelítés képezi, amely az ad hoc működéstől a reziliens és adaptív szervezeti működésig írja le a fejlődés lehetséges állapotait. Az alacsonyabb érettségi szinteken a biztonsági folyamatok jellemzően fragmentáltak, a kockázatkezelés reaktív jellegű, és a safety, security, compliance és governance funkciók elkülönülten működnek. A magasabb szinteken ezzel szemben megjelenik az integrált kockázatkezelés, az egységes kontrollrendszer, a formális döntéstámogatás, valamint a szervezeti tanulás és alkalmazkodóképesség. Az érettségi modell célja nem a maximális fejlettségi szint elérése minden területen, hanem a szervezet kockázati profiljához illeszkedő, fenntartható és indokolható biztonsági képesség kialakítása. [7] [24] A GRC szemléletben a biztonsági teljesítmény mérésének központi eleme a Total Performance megközelítés, amely szerint a szervezeti teljesítmény nem értelmezhető kizárólag megfelelőségi vagy gazdasági mutatók alapján. Veszélyes üzemek esetében a teljesítmény legalább négy egymással összefüggő dimenzióban értelmezhető: safety, security, compliance és governance. A safety dimenzió a technológiai veszélyek kezelésének és a súlyos balesetek megelőzésének képességét, a security dimenzió a kiber- és fizikai fenyegetésekkel szembeni védelmet, a compliance dimenzió a jogszabályi és szabványi követelmények teljesítését, míg a governance dimenzió a vezetői döntéshozatal, az erőforrás-allokáció és a kockázati étvágy kezelésének hatékonyságát méri. Fontos megemlíteni, hogy a dimenziókat egymással összekapcsoltan kell értelmezni. [7]

A teljesítménymérés gyakorlati megvalósítását integrált indikátorrendszer támogatja, amely kulcs teljesítménymutatókra (KPI), kulcs kockázati mutatókra (KRI) és kulcs kontrollindikátorokra (KCI) épül. A KPI-k a biztonsági célok teljesülését, a KRI-k előrejelző jellegű mutatóként a kockázati kitettség változását követik nyomon, míg a KCI-k a kontrollok tényleges működését jelzik. Az indikátorok értelmezése önmagukban nem elegendő; azok csak egymással összefüggésben képesek támogatni a vezetői döntéshozatalt és a szervezeti teljesítmény valós értékelését. Ennek megfelelően a veszélyes üzemek esetén különösen fontos, hogy az indikátorok ne kizárólag informatikai vagy megfelelőségi szempontokat tükrözzenek, hanem figyelembe vegyék a safety következményeket is. Ennek megfelelően például az OT sérülékenységmenedzsment értékelése során nem elegendő a javított sérülékenységek számának mérése; vizsgálni kell a kockázatértékelések meglétét, a kompenzációs kontrollok alkalmazását, a safety hatáselemzések elvégzését és a reziduális kockázatok vezetői elfogadását is. [23] [1] [25]

A bemutatott mérhetőségi és érettségi modell lehetővé teszi, hogy a veszélyes üzemek biztonságirányítása a megfelelőségi minimumkövetelményeken túlmenően a tényleges kockázati kitettséghez igazodjon. Ez különösen fontos azokban az esetekben, amikor a szervezet nem tartozik valamely szabályozás közvetlen hatálya alá, ugyanakkor technológiai folyamatai, veszélyesanyag-készlete vagy beszállítói kapcsolatai révén jelentős kiber-fizikai kockázatot hordoz. A GRC-alapú megközelítés így nem csupán a biztonsági teljesítmény mérését támogatja, hanem a fejlesztési prioritások kijelölését, a vezetői döntéshozatal megalapozását és a szervezeti reziliencia folyamatos növelését is. [7] A modell gyakorlati alkalmazhatóságát jól szemlélteti az OT sérülékenységmenedzsment kérdése. Hagyományos informatikai környezetben egy kritikus sérülékenység javításának gyorsasága önmagában megfelelő teljesítménymutatónak tekinthető. Veszélyes üzemek esetében azonban egy frissítés telepítése a technológiai folyamatokra is hatással lehet, ezért a döntés során a kiberbiztonsági és a safety szempontokat egyaránt figyelembe kell venni. Ebben az esetben a KPI mérheti a kezelt sérülékenységek arányát, a KRI jelezheti a nyitott kritikus sérülékenységek számát, míg a KCI azt mutathatja meg, hogy a szükséges kockázatértékelések, safety hatáselemzések és vezetői jóváhagyások megtörténtek-e. Az indikátorok együttes alkalmazása így lehetővé teszi a kockázatarányos döntéshozatalt és a safety–security szempontok összehangolását és egységben történő kezelését.

8. KÖVETKEZTETÉSEK

A 21. századi ipari környezetei miatt a veszélyes anyagokkal foglalkozó üzemek biztonsági kihívásai egyre inkább megkövetelik az iparbiztonsági, kiberbiztonsági, megfelelőségi és irányítási funkciók integrált kezelését. A szerzők által végzett jogszabályi összehasonlító elemzések alapján megállapítható, hogy a Seveso alapú szabályozás és a NIS2 hazai implementációja eltérő logikára épül. Míg a súlyos ipari balesetek megelőzését és elhárítását célzó szabályozás elsődlegesen következmény- és veszélyalapú megközelítést alkalmaz, addig a kiberbiztonsági szabályozás elsősorban szervezeti és szolgáltatási alapú besorolást követ. Ennek következtében olyan veszélyes üzemek is megjelenhetnek, amelyek jelentős kiber-fizikai kockázatot hordoznak, ugyanakkor nem tartoznak teljes körű kiberbiztonsági követelmények hatálya alá. A bemutatott megközelítés egyik legfontosabb eleme a mérhetőség biztosítása. Az érettségi modell, a Total Performance szemlélet, valamint a KPI–KRI–KCI alapú indikátorrendszer lehetővé teszi, hogy a szervezetek a biztonságot ne statikus megfelelőségi állapotként, hanem folyamatosan fejleszthető, kockázatarányos és vezetői döntésekkel támogatott szervezeti képességként értelmezzék. A vizsgálatok alapján megállapítható továbbá, hogy veszélyes üzemek esetében a kiberbiztonság nem kezelhető kizárólag hagyományos IT- vagy OT-biztonsági megközelítések mentén, hanem azt a technológiai folyamatokból eredő következmények figyelembevételével, üzembiztonság-központú (safety) megközelítésben szükséges értelmezni és kezelni. A kutatás eredményei alapján megállapítható, hogy a GRC nem önálló biztonsági keretrendszerként, hanem integráló meta-keretként alkalmas arra, hogy összekapcsolja a safety, security, governance és compliance dimenziókat. Ennek alkalmazása hozzájárulhat a veszélyes üzemek teljes körű rezilienciájának kialakításához.

9. IRODALOMJEGYZÉK

[1] 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. (10.12.2023)

[2] 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,* 1. évfolyam 265 szám Part B, 01 2026.

[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] International Electrotechnical Commission (IEC), 61511-1:2016 Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements, Geneva: IEC, 2016.

[5] IBM X-Force, „X-Force Threat Intelligence Index 2026," IBM Corporation, 25 02 2026. [Online]. Available: https://www.ibm.com/reports/threat-intelligence. (2026.03.11.)

[6] K. Tamás, Szerző, *ICS/OT kiberbiztonság Bevezetés az OT csodálatos világába.* [Előadás]. 2026.

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

[8] 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.

[9] CISCO Talos, „2025 year in review," CISCO, Online, 2025.

[10] ISO/IEC, 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Geneva, CH: ISO copyright office, 2022.

[11] ISO, „ISO 45001:2018 Occupational health and safety management systems — Requirements with guidance for use," International Organization for Standardization, Geneva, 2018.

[12] Center for Chemical Process Safety (CCPS), Risked Based Process Safety Overview, USA, New York, NY: American Institute of Chemical Engineers, 2014.

[13] ISO/IEC, „ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls," International Organization for Standardization / International Electrotechnical Commission, Geneva, 2022.

[14] Joint Task Force, „Security and Privacy Controls for Information Systems and Organizations-NIST Special Publication," National Institute of Standards and Technology, https://doi.org/10.6028/NIST.SP.800-53r5, 2020.

[15] Miniszterelnöki Kabinetiroda, „Magyar Közlöny / Nemzeti Jogszabálytár," 2024. [Online]. Elérhető: https://njt.hu (2026.06.26.)

[16] Miniszterelnöki Kabinetiroda, „Magyar Közlöny / Nemzeti Jogszabálytár,” 2025. [Online]. Elérhető: https://njt.hu. (2026.06.26.)

[17] National Institute of Standards and Technology, „The NIST Cybersecurity Framework 2.0,” National Institute of Standards and Technology, https://doi.org/10.6028/NIST.CSWP.29, 2024.

[18] ISO, „ISO 31000:2018 Risk management — Guidelines,” International Organization for Standardization, Geneva, 2018.

[19] International Organisation for Standardization (ISO), ISO 22301-2019: Security and resilience - Business continuity management systems - Requirements, Geneva: ISO, 2019.

[20] MITRE, „MITRE ATT&CK,” 2024. [Online]. Elérhető: https://attack.mitre.org/matrices/ics/.

[21] Stouffer, Keith, Pease, Michael, Tang, CheeYee, Zimmerman, Timothy, Pillitteri, Victoria, Lightman, Suzanne, Hahn, Adam, Saravia, Stephanie, Sherule, Angela és Thompson, Michael, „Guide to Operational Technology Security - NIST Special Publication,” National Institute of Standards and Technology, https://doi.org/10.6028/NIST.SP.800-82r3, 2023.

[22] ISACA, COBIT 2019 Framework: Governance and Management Objectives, Schaumburg: ISACA, 2018.

[23] Souppaya, Murugiah és Scarfone, Karen, „Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology - NIST Special Publication,” National Institute of Standards and Technology, https://doi.org/10.6028/NIST.SP.800-40r4, 2022.

[24] CMMI Institute, „CMMI Model V2.0,” CMMI Institute, https://cmmiinstitute.com, 2018.

[25] 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.