

A kockázat alapú gondolkodás gyakorlati elemei a kritikus szervezeteknél I. rész

Practical elements of risk-based thinking in critical entities Part I.

Dr. Mógor Judit tű. vezérőrnagy
szerző

BM Országos Katasztrófavédelmi Főigazgatóság
Hatósági Főigazgató-helyettesi Szervezet
Hatósági Főigazgató-helyettes

ORCID: 0000-0003-3362-2431 

Dr. Baloghné Pruha Mária Anett
szerző

Békés Vármegyei Központi Kórház
Ellenálló Képességért Felelős Vezető

ORCID: 0009-0001-2341-7525 

Absztrakt:

Az EU kritikus szervezetek ellenálló képességére vonatkozó irányelve, valamint a hazai szabályozás ma már részletesen tartalmazza a kockázat alapú gondolkodással, továbbá az összveszély megközelítéssel kapcsolatos követelményeket.

A szerzők ezen fogalmak fejlődésének rövid ismertetését és elemzését követően gyakorlati példákon és ajánlásokon keresztül mutatják be, hogy a kritikus, valamint az ország védelme és biztonsága szempontjából jelentős szervezeteknél mely módon alkalmazhatóak a gyakorlatban az ellenálló képesség fejlesztéséhez kapcsolódó egyes módszertani megoldások.

Kulcsszavak: reziliencia, ellenálló képesség, kritikus szervezet, kritikus infrastruktúra, ellenálló képességi mátrix, kockázat, kockázat alapú szemlélet, kockázat alapú gondolkodás, összveszély megközelítés

Abstract:

The EU Directive on the resilience of critical entities, as well as Hungarian regulations, now include detailed requirements for risk-based thinking and the all-hazard approach.

The authors, after a brief description of the development of these concepts, present how specific methodological solutions related to the development of resilience in critical entities can be applied in practice, through practical examples and recommendations.

Keywords: resilience, resistance ability, critical organization, critical infrastructure, CER Directive, member state regulation

1. BEVEZETÉS

Magyarországon 2025. január 1-én hatályba léptek (a közigazgatási bírságra vonatkozó rész kivételével, amely január 5-én) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács (EU) 2022/2557 irányelv (CER irányelv) rendelkezéseinek nemzeti jogrendbe átültetését biztosító jogszabályok. A CER irányelvben meghatározott követelmények, célkitűzések átültetését, továbbá a nemzeti sajátosságokra figyelemmel kialakított követelmény rendszert a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény (a továbbiakban: Kszetv.), a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról szóló 474/2024. (XII. 31.) Korm. rendelet (a továbbiakban: Vhr.) előírásai, valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (a továbbiakban: Vbö.) módosításai, különösen az V/A. fejezete és az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről szóló 475/2024. (XII. 31.) Korm. rendelet tartalmazzák. A Vbö. az ország védelme és biztonsága szempontjából jelentős szervezetekre és infrastruktúrákra – egyes kivétellel – a Kszetv.-ben foglaltakat rendeli alkalmazni, ezzel egyenértékűnek tekinti a két szabályozás alapján kijelölt szervezeteket és infrastruktúrákat, ezért a továbbiakban együttesen a kritikus szervezetek elnevezést alkalmazzuk a szabályok ismertetése során.

2. A KOCKÁZAT-ALAPÚ MEGKÖZELÍTÉS

A kockázatok azonosítása, értékelése és kezelése a védelmi tervezési feladatok alapja. A kockázat alapú megközelítés hazánkban a kezdetektől megjelenik elsősorban a megelőzési és felkészülési feladatokban, amelyet jól reprezentál a tűzvédelmi kockázati osztályokkal és egységekkel, vagy a települések polgári védelmi, később katasztrófavédelmi osztályba sorolásával összefüggő módszertan. A 2000. január 01-jétől 2011. december 31-ig hatályos katasztrófavédelmi törvény a kihirdetési szövegében a következő fogalmat vezette be: „Kockázat: egy adott területen adott időtartamon belül, meghatározott körülmények között bekövetkező, egészséget, illetve környezetet károsító veszély megvalósulásának valószínűsége.”¹

A jogszabályok fejlődése során a kezdeti értelmező rendelkezés módosult, a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzésén túl a katasztrófák elleni védekezés rendszerében általános fogalomná vált, amelyet a 2012. január 01-től hatályba lépő katasztrófavédelmi törvény is továbbvitt és amely a módosítását követően jelenleg az alábbi szöveggel hatályos: „Kockázat: egy adott területen adott időtartamon belül vagy meghatározott körülmények között jelentkező egészség-, illetve környezetkárosító hatás valószínűsége.”² A kockázat alapú szemlélet erősödését támasztja alá, hogy e hatályos katasztrófavédelmi törvény polgári védelmi feladatként határozza meg a települések kockázatértékelésén alapuló veszélyeztetettségének felmérését, továbbá a végrehajtási kormányrendelet³ részletesen kidolgozott kockázatbecslési eljárást és azon alapuló veszélyelhárítási tervezési folyamatot is tartalmaz. A kritikus infrastruktúrákra vonatkozó szabályozás előzményei során Magyarországon a kockázat-alapú szemlélet a végrehajtásban jelent meg. A korábban hatályos törvény alapján 2013. március 01. és 2024. december 31. között a létfontosságú rendszerelemek védelmével kapcsolatos előírások szerint ez a védelmi tevékenység – mások mellett – a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányult.⁴

¹ a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezéséről szóló 1999. évi LXXIV. törvény 3. § m) pontja, MK 1999/60. szám

² a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 3. § 11. pont

³ 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

⁴ a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 1. §

A CER irányelv 16. cikke alapján a végrehajtás előmozdítása érdekében a tagállamok – amennyiben az hasznos, és anélkül, hogy előírnák vagy előnyben részesítenék egy konkrét technológia-típus alkalmazását – ösztönzik a kritikus szervezetekre alkalmazandó biztonsági és reziliencia-intézkedések szempontjából releváns, európai és nemzetközi szabványok és műszaki előírások alkalmazását.

A Nemzetközi Szabványügyi Szervezet (ISO) egyik minőségirányítási szabványában is megjelenő módszer a kockázat-alapú megközelítés, amelynek hangsúlyos eleme, hogy a szervezetek azonosítsák és értékeljék a kockázatokat és lehetőségeket, amelyek befolyásolják a minőségirányítási rendszer teljesítményét, így proaktívvá válhatnak és jobban felkészülnek a jövőbeli kihívásokra. Mindez rendszeres felülvizsgálatot és aktualizálást is hordoz magában, továbbá a kockázatok kezelésére alkalmazható stratégiák biztosítják a potenciális negatív hatások minimalizálását. [1]

A CER irányelv a kritikus infrastruktúrák ellenálló képességeként (reziliencia) definiálja valamely kritikus szervezet azon képességét, hogy megelőzzön egy eseményt, azzal szemben védekezzen, arra reagáljon, annak ellenálljon, azt enyhítse, tompítsa, ahhoz alkalmazkodjon, és abból helyreálljon. A képesség fejlesztésére vonatkozó intézkedések akkor határozhatóak meg, ha a szervezet előzetesen felméri a fenyegetéseket és kockázatokat. Irányadó fogalommeghatározások mindehhez az irányelvben a következők:

- esemény: olyan esemény, amely alkalmas arra, hogy jelentős zavart okozzon, vagy amely zavart okoz valamely alapvető szolgáltatás nyújtásában, beleértve, amikor érinti a jogállamiság védelmét biztosító nemzeti rendszereket;
- kockázat: valamely esemény által okozott potenciális veszteség vagy zavar, és azt az ilyen veszteség vagy zavar nagyságrendjének és az esemény bekövetkezési valószínűségének kombinációjaként kell kifejezni;
- kockázatértékelés: átfogó eljárás, amely valamely kockázat jellegének és mértékének meghatározására irányul, olyan potenciális releváns fenyegetések, sebezhetőségek és veszélyek azonosításával és elemzésével, amelyek eseményt idézhetnek elő, valamint az alapvető szolgáltatás nyújtása tekintetében felmerülő, az említett esemény által okozott potenciális veszteség vagy zavar értékelésével.⁵

A Magyarországon 2025. január 01-től a kritikus szervezetek üzemfolytonos és biztonságos működése érdekében alkalmazandó normákban rendszerszinten elvárás a kockázat alapú gondolkodás. A Kszetv. értelmező rendelkezései szerint⁶ a kockázat alapú gondolkodás a kockázatmenedzsment működtetése során egyfajta szemlélet alkalmazása, amelyben a kockázatok azonosításának, a kockázatelemzésnek, a kockázatértékelésnek és a kockázatkezelésnek olyan általános folyamata valósul meg, amely célja, hogy megalapozott döntést hozzanak arról, hogyan kezeljék a lehető legmagasabb szinten a felmerülő kockázatokat, mindezt hitelesen dokumentált információ, azaz az ellenálló képességi terv és ellenálló képességi mátrix formájában.

A kockázat alapú gondolkodás gyakorlati végrehajtását jelenti a kritikus szervezet számára az előírás, amely szerint a külső és belső környezete alapján felméri, azonosítja, értékeli és kezeli mindazon kockázatokat, amelyek a kritikus szervezet és kritikus infrastruktúra biztonságos és üzemfolytonos működésére, az alapvető szolgáltatások nyújtásának folytonosságára hatással lehetnek.

⁵ CER irányelv 2. cikk 2-3. és 6-7. pontok

⁶ Kszetv. 3. § 21. pont

A jogalkalmazói gyakorlat szempontjából kiemelt jelentőségű, hogy a Kszetv. értelmező rendelkezései pontosan meghatározzák a kockázat és annak kezelésével összefüggő fogalmakat a 3. § 20-25. pontjaiban az alábbiak szerint:

- kockázat: valamely esemény által okozott veszteség vagy zavar lehetősége, amelyet az ilyen veszteség vagy zavar mértékének, és az esemény bekövetkezési valószínűségének kombinációjaként kell kifejezni,
- kockázatazonosítás: az a folyamat, amelynek célja olyan kockázatok felkutatása, felismerése és leírása, amelyek befolyásolhatják a szervezeti célok elérését,
- kockázatelemzés: az a folyamat, amely célja a kockázat jellegének és jellemzőinek megértése, a kockázati szint megállapítása, a bizonytalanságok, a kockázati források, a következmények, a valószínűség, az események, a forgatókönyvek, az intézkedések valamint azok eredményességének részletes vizsgálata,
- kockázatértékelés: az azonosított kockázatok átfogó elemzésének olyan folyamata, amelyben a kockázatelemzés eredményeinek az előzetesen meghatározott kritériumokkal való összehasonlítása során megállapítható, hogy hol szükséges további intézkedés,
- kockázatkezelés: kockázatmenedzsment által alkalmazott, jóváhagyott döntésen alapuló tervezett folyamat, módszer vagy eszköz, amely egy várható negatív esemény bekövetkezésének valószínűségét, a felmerülő kockázatok hatásait és a kitettséget olyan módon befolyásolja, hogy általa csökkenjen a kockázatpotenciál, valamint a lehetséges kár hatásait enyhítse, ellensúlyozza.

Mely folyamattal juttatja el a kockázat alapú gondolkodás a kritikus szervezeteket a saját kritikus infrastruktúrája jellemzőinek megfelelő egyedi kockázat kezelési módszerekhez? A hatályos szabályozók alapján a kritikus szervezet a nemzeti kockázatértékelés figyelembevételével alakítja ki a kockázatértékelését, az ellenálló képességi mátrixot és az ellenálló képességi intézkedéseit. E lépcsőzetes építkezéshez a törvényi és kormányrendeleti szabályozás mellett rendelkezésre áll Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékelése és nemzeti stratégiája, amelyeket kormányhatározatokkal⁷ hirdettek ki.

Az egyes kritikus szervezet általi kockázatértékeléseknek a nemzeti kockázatértékelés általános és ágazati kockázatértékelésére, további ágazati függőségekre és más ágazatok kitettségére, összességében az ágazatok közötti függőségekre is ki kell terjednie. [2]

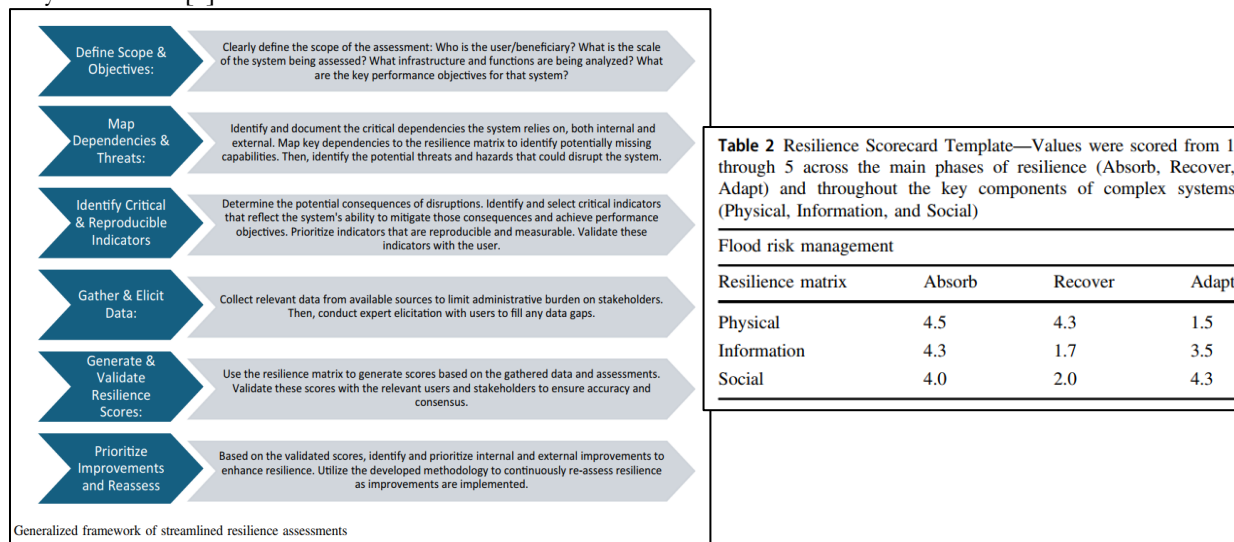
3. AZ ELLENÁLLÓ KÉPESSÉGI MÁTRIX

2013-ban Linkov és kutatótársai egy gyakorlatban is működőképes, mérőszámokat alkalmazó keretrendszer kivántak fejleszteni az ellenálló képességi intézkedések megalapozásához. A kutatás eredményeként egy komplex rendszerekben is alkalmazható ellenálló képességi mátrixot alkottak és tettek közzé, amely az eseménykezelés ciklusai és az egyes alrendszerek szerint az ellenálló képességi funkciókat térképezi fel és mutat rá a szükséges fejlesztendő területekre. A kutatók hangsúlyozták a holisztikus megközelítést, a rendszerszemléletet és a függőségek figyelembevételét, valamint a különböző tudományterületek együttműködésének szükségességét. [3]

A katasztrófavédelmi eseményekre kidolgozott ellenálló képességi mátrix publikálása lehetővé tette annak továbbfejlesztését és adaptációját. 2025-ben jelent meg Watson és kutatótársai (köztük I. Linkov is) tudományos közleménye, amelyben már az egyszerűsítés igénye alapján készített új módszertant mutattak be.

⁷ 1191/2025. (VI. 5.) Korm. határozat és 1192/2025. (VI. 5.) Korm. határozat

A kutatás során egy módosított analitikus hierarchikus eljárást (AHP) alkalmaztak, de az érdekeltek számára ellenálló képességi mátrix-szal ábrázolták egy árvízi kockázat kezelési rendszer ellenálló képességi kritériumainak értékelését. Eredményként megállapították, hogy a kidolgozott egyszerűsített megoldás általános, szisztematikus megközelítést követ, az időbeliség-alapú vizsgálat praktikus alternatíva lehet egy előzetes, átfogóbb reziliencia értékeléshez, de nem célja azok helyettesítése. [4]



1. ábra: Watson és kutatótársai által alkalmazott egyszerűsített módszertan (Forrás: ld. [3])

A Magyarországon kijelölt kritikus szervezetek számára a hazai jogszabályi környezet mellett a BM OKF aktív közreműködése támogatja a kockázat alapú gondolkodás gyakorlati megvalósulását.

A kritikus szervezet vezetője – az ellenálló képességért felelős vezető kezdeményezésével – készíti el a szervezetre és a kijelölt kritikus infrastruktúrákra vonatkozó ellenálló képességi mátrixot, amelynek egyes lépései a következők:

- a kritikus szervezet és a kritikus infrastruktúra azon fenyegetettségének, illetve fenyegetést jelentő kockázatainak felmérése és dokumentálása, amelyek rendkívüli eseményhez⁸ vezethetnek,
- az így azonosított fenyegetések káros hatásainak és azok mértékének, továbbá bekövetkezési valószínűségének, valamint a kitettség mértékének meghatározása,
- az előzőek alapján a kritikus szervezet és a kritikus infrastruktúra ellenálló képességi felkészültségének vizsgálata és annak eredménye szerint intézkedések a fejlesztésére.

Összességében az ellenálló képességi mátrix a kritikus szervezet és kritikus infrastruktúra ellenálló képességével összefüggő kockázatok, a kockázatok következményei, hatásuk, gyakoriságuk, a szervezet kitettségének megjelenítésére, a kockázat jelentőségére vonatkozó értékelés és a kockázatok kezelésének, a maradványkockázatok megjelenítésének módja.⁹

⁸ Kszetv. 3. § 32. pont szerint *rendkívüli esemény*: olyan esemény, amely eléri a rendkívüli esemény kezelésében érintett szervek irányába történő bejelentés kormányrendeletben vagy annak hiányában a kritikus szervezet ellenálló képességi tervében meghatározott küszöbértékét, és

a) a kritikus infrastruktúra vagy az alapvető szolgáltatás olyan mértékű károsodását, sérülését, minőségének romlását vagy mennyiségének fennakadását okozza, amely a kritikus infrastruktúra vagy az alapvető szolgáltatás megszűnését, kiesését eredményezi, vagy

b) a kritikus infrastruktúra vagy az alapvető szolgáltatás megszűnését, kiesését nem eredményezi, de a kritikus infrastruktúra vagy az alapvető szolgáltatás megszűnésének, kiesésének elhárításához szükségessé vált a rendkívüli esemény kezelésében érintett más szervek közreműködése.

⁹ Kszetv. 3. § 10. pont

Az ellenálló képességi mátrix az ellenálló képességi terv kötelezően csatolt, állandó melléklete az általános és ágazatspecifikus kockázatokkal. A szempontrendszer részét képezik a kötelezően vizsgálendő általános és ágazati kockázatok, valamint a szervezet által azonosított egyéb kockázatok. A mátrix elkészítéséhez kiindulópontként szolgál a nemzeti kockázatértékelés¹⁰, a BM OKF honlapján közzétett ellenálló képességi mátrix mintadokumentum és kockázatelemzési segédlet, valamint a jogszabály által megnevezett¹¹, alapvetően vizsgálendő témakörök:

- meteorológia kockázatok,
- geológiai kockázatok,
- humán kockázatok,
- technikai kockázatok,
- technológiai kockázatok,
- tűzeseti kockázatok,
- informatikai kockázatok (a pénzügyi ágazatra vonatkozó egyes kivételes szabályok figyelembevételével¹²)
- veszélyes anyagokkal és technológiákkal kapcsolatos kockázatok,
- ágazatspecifikus kockázatok (az ágazati szakhatóság és az energetikai ágazati kijelölő hatóság készíti).¹³

A	B	C	D	E	F	G	H	I	J
		Valószínűség:		Kockázat értékek kezelése:					
1	nagyon ritka	10 éven belül legalább egyszer bekövetkezik		azonnali beavatkozást igénylő, nem elfogadható kockázat	48-96				
2	ritka	5 éven belül legalább egyszer bekövetkezik		rövidtávon intézkedést igénylő kockázat	15-42				
3	alkalmankénti	3 éven belül többször bekövetkezik		intézkedést igénylő kockázat	6-14				
4	gyakori	1 éven belül legalább egyszer bekövetkezik		elemzés alapján elfogadható kockázat	2-5				
5	nagyon gyakori	1 éven belül többször bekövetkezik		elhanyagolható kockázat	1				
		Hatás:		Kockázat értéke = Valószínűség x (Hatás + Kitérttség)	elhanyagolható	alacsony	közepes	magas	katasztrofális
1	elhanyagolható	- működésre: csekély negatív hatás a belső folyamatokra (1 napon belül megoldható) - személyre: csekély sérülés vagy egészségkárosodás - vagyoni: csekély, vagyoni kár nem mérhető - környezetre: csekély, környezeti károsodás nem keletkezik - hírnévre: csekély, közvélemény figyelmét nem kelti fel - működésre: alacsony negatív hatás a belső folyamatokra (1 napon túl, 5 napon belül megoldható) - személyre: kisebb sérülés vagy egészségkárosodás - vagyoni: kis mértékű, a vagyoni kár a szervezet éves költségvetésének 1 %-át el nem érő összeg - környezetre: korlátozott, a környezetben nem tartós károsodás keletkezik - hírnévre: korlátozott, kizárólag a szervezet belső megítélését érinti, a helyi média figyelmét felkelti - működésre: negatív hatás van a belső folyamatokra (5 napon túl oldható meg) - személyre: súlyos sérülés vagy egészségkárosodás - vagyoni: helyi, a vagyoni kár a szervezet éves költségvetésének 1 %-át meghaladó, de 5 %-át el nem érő összeg - környezetre: helyi, hatással van az infrastruktúrán kívüli környezetre is - hírnévre: helyi, széleskörű figyelem a helyi médiában és közösségben - működésre: jelentősen korlátozott működés - személyre: egy személy halálos balesete vagy tartós egészségkárosodása - vagyoni: súlyos, a vagyoni kár a szervezet éves költségvetésének 5 %-át meghaladó, de 25 %-át el nem érő összeg - környezetre: súlyos környezeti károsodás - hírnévre: országos kiterjedésű aggodalom a médiában és közösségben	nagyon gyakori	5	10	15	30	70	
2	alacsony	- működésre: kisebb sérülés vagy egészségkárosodás - személyre: kisebb sérülés vagy egészségkárosodás - vagyoni: korlátozott, a vagyoni kár a szervezet éves költségvetésének 1 %-át el nem érő összeg - környezetre: korlátozott, a környezetben nem tartós károsodás keletkezik - hírnévre: korlátozott, kizárólag a szervezet belső megítélését érinti, a helyi média figyelmét felkelti - működésre: negatív hatás van a belső folyamatokra (5 napon túl oldható meg) - személyre: súlyos sérülés vagy egészségkárosodás - vagyoni: helyi, a vagyoni kár a szervezet éves költségvetésének 1 %-át meghaladó, de 5 %-át el nem érő összeg - környezetre: helyi, hatással van az infrastruktúrán kívüli környezetre is - hírnévre: helyi, széleskörű figyelem a helyi médiában és közösségben - működésre: jelentősen korlátozott működés - személyre: egy személy halálos balesete vagy tartós egészségkárosodása - vagyoni: súlyos, a vagyoni kár a szervezet éves költségvetésének 5 %-át meghaladó, de 25 %-át el nem érő összeg - környezetre: súlyos környezeti károsodás - hírnévre: országos kiterjedésű aggodalom a médiában és közösségben	gyakori	4	8	12	24	48	
3	közepes	- működésre: kisebb sérülés vagy egészségkárosodás - személyre: kisebb sérülés vagy egészségkárosodás - vagyoni: korlátozott, a vagyoni kár a szervezet éves költségvetésének 1 %-át el nem érő összeg - környezetre: korlátozott, a környezetben nem tartós károsodás keletkezik - hírnévre: korlátozott, kizárólag a szervezet belső megítélését érinti, a helyi média figyelmét felkelti - működésre: negatív hatás van a belső folyamatokra (5 napon túl oldható meg) - személyre: súlyos sérülés vagy egészségkárosodás - vagyoni: helyi, a vagyoni kár a szervezet éves költségvetésének 1 %-át meghaladó, de 5 %-át el nem érő összeg - környezetre: helyi, hatással van az infrastruktúrán kívüli környezetre is - hírnévre: helyi, széleskörű figyelem a helyi médiában és közösségben - működésre: jelentősen korlátozott működés - személyre: egy személy halálos balesete vagy tartós egészségkárosodása - vagyoni: súlyos, a vagyoni kár a szervezet éves költségvetésének 5 %-át meghaladó, de 25 %-át el nem érő összeg - környezetre: súlyos környezeti károsodás - hírnévre: országos kiterjedésű aggodalom a médiában és közösségben	alkalmankénti	3	6	9	18	36	
6	magas	- működésre: kisebb sérülés vagy egészségkárosodás - személyre: kisebb sérülés vagy egészségkárosodás - vagyoni: korlátozott, a vagyoni kár a szervezet éves költségvetésének 1 %-át el nem érő összeg - környezetre: korlátozott, a környezetben nem tartós károsodás keletkezik - hírnévre: korlátozott, kizárólag a szervezet belső megítélését érinti, a helyi média figyelmét felkelti - működésre: negatív hatás van a belső folyamatokra (5 napon túl oldható meg) - személyre: súlyos sérülés vagy egészségkárosodás - vagyoni: helyi, a vagyoni kár a szervezet éves költségvetésének 1 %-át meghaladó, de 5 %-át el nem érő összeg - környezetre: helyi, hatással van az infrastruktúrán kívüli környezetre is - hírnévre: helyi, széleskörű figyelem a helyi médiában és közösségben - működésre: jelentősen korlátozott működés - személyre: egy személy halálos balesete vagy tartós egészségkárosodása - vagyoni: súlyos, a vagyoni kár a szervezet éves költségvetésének 5 %-át meghaladó, de 25 %-át el nem érő összeg - környezetre: súlyos környezeti károsodás - hírnévre: országos kiterjedésű aggodalom a médiában és közösségben	ritka	2	4	6	12	24	
12	katasztrofális	- működésre: kisebb sérülés vagy egészségkárosodás - személyre: kisebb sérülés vagy egészségkárosodás - vagyoni: korlátozott, a vagyoni kár a szervezet éves költségvetésének 1 %-át el nem érő összeg - környezetre: korlátozott, a környezetben nem tartós károsodás keletkezik - hírnévre: korlátozott, kizárólag a szervezet belső megítélését érinti, a helyi média figyelmét felkelti - működésre: negatív hatás van a belső folyamatokra (5 napon túl oldható meg) - személyre: súlyos sérülés vagy egészségkárosodás - vagyoni: helyi, a vagyoni kár a szervezet éves költségvetésének 1 %-át meghaladó, de 5 %-át el nem érő összeg - környezetre: helyi, hatással van az infrastruktúrán kívüli környezetre is - hírnévre: helyi, széleskörű figyelem a helyi médiában és közösségben - működésre: jelentősen korlátozott működés - személyre: egy személy halálos balesete vagy tartós egészségkárosodása - vagyoni: súlyos, a vagyoni kár a szervezet éves költségvetésének 5 %-át meghaladó, de 25 %-át el nem érő összeg - környezetre: súlyos környezeti károsodás - hírnévre: országos kiterjedésű aggodalom a médiában és közösségben	nagyon ritka	1	2	3	6	12	
		Kitérttség:							
0	nincs	nincs kitértég							
1	egyrányú	egy fél fele van kitértég							
2	többirányú	több fél fele van kitértég							
3	teljesen	teljesen van kitértég							
		<i>a kitértég növeli a hatást, de csökkenti a gyakoriságot</i>							

2. ábra: Értékkészlet az ellenálló képességi mátrixhoz (Forrás: BM OKF¹⁴)

A fentiek alapján azonosított kockázatok esetében alkalmazható kockázatkezelési megoldások:

- kockázat csökkentése a védelmi intézkedések bevezetésével és alkalmazásával,
- kockázat elkerülése,
- kockázat átruházása,
- kockázat elfogadása (a kritikus szervezet ellenálló képességéért felelős vezető indokolása szükséges).

¹⁰ Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékeléséről szóló 1191/2025. (VI. 5.) Korm. határozat

¹¹ Vhr. 15. § (6) bekezdése

¹² 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 szóló, 2022. december 14-i (EU) 2022/2554 parlamenti és tanácsi rendeletben (a továbbiakban: DORA rendelet) meghatározottak szerint, az ott meghatározott módon szükséges elsődlegesen értékelni és kezelni

¹³ a kockázatértékelés egymáshoz kapcsolódásáról ld. Mógor J., & Angyal I. (2025). A kritikus infrastruktúrák ellenálló képesség fejlesztését célzó szabályozás mérőkövetői 2022-2025. Védelem Tudomány a Katasztrófavédelem Online Szakmai, tudományos folyóirata, 10(2), 11-21. <https://doi.org/10.61790/vt.2025.19455>

¹⁴ Letölthető EKM minta: <https://katasztrofavedelem.hu/35635/letoltheto-dokumentumok-es-kitoltesi-segedletek>

4. AZ ELLENÁLLÓ KÉPESSÉGI MÁTRIX GYAKORLATI ALKALMAZÁSA

A kockázatelemzés módszertanának kronológiai fejlődése az 1980–90-es években kezdődött az alapfogalmak tisztázásával (kockázat definíciója, bizonytalanság típusai, kezelési szintek), a 2000–2010-es években széles körben terjedt el az alkalmazása különböző ágazatokban (energia, egészségügy), majd a 2020-as években megjelent a kockázatelemzés új fókusza, úgy mint a mesterséges intelligencia rendszerek kockázata, ipari 4.0 és 5.0 komplexitás, gépi tanulás alkalmazása egyes kockázatok értékelésében.

1981-ben Kaplan és Garrick: „On the Quantitative Definition of Risk” című publikációja vezette be a kockázat-tripletet (risk triplet), azaz: mi történhet (scenario), milyen valószínűséggel (probability), és milyen következménnyel (consequence). Ezzel lefektették a kockázatelemzés egységes, formális alapját. [5] 1990-ben George E. Apostolakis a The Concept of Probability in Safety Assessments of Technological Systems című cikkében azt vizsgálta, hogy milyen módon kell értelmezni és alkalmazni a valószínűségi fogalmat olyan technológiai rendszerek kockázatának értékelésekor, ahol a ritka események következményei súlyosak lehetnek, kiemelve a szakértői ítéletek és statisztikai adatok kombinációjának fontosságát. [6] 2022-ben Zhang és munkatársai rámutattak, hogy a „mesterséges intelligencia és gépi tanulás alkalmazása kockázaterzékeny környezetben még gyerekcipőben jár, mivel hiányzik egy szisztematikus keretrendszer a kockázat, a bizonytalanság és azok potenciálisan katasztrofális következményeinek kezelésére.” [7]

Napjainkban az ellenálló képességi mátrix nem pusztán adminisztratív kötelezettség, hanem olyan döntéstámogató eszköz, amely képes átfogóan megjeleníteni a kritikus szervezet kitétségeit, a fenyegetések lehetséges következményeit, valamint a szervezet válaszadó és helyreállító képességeit.

4.1 A gyakorlati alkalmazás három kiemelt szempontja

a) Az összveszély megközelítés alkalmazása

A kockázatok ritkán jelennek meg önmagukban. Egy rendkívüli esemény (pl. árvíz, kibertámadás, járvány) következményei láncreakció-szerűen érinthetnek több ágazatot, vagy akár több tagállamot is. Az ellenálló képességi mátrixban ezért célszerű alkalmazni az összveszély (all-hazard) szemléletet, amely az egyidejű, egymásra ható, egymást erősítő kockázatok hatásait is vizsgálja és amelyet a CER irányelv is megfogalmaz (ld. még [3], [4]).

Saját eljárásrendként javasolt a mátrix kitöltése során az ellenálló képességi terv függőségeket vizsgáló fejezetének folyamatos figyelembevétele, amely bemutatja, hogy az adott szervezet működése mely más ágazatokhoz kötődik (pl. energia, közlekedés, egészségügy). Az ebből kialakított függőségi mátrix kiegészítésként segíthet előre jelezni, hogy mely egyéb kockázatok válhatnak jelentős hatásúvá az azonosított 92 kockázaton túl.

b) Egyenértékűség más szabályozás alatt készült kockázatértékelésekkel

Több kritikus szervezet már jelenleg is végez kockázatértékelést más jogszabályi kötelezettségek alapján (pl. Mvt. szerinti munkavédelmi kockázatértékelés, veszélyes üzemek biztonsági jelentése Seveso III., NIS2 irányelv szerinti információbiztonsági szabályzat és kockázatelemzés).

A gyakorlatban ezek az értékelések összehangolhatók a jogszabályok alapján kötelező ellenálló képességi mátrixszal. A szabályozások közötti átjárhatóság nemcsak adminisztratív tehercsökkentést eredményez, hanem elősegíti a holisztikus kockázatmenedzsment kialakítását.

Saját gyakorlati tapasztalat alapján például egy élelmiszer-feldolgozó üzemnél a HACCP és az élelmiszerbiztonsági auditok eredményei (mikrobiológiai kockázatok, allergénkezelés hiányosságai) közvetlenül beépíthetők az intézmény ellenálló képességi vizsgálatába a kockázatok közé, így ugyanazon biztonsági eseményhez nem kell külön, párhuzamos kockázatelemzést, valamint intézkedési tervet készíteni.

c) A kockázatkezelés döntéstámogató folyamata

A kockázatok kezelésénél (a csökkentés, elkerülés, átruházás és elfogadás kategóriáin belül) a gyakorlati végrehajtást célszerű súlyozási eljárással támogatni. Mint ahogyan a nemzeti kockázattertelékeléshez is, minden kockázati kategóriához rendelhető egy súlyszám (pl. 1–5 skálán a gyakoriságra, hatásra, helyreállíthatóságra). A szervezet így számszerűsíthető módon prioritizálhatja a fejlesztendő területeket.

4.2 Saját tapasztalat alapján ismertetett gyakorlati példák

Az egészségügyben bevált alternatíva a Hiba-mód és hatáselemzés (FMEA) a kockázatokat valószínűség, hatás és felfedezhetőség alapján számszerűsítik, és a magas RPN (Risk Priority Number) értékekhez automatikusan kötelező beavatkozások kapcsolódnak.

$RPN = \text{Kockázati prioritási szám}$

Az FMEA-ban három tényezőt szorzunk össze:

$RPN = \text{Súlyosság (S)} \times \text{Gyakoriság / Előfordulás (O)} \times \text{Felfedezhetőség / Detection (D)}$

A módszer fejlesztési lehetőségei

Integrált ellenálló képességi dashboard: a mátrix adatai vizuálisan megjeleníthetők (pl. kockázati hálón). Ez támogatja a vezetői döntést és a gyors reagálást.

Rendszeres frissítés: a Kszetv. alapján az ellenálló képességi mátrixot legalább évente felül kell vizsgálni. Tapasztalataink szerint azonban a gyorsan változó fenyegetettségek (pl. kibertámadások) miatt érdemes negyedéves „gyorsfelméréseket” is bevezetni a jelentős kockázatok esetében.

Összevethetőség: hosszú távon a különböző kritikus szervezetek mátrixai alapján kialakítható egy országos szintű benchmarking rendszer, amely segíti a közös gyengeségek azonosítását.

I. Példa: Egészségügy ágazat, összveszély szemlélet:

Az egészségügy ágazat egyik legfontosabb jellemzője, hogy a működés folytonossága közvetlenül hat az emberi élet védelmére. Egy rendkívüli esemény gyakran nem önmagában, hanem egymást erősítő hatásokkal jelentkezik dominó elv formájában. Az alábbi eset bemutatja, miként érvényesíthető az **összveszély megközelítés** az ellenálló képességi mátrixban.

Példaszituáció:

Egy kórházban áramszünet következik be, amelyet egy szélsőséges időjárási helyzet (vihar) idéz elő. Az áramszünet következtében:

- a fő áramellátás kiesik,
- az IT-rendszerek egy része leáll,
- az ellátásban kulcsszerepet játszó eszközök (pl. lélegeztetők, CT, MRI, laborautomaták, elektromos műtéti feltételek) nem működnek,
- a személyzet terhelése megnő, mert a kézi dokumentációra kell visszaállni, miközben a betegforgalom nem csökken, csak manuális reanimációt tudnak alkalmazni rövid ideig, lelassul a diagnosztika, téves diagnózisokat állapíthatnak meg a képalkotás hiányában.

Azonosított kockázatok (mátrix fő kategóriái szerint):

- Meteorológiai kockázat: vihar okozta áramszünet.
- Technikai kockázat: áramellátás megszűnése, aggregátor hibás indulása.
- Informatikai kockázat: IT-rendszerek kiesése.
- Humán kockázat: egészségügyi személyzet túlterheltsége, döntési hibák lehetősége.
- Ágazatspecifikus kockázat: betegellátás folyamatosságának megszűnése (pl. műtétek elhalasztása, sürgősségi ellátás romlása).

Függőségek bemutatása:

- Energiaellátás ↔ Informatikai rendszerek működése
- IT-rendszerek ↔ betegadatok elérhetősége
- Humán erőforrás ↔ alternatív eljárások gyors bevezetése
- Orvostechonikai eszközök ↔ közvetlen betegbiztonság

Alkalmazott kockázatkezelési intézkedések:

- Kockázat csökkentése: folyamatos aggregátor karbantartás, redundáns IT-rendszerek, kézi dokumentációs protokoll.
- Kockázat elkerülése: a műtétek és diagnosztikai vizsgálatok előzetes áttervezése viharriasztás idejére.
- Kockázat átruházása: szerződés harmadik féllel mobil áramfejlesztő gyors biztosítására.
- Kockázat elfogadása: bizonyos nem sürgős beavatkozások halasztása (indoklással).

Következtetés:

A példán keresztül látható, hogy az **összveszély szemlélet és a mátrix módszer** kombinációja lehetővé teszi a kórház számára:

- a láncreakció-szerű események előzetes feltérképezését,
- a legsúlyosabb hatású kockázatok rangsorolását,
- a vezetői döntések gyors és dokumentált alátámasztását.

II. Példa: Informatikai ágazat, összveszély szemlélet

Az informatika és a hálózati alapú szolgáltatások (pl. távközlés, felhőszolgáltatás, adatközpontok működése) szinte minden ágazathoz kötődnek. Az adatvesztés, szolgáltatás-kiesés vagy hálózati zavar láncreakció-szerű következményeket okozhat más ágazatokban, így a NIS2 irányelv és a Kszetv. szerinti kockázat-alapú gondolkodás itt különösen hangsúlyos.

Példaszituáció:

Egy adatközpontot célzott kibertámadás ér, amely:

- leállítja a virtualizációs környezet egy részét,
- hozzáférhetlenné teszi a biztonsági mentéseket,
- túlterheli a hűtőrendszert, ami a fizikai infrastruktúrában is hibát idéz elő,
- a támadás idején éppen beszállítói szolgáltatásfrissítés zajlik, amely hibás konfiguráció miatt megnöveli a kiesés időtartamát.

Az összveszély helyzet elemei: informatikai, technikai és beszállítói lánc kockázatok egyidejű hatása.

Azonosított kockázatok:

- Informatikai kockázat: célzott kibertámadás, adatszivárgás, DDoS.
- Technikai kockázat: hűtőrendszer meghibásodása, hardver túlterhelés.

- Humán kockázat: hibás konfiguráció a beszállítói frissítés során.
- Beszállítói kockázat: külső szolgáltató késedelmes reagálása.
- Ágazatspecifikus kockázat: ügyfeladatok elvesztése, alapvető szolgáltatások (pl. banki tranzakciók, állami rendszerek) elérhetetlensége.

Függőségek bemutatása:

- IT-rendszerek ↔ fizikai infrastruktúra (hűtés, energiaellátás)
- Külső szolgáltatók ↔ frissítések, karbantartások időzítése
- Adatbiztonság ↔ kritikus ágazati ügyfeladatok (pl. egészségügy, bank)
- Hálózat ↔ országos szintű szolgáltatás folytonossága

Alkalmazott kockázatkezelési intézkedések:

- Kockázat csökkentése: többszintű biztonsági mentések (offline/offsite backup), kiberbiztonsági gyakorlatok, szigorú változásmenedzsment.
- Kockázat elkerülése: beszállítói frissítések időzítése alacsony kockázatú időszakban, redundáns hűtőrendszer.
- Kockázat átruházása: kiberbiztosítás, SLA-k a beszállítókkal.
- Kockázat elfogadása: alacsony hatású kiesések esetén (pl. nem kritikus ügyfeladatbázis).

Következtetés:

- A kiber- és beszállítói kockázatok a reziliencia egyik legnagyobb kihívását jelentik, amelyben az ellenálló képességi mátrix segít:
- feltérképezni a technológiai és humán tényezők összefüggéseit,
- számszerűsíteni a kritikus pontokat,
- alátámasztani a vezetői döntést a kockázatkezelési stratégiák között (csökkentés, elkerülés, átruházás, elfogadás).

Ez a módszer összhangban van a NIS2 irányelv, a CER irányelv és a Kszetv. követelményeivel, valamint elősegíti a valósidejű rezilienciafejlesztést az IT ágazatban.

4.3 Gyakorlati ajánlások a kritikus szervezetek számára

A kockázat alapú gondolkodás sikeres bevezetése és működtetése érdekében ajánlott az alábbi módszerek alkalmazása:

Rendszeres frissítés és gyorsfelmérések: Az ellenálló képességi mátrixot évente kötelező felülvizsgálni (Kszetv.), azonban a gyorsan változó fenyegetések (pl. kibertámadások, szélsőséges időjárási események) miatt ajánlott negyedéves mini-kockázatfelmérések végrehajtása is.

Gyakorlatok és szimulációk bevezetése: Az azonosított kockázatokra épülő gyakorlatok (pl. áramkimaradás, kibertámadás, beszállítói lánc megszakadása) elősegítik, hogy a szervezet a gyakorlatban, valós végrehajtási elemekkel is tesztelje ellenálló képességét, amelyek illeszkednek a jogszabályok szerinti felkészülési és helyreállítási kötelezettségekhez.

Más szabályozások szerinti kockázatértékelések folyamatának integrálása: A munkavédelmi, a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzése (Seveso III), NIS2 vagy ágazati szabályozás alapján készült kockázatértékelések eredményeit érdemes összevetni az ellenálló képességi mátrixszal, majd közösen továbbgondolni. Ez csökkenti az adminisztratív terheket, növeli a hatékonyságot, és biztosítja a holisztikus kockázatmenedzsmentet.

Függőségi mátrix kidolgozása: Javasolt a szervezet működését érintő legfontosabb ágazatközi függőségek (energia, informatika, humán erőforrás, beszállítók) feltüntetése az ellenálló képességi mátrixban valamint a prioritizálás. Ez elősegíti a kritikus láncreakciók előrejelzését és a célzott védelmi intézkedéseket.

Benchmarking és tudásmegosztás: Célszerű országos vagy ágazati szinten kialakítani az ellenálló képességi mátrixok összehasonlításának (benchmarking) gyakorlatát. Ez segíti az általános gyengeségek azonosítását és a jó gyakorlatok átvételét.

5. ÖSSZEGZÉS

A kockázat alapú gondolkodás a kritikus szervezeteknél az elméleti megközelítés mellett olyan gyakorlati módszer, amely a szervezetek működésbiztonságát és rezilienciáját közvetlenül befolyásolja. A bemutatott módszertani fejlődés és a kapcsolódó gyakorlati esettanulmányok két különböző ágazat példáján keresztül a következőket támasztották alá:

- a) Az összveszély szemlélet együttes alkalmazása a függőségi mátrixszal nélkülözhetetlen, mivel a kockázatok többsége nem önmagában, hanem egymást erősítve, láncreakció-szerűen jelentkezik.
- b) A kockázatok számszerűsítése és rangsorolása (pl. FMEA, CPM (kritikus pont mátrix) alkalmazása) támogatja a vezetői döntéshozatalt. A pontszámok alapján azonosíthatók a legsúlyosabb hatású kockázatok, amelyeknél azonnali intézkedés szükséges, míg más területeken elfogadható a maradványkockázat.
- c) Az egyenértékűség más szabályozásokkal (pl. munkavédelmi kockázatértékelés, veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzése Seveso III, NIS2) lehetőséget ad a párhuzamosságok elkerülésére, és elősegíti az integrált reziliencia-irányítás kialakítását. Ez különösen fontos a gyakorlatban, a széttagolt kockázatmenedzsment elkerülése érdekében.
- d) A függőségek feltárása és dokumentálása a mátrixban segíti a szervezeteket abban, hogy előre azonosítsák, mely más ágazatok, rendszerek és szolgáltatások sérülékenysége válhat kritikus hatásúvá. Ez a holisztikus megközelítés biztosítja, hogy az ellenálló képességi intézkedések rendszerszinten is hatékonyak legyenek, amelyet tovább fejleszthet például a negyedéves mini-kockázatfelmérések bevezetése, illetve a Benchmarking rendszer kialakítása a mátrixokból.
- e) A kritikus, valamint az ország védelme és biztonsága szempontjából jelentős szervezetekre és infrastruktúrákra vonatkozó hazai jogszabályi környezet kifejezetten megköveteli a kockázat alapú gondolkodás dokumentált alkalmazását az ellenálló képességi mátrixban és tervben. Ezzel a kritikus szervezetek működése összhangba kerül az EU normák elvárásaival, miközben a hazai nemzeti sajátosságok is érvényesülnek, amelyek alkalmazhatóságát támogatják az ágazati esettanulmányok, ágazatspecifikus jellemzők.

Összességében a kockázat alapú gondolkodás a kritikus szervezeteknél a jogszabályi megfelelésen túl stratégiai vezetői eszköz is. A bemutatott példák alapján a gyakorlatban is működőképes módszertan ágazattól függetlenül adaptálható. Az ellenálló képességi mátrix és a kapcsolódó elemzések támogatják a szervezeti tanulást, a folyamatos fejlesztést, valamint erősítik a kritikus szervezetek különböző kockázatokkal, veszélyekkel és fenyegetésekkel szembeni megelőzési, reagálási és helyreállási képességeit. Ezen képességek katalógusát és a fejlesztésükkel kapcsolatban megfogalmazottakat a technikai, biztonsági és szervezeti intézkedéseket leíró dokumentum, azaz az ellenálló képességi terv fogja tartalmazni, amelynek részleteit a cikk következő része ismerteti, szintén gyakorlatias megközelítéssel.

6. JOGFORRÁSOK

Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

A kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény

A védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény

A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény

A kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról szóló 474/2024. (XII. 31.) Korm. rendelet

Az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről szóló 475/2024. (XII. 31.) Korm. rendelet

234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékeléséről szóló 1191/2025. (VI. 5.) Korm. határozat

Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégiájáról szóló 1192/2025. (VI. 5.) Korm. határozat

7. IRODALOMJEGYZÉK

[1] Az ISO 9001:2015 szabvány frissített változata (2025-07-28), [Online]. Elérhetőség: <https://isotudastar.hu/az-iso-90012015-szabvany-frissített-valtozata/> (2025.08.13.)

[2] Mógor J., Angyal I. „A kritikus infrastruktúrák ellenálló képesség fejlesztését célzó szabályozás mérőföldkövei 2022-2025”. Védelem Tudomány a Katasztrófavédelem Online Szakmai, tudományos folyóirata, 10(2), p. 18. [Online]. Elérhetőség: DOI: <https://doi.org/10.61790/vt.2025.19455> (2025.08.13.)

[3] Linkov, I. et al. „Measurable Resilience for Actionable Policy, Environmental Science & Technology” 2013 47 (18), 10108-10110, [Online]. Elérhetőség: DOI: <https://doi.org/10.1021/es403443n> (2025.08.11.)

[4] Watson, G. et al. „Streamlined Assessments are Integral to Operationalizing Resilience, Environmental Management” (2025). [Online]. Elérhetőség: DOI: <https://doi.org/10.1007/s00267-025-02200-7> (2025. 08. 11.)

[5] Kaplan, S., & Garrick, B. J. (1981). „On the quantitative definition of risk. Risk Analysis”, 1(1), 11–27. [Online]. Elérhetőség: DOI: <https://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1981.tb01350.x> (2025. 08. 11.)

[6] Apostolakis, G. E. (1990). „The concept of probability in safety assessments of technological systems.” Science, 250(4986), 1359–1364. [Online]. Elérhetőség: DOI: <https://doi.org/10.1126/science.2255909> (2025. 08. 11.)

[7] Zhang, X., Chan, F. T. S., Yan, C., & Bose, I. (2022). „Towards risk-aware artificial intelligence and machine learning systems: An overview.” Decision Support Systems, 159. [Online]. Elérhetőség: DOI: <https://doi.org/10.1016/j.dss.2022.113800> (2025. 08. 11.)