

Üzletmenet folytonosság termelőüzemekben

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/44

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.16	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Termelőüzemi környezetben az üzletmenet-folytonosság nem kezelhető kizárólag informatikai rendelkezésre állási vagy katasztrófa-helyreállítási kérdésként. A termelési képesség fenntartása és helyreállítása az üzleti folyamatok, a gyártástechnológia, az OT (Operational Technology) és IT (Information Technology) infrastruktúra, a közműellátás, az emberi erőforrások, az alapanyag- és alkatrészellátás, a külső szolgáltatók, valamint a munkabiztonsági és minőségbiztosítási feltételek együttes rendelkezésre állásától függ.

Termelőüzemben az üzletmenet-folytonosság akkor tekinthető érdemben kialakítottnak, ha a szervezet nem csupán dokumentált tervekkel rendelkezik, hanem ismeri a kritikus termelési képességek teljes függőségi láncát, üzleti alapon meghatározott helyreállítási célokkal és minimális működési szintekkel rendelkezik, az OT/ICS és IT helyreállításához szükséges konfigurációk és eszközök ténylegesen rendelkezésre állnak, a technológia biztonságos újraindításának feltételei dokumentáltak, és a helyreállítási-képességet mért gyakorlatokkal bizonyítja.

A termelőüzemi üzletmenet folytonosság legnagyobb kockázata az, ha a dokumentum és a tényleges helyreállítási képesség között eltérés van. Ezért a megfelelés és a működőképesség megítélésénél nem a terv terjedelme, hanem a függőségek ismerete, a reális helyreállítási-stratégia, a rendelkezésre álló erőforrások, a biztonságos újraindítás és a tesztekkel igazolt teljesíthetőség tekintendő elsődlegesnek.

A helyreállítás nem tekinthető befejezettnek pusztán az IT vagy OT rendszer technikai elérhetőségének visszaállításával. A termelés újraindítása előtt igazolni kell a technológiai konfigurációk integritását, a biztonsági funkciók és az eszközök megfelelő működését, a termelési adatok konzisztenciáját, a szükséges közművek és anyagellátás rendelkezésre állását, valamint a minőségügyi, munkabiztonsági és – ahol releváns – környezetvédelmi újraindítási feltételek teljesülését.

- az üzletmenet folytonosság tervezés elsődleges tárgya a termelési képesség, nem önmagában az IT-rendszer vagy a gyártógép;
- a helyreállítási célértékeket (helyreállítás maximális ideje, sorrendje) az üzleti és termelési hatásokból kell levezetni, nem a meglévő technológia képességeiből;
- a kiberbiztonság helyreállítása, a technológiai újraindítás és a normál termelésbe történő visszatérés három elkülönítendő, egymásra épülő állapot;
- a deklarált maximális helyreállítási idő csak akkor tekinthető reálisnak, ha azt helyreállítási teszt, mért gyakorlat vagy dokumentált műszaki becslés alátámasztja.

2. CÉL, HATÓKÖR ÉS SZAKMAI FOGALMAK

2.1 Az állásfoglalás célja

Az állásfoglalás célja olyan szakmai szempontrendszer rögzítése, amely termelőüzemi környezetben összekapcsolja a NIS2 irányelv, a Kiberbiztonsági tv. és a 7/2024. (VI. 24.) MK rendelet szerinti kiberbiztonsági folytonossági követelményeket a termelési, OT, IT, ellátási, fizikai, technológiai biztonsági, munkabiztonsági és minőségbiztosítási működéssel. A konkrét megoldást az üzem technológiájához, EIR-jei biztonsági osztályához, termelési modelljéhez, minőség- és munkabiztonsági követelményeihez, valamint kockázataihoz kell igazítani.

2.2 BCP, DRP, védelmi képesség és technológiai újraindítás

Terület	Elsődleges cél	Termelőüzemi értelmezés
BCP	A kritikus működés fenntartása vagy prioritás szerinti visszaállítása.	Minimális gyártási képesség, alternatív sor/telephely, manuális működés, személyzet, közmű, anyagellátás.
DRP	A kiesett technológiai rendszerek és adatok helyreállítása.	MES/ERP/virtualizáció, OT szerverek, PLC/HMI/SCADA konfigurációk, hálózat.
Védelmi képesség helyreállítása	A kompromittált környezet megbízható, ismert jó állapotból történő helyreállítása.	Kompromittált AD, mentések, mérnöki gépek védelmének, PLC-logika, távoli hozzáférés és hitelesítő adatok kezelése.
Biztonságos technológiai újraindítás	A fizikai folyamatok biztonságos újraindulása.	Biztonsági állapot ellenőrzése, biztonsági funkciók újraindulása, paraméterek, receptúrák, kalibráció ellenőrzése és minőségügyi felszabadítás.

A fenti területeket össze kell hangolni, de nem szabad összerosni. Egy rendszer technikailag elérhető lehet úgy is, hogy a termelés biztonságos újraindításának feltételei még nem teljesülnek.

A „védelmi képesség helyreállítása” és a „biztonságos technológiai újraindítás” jelen állásfoglalásban alkalmazott szakmai fogalmak; nem önálló MK rendeleti követelménycsoportok.

3. JOGSZABÁLYI ÉS KONTROLLALAP

A 7/2024. (VI. 24.) MK rendelet 2. mellékletének 7. követelménycsoportja a készenléti tervezés keretében szabályozza az üzletmenet-folytonosságot. A követelmények EIR-központúak, azonban termelőüzemben az EIR-ek folytonossága csak a hozzájuk kapcsolódó termelési folyamatok, kritikus erőforrások, fizikai infrastruktúra és külső függőségek ismeretében értelmezhető.

Követelmény	Osztály	Termelőüzemi értelmezés
7.1. Szabályzat és eljárásrendek	A / J / M	Az üzletmenet-folytonosság (BCP) szervezeti, folyamat- és rendszerszintű követelményeinek, felelősségeinek, eljárásainak, felülvizsgálati gyakoriságának és eseményvezérelt aktualizálásának szabályozása.
7.2. Üzletmenet-folytonossági terv	A / J / M	Alap gyártási, szolgáltató és üzemeltetési feladatok definiálása, helyreállítási célok és prioritások, vészhelyzeti szerepkörök, biztosítandó szolgáltatások és teljes helyreállítás.
7.3. Összehangolás a kapcsolódó tervekkel	J / M	BCP összehangolása incidenskezelési, munkavédelmi, fizikai, minőségügyi és egyéb telephelyi tervekkel.
7.4. Kapacitás tervezése	M	Folyamatos működéshez szükséges információfeldolgozási, kommunikációs és környezeti kapacitások meghatározása, kialakításuk megtervezése.
7.5. Üzleti funkciók	J / M	Az gyártói, szolgáltatói és üzemeltetési

Követelmény	Osztály	Termelőüzemi értelmezés
visszaállítása		funkciók újratekzdési időpontjának meghatározása és a helyreállítás prioritása.
7.6. Alapfeladatok és alapfunkciók folyamatossága	M	A kritikus és/vagy alap funkciók csekély vagy semmilyen veszteséggel történő fenntartásának megtervezése.
7.9. Kritikus erőforrások meghatározása	J / M	Kritikus emberi, technológiai, OT/IT, közmű-, telephelyi és külső erőforrások azonosítása.
7.13–7.14. BCP tesztelése és összehangolása	J / M	A kialakított folytonossági terv(ek) meghatározott gyakoriságú tesztelése, az eredmények értékelése, szükség szerinti javítása és a kapcsolódó tervekkel való összehangolása.
7.7 - 7.15. Alternatív feldolgozási helyszín kialakítása és tesztelése	M	Amennyiben arra lehetőség van adminisztratív, de akár gyártási / üzemi alternatív helyszín igénybevételeének és helyreállítási képességének kialakítása, átállási folyamat dokumentálása és tesztelése
7.19–7.20. Biztonsági tárolási helyszín	J / M	Mentések és helyreállítási adatok elkülönített, védett tárolása, a szervezeti működéstől megfelelően elkülönített helyszínen, ide értve a rendszer és eszköz konfigurációk, tervek, projekt dokumentumok, mérnöki dokumentumok tárolását is.
7.35. Az EIR mentései	A / J / M	Felhasználói, rendszerszintű (adat, konfiguráció és verzió!) és dokumentációs mentések készítése a helyreállítási célokkal összhangban, megfelelő bizalmasság-, sértetlenség- és rendelkezésreállítás-védelemmel.
7.37. Visszaállítás tesztelése mintavétellel	M	A mentett információk és rendszerelemek visszaállításának mintavételes gyakorlati tesztelése minden elemre értve, például, hogy lehet-e ugyanolyan verziójú firmware-t telepíteni valahonnan... stb.
7.43. Az EIR helyreállítása és újraindítása	A / J / M	Rendszer újraindítás előtt esetenként a fizikailag megvalósított gép újraindulásokat is koordinálni kell.

A felsorolás nem kizárólagos, termelési fókusz figyelembe véve emeltük ki a követelményeket. A jelen állásfoglalás további termelőüzemi szempontjai részben e követelmények gyakorlati értelmezését, részben szakmai jó gyakorlatot jelentenek.

4. A TERMELŐÜZEMI FOLYTONOSSÁG FÜGGŐSÉGI MODELLJE

A folytonossági elemzést célszerű a termelési folyamatból kiindulva felépíteni, és visszafelé feltárni azokat az erőforrásokat, amelyek nélkül az adott termék, szolgáltatás vagy gyártási lépés nem tartható fenn. A függőségi térképnek legalább az alábbi rétegeket kell kezelnie.

Réteg	Tipikus elemek	Kritikus kérdés
Termék	/ Vevői termék, szállítási	Mely termelési képességet kell

Réteg	Tipikus elemek	Kritikus kérdés
szolgáltatás	határidők, kritikus batch, kötelező szolgáltatás.	fenntartani, milyen minimális outputtal?
Gyártási folyamat	Technológiai lépés, minőségellenőrzés, csomagolás, anyagmozgatás.	Mi a folyamat maximálisan tolerálható kiesése esetleg mely lépések hagyhatók ki ideiglenesen?
Termelőberendezés	CNC, robot, kemence, töltő, csomagoló, labor- és mérőeszköz...	Van-e redundancia, tartalék gép, pótalkatrész vagy áterhelési lehetőség?
OT	PLC, safety PLC, DCS, MES, SCADA, HMI, historian, OT switch, engineering workstation.	Mely konfigurációk, firmware-ek, licencek és kommunikációs kapcsolatok szükségesek?
IT	MES, ERP, AD/Entra ID, virtualizáció, adatbázis, fájl- és licencszolgáltatás.	Mely folyamat áll le, és mi működtethető kontrollált degraded/manual módban? Mely konfigurációk, firmware-ek, licencek és kommunikációs kapcsolatok szükségesek?
Közmű infrastruktúra /	Villamos energia, gáz, víz, gőz, sűrített levegő, vákuum, hűtés, HVAC.	Milyen autonómia, redundancia és újraindítási sorrend áll rendelkezésre?
Emberi erőforrás	Operátor, karbantartó, automatizálási mérnök, minőségügy, EHS, műszakvezető.	Mely kompetencia szükséges, a szükséges kompetenciák elérhetősége, van-e helyettesítés és 24/7 elérhetőség amennyiben erre szükség van?
Ellátási lánc	Alapanyag, pótalkatrész, OEM szerviz, kalibrálás, fuvar, felhő- és távközlési szolgáltatás.	Mi a beszerzés átfutási ideje, van-e helyettesíthetőség és tényleges alternatíva?

A függőségi modellnek ki kell térnie a „single point of failure” elemekre melyek hiánya önmagában egyetlen hibaként leállást eredményez, a kifutott vagy már nem támogatott technológiákra, a gyártói/vendor lock-in függőségekre, valamint azokra a licencekre, eszközökre és speciális kompetenciákra, amelyek nélkül a helyreállítás nem hajtható végre. A függőségi térképen célszerű minden kritikus erőforráshoz hozzárendelni annak tulajdonosát, helyettesíthetőségét, helyreállítási sorrendjét és az alkalmazható alternatív működési megoldást.

5. KRITIKALITÁS, BIA ÉS HELYREÁLLÍTÁSI CÉLÉRTÉKEK

A kritikalitást nem kizárólag árbevétel vagy leállási költség alapján kell meghatározni. A vizsgálatnak ki kell terjednie a termelési, vevői, munkabiztonsági, környezeti, minőségügyi, jogszabályi és reputációs hatásokra, továbbá az idő függvényében növekvő következményekre.

Fogalom	Termelőüzemi alkalmazás
MTPD – maximálisan tolerálható kiesési idő	Az az időtartam, amelyen túl a folyamat kiesése már elfogadhatatlan üzleti, biztonsági, vevői vagy megfelelőségi következménnyel jár.

Fogalom	Termelőüzemi alkalmazás
MBCO – minimálisan elfogadható működési szint	Az a minimális termelési vagy szolgáltatási képesség, amelyet teljes helyreállítás előtt fenn kell tartani; meghatározható például kritikus termékkör, vevői kör, napi darabszám vagy százalékos kapacitás szerint.
RTO – helyreállítási időcél	Az az idő, amelyen belül a folyamatot vagy támogató rendszert a meghatározott MBCO szintre vissza kell állítani. Az RTO-nak kisebbnek kell lennie a maximálisan tolerálható kiesésnél.
RPO – adatvesztési tolerancia	A tolerálható adatvesztés időbeli mértéke; különösen fontos MES, receptúra, batch, sorozatszám, traceability és minőségügyi adatoknál.
Tényleges helyreállítási idő	A teszt vagy valós esemény során mért helyreállítási idő, amelyet az RTO-val össze kell vetni.
Restart / stabilizálási idő	Az IT/OT technikai helyreállítás után szükséges idő a fizikai technológia biztonságos stabilizálásához és termelésbe engedéséhez.

A célértékeket a folyamatgazda, a termelés, az IT/OT, a karbantartás, a minőség és (ahol releváns) az egészség- és munkabiztonsági terület közös értékelésével kell meghatározni. Nem megfelelő gyakorlat, ha az RTO/RPO értékeket az IT kizárólag a meglévő mentési vagy infrastruktúra-képességek alapján határozza meg. Az MTPD és MBCO jelen állásfoglalásban alkalmazott szakmai BCM-fogalmak; a 7/2024. MK rendelet közvetlenül a helyreállítási célok, prioritások, valamint a helyreállítási időre és helyreállítási pontra vonatkozó célértékek meghatározását követeli meg.

6. OT/ICS HELYREÁLLÍTÁSI KÉSZENLÉT

Termelőüzemi környezetben a helyreállítási képesség jelentős része nem klasszikus szervermentésen múlik. A szervezetnek helyreállítható állapotban kell tartania mindazokat a konfigurációkat, szoftvereket, licenceket, paramétereket és eszközöket, amelyek a gyártástechnológia újraépítéséhez szükségesek. Az OT/ICS mentési és helyreállítási képesség kialakításánál különösen figyelembe veendő a 7.35., 7.36., 7.43. és Magas biztonsági osztály esetén a 7.45. követelmény.

Terület	Minimum helyreállítási tartalom
PLC	Program, hardverkonfiguráció, firmware-verzió, I/O mapping, kommentált forrás, hiteles mentés és visszatöltési eljárás.
HMI / SCADA / DCS	Projektfájlok, szerverkonfiguráció, driverek, kommunikációs beállítások, licencek, historian-kapcsolatok.
Robot / CNC / drive	Robotprogramok, CNC programok, receptúrák, drive-paraméterek, kalibrációs és pozícióadatok.
OT hálózat	Switch/firewall konfiguráció, VLAN, routing, IP-terv, VPN/távoli elérés, eszközlista és szükséges firmware.
Engineering Workstation	Telepítőkészletek, engineering szoftverek és verziók, licencfájlok, driverek, offline recovery image.
MES / historian / adatbázis	Adatbázismentés, interfészek, message queue, receptúra/master data, nyomonkövetési és batch adatok.
Recovery kit	Offline elérhető dokumentáció, telepítők, konfigurációk, kontrollált

Terület	Minimum helyreállítási tartalom
	vészhozzáférési eljárás, valamint a helyreállításhoz szükséges hitelesítési és jogosultsági mechanizmusok biztonságos rendelkezésre állása; továbbá a szükséges kábelek és eszközök.

A mentések esetében nem elegendő a mentési feladat sikeres státusza. Biztosítani kell a verziókezelést, az integritás ellenőrzését, az elkülönített tárolást és a tényleges visszaállíthatóság tesztelését.

7. SAFE STATE, BLACK-START ÉS BIZTONSÁGOS ÚJRAINDÍTÁS

A folytonossági tervnek minden kritikus technológiánál meg kell határoznia, hogyan kerül a folyamat biztonságos állapotba energia-, kommunikációs, vezérlési vagy kiberbiztonsági hiba esetén. A safe state nem minden esetben teljes leállítás; technológiától függően kontrollált hűtés, nyomásmentesítés, cirkuláció vagy más állapot fenntartása lehet szükséges.

Teljes telephelyi vagy technológiai leállítás esetére dokumentálni kell a black-start/cold-start sorrendet. Ennek tartalmaznia kell a közművek, hálózati és identitásszolgáltatások, OT vezérlés, biztonsági felügyelet, MES/ERP és fizikai gyártási lépések helyreállításának függőségi sorrendjét.

Újraindítási kapu	Igazolandó feltétel
Fizikai / EHS	Berendezés és környezet biztonságos állapota, LOTO/engedélyek lezárása, szükséges közművek stabilitása.
OT integritás	PLC/safety PLC logika, HMI/SCADA projekt, hálózati és vezérlési konfiguráció ismert jó állapotból helyreállítva.
Safety funkciók	vészleállítások, biztonsági körök és szükséges műszeres funkciók ellenőrzése.
Minőség	Receptúra, paraméter, kalibráció, mérési rendszer és termékfelszabadítási feltételek rendben.
Adatkonzisztencia	ERP–MES–SCADA/PLC közötti állapot, batch/WIP, sorozatszám, készlet és traceability adatok egyeztetve.
Üzleti jóváhagyás	Termelési vezető és a kijelölt szakmai funkciók dokumentált döntése a normál vagy korlátozott termelés indításáról.

A safety funkciók, reteszlelések és vészleállítási rendszerek ellenőrzését az alkalmazandó munkabiztonsági, funkcionális biztonsági, technológiai és gyártói előírások szerint, arra jogosult és kompetens személynek kell elvégeznie. A kiberbiztonsági helyreállítás önmagában nem jogosítja fel a rendszert a termelés újraindítására.

Kibertámadás után a technológia újraindítása előtt különösen fontos annak kizárása, hogy kompromittált konfiguráció, hitelesítő adat, mentés vagy vezérlési környezet kerüljön vissza a termelésbe.

8. TERMELÉSKÖZI ÁLLAPOT, ADATKONZISZTENCIA ÉS MANUÁLIS FALLBACK

A termelőüzemi kiesések jelentős kockázata a félbemaradt gyártási állapot. A BCP-nek rendelkeznie kell a félkész termék, batch, sorozatszám, alapanyagfelhasználás, készletmozgás, receptúra és minőségügyi státusz rendezéséről.

- Meg kell határozni, mely termelési lépések folytathatók IT/MES nélkül és milyen maximális ideig;

- manuális működés esetén biztosítani kell az offline munkautasításokat, nyomtatványokat, jóváhagyásokat és az egyedi azonosíthatóságot;
- rögzíteni kell a későbbi visszarögzítés, egyeztetés, duplikáció- és hiányellenőrzés menetét;
- a safety, quality, traceability vagy jogosultsági kontrollt érintő automatikus funkciók manuális megkerülése csak előre meghatározott és jóváhagyott feltételekkel engedhető;
- ha a biztonságos vagy megfelelőségi működés manuálisan nem biztosítható, a folyamatot le kell állítani.

9. FORGATÓKÖNYVEK ÉS FOLYTONOSSÁGI STRATÉGIÁK

A BCP-t életszerű, több erőforrás együttes kiesését is figyelembe vevő forgatókönyvekkel kell validálni. A forgatókönyveknek tartalmaznia kell az aktiválási feltételeket, a biztonsági lépéseket, a döntési jogosultságokat, a helyreállítási sorrendet és a normál működésbe történő visszatérés feltételeit.

Példa - Forgatókönyv	Szakmai fókusz
Teljes áramszünet / közműkiesés	UPS/generátor tényleges terhelése és autonómiája, kritikus fogyasztók, hűtés/sűrített levegő/gáz függőség, black-start.
Ransomware / széles körű IT-OT kompromittáció	Tiszta recovery környezet, AD/identity helyreállítás, backup megbízhatóság, OT izoláció, engineering és PLC integrity.
Kritikus gyártósor vagy gép kiesése	Pótalkatrész lead time, OEM szerviz, alternatív sor/telephely, átterhelés, termék- és vevőprioritás.
MES/ERP kiesés	Degraded/manual mode, traceability, készlet és WIP kezelése, visszarögzítés, adatkonzisztencia.
Telephely részleges/teljes kiesése	Alternatív gyártókapacitás, bérnyújtás, készlet, logisztika, személyzet és minőségügyi újraminősítés.
Beszállítói / alkatrészellátási kiesés	Safety stock, second source, helyettesítő anyag, újraminősítés, emergency sourcing és lead time.
Kulcsszemély / műszak kiesése	Többkompetenciás személyzet, helyettesítés, vendor support, offline dokumentáció és döntési jogosultság.
Távközlési / távoli támogatás kiesése	Független másodlagos kapcsolat, onsite recovery képesség, vendor remote access nélküli üzemeltetés.
Technológiai biztonsági vagy környezeti funkció kiesése	Ahol releváns: kritikus safety rendszer, technológiai hűtés, elszívás, szennyvízkezelés vagy más biztonsági/környezeti funkció elvesztése; safe-state és újraindítási feltételek.

10. KRITIKUS ALKATRÉSZEK, VENDOR DEPENDENCY ÉS OBSOLESCENCE

A termelőüzemi helyreállítás gyakran nem adat-, hanem hardver-, alkatrész- vagy szakértelem-függő. A folytonossági elemzésben ezért külön kell értékelni a pótalkatrész-ellátást és a gyártói támogatás rendelkezésre állását.

- Kritikus PLC, IPC, switch, drive, HMI, speciális szenzor, tápegység és kommunikációs modul helyi vagy garantált készlete;
- beszerzési és javítási átfutási idő, gyártói életciklus státusz, end-of-sale/end-of-support kockázat;

- a tartalék alkatrész tényleges kompatibilitásának igazolása, beleértve a hardververziót, firmware-t, licencet, konfigurálhatóságot és a szükséges eszközöket;
- speciális vezérlő szoftver, licenc, firmware és speciális szervizkompetencia elérhetősége;
- beszállító és kulcsemberek függőségei, illetve azok helyettesítési stratégiája;
- kifutott technológia esetén előre meghatározott migrációs vagy tartalékolási stratégia.

11. KÜLSŐ SZOLGÁLTATÓK ÉS ELLÁTÁSI LÁNC

A termelőüzem folytonossági képességét olyan külső szereplők is meghatározzák, amelyek nem klasszikus IT-szolgáltatók: gépgyártók, automatizálási integrátorok, karbantartók, energia- és közműszolgáltatók, alapanyag-beszállítók, fuvarozók, kalibráló laborok és felhőszolgáltatók.

- Kritikus, illetve egyedi szolgáltatók és függőségek azonosítása, szolgáltatási és pótalkatrész átfutási időikkel;
- reagálási és helyreállítási idők, 24/7 elérhetőség, kapcsolattartók és eskalációs rend;
- alternatív beszállító vagy szolgáltatási lehetőség tényleges használhatósága, beleértve a minőségügyi jóváhagyás időigényét;
- kritikus berendezésgyártó és integrátor esetén helyszíni helyreállítás lehetősége akkor is, ha távoli kapcsolat nem elérhető;
- a szervezet által elvárt folytonossági, helyreállítási és bizonyítékatadási követelmények szerződéses rögzítése, valamint kritikus szolgáltatóknál azok teljesülésének időszakos ellenőrzése;
- kritikus szolgáltatóknál saját üzletmenet fenntartási / folytonossági képesség és tesztelési eredmény megfelelő mélységű igazolása.

12. VÁLSÁGIRÁNYÍTÁS ÉS DÖNTÉSI JOGOSULTSÁGOK

A technikai helyreállítási terv mellett egyértelmű döntési modell szükséges. A termelés leállítására, folytonossági terv aktiválására, csökkentett üzemmód engedélyezésére, helyreállítási prioritás megváltoztatására és újraindításra jogosult szerepköröket előre ki kell jelölni.

Döntés	Tipikus bevonandó szerepkörök
BCP / folytonossági terv aktiválása	Telephelyvezetés, termelés, BCM/IBF vagy kijelölt koordinátor vagy kijelölt vezető; kiberbiztonsági kiváltó esemény esetén az EIR biztonságáért felelős személy bevonásával.
Technológia biztonságos leállítása	Termelés, karbantartás/automatizálás, környezet- és munkavédelem, műszakvezetés.
Hálózat izoláció vagy szegmentáció / OT leválasztás	IT/OT security, automatizálás, üzemeltetés, incidenskezelés.
Csökkentett üzemmód engedélyezése	Termelés, minőség, környezet- és munkavédelem, folyamatgazda, szükség szerint IT/OT.
Újraindítás engedélyezése	Termelés + karbantartás/OT + minőség + környezet- és munkavédelem; a helyi irányítási rend szerint.
Normál működésbe visszatérés	Válságvezetés / telephelyvezetés, a technikai és üzleti feltételek igazolása alapján.

13. TESZTELÉS ÉS HELYREÁLLÍTÁSI KÉPESSÉG VALIDÁLÁSA

A 7.13. követelmény Jelentős és Magas biztonsági osztály esetén meghatározott gyakoriságú tesztelést, az eredmények értékelését és szükség szerinti tervjavítást ír elő. Termelőüzemben a tesztelést eltérő szintekben célszerű felépíteni, nem szabad kizárólag elméleti (tabletop – asztal mellett ülve) tesztelési gyakorlatra korlátozni. Teljes leállást természetesen nem szívesen szimulál senki, de az eltérő tesztelési szintek megfelelő visszajelzést adhatnak a problémákról.

Egyes tesztelések tulajdonképpen karbantartáshoz való leállítási/újraindítás esetén is végezhetők, nem szükséges ezeket külön időszakban végezni.

Teszt szint	Mit validál?	Elvárt eredmény
1. Tabletop	Döntési, kommunikációs, eszkalációs és szerepköri rend.	Megállapítások, döntési hiányok, akciólista.
2. Komponens helyreállítás	Mentés-visszaállítás, PLC/HMI konfiguráció, virtuális gép, adatbázis, hálózati eszköz.	Mért RTO, sikeres integritásellenőrzés, hibák.
3. Integrált technikai helyreállítás	Több IT/OT komponens függőségi sorrendű helyreállítása.	Interfészek és adatkapcsolatok helyreállása, időmérés.
4. Csökkentett módban működés	Minimális termelési szint és offline eljárások.	MBCO tarthatósága, visszarögzítés és kontrollok működése.
5. Gyártási újraindítási gyakorlat	Biztonságos állapotból való újraindulást, biztonságos állapot ellenőrzési listát.	Biztonságos és minőségileg elfogadható újraindítás, tényleges időadatok.

A tesztnek igazolnia kell, hogy a meghatározott minimális működési szint és az újraindítási feltételek teljesíthetők bizonyos előfeltételezések, illetve előkészületek mellett. Ha valamely célérték nem teljesül, javítóintézkedést, erőforrás- vagy technológiai fejlesztést, illetve indokolt esetben az üzleti célérték felülvizsgálatát kell kezdeményezni. Veszélyes vagy termelést érdemben kockáztató forgatókönyvnél izolált, részleges vagy szimulált teszt alkalmazható, de a nem tesztelt feltételezéseket dokumentálni kell.

14. DOKUMENTÁCIÓ ÉS AUDITÁLHATÓSÁG

A folytonossági rendszernek (mentések, tervek, gyakorlatok rendszere) olyan bizonyítékokat kell eredményeznie, amelyekből utólag megállapítható a kritikus folyamatok és erőforrások meghatározásának alapja, a célértékek jóváhagyása, az üzletmenet folytonossági és helyreállási képesség aktuális állapota, a tesztek tényleges eredménye és a hiányosságok kezelése.

Rendszer elemek:

- jóváhagyott üzletmenet-folytonossági szabályzat, eljárásrend és EIR-/folyamatszintű BCP;
- termék–folyamat–gép–OT/IT–közmű–személyzet–beszállító függőségi térkép;
- MTPD, MBCO, RTO, RPO és restart/stabilizálási célértékek, jóváhagyásokkal;
- PLC/HMI/SCADA/robot/CNC/hálózat konfiguráció- és mentési jegyzék, verzióval és tárolási hellyel;
- kritikus pótalkatrész-, licenc-, szállító függőségi nyilvántartás;
- biztonsági ellenőrzési listák és újraindítási eljárások és felelősökkel;
- tesztervek, jegyzőkönyvek, mért RTO-k, eltérések, tanulságok és javítóintézkedések;

- külső szolgáltatói SLA-k, folytonossági vállalások és alternatív ellátási megoldások.

15. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.).
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről.
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról.
- NIST SP 1339 – Operational Technology (OT) Backup Quick Start Guide
- NIST SP 800-82 Rev. 3 – Guide to Operational Technology (OT) Security