



FV-18. sz. útmutató

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

Verzió száma:

3.

2020. március

Kiadta:

Fichtinger Gyula
az OAH főigazgatója
Budapest, 2020.

A kiadvány beszerezhető:
Országos Atomenergia Hivatal
Budapest

FŐIGAZGATÓI ELŐSZÓ

Az Országos Atomenergia Hivatal (a továbbiakban: OAH) az atomenergia békés célú alkalmazása területén működő, önálló feladat- és hatáskörrel rendelkező, országos illetékességű, központi kormányzati igazgatási szerv, kormányzati főhivatal. Az OAH-t a Magyar Köztársaság Kormánya 1990-ben alapította.

Az OAH jogszabályban meghatározott közfeladata, hogy az atomenergia alkalmazásában érdekelt szervektől függetlenül ellássa és összehangolja az atomenergia békés célú, biztonságos és védett alkalmazásával, így a nukleáris és radioaktív hulladék-tároló létesítmények, nukleáris és más radioaktív anyagok biztonságával, nukleárisveszélyhelyzet-kezeléssel, nukleáris védettséggel kapcsolatos hatósági feladatokat, valamint az ezekkel összefüggő tájékoztatási tevékenységet, továbbá javaslatot tegyen az atomenergia alkalmazásával kapcsolatos jogszabályok megalkotására, módosítására, és előzetesen véleményezze az atomenergia alkalmazásával összefüggő jogszabályokat.

Az atomenergia alkalmazása hatósági felügyeletének alapvető célkitűzése, hogy az atomenergia békés célú felhasználása semmilyen módon ne okozhasson kárt a személyekben és a környezetben, de a hatóság az indokoltnál nagyobb mértékben ne korlátozza a kockázatokkal járó létesítmények üzemeltetését, illetve tevékenységek folytatását. Az alapvető biztonsági célkitűzés minden létesítményre és tevékenységre, továbbá egy létesítmény vagy sugárforrás élettartamának minden szakaszára érvényes, beleértve létesítmény esetében a tervezést, a telephely-kiválasztást, a létesítést, az üzembe helyezést és az üzemeltetést, valamint a leszerelést, az üzemem kívül helyezést és a bezárást, radioaktív hulladék-tárolók esetén a lezárást követő időszakot, radioaktív anyagok alkalmazása esetén a szóban forgó tevékenységekhez kapcsolódó szállítást és a radioaktív hulladék kezelését, míg ionizáló sugárzást kibocsátó berendezések esetén azok üzemeltetését és karbantartását.

Az OAH a jogszabályi követelmények teljesítésének módját az atomenergia alkalmazóival egyeztetett módon, világos és egyértelmű ajánlásokat tartalmazó útmutatókban fejt ki, azokat az érintettekhez eljuttatja, és a társadalom minden tagja számára hozzáférhetővé teszi. Az atomenergia alkalmazásához kapcsolódó nukleáris biztonsági, védettségi és non-proliferációs követelmények teljesítésének módjára vonatkozó útmutatókat az OAH főigazgatója adja ki.

Az útmutatók alkalmazása előtt mindig győződjön meg arról, hogy a legújabb, érvényes kiadást használja! Az érvényes útmutatókat az OAH honlapjáról (www.oah.hu) töltheti le.

ELŐSZÓ

A fizikai védelem nemzetközileg elfogadott alapjait a nukleáris anyagok fizikai védelméről szóló egyezmény kihirdetéséről szóló 1987. évi 8. törvényerejű rendelet, valamint a Nemzetközi Atomenergia Ügynökség (NAÜ) keretében 1979-ben elfogadott és az 1987. évi 8. törvényerejű rendelettel kihirdetett, a nukleáris anyagok fizikai védelméről szóló Egyezménynek a NAÜ által szervezett diplomáciai konferencia keretében, 2005. július 8-án aláírt módosítása kihirdetéséről szóló 2008. évi LXII. törvény, valamint a nukleáris terrorcselekmények visszaszorításáról szóló Nemzetközi Egyezmény kihirdetéséről szóló 2007. XX. törvény határozza meg.

A nemzetközi egyezményben vállaltak hazai alkalmazásának legfelső szintjét az 1996. évi CXVI. törvény (a továbbiakban: Atv.) képviseli, amely tartalmazza a nukleáris védettség alapelveit és megteremti a fizikai védelem részletes szabályozásának kereteit.

Az Atv. felhatalmazása alapján kiadott – az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló – 190/2011. (IX. 19.) Korm. rendelet (a továbbiakban: Rendelet) tartalmazza a részletes jogszabályi követelményeket.

A jogszabályban meghatározott követelmények teljesítésére az OAH ajánlásokat fogalmazhat meg, amelyeket útmutatók formájában ad ki és az OAH honlapján közzétesz. Jelen útmutató az engedélyesek önkéntes alávetésével érvényesül, nem tartalmaz általánosan kötelező érvényű normákat.

A hatósági felügyeleti tevékenységhez kapcsolódó engedélyezési és ellenőrzési eljárások gyors és akadálymentes lefolytatásának érdekében az OAH az engedélyeseket az útmutatókban foglalt ajánlások minél teljesebb követésére ösztönzi.

Az útmutatókban foglaltaktól eltérő módszerek alkalmazása esetén az OAH az alkalmazott módszer helyességét, megfelelőségét és teljes körűségét részleteiben vizsgálja, ami hosszabb ügyintézési idővel, külső szakértő igénybevételével és további költségekkel járhat. Ha az engedélyes által választott módszer eltér az útmutató által ajánlottól, az eltérést indokolnia kell.

Az útmutatók felülvizsgálata az OAH által meghatározott időszakonként, vagy az engedélyesek javaslatára soron kívül történik.

A fenti szabályozást kiegészítik az engedélyesek, illetve más, a nukleáris energia alkalmazásában közreműködő szervezetek (tervezők, gyártók stb.) belső szabályozási dokumentumai, amelyeket az irányítási rendszerükkel összhangban készítenek.

TARTALOMJEGYZÉK

1. BEVEZETÉS	8
1.1. Az útmutató tárgya és célja	8
1.2. Vonatkozó jogszabályok és előírások	10
1.3. Nemzetközi és hazai ajánlások	17
1.3.1. Általánosan alkalmazott alapelvek	21
2. MEGHATÁROZÁSOK ÉS RÖVIDÍTÉSEK	23
2.1. Meghatározások	23
2.2. Rövidítések	31
3. AZ ÚTMUTATÓ AJÁNLÁSAI	32
3.1. A programozható rendszerek védelmének szervezete, felelőségek	32
3.1.1. Az engedélyes szervezet és a hozzá tartozó létesítmény felső vezetésének felelőssége	32
3.1.2. A programozható rendszerek védelmi felelőse	33
3.1.3. A programozható rendszerek védelmi megbízottai	34
3.1.4. A szervezeti egységek vezetőinek felelőssége	34
3.1.5. A létesítmény minden, programozható rendszerrel kapcsolatba kerülő dolgozójának felelőssége és kötelezettsége	35
3.2. A programozható rendszerek védelmének kapcsolata a védettség más területeivel	35
3.2.1. A létesítmény védettségi keretrendszere	35
3.2.2. A teljeskörűsége vonatkozó alapelv alkalmazása a védettségi keretrendszerben	36
3.2.3. Védettségi szakterületekkel való együttműködés jellege	37
3.2.4. Nukleáris biztonsági és üzemfenntartási szakterületekkel való együttműködés jellege	38
3.3. A programozható rendszerek védelmi besorolása	39
3.3.1. A rendszer mint rendező fogalom	39
3.3.2. A védelmi besorolás	40
3.3.3. Kockázatelemzés (fenyegetettség-elemzés, sérülékenységelemzés, kockázatértékelés)	40
3.3.3.1. A kockázat és a kockázatmeghatározás alapjai	41
3.3.3.2. Kockázatértékelés és -kezelés	42
3.3.3.3. Fenyegetettségek azonosítása és jellemzése	45
3.3.3.4. Sérülékenységek vizsgálata, monitorozása és kezelése	45
3.3.4. Az egyes rendszerek védelmi besorolása	48
3.3.4.1. Az 5. védelmi szintbe sorolt rendszerek	53
3.3.4.2. A 4. védelmi szintbe sorolt rendszerek	53
3.3.4.3. A 3. védelmi szintbe sorolt rendszerek	54

Nukleáris létesítmények programozható rendszereinek védelmi követelményei	
3.3.4.4.	<i>A 2. védelmi szintbe sorolt rendszerek</i> 55
3.3.4.5.	<i>Az 1. védelmi szintbe sorolt rendszerek</i> 56
3.3.4.6.	<i>Jelátviteli utak védelmi szintje</i> 56
3.4.	Védelmi szintekre vonatkozó követelmények 57
3.4.1.	<i>A védelmi szintekre vonatkozó általános követelmények</i> 58
3.4.2.	<i>A védelmi szintek speciális követelményei</i> 59
3.4.2.1.	<i>Az 5. szintre vonatkozó speciális követelmények</i> 59
3.4.2.2.	<i>A 4. szintre vonatkozó követelmények</i> 59
3.4.2.3.	<i>A 3. szintre vonatkozó követelmények</i> 60
3.4.2.4.	<i>A 2. szintre vonatkozó követelmények</i> 60
3.4.2.5.	<i>Az 1. szintre vonatkozó követelmények</i> 61
3.5.	A programozható rendszerek védelmi tervének összeállítása 62
3.5.1.	<i>A rendszerek jegyzéke (rendszerek, hálózatok, alkalmazások és kapcsolataik)</i> 67
3.5.1.1.	<i>Alapkonfiguráció</i> 68
3.5.1.2.	<i>Konfigurációs változtatások</i> 69
3.5.2.	<i>A védelmi intézkedések megvalósítása</i> 72
3.5.2.1.	<i>Védelemtervezési Alapelvek</i> 72
3.5.2.2.	<i>Mélységben Tagolt Védelem</i> 73
3.5.2.3.	<i>Szabályzatok, eljárások és képzés</i> 74
3.5.2.4.	<i>Környezetállósági feltételek</i> 74
3.5.2.5.	<i>Fizikai hozzáférési védelem</i> 75
3.5.2.6.	<i>Hálózati határvédelem, peremvédelem</i> 75
3.5.2.7.	<i>Technikai, logikai hozzáférési védelem</i> 76
3.5.2.8.	<i>Belső hálózat védelme</i> 78
3.5.2.9.	<i>Szerverek, munkaállomások és HMI-k védelme</i> 79
3.5.2.10.	<i>Alkalmazások, futó programok védelme</i> 80
3.5.2.11.	<i>Adatok védelme</i> 80
3.5.2.12.	<i>A jól ismert sérülékenységek vizsgálata, monitorozása és kezelése</i> 82
3.5.2.13.	<i>Programfrissítések és biztonsági javítócsomagok telepítése</i> 82
3.5.2.14.	<i>Elektromágneses impulzusok elleni védelem</i> 85
3.5.2.15.	<i>Azonosító- és jelszókezelés</i> 86
3.5.2.16.	<i>Hordozható eszközök és mobil adathordozók használata</i> 87
3.5.2.17.	<i>Vezeték nélküli készülékek és hálózatok</i> 87
3.5.3.	<i>Folytonos üzemvitel, rendszerek biztonsági mentése</i> 88
3.5.3.1.	<i>Folytonos üzemvitel</i> 88
3.5.3.2.	<i>Rendszerek biztonsági mentése</i> 89

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

3.5.4. Szerződéses partnerek, beszállítók, szolgáltatók, alvállalkozók kiberbiztonsága	92
3.5.5. A védelemmel összefüggő oktatás, továbbképzés, védelmi kultúra	94
3.5.5.1. A védelmi oktatás és továbbképzés céljainak, rendjének meghatározása	94
3.5.5.2. A kialakított jogosultsági szinteknek megfelelő védelmi oktatási kritériumok a korábban meghatározott védelmi szintek követelményeit figyelembe véve	95
3.5.5.3. Speciális oktatások, továbbképzések rendje	95
3.5.5.4. Védelmi kultúra kialakítása	96
3.5.6. Védelmi felülvizsgálat	98
3.5.7. A védelmi terv hatékonyságának ellenőrzésére vonatkozó követelmények	99
3.5.8. A rendszerek védelmével összefüggő változáskezelés, életciklus	99
3.5.9. Események kezelése	101
3.5.9.1. A kivizsgálás rendje, kivizsgálást segítő intézkedések	101
3.5.9.2. Válasz intézkedési terv	102

1. BEVEZETÉS

1.1. Az útmutató tárgya és célja

Tekintettel arra, hogy a programozható rendszerek fontos szerepet játszanak mind a békés céllal, a biztonsággal és a védettséggel összefüggésben, továbbá hogy az útmutatóban foglaltak megvalósításában szerepet játszó személyi kör azonos, ezért a jelen útmutató speciális abban a tekintetben, hogy tárgyi hatálya kiterjed a békés célú alkalmazással, a nukleáris biztonsággal (beleértve a műszaki sugárvédelmet) és a nukleáris védettséggel összefüggő programozható rendszerekre, valamint célja a szándékolatlan és a szándékos fenyegetések kezelésére kiterjedő hatósági útmutatás. Ennek megfelelően az útmutató az érintett rendszereket, a velük kapcsolatos követelményeket és ajánlásokat együttesen tárgyalja (ezt a célt jeleníti meg a címben található védelmi követelmények kifejezés is).

Az útmutató a fentieknek megfelelően ajánlásokat tartalmaz:

- a) A nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről szóló 118/2011. (VII.11) Korm. rendelet mellékleteként megjelent Nukleáris Biztonsági Szabályzatok (a továbbiakban: NBSZ) hatálya alá tartozó technológiai rendszerekhez közvetlenül vagy a tárolt információ révén kapcsolódó programozható irányítástechnikai rendszerek és rendszerelemek védettségen alapuló biztonsága hozzájárul a nukleáris biztonsághoz;
- b) a Rendelet hatálya alá tartozó informatikai és irányítástechnikai rendszerek és rendszerelemek fizikai védelmének megvalósítása céljából;
- c) a nukleáris anyagok nyilvántartásának és ellenőrzésének szabályairól szóló 7/2007. (III. 6.) IRM rendeletben (a továbbiakban: IRMr.) a nyilvántartásra és az üzemeltetési feljegyzések biztonságának, az adatokhoz való illetéktelen hozzáférés megakadályozásának biztosítása céljából;
- d) a radioaktív anyagok nyilvántartásának és ellenőrzésének rendjéről, valamint a kapcsolódó adatszolgáltatásról szóló 11/2010. (III.4). KHEM rendelet (a továbbiakban: KHEMr) szerinti nyilvántartásokban szereplő adatok biztonságának és az azokhoz való illetéktelen hozzáférés megakadályozásának biztosítása céljából.

Az útmutató iránymutatást ad a nukleáris biztonsági funkcióval (beleértve a műszaki sugárvédelmi funkciókat), a fizikai védelmi funkcióval, a nukleáris biztosítéki követelmény teljesítési, valamint a radioaktív anyag nyilvántartási funkcióval rendelkező programozható rendszerek szándékolatlan és

Nukleáris létesítmények programozható rendszereinek védelmi követelményei szándékos fenyegetések elleni védelme követelményeire, a programozható rendszerek védelmi tervének tartalmi felépítésére.

Az útmutató iránymutatásai nem vonatkoznak az ügyviteli hálózatok általános védelmi követelményeire. Az iránymutatások az ügyviteli hálózatoknak azon részére terjednek ki, melyek összefüggnek valamely nukleáris biztonsági funkcióval, fizikai védelmi funkcióval, a nukleáris biztosítéki vagy radioaktív anyag nyilvántartási funkcióval rendelkező programozható rendszerrel. Az útmutató nem tartalmaz iránymutatást általános adatvédelmi kérdésekre.

Az útmutató célja, hogy a programozható rendszerekhez olyan, a védelmi intézkedéseket összefoglaló védelmi terv készüljön, amely megfelelő szinten biztosítja,

- a) a nukleáris biztonsági (beleértve műszaki sugárvédelmi) funkciót ellátó rendszerelemekhez kapcsolódó,
- b) a fizikai védelmi funkciót ellátó rendszerelemekhez kapcsolódó,
- a létesítmény üzemeltetése szempontjából fontos rendszerelemekhez kapcsolódó,
- c) a nukleáris biztosítéki követelmények funkciót ellátó rendszerelemekhez kapcsolódó,
- d) a radioaktív anyagok nyilvántartásához kapcsolódó

programozható rendszerek tervezett működési módját és a programozható rendszerekben feldolgozott, tárolt, vagy továbbított adatok

- a) rendelkezésre állását,
- b) sértetlenségét és
- c) bizalmasságát.

A javasolt védelmi intézkedések a szándékolatlan fenyegetések mellett az alábbi szándékos fenyegetettségek elleni védelmet hivatottak biztosítani:

- a) információszerzés egy később végrehajtandó akció tervezéséhez és végrehajtásához;
- b) a létesítmény biztonságos üzemeltetése és védettsége szempontjából alapvető számítógépes rendszerek működésének ellehetetlenítése vagy megzavarása.

A programozható rendszerek védelme igen gyorsan változó szakterület, ennek következtében az útmutatónak nem lehet célja konkrét egyedi védelmi intézkedések szorgalmazása, ehelyett általános elveket fogalmaz meg és módszerekre ad iránymutatást.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

1.2. Vonatkozó jogszabályok és előírások

A Kormány az Atv. 67. § felhatalmazó rendelkezése alapján szabályozásokat adhat ki

- a) az egyébek mellett a nukleáris létesítmény és a hozzá tartozó rendszerek és rendszerelemek tervezésére, gyártására, beszerzésére, üzemeltetésére, az átalakításokra vonatkozó nukleáris biztonsági és az ebben résztvevő szervezetek irányítási rendszerével szemben támasztott követelményekről szóló d) pont szerint;
- b) az atomenergia alkalmazóinak, valamint az illetékes hatóságoknak a feladatait és kötelezettségeit tárgyaló e) pont szerint;
- c) a nukleáris védettséggel összefüggésben a fenyegetettséggel kapcsolatos elemzéseket elvégző és a tervezési alapfenyegetettséget meghatározó szervezetek működéséről szóló q) pont szerint;
- d) az atomenergia alkalmazása körében a fizikai védelmi rendszerrel kapcsolatos követelményeket és a vonatkozó hatósági rendszert és eljárásokat az r) pont szerint;

valamint a 2016. évi CL. törvény az általános közigazgatási rendtartásról és az Atv., továbbá annak végrehajtási rendeletei alapján.

Azokat a követelményeket, amelyekre az útmutató ajánlásokat fogalmaz meg, a 3-as és 3a-s NBSZ, a Rendelet és az IRMr. tartalmazza az alábbiak szerint:

Az útmutató a programozható rendszerek védelmi követelményeire terjed ki. A programozható rendszert a Rendelet 2. § (1) 17a. pontja az alábbiak szerint határozza meg:

„17a. programozható rendszer: olyan funkcionális eszköz vagy struktúra, amely alkalmas számítási, kommunikációs, automatizálási, vezérlési, ellenőrzési feladatok ellátására, ezen belül:

- a) a létesítmény technológiájához kapcsolódó irányítástechnikai rendszerek,*
- b) a fizikai védelmi rendszerek,*
- c) a nukleáris biztosítéki rendszerek,*
- d) a radioaktív anyag nyilvántartási rendszerek, valamint*
- e) a létesítmény technológiájához közvetlenül nem csatlakozó olyan nukleáris biztonsági, fizikai védelmi, nukleáris biztosítéki és radioaktív anyag nyilvántartási rendszerek, amelyekhez, valamint az azokban tárolt, kezelt adatokhoz, információkhoz engedélyesi felelősség kapcsolódik.”*

A programozható rendszer meghatározásának e) pontja alapján a Rendeletet alkalmazni kell az ügyviteli hálózat mindazon rendszereire, melyekben a

Nukleáris létesítmények programozható rendszereinek védelmi követelményei nukleáris biztonsági, fizikai védelmi, nukleáris biztosítéki és radioaktív anyag nyilvántartási rendszerekkel összefüggő adatokat, információkat tárolnak, kezelnek. A Rendelet alkalmazásában nem tartoznak a programozható rendszerek körébe a vállalatirányítási rendszerek, a vállalat általános működését támogató ügyviteli, irodai rendszerek pl. ERP-rendszerek, csoportmunka-támogató rendszerek, elektronikus levelezés stb.

A kiégett nukleáris üzemanyag tárolására szolgáló létesítmény esetében az NBSZ 6. kötet 6.2.4. fejezetének hatálya alá tartozó rendszerek és rendszerelemek védeltségét kell biztosítani.

A Rendelet 20. §-a írja elő a nukleáris létesítmény engedélyesének kötelezettségeit a programozható rendszerek védelmével összefüggésben:

- a) biztosítani kell a programozható rendszerekben tárolt, kezelt adatok és információk bizalmosságát, sértetlenségét és rendelkezésre állását, valamint a programozható rendszer sértetlensége és rendelkezésre állása kockázatokkal arányos védelmét;
- b) a fizikai védelmi terv részeként, a programozható rendszerek védelmének felépítését és működését leíró védelmi tervet kell készítenie;
- c) a programozható rendszerek védelmének felügyeletére a létesítmény legfelső vezetésének közvetlenül alárendelt szervezetet kell létrehoznia vagy kijelölnie;
- d) a létrehozott vagy kijelölt szervezet vezetője felelős a programozható rendszerek védelmének felügyeletéért, a szervezet a programozható rendszerek védelmével összefüggésben érintett szervezeti egységek delegáltjaiból vagy a kijelölt szervezeti egység beosztottjaiból áll;
- e) a programozható rendszerek tervezése, létesítése és módosítása során a Rendelet 6. melléklete alapján kell eljárnia.

Az üzemelő atomerőmű esetében az NBSZ 3. kötet 3.4.5 fejezete, és ezen belül a 3.4.5.2000., 3.4.5.2100., a 3.4.5.2400., a 3.4.5.2700., a 3.4.5.2800., a 3.4.5.3100., a 3.4.5.3200., és a 3.4.5.3300. pontok együttes megvalósítása a nukleáris biztonságot szolgálja úgy, hogy közben a védeltséget is támogatja. A 3.4.5.3500–3.4.5.4000. pontok a védeltség szempontjait képviselik, hozzájárulva a nukleáris biztonság megvalósításához.

Ez a szabályozás jól illeszkedik a Rendelet szelleméhez.

3.4.5.2000. „Az irányítástechnikai rendszerek és rendszerelemek tervezését és kivitelezését az adott biztonsági besorolású, rendszerekre és rendszerelemekre vonatkozó kiválasztott szabványoknak megfelelően, differenciált követelmények szerint kell végezni.”

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
Ebből az általános előírásból azonban több olyan IEC-szabvány követése adódik, amiknek követniük kell az IEC 61513, *Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems* című főszabványt. Az itt említendő szabványokat az 1.3 pont sorolja fel.

A következő előírás nagyon fontos informatikai kötöttséget ír le.

3.4.5.2100. „Meg kell határozni az irányítástechnikai rendszerek és a külvilág közötti emberi és automatikus kölcsönhatásokat logikai és fizikai interfészek formájában. A tervezett kölcsönhatások nem akadályozhatják az automatikus biztonsági funkciók teljesítését.”

Fontos körülmény, hogy ez az előírás jól képviseli azt az elvet, hogy ha a technológiához kapcsolódó rendszerek szeparációja nem lenne megoldható, olyan védelmi kiegészítéseket kellene ezekre a rendszerekre telepíteni, ami nem fér össze az IEC61226 szabvány „A” kategóriában a determinisztikus működés, az „A” és „B” kategóriában pedig az egyszerűség, és az ebből következő, a kizárólag a technológiai funkciók megvalósítására szolgáló szoftverkomponensek telepítésének elvével.

A harmadik előírás nagyon fontos informatikai és fizikai védelmi, adott esetben a beléptetési rendszerre vonatkozó követelményt ír le.

3.4.5.3200. „Megfelelő tervezési megoldásokkal továbbá intézkedésekkel kell biztosítani, hogy a programozható irányítástechnikai rendszerekhez – mind fizikailag, mind logikailag – csak azok a személyek férjenek hozzá, akiknek az szükséges és megengedett, és csak olyan szinten, olyan lehetőségekkel, amelyek a számukra előírt feladatok elvégzését lehetővé teszik.”

Az NBSZ-hez tartozó 3.5 jelű útmutató a technológiához kapcsolódó programozható rendszerek nukleáris biztonsági követelményeinek kielégítéséről szól, a jelen útmutató ezeket az ajánlásokat egészíti ki, egységes szerkezetben bemutatva a programozható rendszerek védelmi követelményeit a nukleáris biztonsági szabályozás hatálya alá nem tartozó programozható rendszerekkel.

Új atomerőmű esetében a nukleáris biztonság és a védelmi szempontok együttes kezelése a tervezéskor kezdődik. Az új atomerőmű tervezési követelményeit leíró NBSZ 3a kötetének 3a.4.5 fejezete, és ezen belül a következő pontok

3a.4.5.1600; 3a.4.5.1800; 3a.4.5.2000; 3a.4.5.2100; 3a.4.5.2200;
3a.4.5.2400; 3a.4.5.2600 (függetlenség); 3a.4.5.2700 d) pont;
3a.4.5.2800. (válaszidő); 3a.4.5.3100; 3a.4.5.3200 c), d) és e) pont;
3a.4.5.3300; 3a.4.5.3400; 3a.4.5.3500; 3a.4.5.3600;

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

3a.4.5.4000. (hibatűrő képesség és redundancia);

3a.4.5.4200 és 4300 (alacsonyabb biztonsági osztályú alrendszer nem okozhat hibát);

3a.4.5.4600. (emberi kezdeményezésű ellenőrzés lehetősége);

3a.4.5.4900 (teljes körű tesztelés);

3a.4.5.5100 (tanúsítás);

olyan biztonsági követelményeket és ezeken keresztül rendszertulajdonságokat írnak elő, amelyek a más jogszabályban a programozható rendszerek védelmére előírt követelmények teljesítését is támogatják.

Az NBSZ 3a kötetének a következő pontjai kimondottan a védettséget szolgálják:

3a.4.5.3700 (nincs kapcsolat a külvilággal, fizikailag egyirányú kommunikáció)

3a.4.5.3800 (fizikailag egyirányú kommunikáció)

3a.4.5.3900. (fizikailag egyirányú kommunikáció, teszteszközök csatlakoztatása)

3a.4.5.4100. (mélységi védelem)

3a.4.5.4500 (önellenőrző képesség)

3a.4.5.4700 (közös okú hibák lehetőségét minimalizálása)

3a.4.5.5000 (hozzáférés)

3a.4.5.5300 (Tervezési Alapfenyegetettség, és a fizikai védelemről szóló kormányrendelet)

3a.3.6.2800. „Ha a telephelyen vagy annak környezetében jelentős energiasűrűségű rádiófrekvenciás vagy mikrohullámú elektromágneses sugárforrás található, akkor vizsgálni kell annak hatását a nukleáris biztonság szempontjából fontos rendszerekre, rendszerelemekre. Ha ilyen hatás lehetősége fennáll, akkor megfelelő védelmi intézkedésekről kell gondoskodni.”

3a.3.6.2900. „A tervezési alap meghatározásakor figyelembe kell venni az emberi tevékenységgel összefüggő veszélyeztető tényezőket, és ezek hatását a biztonsági funkcióval rendelkező rendszerekre, rendszerelemekre. Ha ezek a hatások a biztonsági funkció teljesülését befolyásolnák, e hatásokkal szemben védelmet kell biztosítani. A védelem biztosítható adminisztratív eszközökkel is, azaz a veszélyt jelentő emberi tevékenység korlátozásával, de a védelem műszaki megoldásait ezekkel szemben előnyben kell részesíteni, amennyiben ilyen megoldások ésszerűen megvalósíthatók.”

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

3a.4.5.1400. *„Biztosítani kell az alapvető biztonsági funkciók ellenőrzéséhez szükséges paraméterek mérésére alkalmas műszerezést, megteremtve ezzel az atomerőművi blokk megbízható és biztonságos üzemeltetéséhez, a TA2-4 és a TAK1-2 üzemállapotot eredményező események kezeléséhez szükséges információk rendelkezésre állását.”*

3a.4.5.1900. *„Az irányítástechnikai rendszereket úgy kell tervezni, hogy a blokk üzemideje alatt akár többször is egyszerűen felújíthatók legyenek. A létesítési engedélykérelemben be kell mutatni a blokk üzemideje során alkalmazandó felújítási stratégiát az irányítástechnikai rendszerekre.”*

3a.4.5.2200. *„A nukleáris biztonság szempontjából fontos rendszer, rendszerelem műszer- és irányítástechnikai konfigurációja, működtető logikája vagy a hozzá tartozó adatok megváltoztatására szigorú adminisztratív ellenőrzés alatt álló lehetőségeket kell biztosítani.”*

3a.4.5.3100. *„Minden, a biztonság szempontjából fontos adatot archiválni kell. Az adathoz időbélyeg is tartozik. Az időbélyeget az adatfolyamban a keletkezéséhez legközelebb, minél korábban kell generálni. Az archívot a blokkok üzemidejének végéig meg kell őrizni.”*

3a.4.5.3700. *„ABOS 2. rendszer vagy rendszerelem az adott blokkon kívüli rendszerrel nem kommunikálhat, ugyanazon blokk alacsonyabb biztonsági osztályú rendszere vagy rendszereleme számára pedig csak fizikailag egyirányú kommunikáción keresztül adhat adatot.”*

3a.4.5.3800. *„A technológiához kapcsolódó irányítástechnikai rendszer másik blokk irányítástechnikai rendszere számára vagy külső rendszerek felé csak fizikailag egyirányú adatkapcsolaton keresztül szolgáltatathat adatot.”*

3a.4.5.3900. *„ABOS 2. rendszer adat kicsatolása céljából csak fizikailag egyirányú kommunikációval csatlakozhat alacsonyabb osztályú irányítástechnikai rendszerekhez. Diagnosztikai és szerviz célú eszközök alkalmazása esetén igazolni kell, hogy szándékolatlan vagy rosszindulatú parancsok bejutása a biztonsági rendszerbe a csatlakoztatott diagnosztikai és szerviz célú eszközök felől kizárt. ABOS 3. rendszerek esetében igazolni kell, hogy a csatlakoztatott alacsonyabb osztályú rendszerek vagy rendszerelemek felől szándékolatlan vagy rosszindulatú parancsok bejutása kizárt.”*

3a.4.5.4000. *„Az ABOS 2. biztonsági osztályba sorolt irányítástechnikai rendszerek alrendszereinek a megkövetelt hibatűrő képesség teljesítéséhez elegendő mértékben redundánsnak kell lenniük. A redundáns készleteknek funkcionálisan a lehető legnagyobb mértékben azonosak kell lenniük a szándékolt diverzitás alkalmazása mellett.”*

3a.4.5.4100. *„Az irányítástechnikai rendszerek architektúrájának illeszkedni kell a mélységben tagolt védelem szintjeihez. A mélységi védelemhez illeszkedő*

Nukleáris létesítmények programozható rendszereinek védelmi követelményei szinteket az ésszerűen megvalósítható legteljesebb mértékben el kell választani egymástól.”

3a.4.5.4200. „A nem biztonsági, vagy az alacsonyabb funkcionális biztonsági szinthez rendelt funkciók nem építhetők be egy biztonsági osztályba sorolt, vagy a szükségesnél magasabb biztonsági osztályba sorolt alrendszerbe. Amennyiben erre nincs lehetőség, biztonsági elemzéssel kell igazolni, hogy az alacsonyabb biztonsági szinthez rendelt funkciót teljesítő alrendszer semmilyen módon nem akadályozza valamely magasabb biztonsági szinthez rendelt funkció ellátását.”

3a.4.5.4300. „Különböző biztonsági osztályba sorolt irányítástechnikai rendszerek közötti kapcsolat esetén igazolni kell, hogy az alacsonyabb osztályba sorolt rendszer a magasabb osztályba sorolt rendszer működését nem befolyásolja. Azonos biztonsági osztályba sorolt irányítástechnikai rendszerek közötti kapcsolat esetén igazolni kell, hogy az egyik rendszer hibája a másik autonóm biztonsági funkcióinak teljesítését nem gátolja.”

3a.4.5.4700. „Az ABOS 2. biztonsági osztályba sorolt irányítástechnikai rendszerek esetén, a közös okú hibák lehetőségét minimalizálni kell megfelelő mértékű funkcionális vagy rendszerelem szintű diverzitás alkalmazásával. A diverzitás szükséges mértékét a megkívánt megbízhatósági követelményekből kell levezetni. Elemzéssel kell igazolni, hogy a választott megoldás mellett a közös okú meghibásodások valószínűsége elegendően alacsony.”

3a.4.5.4800. „Az atomerőmű tervezési alapjával összhangban követelményeket kell meghatározni - adott működési igény esetén - a működéselmaradás valószínűségére, valamint, ABOS 2. biztonsági osztályba sorolt irányítástechnikai rendszerek esetén, a téves működés gyakoriságára vonatkozóan.”

3a.4.5.4900. „Biztonsági osztályba sorolt irányítástechnikai rendszereket és rendszerelemeket az adott környezetben teljes körűen kell tesztelni, a tesztelési és az elfogadási kritériumok előzetes meghatározásával.”

3a.4.5.5000. „Megfelelő tervezési megoldásokkal, továbbá intézkedésekkel kell biztosítani, hogy irányítástechnikai rendszerekhez - mind fizikailag, mind logikailag - csak azok a személyek férjenek hozzá, akiknek az szükséges és megengedett, és csak olyan szinten, olyan lehetőségekkel, amelyek a számukra előírt feladatok elvégzését lehetővé teszik.”

3a.4.5.5300. „A programozható irányítástechnika tervezésekor a Tervezési Alapfenyegetettség vonatkozó részeit és az atomenergia alkalmazások fizikai védelemről szóló kormányrendelet előírásait is figyelembe kell venni.”

3a.4.5.5400. „A tervezésben a programozható rendszerek védelmi szempontjait is figyelembe kell venni. Ha a tervezés során a nukleáris biztonsági

Nukleáris létesítmények programozható rendszereinek védelmi követelményei és a programozható rendszerek védelmi szempontjai konfliktusba kerülnek, a nukleáris biztonsági szempont prioritást élvez.

3a.4.5.5500. „Az Előzetes Biztonsági Jelentésben és a Végleges Biztonsági Jelentésben meg kell határozni az atomerőművi blokk irányítástechnikájával összefüggésben a mereven huzalozott - a félvezető alapú áramkörökkel gyártott logikákat beleértve - és a programozott eszközök megkülönböztetésével az informatikai és irányítástechnikai biztonság szempontjából kockázatot jelentő hozzáférések, valamint a funkció, a programok és az adatok módosításának fizikai lehetőségeit. Ezeket a lehetőségeket a megvalósíthatóság, valamint a módosítás eléréséhez szükséges szakértelem szintjének szempontjából sorrendbe kell állítani, és ennek megfelelően kell a beavatkozásokat elvégezni.”

3a.4.5.5600. „A programozható eszközök rendellenességeit detektálni kell. Biztosítani kell, hogy a program és a konstans adatfájlok át nem írható adathordozóról beolvasott, installáláskor képzett megbízható adatok szerint ellenőrizhetőek legyenek. Ahol ésszerűen megvalósítható, szükséges a technológiából beolvasott adatok hihetőségének vizsgálata.”

3a.4.5.5700. „A védelmi és biztonsági rendszerekhez tartozó végrehajtó szerveket működtető, továbbá a nukleáris biztonság szempontjából fontos, az üzemeltető személyzet döntéseit befolyásoló adatokat gyűjtő és megjelenítő funkciókat ellátó rendszereket és eszközöket meg kell védeni a biztonsági funkció megváltoztatását lehetővé tévő külső befolyásolás ellen.”

3a.4.5.5800. „A fizikai hozzáférés lehetőségeit, az adattovábbító eszközök és adatkábelek elhelyezését a fizikai védelmi zónákkal összhangban kell kialakítani.”

3a.4.5.5900. „Ki kell dolgozni a szükséges adminisztratív rendszert és az ehhez tartozó belső eljárás és a hozzáférések biztonsági protokolljait:

- a) a rendszerekben szükséges karbantartás elvégzésére,
- b) a digitális rendszerek szükséges módosítására,
- c) a feltárt program- és adathibák kijavítására, és
- d) az adathordozók ellenőrzésére, ki- és beszállítására.”

3a.4.5.6000. „Az irányítástechnikai konfigurációkezelésnek az alábbi területeket is le kell fednie:

- a) a rendszer és a rendszerelemek dokumentációját, kereskedelmi termék esetén is,
- b) a hardverdokumentációt,
- c) a szoftverdokumentáció és -kód minden formáját, így többek között a specifikációkat, a tervezési dokumentumokat, a forráskódokat, a futtatható kódokat, gépi kódokat, könyvtárakat,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- d) fejlesztőrendszereket, beleértve a kódgenerátorokat, fordítóprogramokat, tesztkörnyezeteket és teszteszközöket,
- e) a teszteseteket és eredményeket,
- f) a módosításokat és az azokhoz kapcsolódó elemzéseket, valamint
- g) az oktatási anyagokat."

A nukleáris biztosítéki követelmények szempontjából irányadó az IRMr.:

5. § (1) „A nukleáris anyaggal rendelkező szervezet a rendelkezése alá eső nukleáris anyagokról helyi nyilvántartást vezet. A helyi nyilvántartásnak meg kell felelnie a Biztosítéki Egyezményben foglalt követelményeknek.

...

(5) A helyi nyilvántartást úgy kell vezetni, hogy abból bármikor megállapítható legyen a szervezet rendelkezése alá tartozó nukleáris anyagok minősége és mennyisége elemenként (urán, plutónium, tórium), valamint hasadóanyag tartalma.

...

6. § (6) A nukleáris nyilvántartást vezető szervezetnek gondoskodnia kell a nyilvántartás és az üzemeltetési feljegyzések biztonságáról, az adatokhoz való illetéktelen hozzáférés megakadályozásáról."

1.3. Nemzetközi és hazai ajánlások

A NAÜ Védettségi Sorozat 17. kötetének, a 'Számítógépes védettség nukleáris létesítményekben' („Computer Security at Nuclear Facilities”, IAEA Nuclear Security Series 17) című műszaki útmutató kidolgozásának elsődleges célja az volt, hogy felhívja a figyelmet a számítógépes védettség fontosságára a nukleáris létesítmények teljes fizikai védelmi tervezésének részeként. A kiadvány megmutatja a számítógépes védettségi program végrehajtására javasolt módszereket, szerkezeteket és végrehajtási eljárásokat.

Az IEC 61513, *Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems* című főszabványt követő, programozható irányítástechnikai rendszerek védelme témában is alkalmazandó szabványok a következők.

- a) IEC 61226 Edition 3.0 (2009) Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions
- b) IEC 60987 ed2.0 (2007) Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- c) IEC 60880:2006 Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category “A” functions
- d) IEC 62138 (2004) Nuclear power plants –Instrumentation and control important for safety –Software aspects for computer-based systems performing category “B” or “C” functions
- e) IEC 62645 Ed.1: Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems

Az irányítástechnikai funkciók biztonsági kategorizálására, az „A”, “B” és “C” kategóriájú funkciók hardver- és szoftverösszetevőinek megvalósítására vonatkozó szabványok követése elsősorban a nukleáris biztonság szempontjából fontos; de ezek követése, és az így előálló rendszer- és rendszerelem-tulajdonságok fontos összetevői lehetnek a védelmi célok megvalósításának is.

A hibák és működési anomáliák biztonsági rést jelenthetnek a szoftver termékekben. A védelem első fokozatát jelenti a hibák kiküszöbölése, amelynek egyik megoldása a minőségügyi rendszerek szerint elvégzett szoftverfejlesztés. Ehhez nyújtott segítséget a minőségirányításról szóló ISO 9000-es szabványsorozat (Quality management and quality assurance standards) 1997-ben kiadott 3. része: *“Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software”*.

A szabványt 2004-ben adták ki újra az IEC-szabványtestület közreműködésével ISO/IEC 90003:2004 azonosítóval. A szabvány útmutatót nyújt az ISO 9001:2000 szabványban megtestesülő minőségirányítási elvek érvényesítéséhez a szoftvertermékek és támogatószolgáltatások beszerzése, fejlesztése, üzemeltetése, és karbantartása során. A szabvány útmutatóval szolgál a

- a) kereskedelmi szerződésekben leírandó szempontokra,
- b) a piacon elérhető termékekre,
- c) a szervezetek belső folyamatainak támogatására,
- d) a hardvertermékekbe beágyazott szoftvertermékek szempontjaira, és
- e) a szoftverekkel kapcsolatos szolgáltatásokra.

A szoftverszabvány előszava szerint a szabvány ugyanakkor nem jelent kritériumot a minőségirányítási rendszerek tanúsításához.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
Az ISO/IEC 9000-3 szabvány minden technológiától függetlenül útmutatást ad az életciklusmodellekre, a fejlesztés folyamatára, az egyes tevékenységek sorrendjére és a vállalati, mérnökirodai vagy más szervezet feladatokkal összefüggő szervezeti felépítésére. További szabványok és műszaki jelentések (Technical Report) érhetőek el a szoftverfejlesztés, üzemeltetés és karbantartás (software engineering) további szempontjairól az ISO 9001 elveinek követésében: ISO/IEC 12207, ISO/IEC TR 9126, ISO/IEC 14598, ISO/IEC 15939 és ISO/IEC TR 15504.

A mai világban szükséges számítógépes védelem alapszabványa az ISO/IEC 27000 szabvány, amely az információ védelmének irányítási rendszerét (*information security management system*) tekinti át, és leírja a szükséges definíciókat és terminológiát.

A szabványsorozat másik tagja az ISO/IEC 27001 szabvány azt vállalja, hogy minden típusú szervezethez szól, legyenek azok piaci vállalkozások, kormányzati szervek vagy non-profit szervezetek. A szabvány leírja azokat a követelményeket, amelyekkel megalapozható, megteremthető, működtethető, felügyelhető, karbantartható és fejleszthető a szervezet üzleti kockázatokat csökkentő információbiztonságirányítási rendszere. A követelmények kiterjeszthetők az egész szervezetre, de alkalmazhatók a szervezet egyik vagy másik részére is. A szabvány követelményeinek alkalmazása lehetővé teszi az adekvát, de arányos védelmi intézkedések bevezetését és fenntartását a szervezet birtokában lévő bizalmas információk megvédésére, a más szervezetekkel való együttműködés akadályozása nélkül, és tiszteletben tartva a jogszabályokban írottakat. A szabvány felhasználható a külső és belső auditorok számára.

A szabványsorozat következő tagja a több korábbi szabványt magába foglaló ISO/IEC 27002 szabvány. Általános elveket és útmutatást közöl az információvédelem irányítási rendszerének bevezetésére, megvalósítására, karbantartására és fejlesztésére, általában elfogadott célokat is megfogalmazva, bemutatva a jó gyakorlatot

- a) a védettségi politika (security policy),
- b) az információvédelem szervezeti kérdései,
- c) a szervezet tulajdonában lévő ingatlanok, berendezések és más műszaki felszerelések fenntartására,
- d) az ezekhez való hozzáférés szabályozásának megoldására,
- e) az emberi erőforrások védelmi kérdései terén
- f) a fizikai védelem és védettség terén, beleértve a környezeti tényezőket
- g) a vezetés tevékenysége és kommunikációja terén,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- h) az informatikai rendszerek beszerzése, fejlesztése és karbantartása terén,
- i) az incidensek kezelése és a védettség helyreállítása terén,
- j) az üzleti tevékenység fenntartásának szempontjairól, és
- k) a követelményeknek való megfelelés szempontjairól.

Az irányítás céljait és eszközeit a kockázatelemzés kell, hogy megalapozza. A szervezet belső biztonsági szabványában kell a teendőket úgy leírni, hogy ezek támogassák a hatékony biztonságirányítást, miközben nem akadályozzák a bizalmi elven működtetett külső kapcsolatokat.

Fontos kiegészítést jelent az ISO/IEC 27010 szabvány, amely az egyszerre megosztandó és védendő információk védelméről és a védelmi irányítási rendszeréről szól. A szabványt a problémák természete miatt kell alkalmazni a nukleáris iparban együttműködő vállalatok, mérnökirodák és szolgáltatók közti kommunikáció és információszolgáltatás során; beleértve a hatósági feladatokat ellátó szervezeteket! A szabvány releváns a műszaki fejlesztések, a nukleáris létesítmények és technológiai rendszereinek a megtervezése, üzembe helyezése és későbbi üzemeltetése során. A szabvány felhasználható a kritikus infrastruktúrák védelmében.

Az IEC 45-ös bizottsága az IEC62645 szabvány (tervezet) bevezetőjében nukleáris létesítmények számára a következőket ajánlja a számítógépek veszélyeztetésének elkerülése tárgyában:

- a) Olyan szabványok, mint az ISO/IEC 27000, 27001 és 27002 nem alkalmazhatók közvetlenül a nukleáris létesítmények irányítástechnikai rendszereire, ezek sajátosságai miatt.
- b) A számítógépek veszélyeztetésének elkerüléséről szóló általános ipari szabványok és más útmutatások felhasználása a nukleáris létesítményekben azonban járhat előnyökkel, de önmagában ez nem elégséges.
- c) Minden szabályozásnak illeszkednie kell az IEC61513, Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems főszabványba.

A számítógépek veszélyeztetése hatással lehet a nukleáris létesítmény üzemelésére, a nukleáris biztonságra, és elvezethet az üzemeltető személyzetet, a környezetet és a lakosságot fenyegető hatáig. A számítógépek veszélyeztetésének a célpontja a berendezések és a technológia, nem pedig maga a digitális rendszer. A digitális rendszerek a támadás eszközt jelentik.

Az irányítástechnika meghibásodása és működésképtelensége a létesítmény nukleáris biztonságát az el nem fogadható szintig leronthatja, és

Nukleáris létesítmények programozható rendszereinek védelmi követelményei megnövelheti egy nukleáris baleset, a reaktor üzemanyag-károsodásának, a zóna megolvadásának, és nagymértékű radioaktív anyag kibocsátásnak a valószínűségét. A számítógépek veszélyeztetése egy nukleáris létesítményben sokkal nagyobb károkat okozhat, mint más iparágakban.

A számítógépek veszélyeztetése a kritikus fontosságú berendezések kockázatával járhat, a turbina vagy a blokktranszformátor károsodása pedig költséges javításokra és hosszán tartó energiatermelés-képtelenségre vezet.

A nukleáris létesítmény egy olyan biztonságkritikus alkalmazás, amely gyors, valós idejű válaszokat igényel egy súlyosbodó helyzetben. Az üzemeltető személyzetnek gyorsan kell reagálni a fejleményekre, és ehhez fel kell, hogy használja a technológiából beolvasott paraméterek értékeit, és meg kell tudnia bízni ezek valóságosságában.

Az ISO/IEC 27000, 27001 és 27002 szabványok felhasználása nagyon fontos a nukleáris létesítmény technológiai rendszereinek tervezését, gyártását, minősítő tesztelését, majd a létesítményben történő telepítés után az üzemeltetést és karbantartást végző vállalati, mérnökirodai és informatikai szolgáltatásokat végző szervezeteknél; a technológiához kapcsolódó irányítástechnika védelme azonban további követelmények alkalmazását igényli, a nukleáris biztonságra és a fizikai védelemre vonatkozó szabályozások együttes felhasználásával.

Fontos előírást tartalmaz „A Bizottság ajánlása (2009. február 11.) a nukleáris anyagok nyilvántartási és ellenőrzési rendszerének nukleáris létesítmények üzemeltetői általi alkalmazásáról” (2009/120/Euratom), melynek 6. szakasza kimondja, hogy „adatfeldolgozási rendszert szükséges alkalmazni az NMAC-rendszer megfelelő működéséhez szükséges adatok biztonságos és védett tárolása érdekében”, az adatfeldolgozási eljárások szolgáljanak a 302/2005/Euratom rendelet szerinti információkkal és biztosítsák mindezen információk nyomon követhetőségének folytonosságát. Lehetővé kell tenni minden olyan információ és adat meghatározását, amelyre szükség lehet a 302/2005/Euratom rendelet követelményeiből fakadó eltérések és rendellenességek tisztázásához.

1.3.1. *Általánosan alkalmazott alapelvek*

Az útmutató ajánlásaiban gyakran történik utalás a kockázatelemzésre. A Rendelet 20. § (1) előírja a programozható rendszer kockázatokkal arányos védelmét. Az útmutatóban ezeket a fogalmakat úgy értjük, hogy a megfelelő elemzéseket, valamint az alkalmazott védelmet úgy kell elvégezni, illetve kialakítani, hogy az mindenkor arányos legyen a védett programozható rendszer fenyegetettségével. Ebben az összefüggésben jól alkalmazhatónak véljük a sugárvédelemben bevált ALARA-elvet: sugárveszélyes munkahelyen

Nukleáris létesítmények programozható rendszereinek védelmi követelményei foglalkoztatott személyek sugárterhelését az ésszerűen elérhető legalacsonyabb szinten kell tartani a gazdasági-társadalmi tényezők figyelembevételével. Ezzel összhangban tehát az ALARA-elvvel analóg követelményt így fogalmazhatjuk meg: az elemzéseket és a védelmet az ésszerűen elérhető legmagasabb szinten kell elvégezni és megvalósítani a gazdasági-társadalmi tényezők figyelembevételével.

A programozható rendszerek védelmét illető elemi alapelv még a fokozatosság elve. Ezen azt értjük, hogy az alkalmazott védelmi intézkedéseknek mindenkor arányosaknak kell lenniük a támadás várható következményeivel.

2. MEGHATÁROZÁSOK ÉS RÖVIDÍTÉSEK

2.1. Meghatározások

Az útmutató az Atv. 2. §-ában, valamint a Rendelet 2. §-ában ismertetett meghatározásokon kívül az alábbi definíciókat tartalmazza.

Adat:

Adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

Bizalmasság:

Az adatnak az a tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Behatolástesztelés:

A sérülékenység vizsgálat során alkalmazható vizsgálati módszer, amelyben a vizsgáló személy meghatározott megszorításokkal megpróbálja a rendszerek védelmi kontrolljait megkerülni vagy kijátszani, hogy bejusson a rendszerbe.

Belső fenyegetések, belső elkövetők jelentette fenyegetések:

Azon személyek jelentette fenyegetések, akik a nukleáris létesítmény programozható rendszereinek működésével és védelmével kapcsolatban (akár jelentős) ismeretekkel, jogosultsággal és hatáskörrel rendelkeznek. Emellett ezen személyeket olyan motivációs erők befolyásolják, amelyek arra készítetik az elkövetőt vagy támadót, hogy elkövesse vagy megkísérelje elkövetni a rosszindulatú cselekményt. A belső elkövetők elleni védekezés vonatkozásában lásd az FV-13. számú, „Belső elkövetők elleni védelem” című útmutatót.

Elszámoltathatóság:

Annak a biztosítéka, hogy az adatokkal végzett műveletek végrehajtója később azonosítható legyen.

Felhasználó:

Védett információt munkaköri leírása vagy szerződése szerint használó, az informatikai rendszer használatára képesített és feljogosított személy. A felhasználó fogalmába beleértjük a felügyeleti joggal eljáró hatóság képviselőjét.

Felhasználói belépés ellenőrző rendszer:

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
Olyan eszközök és módok, amelyek biztosítják, hogy az arra feljogosított személy a védelmi követelményeknek megfelelően férjen hozzá az adott rendszerhez

Fenyegetés:

Az emberek, a tulajdon vagy a környezet sérelmével járó káresemények okozásának lehetősége olyan személyek által, akik motivációval, szándékkal és lehetőséggel rendelkeznek a rosszindulatú cselekmények elkövetésére.

Határ:

Az a fizikai vagy logikai választóvonal, amely egy ellenőrzött módon hozzáférhető, hálózatba kapcsolt kritikus eszközök együttesét körülveszi.

Helyettesítő védelmi kontroll:

Egy védelmi kontroll helyett vagy mellett olyan védelmi kontroll használata, amely legalább ugyanolyan erősségű, mint az eredeti kontroll.

Hitelesség:

Az adatnak az a tulajdonsága, hogy a tartalma az elvárt forrásból származik.

Hitelesítés:

Felhasználó, folyamat vagy eszköz azonosságának ellenőrzése. Gyakran az erőforrásokhoz történő hozzáférés előfeltétele.

Információ:

Információ bizonyos tényekről, tárgyakról vagy jelenségekről; hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.

Megjegyzés: A fentiekén kívül az információnak vannak más tulajdonságai, mint a hitelesség, az elszámoltathatóság, a letagadhatatlanság (és a megbízhatóság).

Információvédelem:

Az információ bizalmosságának, sértetlenségének és rendelkezésre állásának megőrzése.

Jelentésköteles incidens:

Olyan, programozható rendszerekkel kapcsolatban bekövetkezett incidens, amelynek során az elkövető magatartása és tevékenysége megalapozottan

- szabotázsra vagy

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- radioaktív anyag, nukleáris anyag, radioaktív hulladék jogtalan eltulajdonítására

irányul. Az ilyen eseményt az engedélyes köteles jelenteni a Rendelet 33. § (1) szerint.

Jelentős energiasűrűségű rádiófrekvenciás vagy mikrohullámú elektromágneses sugárforrás:

A 0 Hz-300 GHz frekvenciájú elektromos, mágneses és elektromágneses terek lakosságra vonatkozó egészségügyi határértékeinek a 10%-át; és azt a körülményt tekintjük a védett objektum környezetében lévő jelentős energiasűrűségű rádiófrekvenciás vagy mikrohullámú elektromágneses sugárforrás meglétének, ha kimutatható, megmérhető hatások érik a védendő készüléktechnika vezető, félvezető, és poláris molekulákat tartalmazó anyagból készült részegységeit, alkatrészeit.

Kibertámadás:

Olyan művelet vagy esemény, amely sértheti a programozható rendszerek védeltségét vagy biztonságát.

Kockázat:

Annak a lehetőségnek a mértéke, hogy egy adott fenyegetés kihasználja egy adott rendszer vagy rendszercsoport sérülékenységeit, és ezzel kárt okoz a rendszert üzemeltető szervezetnek. Mérése a támadás valószínűségének (T), amely függ a motivációtól, képességtől és a szándék rosszindulatától, a támadás sikeressége valószínűségének (S), amely függ a sérülékenységektől és a következmények (K) kombinációjából adódik. $Kockázat = T \times S \times K$.

Kockázatkezelés:

Folyamat, amely a programozható rendszerek működéséből adódó kockázatokat kezeli, amelyek kihatással vannak a szervezet működésére (beleértve a küldetést, funkciókat, hírnevet, stb.), a szervezet vagyontárgyaira, személyzetre, más szervezetre és a nemzetre. Magában foglalja a kockázatelemzést, kockázatcsökkentő stratégia megvalósítását, valamint eszközök és eljárások alkalmazását a védelmi állapot állandó monitorozására.

Kockázatkezelési keretrendszer:

Egy strukturált folyamatot biztosít, amely integrálja a programozható rendszerek védelmével kapcsolatos - és a kockázatkezelési tevékenységeket a programozható rendszerek életciklusába.

Letagadhatatlanság:

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
Az adatnak az a tulajdonsága, amely megfelelő bizonyítékokkal szolgál a programozható rendszerben végrehajtott tevékenységek ellenőrizhetőségét illetően.

Maradványkockázat:

A védelmikontroll-intézkedések megvalósítása után fennmaradó kockázat.

Minimális felhasználói létszám:

A programozható rendszerekhez hozzáférő személyzet létszámát esetenként ajánlatos a szükséges mértékig vagy az abszolút minimum értékéig korlátozni. A korlátozás minimum értékét indokolni kell.

Nagyon gyors elektromágneses impulzusok:

A 300 MHz - 300 GHz (hullámhossz: 1 m - 1mm) mikrohullámú sávba sorolható, vagy e fölötti frekvenciájú felharmonikusokat is tartalmazó elektromágneses sugárzás, amely spontán létrejön természeti jelenség (pl. villám) vagy ember által készített eszköz működtetésekor, beleértve a híradástechnikában az információátvitelhez használt moduláció lehetőségét. Az ilyen impulzusok fizikai hatásaik révén, ha nagy energiájúak, az elektronikus és villamos rendszereket károsíthatják, vagy a károkozás irányába kifejlődő effektusokat hozhatnak létre. A kis energiájú impulzusok az elektronikus és villamos rendszerek és eszközök működését közvetlen degradáció és károkozás nélkül időlegesen befolyásolhatják, mivel az impulzusok az adatátvitelhez hasonló effektust jelenthetnek.

Napló:

A programozható rendszerek folyamatos működése során a rendszer működéséről, állapotáról, az esetleges hibák, fennakadások vagy egyéb események körülményeiről készült szöveges állomány.

Programozható rendszer:

A számítási, számítástechnikai, kommunikációs vagy irányítástechnikai feladatok ellátására alkalmas eszközök, ide értve nemcsak pl. a személyi (asztali vagy hordozható) számítógépeket, a mainframe-eket, szervereket, hálózati eszközöket stb., hanem alacsonyabb szintű eszközöket is, mint pl. a beágyazott rendszereket, PLC-ket (programozható logikai vezérlő) stb., vagyis bármely valamilyen módon elektronikus fenyegetettségnek kitett eszközt.

Programozható rendszerek védelme (informatikai védelem):

Megjegyzés: a biztonság (safety) kifejezést ebben az útmutatóban csak a nukleáris biztonságra (nuclear safety), a védettség (security) kifejezést csak a nukleáris védettségre értjük, míg a biztonsági, védettségi és békés célra való

Nukleáris létesítmények programozható rendszereinek védelmi követelményei alkalmazással együttesen összefüggő kérdésekben mindig védelemről beszélünk.

Programozható rendszerek védelmi felelőse:

A Rendelet 20. § (3) bekezdése szerint a programozható rendszerek védelmének felügyeletére kijelölt vagy megbízott, a létesítmény legfelső vezetésének közvetlenül alárendelt szervezet vezetője.

Programozható rendszerek védelmi politikája:

Egy adott szervezetre érvényes, programozható rendszer védelmi elveinek olyan összessége, amely a teljes szervezet működésére kihat. Ez a dokumentum fogalmazza meg egységes szemlélettel a szervezetnek és a szervezet tagjainak a programozható rendszerek védelméhez kívánatos viszonyulását és az érvényesítés alapelveit az intézmény egészére. A programozható rendszerek védelmi politikája alapján kell kidolgozni az egységes szerkezetbe foglalt, az egész intézményre érvényes, és a más területekre vonatkozó többi szabállyal összhangban álló programozható rendszerek védelmi szabályzatát.

Programozható rendszerek védelmi szervezete:

A Rendelet 20. § (3) bekezdése szerint a programozható rendszerek védelmének felügyeletére a létesítmény legfelső vezetésének közvetlenül alárendelt szervezet.

Rendelkezésre állás:

Az adat, illetve a programozható rendszer elemeinek az a tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható.

Sérülékenység:

Egy hiba vagy gyenge, sebezhető pont a programozható rendszerek tervezésében, megvalósításában vagy működtetésében és menedzselésében, amit a fenyegetettség forrásai kiaknáznak károkozás céljából.

Sérülékenységmonitorozás:

A programozható rendszerek sérülékenységét folyamatosan figyelő és az ismertté vált sebezhetőségeket beazonosító, automatizált eszköz által vagy manuálisan végzett folyamat, amelynek során jellemzően passzív, non-intruzív technikák kerülnek alkalmazásra. Ideális esetben ennek eredménye egy folyamatosan aktualizált helyzetkép a monitorozott programozható rendszereket érintő sérülékenységekről. Elsődleges célja a sérülékenységek figyelemmel kísérése és indokolt esetben kezelése.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

Sérülékenységvizsgálat:

A programozható rendszerek sérülékenységeinek felderítése érdekében végzett, klasszikusan aktív és passzív elemeket, automatizált és manuális felderítő eszközöket, intruzív és non-intruzív technikákat egyaránt alkalmazó vizsgálat, amelynek eredménye az adott rendszer adott pillanatban feltárt sérülékenységeit mutatja.

Sértetlenség:

Az adatnak az a tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a hitelességet és a letagadhatatlanságot.

A programozható rendszerelemnek az a tulajdonsága, amely arra vonatkozik, hogy a rendszerelem rendeltetésének megfelelően használható.

Social engineering:

A social engineering (pszichológiai manipuláció) a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni, jellemzően adatok kiszolgáltatására vagy biztonsági kockázatot jelentő cselekedetek elvégzésére rávenni.

Támadási vektor:

Olyan útvonal, mód vagy eszköz, amit a támadó ahhoz használ, hogy a célt megtámadja.

Támadási fa:

Koncepcionális diagram, amely egy faszerkezetben mutatja a gyökércsomópontban meghatározott támadási cél elérési módjait.

Támadási gráf:

A támadási gráf egy célpont és a vele kapcsolatos támadási lehetőségek, eszközök és módok olyan együttes reprezentációja, amely az egyes elemek (csomópontok) közötti kölcsönös függőségeket (kapcsolatokat) feltárva képes modellezni a célpont ellen irányuló támadásokat.

Távoli hozzáférés:

Távoli hozzáférésnek tekinthető, ha bármely felhasználó a programozható rendszer jelátviteli rendszerén keresztül, védelmi szinteket átlépve adatokat, programokat, informatikai eszközöket tud elérni, vagy használni.

Távoli karbantartás:

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

Távoli karbantartásnak tekinthető az a távoli hozzáférés, amelynek célja a rendszerek, berendezések állapotának, eredeti működképességének, megbízhatóságának fenntartása. Formája a folyamatokkal, berendezésekkel kapcsolatos információszerzés, feldolgozás, és menedzselési feladatok ellátása. Távoli karbantartásnak tekinthető a rendszerelemek távoli szoftver frissítése, fejlesztési célú programösszetevők távoli telepítése.

Védelmi esemény:

Bármilyen észlelhető vagy megkülönböztethető történés, amelynek jelentősége van a programozható rendszer üzemeltetésére vagy szolgáltatás nyújtására, valamint annak a hatásnak az értékelésére, amelyet egy adott eltérés okozhat a szolgáltatásokban.

Védelmi incidens:

Olyan szándékosan előidézett vagy véletlenül bekövetkező védelmi esemény (vagy eseménysorozat), amely ténylegesen vagy potenciálisan veszélyezteti egy programozható rendszer vagy az abban tárolt, feldolgozott illetve továbbított információ bizalmasságát, sértetlenségét vagy rendelkezésre állását; vagy a biztonsági politikák, biztonsági eljárások illetve a kapcsolódó házirendek megsértésével vagy annak közvetlen veszélyével jár.

Védelmi kontroll, (kontroll):

Védelmi kontrolloknak nevezzük mindazokat a technikai (logikai), fizikai és adminisztratív védelmi intézkedéseket, amelyek alkalmazása biztosítja a programozható rendszerek védelmét az ember által okozott szándékolatlan károkozás és a tervezési alapfenyegetettségben meghatározott kibertámadásokkal szemben.

Védelmi követelmények:

Olyan irányelvek, előírások, szabályok és eljárások összessége, amelyek előírják, hogy egy szervezet hogyan kezeli és védi a programozható rendszereit.

Védelmi program:

A védelmi program menedzseli és rangsorolja azokat a folyamatokat és tevékenységeket, amelyek a programozható rendszerek különböző nézőpontból történő védelmét valósítják meg a védelmi célok elérése érdekében.

Védelmi szint:

A védelmikontroll-intézkedések megvalósításával elért védettség, amelyet a kockázatelemzés állapít meg a maradványkockázat kimutatásával. A védelmi szint elfogadható, ha a maradványkockázat mértéke elfogadható.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

Védelmi zóna:

A védelmi zóna a megállapított kockázatok szerint csoportosítja a programozható rendszereket. Ugyanabba a védelmi zónába tartozó programozható rendszerek azonos humán, fizikai és kibervédelmi követelményeknek felelnek meg és így a védelmi szintjük azonos.

2.2. Rövidítések

CPU	Central Processing Unit
DMZ	De-Militarized Zone
ERP	Enterprise Resource Planning
FAT	Factory Acceptance Test
FPGA	Field Programmable Gate Array
HIDS	Host Intrusion Detection System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
NBSZ	Nukleáris Biztonsági Szabályzatok, azaz a 118/2011. (VII.11.) Korm. rendelet 1-10-ig számozott mellékletei, amelyekre mint az NBSZ kötetekre történik hivatkozás
PAM	Privileged Access Management
PLC	Programmable Logic Controller
PKI	Public Key Infrastructure
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAT	Site Acceptance Test
SDA	Sensitive Digital Asset
UBA	User Behavior Analytics
USB	Universal Serial Bus
UTM	Unified Threat Management
VPN	Virtual Private Network
WLAN	Wireless Lan

3. AZ ÚTMUTATÓ AJÁNLÁSAI

3.1. A programozható rendszerek védelmének szervezete, felelőségek

3.1.1. Az engedélyes szervezet és a hozzá tartozó létesítmény felső vezetésének felelőssége

Az engedélyes szervezetnek és a hozzá tartozó létesítmény felső vezetésének tisztában kell lennie azzal, hogy a létesítményben egyre szélesebb körben, a nukleáris biztonság, a fizikai védelem, a nukleáris biztosítéki követelmények és a sugárvédelem szempontjából létfontosságú tevékenységek ellátására használnak programozható rendszereket. Ez a fejlődés számos előnnyel jár a nukleáris biztonság, a fizikai védelem, a nukleáris biztosítéki követelmények és a sugárvédelem területén. Az előnyök kihasználása érdekében a programozható rendszerek megfelelően biztonságos működését alkalmas és kiegyensúlyozott védelmi intézkedésekkel kell biztosítani. A védelmi intézkedéseknek maximalizálniuk kell a külső hatások, a véletlen és a szándékos (rosszindulatú) cselekmények elleni védelmet anélkül, hogy szükségtelenül akadályoznák a rendszerek működését.

Az engedélyes szervezet és a hozzá tartozó létesítmény felső vezetése általános felelősséget visel a jogszabályi háttérnek megfelelő, a programozható rendszerekre vonatkozó védelmi előírások bevezetéséért és azok betartatásáért. Ennek érdekében

- a) gondoskodik a létesítmény jogszabályi- és hatósági előírásoknak megfelelő működéséről,
- b) meghatározza a programozható rendszerek elfogadható kockázatának mértékét,
- c) gondoskodik arról, hogy a létesítménynek legyen érvényes, a programozható rendszerekre vonatkozó védelmi politikája,
- d) gondoskodik arról, hogy a programozható rendszerek védelmi feladatainak ellátásához megfelelő erőforrások álljanak rendelkezésre,
- e) gondoskodik a programozható rendszerekre vonatkozó védelmi politika és a programozható rendszerekre vonatkozó védelmi eljárások időszakos felülvizsgálatáról és frissítéséről,
- f) gondoskodik a programozható rendszerek védelméhez kapcsolódó képzésekről, továbbképzésekről és tájékoztatásról.

A programozható rendszerek védelmi politikája részét kell, hogy képezze a nukleáris létesítmény védelmi politikájának (a védelmi politika vagy önálló dokumentum, vagy része a létesítmény minőségügyi politikájának). A

Nukleáris létesítmények programozható rendszereinek védelmi követelményei programozható rendszerek védelmi politikája meghatározza a létesítmény általános, magas szintű, a programozható rendszerekre vonatkozó védelmi céljait, összhangban a nukleáris biztonság, a fizikai védelem, a nukleáris biztosítéki követelmények és a sugárvédelem területén kitűzött célokkal, figyelembe véve az ebből adódó jogi és az emberi erőforrásra gyakorolt hatásokat.

A programozható rendszerekre vonatkozó védelmi politikában megfogalmazott követelményeket alacsonyabb szintű dokumentumokban le kell bontani olyan előírásokra, amelyek a végrehajtás és az ellenőrzés során használhatók. A programozható rendszerekre vonatkozó védelmi politikában érvényesíthető, végrehajtható és ellenőrizhető célokat kell megfogalmazni.

Az engedélyes szervezet és a hozzá tartozó létesítmény felső vezetése a programozható rendszerek védelmével kapcsolatos felügyeleti és koordinációs tevékenység ellátása érdekében felelős szervezetet hoz létre vagy jelöl ki, aminek élén a felső vezetés közvetlen alárendeltségéhez tartozó programozható rendszerek védelmi felelőse áll. A szervezet a programozható rendszerek védelmi felelősének irányítása mellett a közvetlen beosztottjaiból és/vagy a programozható rendszerek működtetéséért és a programozható rendszerek védelmének működtetéséért felelős személyek által kijelölt védelmi megbízottakból áll.

3.1.2. *A programozható rendszerek védelmi felelőse*

A programozható rendszerek védelmi felelőse közvetlenül az engedélyes szervezet és a hozzá tartozó létesítmény felső vezetésének alárendelt beosztott vagy vezető, aki

- a) a programozható rendszerekre vonatkozó védelmi feladatok felügyeletére, koordinálására létrehozott, a védelem tervezésében és megvalósításában érdekelt szervezetek megbízottjaiból álló testület élén áll,
- b) a programozható rendszerek védelmével összefüggő védelmi intézkedések és tevékenységek megfelelőségét ellenőrzi,
- c) összehangolja és ellenőrzi a létesítményben a programozható rendszerekre vonatkozó védelmi tevékenységek tervezési alapjának meghatározását és az azokra alapozott megoldások megfelelőségét,
- d) együttműködik a nukleáris biztonságért, a fizika védelemért, a nukleáris biztosítéki követelmények végrehajtásáért és a sugárvédelemért felelős szervezetekkel a védelmi intézkedések összehangolásában,
- e) biztosítja az információcserét a különböző programozható rendszerekre vonatkozó védelmi feladatokat ellátó szervezeti egységek között,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- f) védelmi felügyeleti jelentés rendszerén keresztül intézkedik a létesítmény programozható rendszerekre vonatkozó időszakos kockázatelemzésének elkészítéséről, annak eredményei alapján meghatározza a létesítmény védelmi szempontból kritikus elemeit,
- g) időszakosan ellenőrzi és értékeli a programozható rendszerek védelmi intézkedéseinek és az intézkedésekhez rendelt erőforrások megfelelőségét, az ellenőrzések és értékelések eredményéről és az ezekre alapozott javaslatairól jelentést készít a felső vezetésnek,
- h) védelmi felügyeleti jelentés rendszerén keresztül intézkedik a programozható rendszerekre vonatkozó védelmi képzésről rendelkező eljárásrend elkészítéséről, figyelemmel kíséri és ellenőrzi a képzések megvalósítását, megfelelőségét és folyamatos fejlesztését,
- i) a védelmi intézkedések megfelelőségét ellenőrzi, felülvizsgálja és ezek alapján javaslatot tesz a normálistól eltérő események kezelésére vonatkozó eljárásokra, intézkedésekre, azok kialakításában együttműködik az érintett belső és külső szervezetekkel,
- j) összehangolja a programozható rendszerekre vonatkozó védelmi események kivizsgálását, ellenőrzi a kivizsgálási jelentés alapján meghozott intézkedések végrehajtását.

3.1.3. *A programozható rendszerek védelmi megbízottai*

A programozható rendszerek védelmi megbízottai felelősek a hatáskörükbe tartozó programozható rendszerek esetén:

- a) a létesítmény programozható rendszerekre vonatkozó védelmi szabályozóiban meghatározott célkitűzéseknek megfelelő végrehajtásáért a hatáskörükbe tartozó programozható rendszerek esetén,
- b) hatáskörükbe tartozó programozható rendszerek védelmét érintő változás esetében a programozható rendszerek védelmi felelősének tájékoztatásáért,
- c) a hatáskörükbe tartozó programozható rendszerek védelmét javító intézkedések tervezéséért, kidolgozásáért és megvalósításáért az érintett szervezetekkel együttműködve, valamint azok alkalmazásának elvárt szintű megvalósításának ellenőrzéséért.

3.1.4. *A szervezeti egységek vezetőinek felelőssége*

A létesítmény minden szervezeti egységének vezetője felelős a hatáskörében működő programozható rendszerek védelmi megbízottjának vagy felelősének a védelem felügyeletével való együttműködés zavartalanságának

Nukleáris létesítmények programozható rendszereinek védelmi követelményei biztosításáért, a szervezetére vonatkozó védelmi intézkedések kidolgozásáért és végrehajtásáért.

A védelemi tevékenységeket biztosító vagy ellátó szervezeti egységek vezetőinek felelőssége, hogy a szervezeti egységénél a programozható rendszerek védelmi megbízottját kijelölje, biztosítsa a védelmi megbízott képzéséhez és a védelmi feladatokban megfogalmazott felügyelettel való együttműködéshez szükséges munkaidőt.

3.1.5. *A létesítmény minden, programozható rendszerrel kapcsolatba kerülő dolgozójának felelőssége és kötelezettsége*

A létesítmény minden, programozható rendszerrel kapcsolatba kerülő dolgozója felelős

- a) a programozható rendszerekre vonatkozó alapvető védelmi eljárások ismeretéért,
- b) a munkájához szükséges programozható rendszerekre vonatkozó védelmi szabályozók ismeretéért,
- c) a létesítmény programozható rendszerekre vonatkozó védelmi politikájában és szabályozóiban meghatározott célkitűzéseknek és követelményeknek megfelelő munkavégzésért.

A létesítmény minden, programozható rendszerrel kapcsolatba kerülő dolgozója köteles

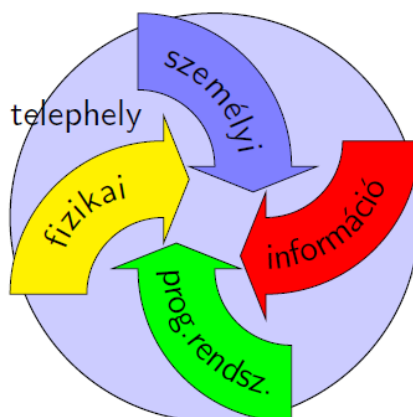
- a) vezetőit tájékoztatni minden olyan tudomására jutott körülményről, tényleges vagy valószínű eseményről, amely a programozható rendszerek védelmi színvonalának csökkenéséhez vagy károsodásához vezethet,
- b) a programozható rendszerekre vonatkozó védelmi alap- és továbbképzéseken részt venni.

3.2. A programozható rendszerek védelmének kapcsolata a védettség más területeivel

3.2.1. *A létesítmény védettségi keretrendszere*

A létesítmény védettségi keretrendszerét a NAÜ: NSS17 Computer security for nuclear security c. dokumentuma vázolja fel. A létesítmény védettsége a létesítmény felső vezetésének felelőssége. A védettség minden szakterülete, beleértve a humánbiztonságot, fizikai védelmet, információbiztonságot és a programozható rendszerek védelmét, kölcsönhatásban van egymással, kiegészítik egymást és együttesen biztosítják a létesítmény védettségi állapotát. Bármelyik védettségi szakterület sérülése, működésképtelensége

Nukleáris létesítmények programozható rendszereinek védelmi követelményei hatással van a többi területre, ami ahhoz vezethet, hogy ilyen esetekben kiegészítő intézkedések bevezetésére kell sort keríteni.



1. ábra. A különböző védeltségi szakterületek kölcsönhatása

A védeltségi szakterületek közötti szoros, jól szervezett együttműködés megteremtése tehát kulcsfontosságú az adott létesítmény védelme szempontjából. A felső vezetés felelőssége biztosítani a megfelelő minőségű koordinációt a védeltségi szakterületek között. A védeltség keretrendszerének kialakításakor célszerű lehet valamely elterjedt és alkalmazási tapasztalatok során már bevált keretrendszert kiválasztani (pl.: NIST, ISO 27001 stb.).

3.2.2. A teljes körűsége vonatkozó alapelv alkalmazása a védeltségi keretrendszerben

Minden védeltségi szakterület illetékességi és működési területének jól elhatároltnak kell lennie a vonatkozó jogszabályoknak megfelelően. A programozható rendszerek védelme során alkalmazandó egyik alapelv a teljeskörűség, amelynek értelmében minden releváns komponens figyelembevételre kerül. Azokban az esetekben, amikor egy-egy releváns komponens „túlnyúlik” a saját illetékességi körén, a programozható rendszerek védelmének keretén, akkor azokat - az alkalmazott kockázatkezelési rendszerben - kockázati tényezőkként kell figyelembe venni és számon tartani. Így elkerülhető a védendő objektumok (programozható rendszerek, más szóhasználatnál érzékeny digitális vagyonelemek: SDA-k) számának indokolatlan növekedése úgy, hogy a védelem teljeskörűsége biztosítható legyen.

Az alapelv alkalmazása során biztosítani kell a többi védeltségi szakterülettel, az üzemeltetésben érintett informatikai/műszaki szakterületekkel való szoros együttműködést és az információáramlást. Az együttműködés jellegét tekintve jelentős különbségek adódhatnak a két nagy csoport, a védeltségi szakterületek és a nukleáris biztonsági/üzemeltetési szakterületek között.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

3.2.3. Védetség szakterületekkel való együttműködés jellege

Információbiztonság, (információvédelem)

A programozható rendszerek védelmének és az információbiztonságnak a céljai, eszközei, indokai, alapelvei hozzávetőlegesen azonosak, a programozható rendszerek védelme végső soron az információbiztonság céljainak műszaki-technikai megvalósítása egy szűkebben értelmezett rendszercsoporton (mint ahogy a nukleáris biztonságé a biztonsági irányítástechnikai rendszereken). Ennek megfelelően biztosítani kell, hogy az engedélyesnél az információbiztonság és a programozható rendszerek védelme egységes szemlélettel valósuljon meg.

Mivel az információbiztonság területe a nem programozható rendszerek körébe eső digitális eszközök és alkalmazások védelmét hivatott irányítani, így a programozható rendszerek védelmének kialakítása és működtetése során az ezzel a szakterülettel való szoros együttműködés biztosíthatja a programozható rendszerek védelme határain túl megjelenő kockázati tényezők azonosítását és kezelését (pl.: általános irodai célú eszközök biztonsága, úgy mint mobiltelefon, otthoni munkavégzést támogató eszközök stb.).

Fizikai védelem (és vagyonvédelem)

A fizikai védelem és a programozható rendszerek védelmének kapcsolatát a NAÜ NST045 Computer Security for Nuclear Security c. dokumentuma ismerteti. A fizikai védelem és a vagyonvédelem kontrolljai, mint pl.: a fizikai hozzáférés korlátozása, alapvető komponensei a programozható rendszerek védelmének, amelyeket célszerű felhasználni annak kialakításakor és működtetésekor.

Hasonlóan a fizikai védelmi technikai rendszerek védetségében, a programozható rendszerek védelme jelentős mértékben járulhat hozzá a védetség szintjének kialakításához és fenntartásához. Az engedélyesnek biztosítani kell, hogy ezen védelegési célrendszerek üzemeltetői és karbantartói műszaki állománya tisztában legyen mind a fenyegetésekkel, mind pedig a lehetséges hatásokkal az általuk biztosított fizikai védelmi funkciókra.

A nagyobb fokú együttműködés számos további védelmi előnnyel jár, pl.: költséghatékonyabb, a kockázatokkal arányos kontrollok kialakításához vezethet, ezen felül pedig olyan szinergiák kihasználását teheti lehetővé, amelyek a másik szakterület eredményeinek, kontrolljainak felhasználásán alapulnak (pl.: a fizikai védelemnél alkalmazott belépőkártyák alkalmazása informatikai rendszerek felhasználói autentikációja során).

Humánbiztonság

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

A létesítmény humánbiztonságával kapcsolatban a NAÜ: NSS17 Computer Security for Nuclear Security c. dokumentuma tartalmaz részleteket. A tudatosság fejlesztésén (awareness) és az oktatáson kívül jellemzően a humánbiztonság szakterületét érinti több olyan tevékenység, amelyek elengedhetetlenek a konzisztens módon kialakított programozható rendszerek védelme szempontjából. A megfelelő minőségű humánbiztonsági átvizsgálás az új munkavállalók felvételekor, az információk bizalmasságának megőrzésére irányuló követelmények, a munkaviszony megszűnésével járó folyamatok, valamint az álláshirdetésekhöz tartozó humánbiztonsági követelmények érvényesítését koordinálni szükséges a programozható rendszerek védelme és a humánbiztonság irányítása között. Például szükséges lehet a védelmi kulcspozícióban levő személyek (pl.: rendszeradminisztrátorok, biztonsági szakterület munkavállalói) nagyobb fokú humánbiztonsági ellenőrzése.

3.2.4. *Nukleáris biztonsági és üzemfenntartási szakterületekkel való együttműködés jellege*

Nukleáris biztonság

A programozható rendszerek védelmi intézkedéseinek nem szabad a nukleáris biztonság hatékonyságát, megbízhatóságát vagy működését negatívan befolyásolniuk.

Az irányítástechnikai rendszerek üzemeltetői, karbantartói műszaki állományának egyaránt tisztában kell lenniük az általuk üzemeltetett rendszerek nukleáris biztonsági és nukleáris védettségi jelentőségével.

Üzemfenntartás

A programozható rendszerek védelmének fenntartásáról a NAÜ NST045 Computer Security for Nuclear Security c. dokumentuma tartalmaz részleteket. A technológiai rendszerek programozható rendszerei és az ügyviteli informatikai rendszerek üzemfenntartásának és védelmének irányítása jellemzően elkülönül az engedélyeseknél. Mivel a múltbeli kibertámadások megmutatták, hogy az általános ügyviteli informatikai rendszerek a felderítési szakaszban információforrásként szolgálnak a támadóknak, és egyúttal a támadás vektorát jelenthetik a technológiai berendezések vonatkozásában, ezeknek a területeknek a hatékony védelmi együttműködése elengedhetetlen a megfelelő védettség biztosításához.

Ezeknek a területeknek a folyamatai, leírásai, szakkifejezései és kockázatkezelési módszerei jelentős mértékben eltérőek lehetnek, így az engedélyesnek törekednie kell az ebből fakadó kockázatok minimalizálására.

A programozható rendszerek védelmének megvalósítása során az üzemfenntartás szakterületeinek kulcsszerepe van, ezért a programozható

Nukleáris létesítmények programozható rendszereinek védelmi követelményei rendszerek védelmének kialakítása és működtetése során egyértelműen és pontosan le kell fektetni az üzemfenntartási szakterület feladatait és felelősségeit.

3.3. A programozható rendszerek védelmi besorolása

3.3.1. A rendszer mint rendező fogalom

A rendszer mint rendező fogalom a következő markánsan eltérő módokon értelmezhető a programozható rendszerek védelme körében:

- a) **struktúraalapú rendszerszemlélet:** a rendszert értelmezhetjük úgy, mint digitális berendezések és eszközök valamilyen architektúrába szervezett egységét. Legkisebb egysége a rendszerstruktúra, amely tipikusan valamilyen nagyobb hálózatot és az azon elérhető digitális berendezések összességét jelöli, pl.: technológiai számítógéphálózat.
Rendszerstruktúrák értelmezésekor minden, a struktúrában érintett eszközt és berendezést figyelembe kell venni. Ennek a megközelítésnek az alkalmazása kevesebb védendő objektumot eredményez, viszont csökkenti vagy nehezíti a védelmi kontrollok berendezésszintű testreszabhatóságát.
- b) **funkcionálisegység-alapú rendszerszemlélet:** a rendszert értelmezhetjük úgy, mint olyan digitális berendezések és eszközök halmaza, amelyek együttműködésükön keresztül valamilyen funkcionalitást biztosítanak. Legkisebb egysége a funkcionális rendszer, amely tipikusan olyan berendezések összessége, amelyek jól körülhatárolhatóan biztosítanak valamilyen funkcionalitást. Funkcionális rendszerek alkalmazásakor minden, az adott funkció biztosításában érintett eszközt és berendezést figyelembe kell venni, kivéve, ha a funkció jellegét tekintve alpinfrastruktúra, azaz több más funkcionális rendszer számára biztosít pl. adatátvitelt. Ezeket az alpinfrastruktúrákat külön funkcionális rendszerként kell azonosítani. Ez a megközelítés jobban illeszkedik a nukleáris biztonság területén alkalmazott megközelítésekhez, így megkönnyítve a nukleáris biztonság és üzemfenntartás területeivel a koordinációt, viszont nehezebb lehet benne kezelni a többféle célt kiszolgáló rendszereket.
- c) **szolgáltatásalapú rendszerszemlélet:** a rendszert értelmezhetjük úgy, mint szolgáltatás. Ilyenkor a különféle szolgáltatásokat vesszük eleminek, ami alapján az eszközök és berendezések egymásnak és a környezetnek biztosítanak szolgáltatásokat, így látva el feladatukat. Legkisebb egysége a szolgáltatás, amely tipikusan illeszkedik az informatika szakterületén alkalmazott megközelítésekhez. Ez a szemlélet jár a legtöbb védendő objektum azonosításával, viszont lehetővé teszi a nagyon pontos, vagyis hatékony és kockázatokkal arányos kontrollok alkalmazását.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
A létesítmény programozható rendszereinek meghatározása és védelmi szintbe sorolása során mindhárom értelmezés alkalmazható.

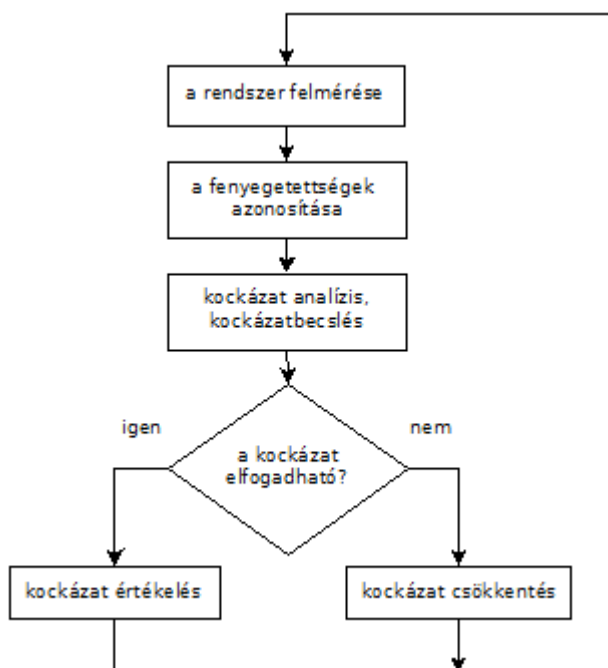
3.3.2. A védelmi besorolás

A programozható rendszerek védelmi besorolását a nukleáris biztonsági, fizikai védelmi, nukleáris biztosítéki és radioaktív anyag nyilvántartási funkciójuk alapján, az adott programozható rendszerre vonatkozó kockázatelemzés alapján kell elvégezni.

A programozható rendszerek védelme a kockázatok elfogadott szint alá történő csökkentését jelenti. Így a kockázatok elemzése a mélységi védelemben a zónák tervezésének és a védelmi intézkedések tervezésének alapvető kiindulópontja, másrészt a kialakított védelmi szintek megfelelőségének igazolóeszköze.

A programozható rendszerek életciklusának tervezési fázisában, az átalakítások és létesítések engedélyezése során az elvárt követelmények teljesülését és a védelmi intézkedések megfelelőségét kell bemutatni a változásban érintett műszaki változás terjedelmében. Amennyiben a védelmi intézkedések nem, vagy csak részlegesen felelnek meg, a következőkben ismertetett kockázatkezelési eljárás szerint be kell mutatni azokat a tervezett intézkedéseket, amelyek a kockázatokat az elfogadható szintre csökkentik.

3.3.3. Kockázatelemzés (fenyegetettség elemzés, sérülékenység elemzés, kockázat értékelés)



2. ábra. A kockázatelemzés folyamata

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
A kockázatelemzést az MSZ ISO 31000 szabványcsalád vagy az IEC 31010 szabvány szerint lehet elvégezni.

3.3.3.1. A kockázat és a kockázatmeghatározás alapjai

Programozható rendszerek kockázatának nevezzük annak a lehetőségnek a mértékét, hogy egy adott fenyegetés kihasználja egy adott rendszer vagy rendszercsoport sérülékenységeit, és ezzel kárt okoz a rendszert üzemeltető szervezetnek.

A nukleáris létesítmények programozható rendszerei esetében a kockázat meghatározása során az elsődlegesen figyelembe veendő kockázati tényező a nukleáris biztonság sérüléséből adódó kockázat. A kockázat meghatározása során figyelembe kell venni a programozható rendszerek védelmének és a fizikai védelmi rendszer sérüléséből adódó kockázatot. Az engedélyes belső eljárásai alapján a kockázatelemzés végezhető kvalitatív vagy kvantitatív módszerrel.

A programozható rendszerek kockázatelemzéséhez a tervezési alapfenyegetettséget (Design Basis Threat, DBT) figyelembe kell venni. A kockázatok megfelelő felméréséhez szükséges a DBT ismerete melynek megállapítását célszerűen úgy kell kérelmezni, hogy az időben rendelkezésre álljon.

Ezeken felül további kockázatok figyelembe vehetők (pl. üzemviteli célok, üzleti érdek sérüléséből adódó kockázat). Ezek körét az adott létesítmény programozható rendszerek védelméért felelős szervezete állapítja meg, a létesítmény többi szervezetével együttműködve és egyetértésben.

A kockázat meghatározása során alkalmazott jellemzőket, előfeltételezéseket, követelményeket és analízismódszereket dokumentálni kell. Az egyes programozható rendszerek védelmi szintjét a kockázatelemzés eredménye alapján az adott létesítmény programozható rendszerek védelméért felelős szervezete állapítja meg, figyelemmel a 3.2.2. pontban leírt iránymutatásra.

A kockázatelemzést a bevezetésre kész, vagy már üzemelő programozható rendszereknél is el kell végezni az alábbi okokból:

- a) A kialakított rendszer tervezett védelmi képességének igazolására.
- b) (üzemelő létesítményekre) Átalakítások után a védelmi képességek megőrzésének igazolására.
- c) A fenyegetettségek körének és valószínűségének változásakor.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

3.3.3.2. Kockázatértékelés és -kezelés

A kockázatértékelés megkönnyíti azokat a döntéseket, hogy mely erőforrásokat mely sérülékenységek kezelésére illetve kihasználásuk valószínűségének csökkentésére fordítjuk.

A kockázatértékelés az a folyamat, melynek során bizonyos fenyegetéseket, sérülékenységeket és hatásokat azonosítunk, amelyekhez megfelelő védelmi mechanizmusokat rendelünk. A fenyegetettség és sérülékenység elemzésével alapozhatók meg azok az ellenintézkedések, amelyek a programozható rendszerek elleni támadások megelőzéséhez vagy a következmények enyhítéséhez szükségesek.

A kockázatelemzés és -kezelés metodológiájának alaplépései a következők:

- a) peremfelületek és -hatások meghatározása,
- b) fenyegetettség azonosítása és jellemzése,
- c) sérülékenységek felmérése,
- d) külső és belső elkövetők általi támadási forgatókönyvek kidolgozása,
- e) az egyes sérülékenységek sikeres kihasználási valószínűségeinek meghatározása,
- f) kockázati szint meghatározása,
- g) ellenintézkedések kidolgozása.

A rendszeres és következetes kockázatelemzési és -értékelési feladatok végrehajtása érdekében a hatályos előírásoknak megfelelő, jól definiált eljárást kell használni. Számos hatékony kockázatelemzési és -kezelési metodológia és eszköz áll ma már nyilvánosan rendelkezésre, legtöbbjüket közismert fogalmak és végrehajtási logika alapozza meg. A kockázatelemzési és -kezelési metodológia lehet az ISO/IEC 27005 nemzetközi, vagy MSZ ISO 31000 hazai szabvány módszertana, de más nemzetközileg elfogadott kockázatértékelési módszertan is használható.

Az egyes rendszerek kiértékelésének szükségessége, a kiértékelés mélysége és a frissítés gyakorisága függ a rendszer biztonsági és védelmi funkciójának fontosságától. Új elemzést kell készíteni, vagy a régit legalább felül kell vizsgálni, ha a rendszeren módosítást hajtanak végre. Új berendezés, szoftver, eljárás bevezetése vagy az üzemeltetői szakértelem jelentős változása lehetnek ennek indokai. Az összekapcsolt rendszerek fenyegetettsége és sérülékenysége rendszerint növekszik a szigetüzeműekéhez képest.

Ha egyes fenyegetettségekre nem végezhető el a kockázatelemzés, akkor a legjobb gyakorlatok illetve a jó mérnöki megoldások módszere javasolt.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
A kockázatelemzés és -kezelés metodológiájának alaplépései a következők:

a) peremfelületek és -hatások meghatározása,

- Meg kell határozni a kockázatelemzés célját, terjedelmét, és a feltételeket, amelyek között az elemzést végre kell hajtani. A terjedelmet a programozható rendszerek jegyzéke alapján kell meghatározni, amelynek tartalmaznia kell a kockázatelemzés elvégzéséhez szükséges minden információt és adatot.

b) fenyegetettség azonosítása és jellemzése, sérülékenységek felmérése,

- Össze kell gyűjteni a fenyegetettség forrásairól, a sérülékenységekről és a hatásokról szóló információkat, ideértve a DBT információit, amelyek felhasználásra kerülnek az elemzés során. Meg kell határozni, vagy pontosítani kell az értékelésben használt kockázati modellt és az elemzési, illetve értékelési megközelítést.
- A DBT alapján számba kell venni, hogy kik jelenthetnek veszélyt, hol lehetnek (országon belül vagy kívül, létesítményen belül), milyen képességekkel rendelkezhetnek, mi lehet a szándékuk és indítékuk, és mihez férhetnek hozzá.
- Meg kell határozni a fenyegetettség forrásait típusok szerint (szándékos, véletlen, strukturális, környezeti). Közülük ki kell választani azokat, amelyek fenyegetik a vizsgálandó rendszert. A szándékos fenyegetettség esetén értékelni kell a képességet, szándékot és a célokat. Szándékolatlan fenyegetettségknél a hatás tartományát, hogy mettől meddig terjedhet.
- Meg kell határozni a sérülékenységeket a forrásokkal együtt és azokat a körülményeket, amelyek fokozhatják a sérülékenységeket, vagy újakat idézhetnek elő. Értékelni kell a sérülékenységek súlyosságát.
- Meg kell határozni az elvárt maradványkockázatot a védelmi zónamodell alapján.

c) támadási forgatókönyvek kidolgozása,

- Támadási vektorokat, támadási profilokat és támadási forgatókönyveket kell kidolgozni külső és belső elkövetőkre egyaránt, és el kell végezni a támadások erőforrásigényeinek a becslését.

d) az egyes sérülékenységek sikeres kihasználási valószínűségeinek meghatározása,

- Meg kell becsülni támadási események bekövetkezésének valószínűségeit és a támadási események sikerességének valószínűségeit a károkozásokat illetően. A becsült valószínűségek értéktartománya az

Nukleáris létesítmények programozható rendszereinek védelmi követelményei alkalmazott elemzési modelltől függ. Felvehetnek kvalitatív értékeket (pl. nagyon magas, magas, közepes, alacsony, nagyon alacsony), vagy kvázi kvantitatív értékeket (pl. 10, 8, 5, 2, 0).

e) kockázati szint meghatározása,

- Elemezni kell a támadási események által okozott károkat és azok következményeit, és meg kell határozni a következmények nagyságát, amire szintén kvalitatív vagy kvázi kvantitatív leképezést lehet használni. A programozható rendszereknél elsődlegesen a nukleáris biztonságot érintő következményeket kell figyelembe venni. Elemezni kell a támadási események következményeit a létesítmény tervezett üzemi állapotaira és a tervezett üzemi állapotok közötti átmenetekre vonatkozóan.
- Meg kell határozni a kockázatokat a valószínűségek és következmények alapján és a kockázatokat fontossági sorrendbe kell állítani.
- A kockázatértékelés eredményeit kommunikálni kell az érintettekkel, és ehhez meg kell határozni a kommunikáció módját (riport, dashboard, stb.). Meg kell osztani az eredményeket és az azokat alátámasztó bizonyítékokat az erre meghatározott szabályzatok szerint.

f) ellenintézkedések kidolgozása.

A kockázatelemzés eredményeként azonosított kockázatokhoz kockázatkezelési eljárást kell készíteni a kockázatok csökkentése érdekében, hogy a maradványkockázat elfogadható legyen. A kockázatkezelés lehetőségei:

- a) Kockázat csökkentése (risk reduction) védelmi intézkedések meghatározásával. A meghatározott védelmi intézkedések implementálása után fel kell mérni a maradványkockázatot, hogy a kívánt szint alá süllyedt-e.
- b) Kockázat elfogadása (risk retention). Tudatos döntés, nem igényel intézkedést.
- c) Kockázat elkerülése (risk avoidance). A feltételek vagy tevékenységek változtatásával történik a kockázat elkerülése. Pl. a veszélyeztetett funkció kikapcsolása.
- d) Kockázat áthárítása (risk transfer) másokhoz, akik tudják kezelni. Pl. biztosításkötés.

A kockázatelemzés és kezelés főnti ajánlásai az üzemelő nukleáris létesítmény esetén követendő a megszorítással, hogy tudomásul veszik és az elemzésekben külön vizsgálják azt a körülményt, hogy a védelmi zónamodellnek egy meglévő létesítmény adottságaihoz kell alkalmazkodnia,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei tekintettel a már meglévő építészeti, technológiai, irányítástechnikai és a fizikai védelmi adottságokra.

3.3.3.3. Fenyegtettségek azonosítása és jellemzése

A programozható rendszerek védelmi tervezésének elsőként az esetleges külső és belső támadók áttekintő jellemzésére és – támadási forgatókönyvekre alapozva – a potenciális fenyegetések elemzésére kell összpontosítani. Első közelítésben alkothatunk egy a támadó félre vonatkozó áttekintő jellemzést, amely az esetleges támadókat, motivációkat és potenciális célpontokat rendszerezi. Külső és belső elkövetők esetében ez meglehetősen különböző lehet, így azokat javasolt külön-külön megvizsgálni. Az áttekintő jellemzés alapján támadási forgatókönyveket szerkeszthetünk. A programozható rendszerek aktuális fenyegetettségi szintjének felméréséhez segítséget nyújthatnak a Rendelet 3. § (2) szerinti állami szervek, továbbá a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, az FV-13 sz. Belső elkövetők elleni védelem c. útmutató, valamint az IAEA NSS 8 Preventive and Protective Measures against Insider Threats c. útmutató ajánlásainak figyelembevétele.

A kockázat meghatározása során alkalmazott jellemzőket, előfeltételezéseket, követelményeket és elemző módszereket a létesítmény programozható rendszerek védelméért felelős szervezete választja ki a létesítmény többi szervezetével együttműködve és egyetértésben. A kiválasztott jellemzőket, előfeltételezéseket, követelményeket és elemzőmódszereket dokumentálni kell. Ez magában foglalja a figyelembe vett kockázati tényezőket, sérülékenységeket, fenyegetettségeket, külső és belső támadói jellemzéseket és potenciált, valószínűségeket és következményeket, valamint mindazon további jellemzőket, amiket a programozható rendszerekre vonatkozó védelem irányítási rendszerének és architektúrájának megtervezése során figyelembe vettek. Ezt nevezzük tervezési alapnak.

3.3.3.4. Sérülékenységek vizsgálata, monitorozása és kezelése

A sérülékenységek vizsgálatának és monitorozásának célja a programozható rendszerek sérülékenységeinek feltárása.

A létesítmény és a programozható rendszerek életciklusaiban az alábbiak szerint kell elvégezni a sérülékenységek kezelését:

- a) A létesítmény és a programozható rendszereinek tervezési fázisában a programozható rendszereket úgy kell megtervezni, hogy minél kisebb legyen a sérülékenységük védelmi kontrollok alkalmazása nélkül is („secure by design” alapelv). Mind a testre szabott („tailor-made”), mind pedig a kész rendszerek beszerzésénél figyelemmel kell lenni a

Nukleáris létesítmények programozható rendszereinek védelmi követelményei sérülékenységekre, ezért a programozható rendszerek védelmi felelősét be kell vonni a beszerzési döntések meghozatalába a tervezési folyamatától kezdve. Az ismert sérülékenységekkel kapcsolatos információkat nyílt adatbázisokból vagy a szállítótól be kell szerezni.

- b) A gyártás során a gyártónak ügyelnie kell arra, hogy a gyártási folyamatból adódóan ne keletkezzenek sérülékenységek. A gyártónak mentesítenie kell a programozható rendszereket a szükségtelen hozzáférésektől, el kell látnia a programozható rendszereket az aktuális gyártói frissítésekkel, és a FAT során el kell végeznie a gyártói sérülékenységi vizsgálatot úgy, hogy minden információ birtokában van (white box), valamint a vizsgálati jelentést a programozható rendszer teljes műszaki dokumentációjával együtt át kell adnia az engedélyesnek. Amennyiben a létesítési engedély iránti kérelem benyújtásának időpontjában már rendelkezésre áll a gyártói sérülékenységi vizsgálat eredménye, akkor a vizsgálati jelentést fel kell használni a létesítési engedély-kérelem részeként elvégzendő előzetes kockázatelemzéshez, és mellékelni kell a létesítési engedélykérelemhez. Amennyiben ebben a fázisban még nem végezhető el a gyártói sérülékenységi vizsgálat vagy nem áll rendelkezésre a vizsgálat eredménye, akkor ezt a létesítési engedélykérelem részeként elvégzendő előzetes kockázatelemzésben jelezni kell és legkésőbb az üzemeltetési engedély-kérelemben pótolni kell.
- c) A létesített programozható rendszereket a beszállítónak el kell látnia az aktuális frissítésekkel az érvényes programfrissítési és biztonsági javítócsomag telepítési (Patch Management) útmutató szerint. Meg kell változtatnia az alapértelmezett védelmi beállításokat (pl. felhasználónév, jelszó), és az engedéllyel együttműködve a SAT részeként el kell végeznie a helyszíni sérülékenységi vizsgálatot úgy, hogy az információk egy részének (alapszintű felhasználói és adminisztrátori ismeretek, jogosultságok) birtokában van (gray box). Ilyenkor a programozható rendszereket már a valós üzemi környezetükbe integrált állapotban kell vizsgálni. A vizsgálatok előtt a programozható rendszereket el kell látni az aktuális biztonsági frissítésekkel és az aktív védelmi kontroll eszközök működése mellett kell a vizsgálatot elvégezni. A vizsgálati jelentést fel kell használni az üzemeltetési engedély-kérelemhez elvégzendő kockázatelemzéshez és mellékelni kell az üzemeltetési engedély-kérelemhez.
- d) Az üzembe helyezést követően gondoskodni kell a programozható rendszerek sérülékenységeinek folyamatos (automatizált vagy manuális) monitorozásáról és a feltárt sérülékenységek mielőbbi kezeléséről. A programozható rendszerek sérülékenységmonitorozásának eredményei alapján a rendszerek feltárt sebezhetőségeit rendszeresen újra kell

Nukleáris létesítmények programozható rendszereinek védelmi követelményei értékelni, az értékelés eredménye alapján – amennyiben az szükséges és indokolt – ellenintézkedéseket kell foganatosítani. Az engedélyesnek az éles üzemi programozható rendszerek sérülékenységeinek folyamatos, automatizáltan vagy manuálisan végzett monitorozására és a feltárt sebezhetőségek kezelésére megfelelő módszereket kell kidolgoznia és formális eljárásokat kell alkalmaznia. A sérülékenységek folyamatos monitorozására és a feltárt sebezhetőségek kezelésére vonatkozó módszereket, technikai eszközöket valamint az alkalmazott eljárásokat az engedélyesnek legkésőbb az üzemeltetési engedélykérelemben be kell mutatnia. Továbbá a programozható rendszerek védelmével kapcsolatos OAH ellenőrzések, felülvizsgálatok vagy auditok alkalmával a kialakított folyamatot és eljárásokat, a sérülékenységmonitorozás aktuális eredményeit és a sebezhetőségek kezelésével kapcsolatos döntések dokumentálását be kell mutatnia. A már üzembe helyezett és éles üzemű programozható rendszereken a klasszikus aktív, intruzív sérülékenységvizsgálati és behatolástesztelési (penetration test) technikák és módszerek alkalmazása nem javasolt. Az éles üzemi programozható rendszerek esetében a jellemzően passzív, non-intruzív technikákat alkalmazó sérülékenységmonitorozás mellett, kiegészítő, klasszikus sérülékenységvizsgálatok vagy behatolási tesztelések elvégzése – a megfelelő előkészítés és körülmények biztosítása mellett – az engedélyes hatáskörébe tartozó döntés.

- e) A programozható rendszerek rekonstrukciója, felújítása során és a létesítmény vagy a rendszerek leszerelési fázisában a leszerelt programozható rendszer helyébe állított új programozható rendszer üzembe helyezésével kapcsolatosan kell elvégezni a sérülékenységi vizsgálatokat, és biztosítani az üzem közbeni folyamatos sérülékenységmonitorozást.

A sérülékenységi vizsgálat előkészítésekor meg kell határozni a vizsgálat terjedelmét, irányát és a felfedett információt. A terjedelmet a programozható rendszerek jegyzéke alapján kell meghatározni. A vizsgálat iránya a támadás feltételezett iránya (attack vector), ami lehet az internet, belső vezetékes hálózat, azon belül ugyanaz vagy egy másik védelmi zóna vagy vezeték nélküli hálózat. Manapság ritka, hogy a rendszerekről nem áll rendelkezésre információ (Black Box), ezért abból kell kiindulni, hogy a támadó birtokában van az információk egy része (Grey Box), vagy akár minden információ (White Box).

Az előkészítés után a sérülékenységi vizsgálatához az alábbi lépéseket kell megtenni:

- a) Általános információk begyűjtése.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- b) Technikai információk begyűjtése (pl. szállító, gyártó, hálózati diagram).
- c) Az elérhető rendszerek és szolgáltatások feltérképezése automatikus eszközökkel (IP és port scanner eszközökkel pl. NMAP), vagy manuálisan.
- d) Ennek eredménye alapján be kell azonosítani a sérülékenységeket automatikus sérülékenységi vizsgálati eszközökkel (pl. Nessus), amelyek a nyilvános adatbázisok információit felhasználják. A manuális felderítés meg tudja erősíteni az automatikus eszközök eredményeit, és speciális sérülékenységeket (pl. hozzáféréssel, hálózati kapcsolattal és adatbázissal kapcsolatosakat) tud vizsgálni.
- e) Behatolásteresztelés (penetration test) szükségességének eldöntése, és amennyiben szükséges, a behatolásteresztelés elvégzése.
- f) A vizsgálatnak ki kell terjedni a dokumentációk és programkódok felülvizsgálatára, az eszközök konfigurációs beállításainak felülvizsgálatára, az eszközök fizikai vizsgálatára, és a személyzet interjúztatására.

A vizsgálat eredményeiről jelentést kell készíteni, amely tartalmazza fontossági sorrendben a felderített sérülékenységeket, és a javasolt javító intézkedéseket. A jelentés részletei tartalmazhatják a vizsgálati módszereket, sérülékenységeket, támadásokat, sérülékenység lenyomatot (vulnerability footprint), a kiaknázási módokat és azok bizonyítékait, a sérülékenység hatásait, támadási forgatókönyveket, a javításra vonatkozó intézkedéseket és a következtetéseket a tanulságok levonásával.

A jelentés fontos része a feltárt sérülékenységek mérése. A mérésre egy mérési rendszert kell kidolgozni és elfogadni. Javasolt egy elterjedt – pl. az általános sebezhetőségi mérési rendszerből (Common Vulnerability Scoring System – CVSS) – kiindulni. A mérési eredmények a sérülékenységekből adódó hatásokat és kockázatokat számszerűsítik.

3.3.4. *Az egyes rendszerek védelmi besorolása*

A programozható rendszerek besorolását az általuk megvalósított funkciók alapján célszerű elvégezni a NAÜ Computer Security at Nuclear Facilities ajánlása szerint. Amennyiben a nukleáris létesítmény fizikai kialakítása nem teszi lehetővé a rendszerek fizikai védelmi besorolása, a programozható rendszerek szerinti besorolása és a nukleáris biztonsági osztályba történő besorolása közötti megfeleltetést, és fizikailag azonos helyen eltérő nukleáris biztonsági osztályba vagy programozható rendszerek védelmi szintjébe sorolt rendszerek üzemelnek/üzemelhetnek, akkor a védelmi szinteket csak funkcionális értelemben lehet meghatározni, de ennek következtében az alacsonyabb védelmi szintbe tartozó technológiai digitális rendszerek esetében is a szigorúbb szabályokat, vagy azokkal egyenértékű kiegészítő

Nukleáris létesítmények programozható rendszereinek védelmi követelményei védelmi intézkedéseket kell alkalmazni. A nukleáris biztonsági osztályba sorolás az atomerőmű esetében az ABOS, a kiégett nukleáris üzemanyag és radioaktív hulladék tárolására szolgáló létesítmény esetében a BIOS besorolási rendszert jelenti.

A programozható rendszerek védelmi architektúrájának egy védelmi zónarendszert kell kialakítani. A védelmi zónák szervezésének meg kell felelnie a mélységben tagolt védelem (defence-in-depth) elvének. A védelmi zóna csoportba rendezi azokat a programozható rendszereket, amelyeknek azonos védelmi követelményeknek kell megfelelniük. A védelmi zónában lévő minden eszköz rendelkezik bizonyos védelmi szintű képességgel. Ha ez a védelmi szint kisebb, mint ami a zónában elvárt, akkor kiegészítő védelmi kontrollokat kell alkalmazni. A védelmi zónák közötti kommunikáció csak meghatározott és megfelelően védett kommunikációs csatornákon keresztül történhet, amelyek lehetnek hálózati és nem hálózati (pl. hordozható eszköz) kommunikációs csatornák.

A védelmi zónák kialakításánál a zónákban lévő programozható rendszerek által megvalósított funkciók hasonlóságát és kritikusságát figyelembe kell venni, mert minél kritikusabb egy funkció, annál jobban kell védeni, és a hasonló funkciókat hasonló módon kell védeni. Minden programozható rendszert lehetőleg olyan védelmi zónába kell helyezni, ami a megvalósított funkció védettséget biztosítani tudja a funkció kritikusságának megfelelően. Az így el nem helyezhető programozható rendszereket kivételként kell kezelni.

El kell készíteni a programozható rendszerek kockázatelemzését. A kockázatelemzés során meg kell határozni a programozható rendszerek védelmi képességét, a fenyegetettségeket, sérülékenységeket és a károkozások következményeit. A következmények súlyosságát a programozható rendszerek által megvalósított funkciók fontossága szerint kell figyelembe venni. A funkciók fontosságának mérésére ki kell dolgozni egy kvalitatív vagy kvázi kvantitatív rendszert, és a funkciókat a rendszer alapján besorolni az osztályokba, hogy azok fontossága összemérhető és sorrendbe állítható legyen:

- a) A nukleáris biztonsági funkciók fontossága a biztonsági osztályokból levezethető.
- b) A rendelkezésre állás fontossága a funkciók számára előírt rendelkezésre állásból megkapható.
- c) Az adatok és információk bizalmosságának fontosságát a bizalmosság mint védelmi alapelv megsértéséből adódó kockázatok alapján kell meghatározni.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- d) A nukleáris biztosítéki funkciók fontosságának meghatározásához kockázatelemzést kell készíteni, és a hatások és következmények alapján kell a fontosságot számszerűsíteni.

A védelmi zónák kialakításánál a fizikai védelmi zónákat figyelembe kell venni (és fordítva), mert a fizikai védelmi zónák védelmi követelményt teljesítenek. Minden programozható rendszert lehetőleg olyan védelmi zónába kell helyezni, amely a programozható rendszernek a fizikai védelmi zónából adódó, elvárt védetségét biztosítani tudja. Az így el nem helyezhető programozható rendszereket kivételként kell kezelni. A védelmi zónahatárok nem nyúlhatnak át a fizikai védelmi zónahatárokon, csak a kommunikációs csatornák. A fizikai védelmi zóna maga egy védelmi kontroll a kommunikációs csatornákra vonatkozóan. Egy fizikai védelmi zónán belül lehet több védelmi zóna, ha a hasonló védelmi intézkedések csoportjai ezt indokolják. Viszont minimális számú zónával kell biztosítani a szükséges védelmi intézkedéseket.

A védelmi zónák kialakításánál a zónákban lévő programozható rendszerek nukleáris biztonsági osztályba történt besorolását figyelembe kell venni, mert minél szigorúbb egy nukleáris biztonsági osztály, annál jobban kell védeni. Minden programozható rendszert lehetőleg olyan védelmi zónába kell helyezni, amely a programozható rendszer nukleáris biztonsági osztályba történt besorolásának megfelelő védetségét biztosítani tudja. Az így el nem helyezhető programozható rendszereket kivételként kell kezelni.

A védelmi zónák kialakításánál javasolt először a nagyobb védelmi zónák meghatározása, majd azok további szegmentálása. Arra kell törekedni, hogy az egyes védelmi zónák minél több programozható rendszert tartalmazzanak, másrészt a tartalmazott programozható rendszerek minél hasonlóbbak legyenek a szükséges védelmi kontrollok szempontjából. A védelmi zónák kialakítása és programozható rendszerek besorolása egy iteratív folyamat kell, hogy legyen.

A kialakított védelmi zónákat dokumentálni kell a védelmi tervben legalább a következő adatok megadásával:

- a) a védelmi zóna leírása (neve, meghatározása, funkciói),
- b) a védelmi zóna határai,
- c) a védelmi zóna programozható rendszerei,
- d) a védelmi zóna kockázatelemzésének eredményei (maradványkockázat, programozható rendszerek védelmi képességei, fenyegetettségek, sérülékenységek, következmények),
- e) védelmi célok (rendelkezésre állás, sértetlenség, bizalmasság szempontjai szerint röviden)

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- f) védelmikontroll-intézkedések,
- g) külső kapcsolatok, beleértve a nem hálózati csatornákat,
- h) a védelmi zóna programozható rendszerei által megvalósított funkciók fontossága,
- i) a védelmi zóna programozható rendszereinek nukleáris biztonsági osztálya,
- j) a védelmi zónát tartalmazó fizikai zóna,
- k) a védelmi zónát körülvevő védelmi zóna neve, ha létezik.

Ha fizikai elhelyezésből adódó, hálózati vagy funkcionális kötöttségek miatt bizonyos programozható rendszereket nem lehet olyan védelmi zónába elhelyezni, amely a funkciók fontosságának és a nukleáris biztonsági osztálynak megfelelő védettséget biztosítani tudja a szükséges fizikai zónán belül, akkor azokat kivételként kell kezelni és a védelmet az alábbiak egyikével kell biztosítani:

- a) A programozható rendszer elhelyezése olyan zónába, amely nagyobb védettséget tud biztosítani, mint amire szükség van. Az elvárt maradványkockázat így teljesül, de a szükségesnél nagyobb védettség kedvezőtlenül hathat a funkcionalitásra és a használatra, ezért ilyen esetekben a védelmi intézkedések kihatásait vizsgálni kell.
- b) A programozható rendszer védelmének növelése kiegészítő védelmi kontrollok alkalmazásával, amelyek kiegészítik az őt körülvevő védelmi zónák és fizikai védelmi zónák által biztosított védettséget és a programozható rendszer meglévő védelmi képességét úgy, hogy a maradványkockázat elfogadható legyen.
- c) A programozható rendszer védelmének növelése egy körülötte kialakított védettebb védelmi zónával, hogy a védettség növelése miatt a programozható rendszer maradványkockázata elfogadható legyen. Javasolt a szomszédos programozható rendszerek bevonhatóságának vizsgálata és esetleges bevonása.

Az így kialakított védelmi zónák biztosítják a hozzájuk rendelt programozható rendszerek számára a szükséges védettséget a megfelelő fizikai zónán belül a nukleáris biztonsági osztályokba történt besorolásuk és az általuk megvalósított funkciók fontossága szerint. Ez jelenti a védelmi zónák, fizikai védelmi zónák és a nukleáris biztonsági osztályok illesztettségét, amit be kell mutatni a védelmi tervben az alábbiak szerint:

- a) Az egyes védelmi zónához rendelt programozható rendszerek felsorolása és a hozzárendelések alátámasztása.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- b) A kivételként kezelt programozható rendszerek megnevezése, az adott kivételek szükségességének indoklása és a megfelelő védetség biztosításának leírása.
- c) A kialakított védelmizóna-modell optimális jellegének alátámasztása a következőket illetően: védelmi zónák száma, a védelmi kontrollok hasonlósága a védelmi zónákban lévő programozható rendszerek számára, a védelmi zónához rendelt programozható rendszerek száma és a kivételként kezelt programozható rendszerek száma.

Védelmi zónánként a meghatározott védelmi szint, a programozható rendszerek védelmi képessége, a körülvevő védelmi zónák és a külső kapcsolatok alapján meg kell tervezni a szükséges védelmikontroll-intézkedéseket a védelmi zónára és a védelmi zónahatárra (kommunikációs csatornákra) vonatkozóan. A védelmikontroll-intézkedések segítségével a zónában lévő programozható rendszerek maradványkockázatát az elfogadható szintre kell csökkenteni. A védelmi zónák védelmi intézkedéseinek meghatározásához ki kell alakítani a védelmi kontrollok egy alapcsoportját (baseline controls), ami mindegyik zónában alkalmazandó, és ezt bővíteni kell az egyes védelmi zónák védelmi követelményei szerint. A védelmikontroll-követelmények meghatározásánál, *új létesítmények építése esetében* figyelembe kell venni az alábbiakat:

- a) Egyetlen védelmi zóna védelmi kontrolljainak működőképessége sem függhet egy másik zóna védelmi kontrolljainak működőképességétől (lásd 3.4.5.2400, 3a.4.5.4300).
- b) Az egymást körülvevő különböző védelmi zónák védelmikontroll-intézkedései nem tartalmazhatnak közös sérülékenységeket (lásd 3a.4.5.4700).
- c) A legvédettebb védelmi zóna esetén fizikai elvű visszahatás-mentességet kell biztosítani az alacsonyabb védelmi szintű zónákkal szemben (lásd 3a.4.5.3700, 3a.4.5.3800, 3a.4.5.3900). Ezért a legvédettebb védelmi zóna kommunikációs csatornáin a fizikailag garantáltan egyirányú adattovábbítás elvét kell alkalmazni. Az adattovábbítás iránya csak a biztonsági zónában elhelyezett programozható rendszerek felől folyhat az alacsonyabb védelmi szintű zónák felé. A fizikailag garantáltan egyirányú adattovábbítás elvének egy lehetséges megvalósítása az adatdióda.
- d) A legvédettebb védelmi zónában kétirányú kommunikációt csak a zónán belüli programozható rendszerek között szabad engedélyezni.
- e) A legvédettebb védelmi zónában lévő programozható rendszerek távoli hozzáféréssel történő elérését (pl. távkarbantartás, adminisztráció és

Nukleáris létesítmények programozható rendszereinek védelmi követelményei felügyelet távoli asztali kapcsolat vagy SSH session segítségével, FTP hozzáférés) meg kell tiltani.

- f) Alacsonyabb védelmi szintű zónában lévő programozható rendszer nem kezdeményezhet kommunikációt magasabb védelmi szinten lévő programozható rendszerrel.
- g) Alacsonyabb védelmi szintű zónából a magasabba történő adat, szoftver, firmware és eszköz mozgásánál olyan dokumentált validációs eljárásokat kell használni, amelyek által biztosított védelem szintje legalább olyan magas, mint a cél programozható rendszer védelmi szintje, amire az adat, szoftver, firmware kerül, illetve a programozható rendszer kapcsolódik. Ilyen módon biztosítani lehessen a programozható rendszernek az adat, szoftver, firmware, és eszköz fertőzött kódtól, trójai programtól és egyéb passzív támadásoktól való mentességét.

3.3.4.1. Az 5. védelmi szintbe sorolt rendszerek

Az 5-ös védelmi szintbe tartoznak az adminisztratív és ügyviteli programozható rendszerek. Az 5-ös védelmi szintbe kell sorolni az ügyviteli hálózat azon szegmenseit, amelyek a fizikai védelmi rendszerrel közvetlen összeköttetésben vannak, onnan adatot fogadnak, abba az irányba adatot továbbítanak. 5-ös védelmi szintbe tartozik az ügyviteli hálózat, ha az bármelyik fizikai védelmi rendszerem felé internetalapú kapcsolatot, vagy a jelen szabályozás hatályán kívül eső hálózat felé adatkapcsolatot biztosít.

3.3.4.2. A 4. védelmi szintbe sorolt rendszerek

A 4-es védelmi szintbe sorolandó valamennyi szakértői rendszer. A szakértői rendszerek csupán betekintési lehetőséget nyújtanak a technológiai adatok kiértékeléséhez, elemzéséhez, a technológiai folyamatok tervezéséhez (pl. reaktorzóna komplex számításos elemzése, reaktorfizikai jellemzők meghatározása).

A 4-es védelmi szintbe tartozó rendszerek a 2-es és 3-as védelmi szint rendszereitől fizikailag elkülönített hardver- és szoftvereszközökön működnek.

A 4-es védelmi szintbe kell sorolni azon programozható rendszereket, amelyek a Fizikai Védelmi Technikai Rendszer perifériáin elhelyezkedő végpontokat jelentik. A végpontok a beléptető, videotechnikai megfigyelő, objektum-, kerítésvédelmi rendszer, vagy a riasztáskezelő, informatikai jelátviteli rendszerem ellenőrző áteresztő pontjai; kamerái; kerítés és objektumvédelmi eszközei; média konverterei; és a rendszeremek további végponti funkcióval ellátott berendezései. Ebbe a védelmi szintbe sorolandók azon munkaállomások, amelyek betekintési, lekérdezési, megjelenítési

Nukleáris létesítmények programozható rendszereinek védelmi követelményei funkcióval bírnak, valamint ellátják a beléptető rendszer kiegészítő funkcióit (pl.: rendszám-azonosítás, kísérőkezelés, egyéb portai funkciók). A Fizikai Védelmi Technikai Rendszer kialakításából adódóan tudnia kell kezelni a végponti rendszerelemek kiesését, így azok elhelyezkedéstől függően vagy kellő redundanciával, vagy helyszínen lévő élőerővel helyettesíthetők. A védelmet úgy kell felépíteni, hogy 4-es szint irányából érkező támadásokat a 3-as, és a 2-es szint védelmi berendezései detektálni tudják, és fel tudják azokat tartóztatni.

A 4-es védelmi szintbe kell sorolni a nukleáris és más radioaktív anyagok nyilvántartását tartalmazó munkaállomásokat.

3.3.4.3. A 3. védelmi szintbe sorolt rendszerek

A 3-as védelmi szintbe kell sorolni azokat a programozható rendszereket és berendezéseket, amelyek a nukleáris létesítmény technológiájához közvetlenül kapcsolódó villamos és irányítástechnikai rendszerektől, védelmi, beavatkozó és vezérlő rendszerektől, vagy saját független adatgyűjtőiktől közvetlenül kapnak technológiai paraméter adatokat. Nukleáris biztonság szempontjából közvetlenül nem releváns rendszerek (NBSZ 3. kötet *Biztonsági osztályba sorolás fejezet* alapján 3. biztonsági osztályba (3.2.2.2150.) vagy 4. – nem biztonsági osztályba (3.2.2.2160.) tartoznak), a technológiai folyamatokba való közvetlen beavatkozást nem teszik, illetve nem tehetik lehetővé. A 3-as védelmi szintbe sorolt programozható rendszerek a technológiai folyamatok felügyeletét biztosítják. Funkcióik egyrészt az üzemeltető személyzet munkáját, valamint a 2-es védelmi szintbe tartozó biztonsági rendszerek ellenőrzését támogatják. Ennek érdekében a 3-as védelmi szintbe sorolt technológiai digitális rendszerek folyamatosan mérik a technológiai folyamatokat leíró paramétereket, begyűjtik, feldolgozzák és az operatív személyzet számára jelzik azokat. A mért, vagy számított paramétereket utólagos kiértékelésre eltárolják.

A 3-as védelmi szintbe tartoznak a programozható rendszerek mérésadatgyűjtői, melyek a technológiából származó mérési jelek ciklikus lekérdezését, átalakítását, elsődleges feldolgozását és továbbítását végzik a központi számítógépek felé.

A 3-as védelmi szintbe kell sorolni a Fizikai Védelmi Technikai Rendszer azon rendszerelemait, amelyek befolyásolása az érintett rendszerellel felügyelt terület lokális rendszerkiesését okozza. Ilyen rendszerelem lehet a beléptető, videotechnikai megfigyelő, objektum- és kerítésvédelmi rendszer, a riasztáskezelő, informatikai jelátviteli rendszerelem alközpontjai; jelátviteli és vezérlőszekrényei; informatikai hálózat aktív eszközei; valamint azon munkaállomások, amelyeken keresztül a különböző rendszerelemek lokális paraméterei módosíthatók. A felsorolt rendszerelemek lokálisan szolgálják ki

Nukleáris létesítmények programozható rendszereinek védelmi követelményei a 2-es védelmi szintbe sorolt rendszerközpontok jelfeldolgozó berendezéseit. Mivel a Fizikai Védelmi Rendszer több különböző főrendszerből (pl.: technikai rendszer, élőerős szolgálat, szabályozási rendszer, kommunikációs rendszer), a technikai rendszer több rendszerelemből, a különböző rendszerelmek több védelmi körből állnak, így a Fizikai Védelmi Rendszer kialakításából adódóan a lokális kiesést megfelelő hatékonysággal kell tudnia kezelni. A védelmet úgy kell felépíteni, hogy a 3. szint irányából érkező támadásokat a 2. szint rendszerközpontjának védelmi berendezései detektálni tudják, és fel tudják azt tartóztatni.

A kiégett nukleáris üzemanyag tárolására szolgáló létesítmény esetében a BIOS-besorolás szerinti kiemelten fontos rendszerek az ALARA elv szerint 3-as védelmi szintbe sorolhatók, mert nem valószínű a létesítményben nagy, MW-os nagyságrendbe eső hőteljesítményű elrendezés létrejötte a programozható rendszerek akár szándékosan előidézett hibája miatt.

3.3.4.4. A 2. védelmi szintbe sorolt rendszerek

A 2-es védelmi szintbe kell sorolni azon villamos és irányítástechnikai beavatkozó, szabályzó, vezérlő és védelmi funkciót ellátó programozható rendszereket, amelyek a nukleáris biztonság szempontjából közvetlenül nem relevánsak (NBSZ 3. kötet alapján 3. biztonsági osztályba (3.2.2.2150.) vagy 4., nem biztonsági osztályba (3.2.2.2160.) tartoznak), ugyanakkor a technológiai folyamatokba való közvetlen beavatkozást lehetővé teszik, ezáltal a termelés- és üzembiztonságra hatást gyakorolhatnak.

A szabályzó és védelmi rendszerek működésükkel valamely nagyobb technológiai egységet, berendezést, folyamatot, vagy akár az egész blokkot védik a paramétertúllépésekből, meghibásodásokból adódó veszélyektől, amelyek az üzem- és a termelésbiztonságra hatást gyakorolhatnak, ugyanakkor a nukleáris biztonságra közvetlen hatást nem fejtenek ki. Működésük szükség esetén a folyamat, berendezés teljes leállítását eredményezheti. Feladatuk a technológiai főberendezések biztonságát veszélyeztető kezdeti események azonosítása, az eseményhez rendelt beavatkozások automatikus végrehajtása, a kezdeti események azonosítására szolgáló folyamatparaméterek megjelenítése, biztonsági beavatkozások operátori indítási lehetőségének biztosítása.

A további számítások elvégzéséhez szükséges adatokat olyan módon adhatnak át a 3. védelmi szint rendszereinek, hogy a 3. védelmi szintű rendszer felől történő beavatkozás lehetősége kizárható legyen.

A 2-es védelmi szintbe kell sorolni a Fizikai Védelmi Technikai Rendszer valamennyi olyan rendszerelemét, amely kiesése a technikai rendszer működésében jelentős rendelkezésreállási problémát okoz, tehát a

Nukleáris létesítmények programozható rendszereinek védelmi követelményei beléptető, videotechnikai megfigyelő, objektum-, kerítésvédelmi rendszer, vagy a riasztáskezelő, informatikai jelátviteli rendszerrel teljes kiesését okozza. A 2-es védelmi szintbe sorolandók azon adatbázisok, amelyekben tárolt adatok megismerése, befolyásolása alapvetően érinti a technikai rendszer rendelkezésre állását, hitelességét, a tárolt adatok bizalmasságát.

Ebbe a védelmi szintbe kell besorolni a fizikai védelmi rendszerek rendszerközpontjait, szerverszámítógépeit, betörésetektáló eszközeit (tűzfal), adatbázisait, mivel ezen berendezések sikeres támadása esetén a teljes részrendszerre vonatkozó következményekkel lehet számolni, illetve az adatbázisok észrevétlen módosítása, adatok kinyerése súlyos következményeket eredményezhet.

3.3.4.5. Az 1. védelmi szintbe sorolt rendszerek

Az 1-es védelmi szintbe kell sorolni valamennyi, a nukleáris biztonságra közvetlenül hatást gyakorló (NBSZ 3. kötet *Biztonsági osztályba sorolás* alapján a 2. (3.2.2.2140) biztonsági osztályba sorolandó) villamos és irányítástechnikai beavatkozó, szabályzó, vezérlő és védelmi funkciót ellátó programozható rendszert; atomerőmű esetében például a reaktorvédelmi rendszert, szabályzó- és biztonságvédelmi rendszert. A szabályzó és védelmi rendszerek működésükkel valamely nagyobb technológiai egységet, berendezést, folyamatot, vagy akár az egész blokkot védik a paramétertúllépésekből, meghibásodásokból adódó veszélyektől. Működésük szükség esetén a folyamat, berendezés teljes leállítását eredményezheti. Feladatuk a technológiai főberendezések biztonságát veszélyeztető kezdeti események azonosítása, az eseményhez rendelt beavatkozások automatikus végrehajtása, a kezdeti események azonosítására szolgáló folyamatparaméterek megjelenítése, biztonsági beavatkozások operátori indítási lehetőségének biztosítása.

A további számítások elvégzéséhez szükséges adatokat visszahatásmentes, egyirányú kapcsolaton keresztül adhatnak át az alacsonyabb védelmi szintű (jellemzően 3. védelmi szintű) programozható rendszerek felé.

Megjegyzendő, hogy az 1. védelmi szintű rendszereket a nukleáris biztonságra gyakorolt hatás különbözteti meg a 2. védelmi szintű rendszerektől. Villamos és irányítástechnikai rendszerekről lévén szó, a kommunikációt tekintve mindkét esetben 3. védelmi szintbe tartozó, a technológiai folyamatok felügyeletét biztosító rendszerek felé továbbítanak adatokat.

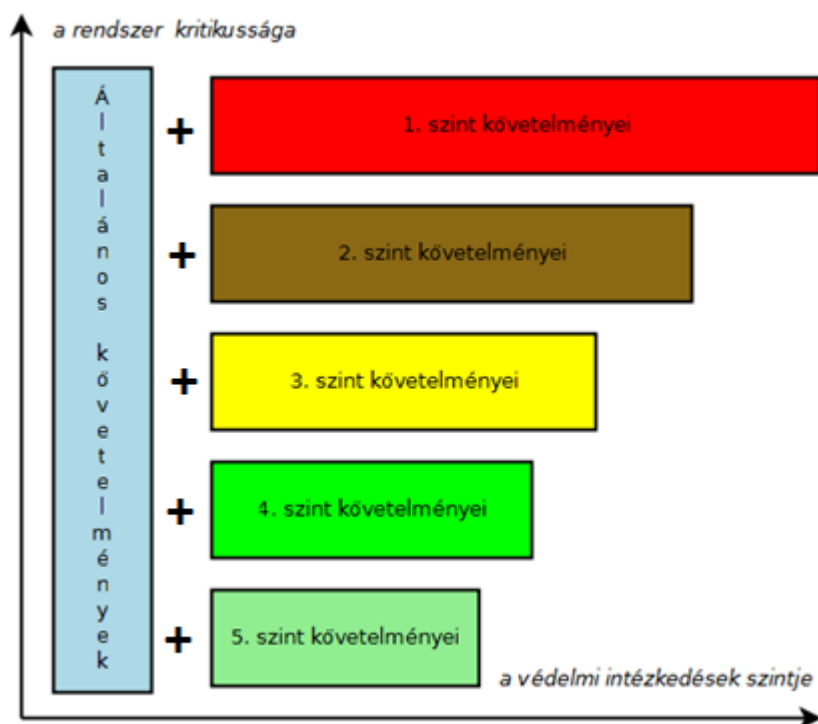
3.3.4.6. Jelátviteli utak védelmi szintje

A jelátviteli utak esetében azokra a követelményekre, amelyek nem tartoznak a programozható rendszerek védelmi követelményei közé (pl. fizikai védelmi,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei (vagyonvédelmi követelmények), fokozottan figyelemmel kell lenni, és figyelembe kell venni ezek hatását a programozható rendszerek védelmére a létesítmény teljes életciklusában.

3.4. Védelmi szintekre vonatkozó követelmények

A védelmi szintek az 5. (legkevésbé védett) szinttől az 1. (legjobban védett) szintig terjednek. Az egyes védelmi szintekre vonatkozó követelmények az általános és az adott szintre vonatkozó specifikus követelményekből tevődnek össze.



3. ábra. A védelmi intézkedések szintje és a rendszer kritikussága közötti összefüggés

A programozható rendszerek védelmi architektúráját a zónákból álló mélységi védelem adja (lásd 3.4.2.2.). Az egyes zónákhoz különböző védelmi szintek tartoznak, és a védelem erőssége annál nagyobb, minél mélyebben van a védelmi zóna. Így egy adott zónában lévő programozható rendszert védik az adott zónához tartozó kontrollintézkedések és a zónán kívüli többi védelmi zóna védelmét biztosító kontrollintézkedések.

A mélységi védelem a kockázatelemzés alapján kerül kialakításra úgy, hogy a zónák mélysége és a védelem szintje arányos a kockázattal. Ilyen módon a mélységi védelem megvalósulását kockázatelemzéssel lehet igazolni. Ehhez el kell végezni a zónákban lévő programozható rendszerek kockázatelemzését, és a maradványkockázatok kimutatásával igazolható a mélységi védelem megfelelése.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
A programozható rendszerek mélységi védelmének stratégiáját meg kell tervezni, dokumentálni kell a védelmi tervben, és a terv szerint meg kell valósítani a programozható rendszerek elfogadható védettsége érdekében. A védelem fenntartásához két alapvető védelmikontroll-eljárást kell működtetni:

- a) A szándékos vagy szándékolatlan károkozások és kibertámadások felderítése, elemzése és elhárítása a megfelelő válaszlépések megtételével, ideértve a helyreállítást.
- b) Változtatások elvégzése ellenőrzött módon úgy, hogy a változtatások ne csökkentsék a rendszerek védelmi szintjét.

3.4.1. A védelmi szintekre vonatkozó általános követelmények

Az érintett rendszerekre a következő általános intézkedéseket kell alkalmazni:

- a) A létesítménynek rendelkeznie kell egyes védelmi szintekkel kapcsolatos alapelveket és eljárásokat szabályozó dokumentumokkal.
- b) Az a) pont szerint kialakított belső szabályozás minden felhasználóra érvényes.
- c) Gondoskodni kell arról, hogy minden felhasználó megfelelően képzett és védelemtudatos legyen.
- d) Gondoskodni kell arról, hogy minden felhasználó köteles legyen betartani a biztonsági irányelveket és eljárásokat.
- e) A felhasználóknak csak azokhoz a rendszerekhez és csak azokhoz a funkciókhoz lehet hozzáférésük, amihez a munkájuk elvégzéséhez szükségük van, azaz törekedni kell a minimális felhasználói létszámra.
- f) Az egyes rendszerekhez megfelelő beléptető- és felhasználóhitelesítési módszereket kell használni.
- g) A rendellenességek észlelésére megfelelő módszereket és eljárásokat kell alkalmazni.
- h) Az alkalmazás- és rendszersérülékenységeket monitorozni kell, és – szükség esetén – megfelelő intézkedéseket kell foganatosítani.
- i) A rendszer(ek) sebezhetőségét rendszeresen újra kell értékelni.
- j) A cserélhető adathordozók kontrolljára belső szabályozást kell létrehozni, a kontrolltevékenységet folyamatosan biztosítani kell.
- k) Gondoskodni kell a számítógépes és hálózati védelmi elemek rendszeres és folyamatos karbantartásáról.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- l) A számítógépes és a hálózati védelmi elemek (pl. biztonsági átjárók, behatolásfelderítő rendszerek, behatoláselhárító rendszerek, virtuális magánhálózati szerverek) működését naplózni és monitorozni kell.
- m) Az programozható rendszerekre megfelelő adatmentési és visszaállítási eljárásokat kell működtetni.
- n) A programozható rendszerekhez való fizikai hozzáférést azok funkcióinak megfelelően korlátozni kell.
- o) A fentiekén túl a 3.5. *Programozható rendszerek védelmi tervének összeállítása* c. fejezet olyan követelményeket és intézkedéseket tartalmaz és fogalmaz meg, amelyek a védelmi szintekre vonatkozó további általános követelményekként is felfoghatók és alkalmazhatók.

3.4.2. A védelmi szintek speciális követelményei

3.4.2.1. Az 5. szintre vonatkozó speciális követelmények

Az általános szintre vonatkozó követelményeken túl:

- a) A rendszereken módosítást csak az arra feljogosított, szakképzett felhasználók végezhetnek.
- b) Az 5. szint rendszereiből az internet-hozzáférés megfelelő védelmi intézkedések alkalmazása esetén engedélyezhető.
- c) A megfelelően ellenőrzött távoli hozzáférés megengedett.

3.4.2.2. A 4. szintre vonatkozó követelmények

Az általános szintre vonatkozó követelményeken túl:

- a) Az rendszereken módosítást csak az arra feljogosított, szakképzett felhasználók végezhetnek.
- b) A 4. szint rendszereiből az internet-hozzáférés megfelelő védelmi intézkedések alkalmazása esetén engedélyezhető.
- c) Ezt a szintet a külső hálózatok felől érkező ellenőrizetlen forgalom ellen, meghatározott és korlátozott tevékenységet engedő biztonsági átjárók telepítésével védeni kell.
- d) A rendszerekhez való fizikai csatlakozást (pl. szervizgép, mobil adathordozó csatlakoztatása) ellenőrizni kell.
- e) Távoli karbantartáshoz a hozzáférés folyamatos ellenőrzés mellett engedélyezhető, ha a távoli számítógépre és a felhasználóra vonatkozó védelmi követelmények betartása biztosított. Nyilvános hálózatról és nem kontrollált eszközről a karbantartást az elvégzésére tervezett

Nukleáris létesítmények programozható rendszereinek védelmi követelményei időintervallumra lehet engedélyezni, egyéb időszakokra a hozzáférést meg kell szüntetni.

- f) A felhasználók rendelkezésére bocsátott rendszerfunkciókat a felhasználói belépést ellenőrző rendszer ellenőrzi. Az ettől eltérő esetekben a védelmet más eszközökkel kell megvalósítani.
- g) A távoli külső hozzáférés az arra feljogosított felhasználók számára engedélyezhető, ha a távoli számítógépre és a felhasználóra vonatkozó védelmi követelmények betartása biztosított.

3.4.2.3. A 3. szintre vonatkozó követelmények

Az általános szintre vonatkozó követelményeken túl:

- a) A 3. szintű rendszerekből az internet elérése tiltott.
- b) Biztosítani kell a rendszer biztonsági naplózását (security log), a naplókat rendszeresen ellenőrizni és értékelni kell.
- c) Ezt a szintet a kevésbé védett irányból származó ellenőrizetlen forgalom ellen, meghatározott és korlátozott tevékenységet engedő biztonsági átjárók telepítésével védeni kell.
- d) A rendszerekhez való fizikai csatlakozást (pl. szervizgép, mobil adathordozó csatlakoztatása) kontroll alatt kell tartani.
- e) A távoli vagy kevésbé védett zónából történő karbantartási hozzáférés eseti elbírálás és folyamatos ellenőrzés mellett engedélyezhető, ha a távoli számítógépre és a felhasználóra vonatkozó védelmi követelmények betartása biztosított.
- f) A felhasználók rendelkezésére bocsátott szükséges és elégséges rendszerfunkciókat a felhasználói belépést ellenőrző rendszer ellenőrzi. Az ettől eltérő esetekben a védelmet más eszközök segítségével kell megvalósítani (pl. fizikai hozzáférés korlátozásával).

3.4.2.4. A 2. szintre vonatkozó követelmények

Az általános szintre vonatkozó követelményeken túl:

- a) A nukleáris biztonság szempontjából közvetlenül nem releváns, de a technológiai folyamatokba való beavatkozást lehetővé tévő villamos és irányítástechnikai programozható rendszerek esetén biztosítani kell, hogy a kevésbé védett szint felől technológiai beavatkozást kiváltó adatforgalom ne mehessen az adott 2. védelmi szintű rendszer irányába. Megfelelő kapcsolatirány-szabályozás alkalmazásával csak a szükséges nyugtázó üzenetek, vagy ellenőrzött jelző üzenetek (pl. TCP/IP nyugta üzenetek), valamint az eszközök felügyeletéhez, üzemeltetéséhez, üzembiztonságának fenntartásához és a rendszer védelméhez szükséges

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
üzenetek haladhatnak az ellenkező (befelé) irányba. A távoli hozzáférésű
vagy kevésbé védett zónából történő karbantartás nem megengedett.

- b) A rendszerekhez való fizikai csatlakozást (pl. szervizgép, mobil adathordozó csatlakoztatása) folyamatosan kontroll alatt kell tartani és minden esetben dokumentálni szükséges.
- c) Azok a sérülékenységvizsgálatok, amelyek a rendszereken végzett műveletekkel járnak, egyes létesítményi folyamatok instabilitásához vezethetnek, ezért csak próbapadon, tartalék rendszeren vizsgálhatók, átvételi tesztek vagy hosszabb tervezett üzemszünetek alkalmával.

3.4.2.5. Az 1. szintre vonatkozó követelmények

Az általános szintre vonatkozó követelményeken túl:

- a) Semmilyen az 1. szintre irányuló, alacsonyabb védelmi szint felől érkező számítógépes hálózati adatforgalom (pl. nyugtázás, szignalizálás) nem megengedett. Csak kifelé irányuló kommunikáció lehetséges. Megjegyzendő, hogy ez a szigorúan kifelé egyirányú kommunikáció természeténél fogva nem biztosítja az adat megbízhatóságát és a sértetlenséget. Szintén megjegyzendő, hogy ez kizárja mindenfajta „handshake protokoll” alkalmazását (pl. TCP/IP), a kapcsolatirány szabályozásával együtt. A kivételek nyomtatékosan ellenjavalltak, az engedélyes csak eseti elbírálás szerint mérlegelhet, amennyiben azt a részéről teljes körű indoklás és az alkalmazás kockázatának elemzése támasztja alá.
- b) Távoli hozzáférésű vagy kevésbé védett zónából történő karbantartás nem megengedett.
- c) A rendszerekhez való fizikai hozzáférést folyamatosan kontroll alatt kell tartani és naplózni kell.
- d) A rendszerekhez hozzáférő felhasználók létszámát a minimumra kell korlátozni.
- e) A rendszereken jóváhagyott minden módosítás csak két, arra feljogosított személy egyidejű közreműködésével végezhető.
- f) Minden tevékenységet naplózni és monitorozni kell.
- g) A rendszerbe irányuló minden adatbevittelt esetenként kell jóváhagyni, és az elvégzését ellenőrizni. (A külső hálózati adatátvitelt az a) pont tiltja.)

Minden módosításra, beleértve a hardverkarbantartást, frissítést és szoftvermódosítást, belső szabályozást kell kialakítani.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

3.5. A programozható rendszerek védelmi tervének összeállítása

A programozható rendszerek védelmi terve a védelmi program megvalósításának kulcsfontosságú dokumentuma.

A programozható rendszerek védelmi tervének tartalmaznia kell a védendő rendszereket, azokra alkalmazott védelmi szintet, a konkrét védelmi intézkedéseket, a védelmi intézkedések végrehajtásáért, a kritikus rendszerek esetén folytonos üzemvitel biztosításáért felelős szervezetet. A védelmi tervnek tartalmaznia kell a védelemmel összefüggő oktatás, továbbképzés rendjét.

A védelmi terv dokumentálja a kitűzött védelmi célok elérésének és fenntartásának módját. Ennél fogva egy élő dokumentum, amit rendszeresen felülvizsgálni, módosítani és jóváhagyni kell. A védelmi tervben dokumentálni kell a védelmi terv felülvizsgálatának, karbantartásának és jóváhagyásának módját és gyakoriságát. A programozható rendszerek védelmi tervének—a fizikai védelmi terv részeként -- összhangban kell lenni a fizikai védelmi terv más rendelkezéseivel, mert számos védelmikontroll-intézkedéshez kapcsolódik fizikai védelem, vagy fordítva. A programozható rendszerek védelmével kapcsolatos különböző bizalmas információk miatt a védelmi terv dokumentumait a tartalom bizalmassága szerint kell strukturálni, minősíteni, és az egyes részekhez a hozzáférést az információk bizalmassága szerint kell meghatározni.

A programozható rendszerek védelmi tervének összeállítása, az egyes fejezetek kidolgozottságának részletezettsége során figyelembe kell venni a létesítmény életciklusa aktuális fázisának (tervezés, létesítés, üzembe helyezés, üzemeltetés, leszerelés) jellegzetességeit, az adott fázisban a létesítmény programozható rendszereivel kapcsolatosan rendelkezésre álló információk jellegét és mennyiségét.

A fentiek alapján a programozható rendszerek védelmi terve, a létesítmény életciklusfázisának függvényében a következőket kell, hogy tartalmazza az egyes fejezetekre lebontva:

	Tervezési fázis	Létesítési fázis	Üzembehelyezési fázis	Üzemeltetési fázis	Leszerelési fázis
A rendszerek jegyzéke (rendszerek, hálózatok, alkalmazások és kapcsolataik)	R	R	T	T	T
Alapkonfiguráció	R	R	T	T	T

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

Konfigurációs változtatások	R	R	T	T	T
A védelmi intézkedések megvalósítása	R	R	T	T	T
Védelemtervezési Alapelvek	T	T	T	T	T
Mélységben Tagolt Védelem	R	R	T	T	T
Szabályzatok, eljárások és képzés	R	R	T	T	T
Környezetállósági feltételek	R	R	T	T	T
Fizikai hozzáférési védelem	R	R	T	T	T
Hálózati határvédelem, peremvédelem	R	R	T	T	T
Technikai, logikai hozzáférési védelem	R	R	T	T	T
Belső hálózat védelme	R	R	T	T	T
Szerverek, munkaállomások és HMI-k védelme	R	R	T	T	T
Alkalmazások, futó programok védelme	R	R	T	T	T
Adatok védelme	R	R	T	T	T
A jól ismert sérülékenységek vizsgálata és kezelése	R	R	T	T	T
Programfrissítések és biztonsági javítócsomagok telepítése	R	R	T	T	T
Elektromágneses impulzusok elleni védelem	O	O	T	T	T

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

Azonosító- és jelszókezelés	R	R	T	T	T
Hordozható eszközök és mobil adathordozók használata	R	R	T	T	T
Vezeték nélküli készülékek és hálózatok	R	R	T	T	T
Folytonos üzemvitel, rendszerek biztonsági mentése	R	R	T	T	T
Folytonos üzemvitel	R	R	T	T	T
Rendszerek biztonsági mentése	R	R	T	T	T
A beszállítói lánc kiberbiztonsága	T	T	T	T	T
A védelemmel összefüggő oktatás, továbbképzés, védelmi kultúra	T	T	T	T	T
A védelmi oktatás és továbbképzés céljainak, rendjének meghatározása	T	T	T	T	T
A kialakított jogosultsági szinteknek megfelelő védelmi oktatási kritériumok a korábban meghatározott védelmi szintek követelményeit figyelembe véve	R	R	T	T	T
Speciális oktatások,	T	T	T	T	T

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

továbbképzések rendje					
Védelmi kultúra kialakítása	T	T	T	T	T
Védelmi felülvizsgálat	T	T	T	T	T
Kiberbiztonsági gyakorlatok	T	T	T	T	T
A rendszerek védelmével összefüggő változáskezelés, életciklus	T	T	T	T	T
Események kezelése	T	T	T	T	T
A kivizsgálás rendje, kivizsgálást segítő intézkedések	T	T	T	T	T
Válasz intézkedési terv	T	T	T	T	T

Jelmagyarázat:

O: A fejezet kidolgozása nem szükséges az adott életciklusfázisban

R: A fejezet kidolgozása a rendelkezésre álló adatok alapján, korlátozott részletezettséggel szükséges

T: Az adott fejezetet teljes részletezettséggel, az összes releváns programozható rendszerre nézve ki kell dolgozni.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
A létesítmény életciklusának egyes fázisaira nézve az alábbi általános követelményeket és ajánlásokat kell figyelembe venni:

Tervezés fázis: A már üzemelő, a tervezéssel kapcsolatos, szenzitív adatokat tároló, kezelő, feldolgozó programozható rendszerekre vonatkozóan szükséges elkészíteni a védelmi tervnek a programozható rendszereket, illetve az azokat védő adminisztratív, logikai és fizikai védelmi kontrollokat leíró fejezeteit. A tervezés alatt álló programozható rendszerek esetében fokozottan kell ügyelni a „Secure by Design” elv, tervezővel szembeni érvényesítésére és ellenőrzésére.

Létesítési fázis: A már üzemelő, a tervezéssel kapcsolatos, szenzitív adatokat tároló, kezelő, feldolgozó programozható rendszerekre, illetve a már üzembe helyezett technológiai rendszerekre vonatkozóan szükséges elkészíteni a védelmi tervnek a programozható rendszereket, illetve az azokat védő adminisztratív- logikai- és fizikai védelmi kontrollokat leíró fejezeteit. A programozható rendszerek tervezése és kivitelezése során fokozottan kell ügyelni a „Secure by Design” elv tervezővel, illetve a hardver- és szoftverkomponensek gyártásra (szoftver esetében a programozásra) és tesztelésre vonatkozó követelmények gyártókkal szembeni érvényesítésére és ellenőrzésére. A programozható rendszerek jegyzékét, a konfigurációkezelési adatbázist, a kapcsolódó védelmi kontrollokat tartalmazó adatbázisokat folyamatosan naprakészen kell tartani, és a PRVT Rendeletben előírt időszakos felülvizsgálata során a vonatkozó fejezeteket frissíteni.

Üzembehelyezési fázis: Az üzembehelyezési fázisban már teljeskörűen rendelkezésre kell állnia a programozható rendszerek jegyzékének, így a védelmi terv vonatkozó fejezeteinek teljes részletezettségű kidolgozása szükséges.

Üzemeltetési fázis: Az üzembe helyezési fázisban már teljes körűen rendelkezésre kell állnia a programozható rendszerek jegyzékének, így a védelmi terv vonatkozó fejezeteinek teljes részletezettségű kidolgozása szükséges. Az üzemeltetési fázisban a programozható rendszerekkel kapcsolatos változáskezelésnek a változáskezelési eljárásban foglaltaknak megfelelően kell történni, a változásokat minden alkalommal át kell vezetni a rendszerek jegyzékébe, a konfigurációkezelési adatbázisba, illetve a kapcsolódó védelmi kontrollokat tartalmazó adatbázisba, és a PRVT Rendeletben előírt időszakos felülvizsgálata során a vonatkozó fejezeteket ezeknek megfelelően frissíteni kell.

Leszerelési fázis: A leszerelési fázisban, a leszerelésre kerülő programozható rendszerek esetében fokozott figyelmet kell fordítani az azokban tárolt adatok archiválására és törlésére. Javasolt már az üzemeltetési fázisban úgy

Nukleáris létesítmények programozható rendszereinek védelmi követelményei megtervezni a programozható rendszerek életciklusát, hogy azok lehetőség szerint illeszkedjenek a létesítmény életciklusához. A leszerelési fázisban kiemelt figyelmet kell fordítani a dozimetriai, a radioaktívanyag-nyilvántartó és a fizikai védelmi rendszerek sértetlenségére és rendelkezésre állására, tekintettel az életciklusfázis jellegzetes munkafolyamataira.

3.5.1. A rendszerek jegyzéke (rendszerek, hálózatok, alkalmazások és kapcsolataik)

A létesítménynek rendelkeznie kell a programozható rendszerek és rendszerelemek teljes körű listáját tartalmazó aktuális vagyoneleltárral. A programozható rendszerek vagyoneleltárát úgy kell összeállítani, hogy az a kockázatfelmérés elvégzéséhez szükséges minden jellemző információt és adatot tartalmazzon. Ezt a vagyoneleltárt folyamatosan frissíteni kell, hogy annak naprakészsége biztosított legyen. A programozható rendszerek vagyoneleltárának legalább a következőket tartalmaznia kell:

- a) a programozható rendszerek felsorolását, listáját,
- b) a programozható rendszerek működési modelljét, funkcióját és feladatát,
- c) a rendszereken futó alkalmazások felsorolását, listáját,
- d) a rendszerek kapcsolódását és összekapcsolását, beleértve a rendszerek áramellátását,
- e) a hálózati diagramot (topológia és topográfia), beleértve minden külső és belső kapcsolatot,
- f) a rendszerek adatkapcsolatainak és adatáramlásának elemzését, hogy ismert legyen, mely rendszerek melyik másik rendszerekkel kommunikálnak,
- g) alkalmazott protokollok,
- h) a programozható rendszerek elhelyezkedését, lokalizációját.

A programozható rendszerek vagyoneleltárának felvétele, valamint a kockázatfelmérés során figyelembe kell venni, hogy mind maga a jegyzék, mind pedig a kockázatfelmérés eredményeként összegyűjtött adatok és információk érzékenyek lehetnek, ezért ezek megfelelő védelméről, szükség esetén minősítéséről gondoskodni kell.

A programozható rendszerek jegyzékének felvétele a konfigurációkezelés keretében történik. A védelmi tervben ki kell térni a programozható rendszerek azonosításának módjára.

A konfigurációkezelés biztosítja a tervezési alap, a terv és a megvalósított üzemi rendszer konzisztenciáját. Ennek érdekében tartalmaznia kell minden információt és adatot a konzisztencia ellenőrzéséhez. A bevezetett üzemi rendszer a tesztelési és ellenőrzési eljárásoknak megfelelt rendszer, amelyek

Nukleáris létesítmények programozható rendszereinek védelmi követelményei így megfelel a védelmi elvárásoknak. A konfigurációkezelés feladata a programozható rendszerek ezen védettségi állapotának alapkonfigurációként történő rögzítése az előélettel együtt (lásd 3.4.1.1), és a védettségi állapot fenntartása a változtatások ellenőrzött módon történő végrehajtásának biztosításával (lásd 3.4.1.2).

3.5.1.1. Alapkonfiguráció

Az alapkonfiguráció kialakításához a következőket kell elvégezni:

- a) A programozható rendszerek komponenseinek nyilvántartására nyilvántartórendszert kell létrehozni. A nyilvántartásnak vissza kell tükröznie minden engedélyezett rendszerkomponenst és úgy kell összeállítani, hogy az a kockázatfelmérés elvégzéséhez szükséges minden jellemző információt és adatot tartalmazzon.
- b) A nyilvántartást automatikus mechanizmusokkal kell támogatni, amelyek képesek az új, még nem rögzített komponensek, illetve az eltávolított komponensek bejegyzéseinek felderítésére.
- c) A programozható rendszerek aktuális állapotáról alapkonfigurációt kell létrehozni
- d) Alapkonfigurációt az üzemi környezet mellett a fejlesztői és tesztkörnyezetről is kell készíteni.
- e) Az alapkonfigurációt a változtatásokkal együtt karban kell tartani, amihez lehetőség szerint automatikus mechanizmusokat alkalmazni kell, hogy biztosított legyen az információk konzisztenciája.
- f) A konfigurációkezelő rendszerhez történő hozzáférést korlátozni kell és a változtatásokat csak erre kiképzett és feljogosított személyeknek szabad megengedni. Minden változtatást naplózni kell. Az adatok konzisztenciáját és pontosságát rendszeresen ellenőrizni kell audit és belső vizsgálat keretében.
- g) A programozható rendszerek konfigurációs változtatásaihoz szigorú fizikai és logikai hozzáféréseket kell meghatározni. A hozzáféréseket naplózni és a naplózást rendszeresen ellenőrizni kell, lehetőleg automatikus mechanizmusokkal. Ha a hozzáférés korlátozása automatikusan nem megoldható, akkor helyettesítő mechanizmusokat kell alkalmazni pl. fizikai korlátozás, fizikai hozzáférés monitorozása, megbízható személyzet alkalmazása, változtatások utólagos ellenőrzése).
- h) Kötelező konfigurációs beállításokat kell meghatározni a programozható rendszerek komponensei számára. A védelmi beállításokat a leghigorúbbra kell konfigurálni, ami még összeegyeztethető a működéssel. A kötelező beállításokhoz képest a kivételeket minden

Nukleáris létesítmények programozható rendszereinek védelmi követelményei esetben dokumentálni és indokolni kell. Lehetőség szerint olyan automatikus mechanizmusokat kell alkalmazni, amelyek központi helytől lehetővé teszik a konfigurációk beállítását és ellenőrzését.

A programozható rendszerek nyilvántartására létrehozott vagyoneletrárnak tartalmaznia kell a programozható rendszereket és komponenseiket, mint konfigurációs elemeket, egyértelmű azonosítóval ellátva, és az egyes konfigurációs elemekhez kapcsolódóan legalább a következő adatokat:

- a) termékjellemzők (pl. gyártó, típus, verzió),
- b) szoftverek (pl. operációs rendszer, alkalmazások, szolgáltatások) és frissítések,
- c) kikapcsolt, illetve letiltott hozzáférési lehetőségek,
- d) fizikai elhelyezkedés, lokalizáció,
- e) működési modell, funkció és feladat,
- f) hálózati diagram (topológia és topográfia), beleértve minden külső és belső kapcsolatot (IP-címek, MAC-címek stb.) és kapcsolódások, beleértve a rendszerek áramellátását, adatkapcsolatok és adatáramlások,
- g) folyamatok és műveletek, amelyek kiváltják a rendszerek közötti kommunikációt, a kommunikáció karakterisztikáját és az alkalmazott protokollokat,
- h) tervezési alap, tervezési és fejlesztési dokumentációk,
- i) tesztelési dokumentációk a tesztesetekkel és a tesztelt konfigurációval,
- j) üzemelési és karbantartási dokumentációk,
- k) alkalmazott védelmi kontrollok,
- l) hozzáférési jogosultságok, a jogosultságokkal rendelkező személyek,
- m) konfigurációs beállítások,
- n) védettségi szint,
- o) időrendben a változtatások (ki, mit, mikor, milyen céllal).

3.5.1.2. Konfigurációs változtatások

A programozható rendszerekre kiható bármilyen átalakításnál biztosítani kell a rendszerre érvényes védelmi szint szerinti követelmények teljesülését, különben a védelmi egyenszilárdság idővel gyengül, és kockázata meghaladja az elfogadható értéket. Ezért az átalakításokat meg kell vizsgálni abból a szempontból, hogy milyen hatással vannak a védettségre, és hogy esetleg milyen védelmi intézkedésekre van szükség az átalakításból adódó sérülékenységek csökkentésére. A vizsgálat a védelmi hatáselemzés (security

Nukleáris létesítmények programozható rendszereinek védelmi követelményei (impact analysis), amelyet el kell végezni az átalakítás előtt a jóváhagyási folyamat részeként, az átalakítás elkészítése után a gyártói átvételi teszt (Factory Acceptance Test - FAT) részeként és az átalakítás üzembe helyezése előtt a helyszíni átvételi teszt (Site Acceptance Test - SAT) részeként.

A védelmi hatáselemzésnél a következő lépéseket kell végrehajtani:

- a) Meg kell vizsgálni az átalakítás megvalósíthatóságát. A rendszerarchitektúrát elemezve fel kell mérni az érintett rendszereket és rendszerkomponenseket, amelyek közvetlenül vagy közvetve érintettek lehetnek az átalakítás miatt. Ki kell dolgozni és mérlegelni kell a megvalósítási lehetőségeket a funkcióra, biztonságra és védelemre gyakorolt hatások figyelembevételével.
- b) Azonosítani kell a sérülékenységeket.
- c) El kell végezni a kockázatok értékelését. Sérülékenység azonosítása esetén fel kell mérni a kockázatokat. Ha a becsült kockázat nagyobb, mint a megengedett, akkor azt vagy csökkenteni kell új védelmi intézkedésekkel vagy a meglévők módosításával, vagy el kell utasítani az átalakítást. Viszont a megnövekedett kockázat addig még elfogadható, amíg az nem lépi túl az elfogadható kockázati szintet.
- d) Meg kell vizsgálni a meglévő védelmi intézkedéseket. Meg kell vizsgálni, hogy az átalakítás kihat-e és hogyan a meglévő védelmi intézkedésekre az átalakítással közvetlenül vagy közvetve érintett rendszerekben és rendszerkomponensekben.
- e) Ha az átalakítás előtti vizsgálat során védelmi problémák merülnek fel, mérlegelni kell újabb védelmi intézkedések bevezetését, vagy meglévők módosítását az átalakításokkal együtt. Ennek ismeretében kell dönteni az átalakítás jóváhagyásáról, vagy elutasításáról.

A programozható rendszerek átalakításai után el kell végezni a FAT-tesztet. A FAT alatt az átalakításokkal kapcsolatosan legalább a következőket kell ellenőrizni:

- a) A változtatások következtében az eredeti problémák megoldódtak.
- b) A változtatásoknak nincsenek káros kihatásai az alkalmazásokra, a funkciók rendelkezésre állnak, és az elvárt módon működnek.
- c) Az eredeti védelmi hatáselemzés helyes volt és az ott feltárt hiányosságok megoldásra kerültek az elvárt módon.
- d) A változtatások visszavonhatók.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

A FAT végén vírusellenőrzést kell végezni a legújabb víruslenyomatokkal annak igazolására, hogy a programozható rendszer nem fertőződött meg a teszt alatt. Dokumentálni kell az átalakításokat.

A létesítés végén el kell végezni a SAT tesztet, amihez fel kell rakni az aktuális frissítéseket, és a teszt végén vírusellenőrzést kell végezni a legújabb víruslenyomatokkal.

Az üzemelő programozható rendszer változtatása előtt meg kell győződni arról, hogy az esetleges helyreállítás a helyreállítási eljárásnak megfelelően végrehajtható a legrosszabb esetre felkészülve (worst case scenario). Ki kell dolgozni a változtatások üzembe helyezésének lépéseit legalább az alábbi szempontok figyelembevételével:

- a) Több rendszer változtatása esetén a változtatások sorrendjének meghatározása. Redundáns programozható rendszereknél, amennyiben rendelkeznek tartalék vagy tesztrendszerrel előbb a tartalék vagy a tesztrendszereken kell végrehajtani a változtatásokat és utoljára az üzemi rendszereken. Amennyiben a programozható rendszer nem rendelkezik tartalék vagy tesztrendszerrel, a változtatás megkezdése előtt teljes rendszermentést kell készíteni.
- b) Változtatások automatikus vagy részben automatikus végrehajtási lehetőségeinek alkalmazása.
- c) Változtatások végrehajtásához szükséges idő és a rendelkezésre álló idő a leállásból vagy üzemelésből adódó korlátok miatt.
- d) Változtatott és még nem változtatott rendszerek kompatibilitásának biztosítása.
- e) Változtatások felfüggesztése és a visszaállítás lehetősége (point of no return).
- f) Üzembe helyezett rendszer vizsgálata, monitorozása.
- g) Változtatások utáni stabil működés kritériumai, és lezárás.

El kell végezni a változtatásokat, és a változtatások sikeres végrehajtása után aktualizálni kell a konfigurációkezelő rendszert a változtatásoknak megfelelően legalább a következő adatok rögzítésével: a változtatások kiváltó okai, változtatások azonosítói, érintett programozható rendszerek és verzióik, változtatások felelősei és végrehajtói, elvégzett tesztesetek és a változtatások végrehajtásának lépései.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

3.5.2. A védelmi intézkedések megvalósítása

3.5.2.1. Védelemtervezési Alapelvek

A programozható rendszerek és hálózatok tervezése és kivitelezése során, a védelmi szempontok már a tervezés lehető legkorábbi fázisától be kell, hogy épüljenek a létesítés életciklusába. Ez alapján a rendszer tervezése során a „Secure by Design” elv érvényesítése alapkövetelmény. Ennek megfelelően már a rendszer tervezése során kiemelkedően fontos szempontként kell kezelni, hogy a választott technológia, az alkalmazott eszközök és megoldások minden eleme a védelem legmagasabb szintjének elérése irányába hasson, a kiválasztott technológiai megoldások biztonsági színvonala egységes és kockázatarányos legyen. A rendszer funkcionalitása és megbízhatósága mellett, a rendszer védelmét egyforma súllyal kell figyelembe venni és kezelni.

A rendszer tervezése és kialakítása során teljes körű, részletes kockázatfelmérést és értékelést kell elvégezni, figyelembe véve a potenciális sebezhetőségeket, a fenyegetéseket és a támadási lehetőségeket. A tervezési fázisban végrehajtott kockázatértékelés eredménye alapján ki kell mutatni a maradványkockázatokat és ezt egyeztetni kell a felső vezetéssel. A kimutatott maradványkockázatok elfogadható mértékéről a létesítmény felső vezetése jogosult dönteni. Az üzemeltetőnek a kockázatfelmérés eredménye alapján, olyan védelmi eszközöket és kontrollintézkedéseket kell alkalmaznia a rendszer védelmére, amelyek szervesen illeszthetők a kiválasztott technológiába, a kockázatokkal arányos védelmet biztosítanak, és ezáltal az elfogadható és elérhető legalacsonyabb szintre csökkentik a maradványkockázatot.

A rendszer tervezése és kialakítása során, a funkcionális követelmények teljesítésén, valamint a megbízhatóságon és a hibatűrő működési elvárásokon túl, biztosítani kell a biztonság három alapkövetelményének megfelelő védelmét, amelyek prioritási sorrendjük szerint a következők:

- a) rendelkezésre állás (a rendszer folyamatos, megbízható működése, elérhetősége, hozzáférhetősége),
- b) sértetlenség (a rendszer eredeti funkciójának biztosítása, adatbevitel /adatmegjelenítés /adatátvitel sértetlensége, adatkonzisztencia és a helyes információ szolgáltatása),
- c) bizalmasság (a rendszer illetéktelen, jogosulatlan használatával szembeni védelme, a funkciókhoz, adatokhoz csak a jogosultak férhetnek hozzá).

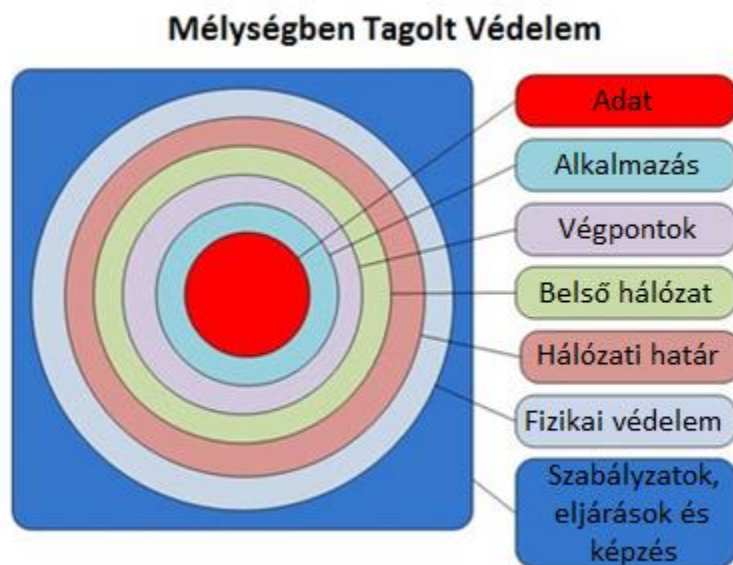
A rendszer tervezése és kialakítása során fel kell készülni a fenti biztonsági követelmények sérülésének kezelésére (megelőzésére, felismerésére), azaz a megfelelő ellenőrzési eljárásokat (eszközöket és intézkedéseket) kell

Nukleáris létesítmények programozható rendszereinek védelmi követelményei alkalmazni a rendszer védelmére. Az alkalmazandó kontrollintézkedések típusai a következők (a PreDeCO védelem-tervezési elv alapján):

- a) megelőző (preventív),
- b) azonosító, korai felismerő (detektáló),
- c) elhárító, helyreállító vagy javító (korrigáló).
- d) A kiválasztott és alkalmazott védelmi eszközöknek, intézkedéseknek illeszkedniük kell az alkalmazott technológiához és annak elemeihez, valamint a következő feltételeknek kell megfelelniük:
- e) zárt (minden potenciális sebezhetőséget és fenyegetést figyelembe vesz),
- f) teljes körű (minden releváns elemet figyelembe vesz),
- g) folytonos (a védelem időben legyen folyamatos, megszakításmentes, nem lehet kihatással a programozható rendszer működésére),
- h) kockázatarányos.

3.5.2.2. Mélységben Tagolt Védelem

A rendszerek védelmének tervezése és az egyes rendszerelemekhez tartozó védelmi intézkedések és eszközök kiválasztása során a „mélységben tagolt védelem (Defence-in-Depth)” tervezési elvet kell követni. A „mélységben tagolt védelem” elv lényege programozható rendszerek esetén, hogy a védendő rendszer különböző rétegeiben különböző védelmi technikákat és eszközöket alkalmazunk annak érdekében, hogy a rendszer minden szintje (rétege) megfelelően védett legyen az illetéktelen beavatkozással vagy támadással szemben.



4. ábra. A mélységben tagolt védelem összetevői

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

Az egyes rétegek védelmére alkalmazott eszközöknek és védelmi technikáknak szervesen illeszkedniük kell a kiválasztott rendszer elemeihez és minden egyes rétegben a kockázatokkal arányos védelmi szintet kell kialakítani. Az egyes rétegekben alkalmazott védelmi technikák és eszközök célja, hogy egy esetleges illetéktelen behatolás vagy támadás kivitelezését szintről szintre, rétegről rétegre haladva folyamatosan akadályozza, egyre több időráfordítást, technikai tudást és egyre speciálisabb támadási technikát és bonyolultabb eszközök használatát tegye szükségessé. Az egyes rétegekben alkalmazható védelmi megoldások kifejtése a következő pontokban történik.

3.5.2.3. Szabályzatok, eljárások és képzés

A programozható rendszerek védelmét a dokumentált adminisztratív és személyi védelmi intézkedések, eljárásrendek összessége szavatolja. Az üzemeltetőnek be kell mutatnia mindazon dokumentumokat, amelyek a rendszer biztonságos üzemeltetéséhez, használatához szükséges ismereteket tartalmazzák, valamint foglalja magában az üzemeltető, a karbantartó és a felhasználói személyzet oktatását és képzését.

Szabályzatokra vonatkozó ajánlásokat tartalmaz a fentiekén kívül a 3.2.1. *A védelmi szintekre vonatkozó általános követelmények* c. fejezet a)–d) pontja.

3.5.2.4. Környezetállósági feltételek

A rendszer alkotóelemeire, az adattovábbító berendezésekre, a végponti mérésadatgyűjtő eszközökre és a terepi berendezésekre jellemző, hogy ezek az eszközök egy elosztott hálózat részeként, az üzemi terület különböző részein, egymástól akár igen nagy távolságban helyezkednek el. Az üzemi terület különböző részein elhelyezett adatgyűjtő berendezéseknek és hálózati eszközöknek egészen eltérő környezeti feltételek között megbízhatóan kell működniük annak érdekében, hogy a rendszer elvártan magas szintű rendelkezésre állása teljesüljön. Ennek érdekében a rendszer és az elosztott hálózat tervezése és kialakítása során figyelembe kell venni az egyes ipari hálózati eszközök és az adatgyűjtő berendezések kitettséget az esetlegesen káros környezeti hatásoknak. Az eszközök kiválasztása során fontos szempont, hogy ezek a berendezések ellenálljanak a tervezett beépítés helyére jellemző extrém külső környezeti hatásoknak. Ilyenek lehetnek például a következők:

- a) szélsőséges hőmérsékleti viszonyok (nagyon magas vagy alacsony),
- b) nedvesség, por és rezgés fokozott jelenléte,
- c) mechanikai károsodás lehetősége vagy vegyszeres károsító hatások jelenléte,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

d) magas elektromágneses interferencia (EMI), rádiófrekvenciás interferencia (RFI) és elektromágneses zavarok (EMC), hatások.

3.5.2.5. Fizikai hozzáférési védelem

Az üzemeltetőnek meg kell határoznia és ki kell alakítania azokat a fizikai hozzáférési védelmi megoldásokat, amelyek az eszközök elhelyezése során korlátozzák a jogosulatlan fizikai hozzáférés lehetőségét. Az eszközök megfelelő elhelyezésével (lokalizáció) biztosítani kell, hogy azokhoz ellenőrizhető módon, csak és kizárólag az üzemeltetési, karbantartási feladatokat ellátó személyzet férhessen hozzá. A fizikai hozzáférési védelem érdekében alkalmazható megoldások a következők lehetnek:

- a) Elhelyezés fizikailag védett, őrzött területen (kerítéssel, kapuval, élőerős védelemmel),
- b) Elhelyezés zárható, beléptetőrendszerrel ellátott épületben, helyiségekben,
- c) Elhelyezés kamerás megfigyelő- és riasztórendszerrel ellátott épületben,
- d) Elhelyezés speciális, zárható, illetéktelen hozzáféréstől védett szekrényekben.

3.5.2.6. Hálózati határvédelem, peremvédelem

Az üzemeltetőnek egy vagy több, de pontos és jól definiált „határvonal” kialakításával egyértelműen szét kell választania a biztonságosnak tekinthető technológiai rendszer belső (védett) hálózatát és az ezen kívüli, „nem biztonságosnak” tekintett külső hálózatot (pl.: a vállalati informatikai/ügyviteli hálózat, vagy más külső fél hálózata). A határvédelmi eszközök alkalmazásának alapvető célja, hogy megakadályozza az illetéktelen kapcsolatok kialakítását két hálózat között és szabályozza (engedélyezze vagy blokkolja) a hálózatok és hálózati eszközök közötti kapcsolatokat és az adatforgalmat. Az üzemeltetőnek hálózati határvédelmi eszközök alkalmazásával el kell választania a védendő belső, biztonságos hálózatot a külső megbízhatatlan hálózattól, ezzel biztosítva, hogy a két hálózat között csak az engedélyezett adatforgalom folyhat. Továbbá el kell „rejtetni” a belső hálózat struktúráját a külső hálózatban lévő eszközök elől, ezzel megakadályozva, hogy a külső hálózatból a belső hálózat eszközeihez illetéktelenül hozzá lehessen férni. A hálózati határvédelemre alkalmazható eszközök:

- a) tűzfalak, demilitarizált zónák kialakítása (DMZ) – csak alacsony kockázat esetén,
- b) virtuális magánhálózatok (VPN) - csak alacsony vagy közepes kockázat esetén,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- c) „gateway” típusú hálózati átjárók – közepes kockázatok esetén,
- d) fizikailag egyirányú, „adatdióda” eszköz – preferált megoldás magas vagy kiemelkedő kockázatra.
- e) Gondoskodni kell a számítógépes és hálózati védelmi elemek rendszeres és folyamatos karbantartásáról.
- f) A számítógépes és a hálózati védelmi elemek (pl. biztonsági átjárók, behatolásfelderítő rendszerek, behatoláselhárító rendszerek, virtuális magánhálózati szerverek) működését naplózni és monitorozni kell.

3.5.2.7. Technikai, logikai hozzáférési védelem

A felhasználóknak csak azokhoz a rendszerekhez és csak azokhoz a funkciókhoz lehet hozzáférésük, amikhez a munkájuk elvégzéséhez szükségük van, azaz törekedni kell a minimális felhasználói létszámra. (Lásd 3.3.1. A védelmi szintekre vonatkozó általános követelmények c. fejezetének e) pontja.)

A technikai, logikai hozzáférés védelme jelenti mindazokat az eszközökbe beépített és alkalmazott technikai védelmi intézkedéseket, amelyek logikai vagy technikai úton a szükséges és elégséges szintre korlátozzák az eszközökre történő helyi bejelentkezés vagy az eszközökhöz történő távoli hozzáférés lehetőségét (pl.: az adminisztrációs vagy menedzsmentfelület elérése), csökkentik az illetéktelen beavatkozás kockázatát. Az egyes eszközökbe beépített és rendelkezésre álló technikai, logikai védelmeket a megfelelő szinten implementálni kell. Ilyen lehetséges védelmi megoldások:

- a) A használaton kívüli ki- és bemeneti (I/O) portok, csatlakozók tiltása,
- b) A hálózati eszközök portjainak és a csatlakozó eszközök összerendelése (MAC-cím szűrése), szabálysértés esetén a port automatikus letiltása (port security beállítások),
- c) Az eszközök adminisztrációs és menedzsmentfelületei hozzáféréseinek korlátozása (IP-cím szűrése),

Autentikációs eljárások (felhasználó azonosítása, jelszavas védelmek) alkalmazása a helyi és távoli hozzáférések esetében,

- d) Szerepköralapú hozzáférés ellenőrzése (RBAC – Role Based Access Control) alkalmazása a helyi és távoli hozzáférések esetében.
- e) A belső elkövetők általi támadások megelőzése céljából adminisztratív és technológiai védelmi kontrollokat kell alkalmazni. Ilyen adminisztratív kontroll például a „Négy szem elv”, mely biztosítja, hogy az adott rendszerekhez csak két személy (két adminisztrátor, biztonsági vezető + adminisztrátor) együttes közreműködésével lehessen rendszergazdai

Nukleáris létesítmények programozható rendszereinek védelmi követelményei jogosultsággal hozzáférni. Emellett monitorozni kell a kiemelt rendszergazdai jogosultsággal bíró (privilegizált) felhasználók tevékenységét, például egy Privileged Access Management (PAM) eszköz alkalmazásával. A kiemelt felhasználók monitorozási folyamatának támogatására, ezáltal pedig a belső elkövetők általi kitettség csökkentésére kiegészítő védelmi kontrollként viselkedésanalizáló eszköz (User Behavior Analytics – UBA) alkalmazása javasolt.

- f) Csak az engedélyezett elektronikus mobil adathordozók és hordozható programozható eszközök létesítményi rendszerre, hálózatra való csatlakoztatása megengedett.
- g) A programozható rendszerekhez csatlakozó szerviszszámítógépekre (pl. karbantartói notebook, mérnökállomás) azokat a védelmi követelményeket kell alkalmazni, amelyek arra a rendszerre vonatkoznak, amelyhez csatlakozik. Ennek megfelelően a szerviszszámítógépeket ugyanazon védelmi szintbe kell sorolni, mint a rendszert, amelyhez szervizcélal csatlakoztatva van.

A programozható rendszerek tervezése során a tervekben be kell mutatni a programozható rendszerekhez tervezett hozzáférési lehetőségeket (szolgáltatások, portok), és igazolni kell a hozzáférési lehetőségek szükségességét. A hozzáférési lehetőségek normál üzemeléshez, karbantartáshoz, vagy vészhelyzet esetén lehetnek szükségesek. Így a hozzáférési lehetőségeket hozzá kell rendelni funkciókhoz.

A legyártott programozható rendszerekhez a FAT részeként kell igazolni a szükségtelen hozzáférési lehetőségektől való mentességet. Az igazolást mellékelni kell a létesítésiengedély-kérelemhez. Ehhez a FAT előtt a programozható rendszerek szükségtelen hozzáférési lehetőségeit el kell távolítani, illetve ki kell kapcsolni. Dokumentálni kell a szükséges hozzáférési lehetőségeket és az eltávolított, illetve kikapcsolt hozzáférési lehetőségeket. A programozható rendszerekre az aktuális frissítéseket fel kell rakni a frissítések tesztelése és ellenőrzés után. A FAT alatt tesztelési eljárásokkal ellenőrizni kell, hogy a programozható rendszerek hozzáférési lehetőségei megfelelnek a dokumentációknak.

A létesített programozható rendszerekhez a SAT részeként kell igazolni a szükségtelen hozzáférési lehetőségektől való mentességet. Az igazolást mellékelni kell az üzemeltetésiengedély-kérelemhez. A programozható rendszerekre az aktuális frissítéseket fel kell rakni a frissítések tesztelése és ellenőrzés után. A SAT alatt tesztelési eljárásokkal ellenőrizni kell, hogy a programozható rendszerek hozzáférési lehetőségei megfelelnek a dokumentációknak.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
Üzemelés alatt rendszeres ellenőrzésekkel kell biztosítani, hogy a programozható rendszereken a szükségtelen hozzáférési lehetőségek megfelelnek a konfigurációkezelés nyilvántartásának. A tartalék és teszt programozható rendszereken és karbantartás alatt az üzemi rendszereken a sértetlenség ellenőrzését biztosítani kell (pl. automatizmusokat kell használni a sértetlenség-ellenőrzésekhez (pl. HIDS)).

3.5.2.8. Belső hálózat védelme

A hálózati határvédelem kialakításán túl, a „mélységben tagolt védelem” elvének alkalmazása szükségessé teszi a rendszerek belső (védett) hálózati forgalmának ellenőrzését és felügyeletét. A belső hálózat védelmét szolgáló eszközök alkalmazásával megakadályozhatók vagy időben észlelhetők a hálózatba történő behatolási kísérletek, detektálható a nemkívánatos vagy rendellenes hálózati forgalom (pl.: férgek, vírusok és egyéb kártékony programok terjedése) és az illetéktelen hálózati aktivitás vagy tevékenység.

A hálózati határvédelmi eszköz (peremvédelem) használata önmagában nem tekinthető elegendő védelemnek. A tűzfal megkerülése esetén, a tűzfal vagy a hálózat sebezhetőségét kihasználó, illetéktelen hozzáférési vagy támadási kísérlet, illetve egyéb rendellenes hálózati forgalom, a belső hálózat adatforgalmának figyelésével és ellenőrzésével detektálható. A belső hálózatvédelmi eszközök nem csak a külső hálózatokból kiinduló támadások, vagy behatolási kísérletek észlelésére használhatók, fontos alkalmazási területük a belső, megbízható hálózatban kezdeményezett támadások időbeni észlelése és kivédése, vagy a belső, abnormális hálózati forgalom érzékelése.

A technológiai rendszerek környezetében, azok belső hálózatában elterjedten használatosak a speciális, ipari kommunikációs és adatátviteli protokollok (pl.: Profibus, Fieldbus, Modbus, DNP, DNP3, ICCP) amelyek a hálózatba kapcsolt eszközök (pl.: IED-ek, PLC-k, RTU-k, adatgyűjtők, hosztok és SCADA/DCS szerverek) közötti egységes adatkommunikációt biztosítják. Ezekkel az ipari hálózati protokollokkal szemben, a tervezésük és kialakításuk idején, a gyors (valós idejű) és megbízható adattovábbítás követelménye volt az elsődleges elvárás, míg ezek a protokollok hálózati- és komputerbiztonsági szempontból viszont nagyon gyengének és könnyen sebezhetőknak bizonyultak. Ennek felismerése szükségessé teszi a technológiai rendszerek belső hálózatbiztonsági kockázatainak kezelését.

Ebből adódóan a technológiai rendszerek hálózatának tervezésekor és az eszközök kiválasztásakor fontos követelmény, hogy a régi, gyenge és sebezhető ipari kommunikációs protokollok helyett az újabb, megfelelő védelmet biztosító protokollok és az ezekkel kompatibilis eszközök kerüljenek alkalmazásra. A belső hálózat védelmére alkalmazható eszközök:

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- a) biztonságos kommunikációs protokollok alkalmazása és használata (pl.: IPv6, SSCP, SSL/TLS, SSHv2, HTTPS, IPSec, SNMPv3),
- b) a hálózati kommunikáció és adatátvitel titkosítása (lehetőség szerint végponttól végpontig terjedő titkosítás használata),
- c) a hálózatban lévő eszközök, berendezések azonosítása és hitelesítése (pl.: RADIUS-szerver, EAP CHAP),
- d) a hálózati forgalom figyelése és monitorozása (biztonsági- és eseménynaplózás, riasztás)

hálózati behatolásérzékelő rendszerek (Network Intrusion Detection Systems – NIDS) alkalmazása.

3.5.2.9. Szerverek, munkaállomások és HMI-k védelme

A technológiai rendszert alkotó minden egyes kiszolgálón, végponti munkaállomáson, operátori HMI (host) eszközön a lehető legmagasabb szintű biztonsági beállítások, konfigurációk és paraméterezés elérésére (system hardening), valamint a végpontok védelmét biztosító egyéb technikai és szoftveres megoldásokra kell törekedni. A host-ok védelemére szolgáló technikák és eszközök a következők lehetnek:

- a) a kiszolgálókon és munkaállomásokon futó operációs rendszerek és szoftverek biztonságának fokozása (system hardening),
- b) a használaton kívüli, szükségtelen programok és szolgáltatások eltávolítása, letiltása,
- c) a használaton kívüli, szükségtelen felhasználói fiókok (pl.: Vendég fiók) eltávolítása, letiltása,
- d) az alapértelmezett (default) felhasználói fiókok és jelszavak megváltoztatása,
- e) az operációs rendszerek file-rendszer hozzáférési jogosultságainak módosítása, szigorítása,
- f) a kiviteli és beviteli portok (I/O portok) tiltása, korlátozása (soros, USB-portok, CD/DVD eszközök tiltása, BIOS jelszavas védelme stb.),
- g) host-alapú behatolásérzékelő rendszerek (Host-based Intrusion Detection Systems – HIDS), a kiszolgálók és munkaállomások integritásellenőrzési vizsgálatára,
- h) a kártékony programkódok (maleware) bejutása elleni szoftveres védelem (Integrált antivirus szoftver alkalmazása),

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- i) életjelek (heartbeatsignal) alkalmazása, a rendszer aktuális, pillanatnyi működési állapotát és kommunikációs kapcsolatainak épségét ellenőrző és jelző eszköz,
- j) az operációs rendszerek, alkalmazások, szoftverek és eszkövezérlő programok frissítése, amennyiben a frissítés hatásának vizsgálata alapján a frissítés az eszköz vagy rendszer alaprendeltetését, funkcióját, folytonos üzemvitelét nem sérti (folyamatos és rendszeres biztonsági javítások és szoftverfrissítések alkalmazása),
- k) egységes és standardizált hardver- és szoftverkörnyezet alkalmazása, komplett „image” telepítő készletek alkalmazása.

3.5.2.10. Alkalmazások, futó programok védelme

A technológiai rendszerekben alkalmazott szerver és kliens operációs rendszerek, a futtató környezet biztonságának fokozásán (system hardening) túl, gondoskodni kell a rendszer funkcióit megvalósító alkalmazások és szoftverek (függetlenül, hogy azok egyedi fejlesztésű vagy kereskedelmi forgalomban kapható „dobozos” szoftverek) elérhető legmagasabb védelemről, ennek során ki kell használni az alkalmazások és szoftverek védelmét szolgáló „beépített”, belső eszközöket és a külső technikai megoldásokat. Az alkalmazások, programok védelmét megvalósító lehetséges eszközök és intézkedések a következők:

- a) Az alapértelmezett felhasználói fiókok letiltása, eltávolítása vagy módosítása,
- b) Az alkalmazás felhasználói fiókjainak felügyelete (azonosítás, jogosultság-ellenőrzés, jelszókezelés, naplózás),
- c) Szerepköralapú hozzáférés-ellenőrző rendszer (Role Based Access Control –RBAC), azonosító és jelszó használata az alkalmazásokban,
- d) Megbízható munkamenet és kapcsolatkezelés (Session Management), SSL, SSH alkalmazása,
- e) Tevékenységek naplózása, a felhasználói tevékenységek nyomon követése és auditálása, különösen a kiemelt rendszergazdai jogosultsággal bíró (privilegizált) felhasználók esetében.

3.5.2.11. Adatok védelme

A technológiai rendszerekben tárolt és kezelt adatok védelme elengedhetetlenül fontos a sértetlenség és a rendelkezésre állás követelményének biztosításához. Az adatok tárolása, kezelése és továbbítása szintjén a megfelelő (végponttól végpontig terjedő) védelemmel kell ellátni a rendszert. Mivel a rendszerben tárolt és kezelt adatok biztonsága szervesen

Nukleáris létesítmények programozható rendszereinek védelmi követelményei összefügg az alkalmazással és a szoftverbiztonsággal, így a biztonságtudatos programtervezés és készítés alapvető elvárás. A biztonságtudatos programfejlesztés során kiemelt figyelmet kell fordítani a következő szempontokra:

A rendszer egészét, és minden szoftverkomponensét úgy kell megtervezni és elkészíteni, hogy védett legyen a következő támadási módszerekkel szemben:

- a) puffer-túlcsordulás (buffer-overflow),
- b) beékelődő típusú támadások (Man-In-The-Middle),
- c) szolgáltatásmegtagadás típusú támadások (DoS és DDoS),
- d) a WEB-alapú alkalmazások - ezeken felül - védettek legyenek a következőkkel szemben;
 - SQL-injection és parancs-beszúrás (SQL-injection, command injection),
 - könyvtárfa-bejárás (path/directory traversal),
 - kereszt-szkriptelés (Cross-Site Scripting – CSS/XSS, CSRF),
 - távoli fájlbeszúrás, feltöltés (Remote File Include – RFI, File Upload),

Annak érdekében, hogy a fenti követelmények teljesüljenek, a kockázatokkal arányos mértékben a következő előírásokat kell szem előtt tartania rendszerek környezetében alkalmazott szoftverekre vonatkozóan:

- a) minden adatbevitel ellenőrzése, szűrése (kizárólag érvényes, validált adat fogadható el),
- b) kizárólag előre meghatározott típusú és formátumú adatok, karakterek bevitele legyen engedélyezett,
- c) az adatbevitel titkosított kódolással védendő a nemkívánatos módosítással szemben,
- d) adatbázisok esetében a tárolt eljárások hívása és használata,
- e) programban, adatállományban, vagy adatbázisban felhasználói azonosítókat és jelszavakat titkosított formában kell tárolni (soha nem plain text formában),
- f) fontos és kritikus adatállományokat titkosított formában kell tárolni,
- g) olyan programnyelvek vagy programfejlesztő eszközök használhatók, amelyek a fordítást követően, a felhasználói program futtatásakor automatikus és biztonságos memóriakezelést eredményeznek,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- h) lehetőség szerint végponttól végpontig terjedő hitelesítést és integritásellenőrzési eljárásokat kell alkalmazni a folyamatok közötti adatátvitelkor és kommunikációban,
- i) a program vagy a forráskód nem tartalmazhat egyszerű szöveg formában jelszavakat vagy titkosítókulcsokat, ezek nem továbbíthatók titkosítatlanul a hálózatban,
- j) alkalmazzanak komplett program- és szoftvertervezést és -készítést támogató fejlesztői keretrendszereket,
- k) alkalmazzanak automatizálható forráskódfelülvizsgálati, vagy forráskódanalizáló és -elemző eszközöket.

Ha a fenti előírások műszaki megvalósítása nem lehetséges, vagy a felmerülő kockázatokkal nem áll arányban, akkor kiegészítő, nem műszaki intézkedésekkel kell biztosítani a megfelelő védettséget.

3.5.2.12. A jól ismert sérülékenységek vizsgálata, monitorozása és kezelése

A programozható rendszerek minden egyes (hardver és szoftver) kritikus komponense és eleme esetében folyamatosan monitorozni vizsgálni és értékelni kell az ismertté vált sérülékenységeket, és ezek eredményét, valamint a sérülékenységek kezelésének módját dokumentálni kell.

A sérülékenységek naprakész kezelése céljából folyamatos kommunikációs kapcsolatot kell kiépíteni a BM Országos Katasztrófavédelmi Főigazgatóság, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet és az engedélyes esetleges belső CERT-szervezeteivel. A kapcsolattartás rendjét szabályozni kell.

3.5.2.13. Programfrissítések és biztonsági javítócsomagok telepítése

A rendszer minden (hardver és szoftver) komponensén és elemén a helyszíni átvételt megelőzően telepíteni kell az egyes rendszerelemek gyártói által hivatalosan kiadott, aktuális programfrissítéseit és biztonsági javítócsomagjait vagy patch-eit. Ez vonatkozik a rendszer hardvereszközeinek firmware-jeire, az egyes operációs rendszerekre és a technológiai szoftverekre egyaránt. A rendszer átadását megelőző helyszíni átvételi tesztelést (SAT – Site Acceptance Test) csak a programfrissítések telepítését követően lehet végrehajtani. A technológiai rendszerek életciklusában valószínűsíthető, hogy az átadást követően bizonyos idő elteltével az egyes hardver- és szoftvergyártók kiadnak újabb programfrissítéseket és biztonsági javítócsomagokat, amelyek a rendszer egyes elemeiben időközben feltárt hibákat hivatottak kijavítani, vagy biztonsági lyukakat foltoznak be. Ezért a programozható rendszerekre vonatkozóan el kell készíteni egy Programfrissítési és Biztonsági Javítócsomag Telepítési Útmutató (Patch

Nukleáris létesítmények programozható rendszereinek védelmi követelményei (Management) dokumentumot, amely követésével az üzemeltető személyzet képes a teljes rendszer komputerbiztonsági szintjét folyamatosan naprakészen tartani.

A rendszeresen vagy alkalmanként elvégzett sérülékenységi vizsgálat vagy incidenskezelés jelentése tartalmazhat olyan sérülékenységeket, amelyeket kijavítani vagy csökkenteni szükséges. Kockázatelemzés eredményeként szükség lehet újabb védelmi intézkedésekre. A rendszerek működésének monitorozása és elemzése során kiderülhetnek olyan hiányosságok a funkciókat, védelmet vagy biztonságot illetően, amik pótlása szükséges, vagy ismertté válhatnak olyan incidensek, amelyeknél válaszlépésekre van szükség. A szállító kiadhat védelmi frissítéseket, ezért biztosítani kell, hogy ez az információ időben rendelkezésre álljon (pl. szerződéses megállapodással, vagy a biztonsági frissítések figyelésével) a nulladik napi támadások (zero-day attack) elkerülése végett.

A programozható rendszerek számára így előálló biztonsági frissítéseket átalakításként kell kezelni, ezért végig kell mennie a programozható rendszerek életciklusán a tervezéstől az elfogadási teszteken keresztül az üzembe helyezésig, és a vonatkozó engedélyezési eljárásokon. Ebben a tekintetben az egyes programozható rendszereket külön kell kezelni. El kell készíteni a programozható rendszerekre vonatkozó biztonsági frissítési eljárásrendet. Az eljárásrendet úgy kell definiálni, hogy az minimalizálja a biztonsági frissítésekből eredő, vagy azzal összefüggő, biztonsági és védelmi kockázatok mértékét. Ennek érdekében az eljárásrendnek tartalmaznia kell a biztonsági frissítésekkel kapcsolatban elvégzendő verifikációs és validációs feladatokat, a szükséges speciális jóváhagyási lépéseket, vagy speciális engedélyezési követelményeket, és az auditálást támogató lépéseket. A módosítással kapcsolatos verifikációs és validációs feladatok közé tartozik a védelmi hatáselemzés és az ezzel összefüggő kockázatelemzés végrehajtása. Az eljárásrendnek összhangban kell lenni számos más eljárásrenddel, amelyek közül legfontosabbak a konfigurációs változtatások, konfigurációkezelés, kockázatkezelés, incidenskezelés és helyreállítás-kezelés.

A frissítés végrehajtásának szükségességéről a kockázatelemzés alapján kell dönteni, tehát van lehetőség a mérlegelésre. Abban az esetben azonban, ha a frissítés nélkül a programozható rendszer maradványkockázata nem elfogadható, végre kell hajtani a frissítést. A frissítések ellenőrzött módon történő végrehajtását a konfigurációs változáskezelés keretében kell végrehajtani az alábbiak figyelembevételével:

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- a) Kiadott általános szállítói biztonsági frissítés esetén pontosan azonosítani kell a verziót, amire szükség van, de mellette érdemes megvizsgálni, hogy milyen frissítések állnak még rendelkezésre.
- b) Meg kell vizsgálni a biztonsági frissítés feltételeit, pl. hogyan kell a rendszert előkészíteni, szükséges-e más frissítés előtte, stb.
- c) Megbízható forrásból be kell szerezni a biztonsági frissítést és ellenőrizni kell az azonosságot, sértetlenséget és a dokumentumokat.
- d) Egyedi biztonsági frissítés esetén a szoftvert el kell készíttetni a rendszerre vonatkozó tervezési és fejlesztési szabályok szerint, és sikeres elfogadási teszten keresztül azt át kell venni.
- e) A beszerzett biztonsági frissítés fájljainak vírusmentességét ellenőrizni kell. A dokumentumok alapján meg kell győződni arról, hogy a biztonsági frissítés végrehajtható-e.
- f) FAT előtt fel kell rakni a programozható rendszerekre az aktuális és ellenőrzött biztonsági frissítéseket, és ezt dokumentálni kell.
- g) SAT előtt – amennyiben indokolt – fel kell rakni a programozható rendszerekre az akkor aktuális és ellenőrzött biztonsági frissítéseket, és ezt dokumentálni kell.

A programozható rendszerek számára el kell készíteni a biztonsági frissítésekre vonatkozó eljárásrendet az első FAT tesztre. Mivel a biztonsági frissítések megváltoztatják a programozható rendszert, és a biztonsági frissítések beszerzésének, tárolásának módja, és egyéb sajátosságok idővel változhatnak, a biztonsági frissítésekre vonatkozó eljárásrendet karban kell tartani, hogy kövesse a változásokat. Így a biztonsági frissítésekre vonatkozó eljárásrend egy élő dokumentum, amit a konfigurációkezelő rendszerben kell nyilvántartani, és követni kell a verzióit az általa végrehajtott biztonsági frissítésekkel együtt.

Az átalakításokhoz megkövetelt kockázatelemzés célja annak igazolása, hogy a tervezett átalakításokkal a rendszerek kockázata nem kerül az elfogadható szint fölé. Ha mégis meghaladná az elfogadható kockázati szintet, akkor a kockázatot csökkentő védelmi kontrollokra van szükség. Mindezek biztosítása miatt az átalakításokat a konfigurációs változtatások eljárásrendjének keretében kell elvégezni.

A kockázatelemzés során vizsgálni kell a konfigurációs beállítások, paraméterek és adatok régi programozható rendszerből az új programozható rendszerbe történő betöltésének (migráció) megvalósíthatóságát. Meg kell győződni arról, hogy a régi adatok

Nukleáris létesítmények programozható rendszereinek védelmi követelményei hozzáférhetőek, másolhatók, teljeseek, összeegyeztethetőek az új rendszerrel, és szükséges-e adattranszformáció.

A programozható rendszereket érintő bármilyen módosítás átalakításnak minősül és végig kell mennie a FAT-teszten, létesítésiengedély-kérelmen, SAT-teszten és üzemeltetésiengedély-kérelmen.

3.5.2.14. Elektromágneses impulzusok elleni védelem

Új nukleáris létesítmények építése esetén kiegészítő ajánlások az alábbiak:

A programozható rendszerek nagyon gyors elektromágneses impulzusok elleni védelmét a létesítmény fizikai védelmével és a mélységi védelem stratégiájával összhangban kell megtervezni és kialakítani. A nagyon gyors elektromágneses impulzusok fenyegetettséget jelentenek a programozható rendszerekre, és ebből adódóan kockázatelemzés keretében kell felmérni a fenyegetettségek programozható rendszerekre gyakorolt hatásait és valószínűségeit, majd az elviselhető kockázat megállapítása alapján a védelmikontroll-intézkedéseket megtervezni. A fenyegetettségek forrásai a védelemre vonatkozóan a mesterségesen is előállítható káros elektromágneses impulzusok. A hatások ellen a programozható rendszerek és adataik sértetlenségét és rendelkezésre állását kell védeni.

Gondolni kell az adathálózatok, a villamos ellátást biztosító elektromos hálózatok, és a hűtési rendszerek védelmére.

A kockázatelemzésnél elemezni kell a kábelek által közvetíthető konduktív és induktív hatásokat és az elektromos mezők hatásait. A káros hatások ellen a védelem fizikai természetű, és ajánlott a rendszereket zónák szerint védeni. Mivel a mélységi védelemben a zónák határvonalai egyben fizikai határok, ajánlott a kétféle védelmi zónát illeszteni. Ilyen módon a védelmi zónákhoz meghatározott védelmi szint biztosításához az elektromágneses impulzusok által jelentett fenyegetettséget számba kell venni. Az alkalmazható védelmikontroll-intézkedések a következők:

- a) Földelés és potenciálkiegyenlítés.
- b) Mágneses árnyékolás a programozható rendszereknél és a kábeleknel.
- c) Nyomvonal-kialakítás a kábeleknel.
- d) Koordinált túlfeszültségvédelem a programozható rendszereknél, a kábeleknel és a kábelek végződéseinél.

Az elektromágneses impulzusokat okozó rosszindulatú támadásokat fizikai határvédelemmel elérhető távolsággal lehet megelőzni, vagy a hatásokat csökkenteni. Ezért a mélységi védelem fizikai határvonalainak kialakításakor az ilyen jellegű támadásokat figyelembe kell venni.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

A tervezett védelmikontroll-intézkedéseket a programozható rendszerek védelmi tervében kell dokumentálni a fizikai védelemi tervvel összhangban.

A már üzemelő létesítmények esetében meg kell vizsgálni az irányítástechnikai helyiségek védettségét, és szükség esetén árnyékolási megoldásokat (lefeldelt, alkalmas lyukméretű fémháló) lehet telepíteni.

3.5.2.15. Azonosító- és jelszókezelés

Az azonosításhoz a személyeket és rendszereket egyértelmű azonosítóval kell ellátni és a hozzárendelést jóvá kell hagyni. Az azonosítókról és a hozzárendelésekről nyilvántartást kell vezetni, és visszavonáskor a nyilvántartást aktualizálni kell.

A hozzáférésekhez megfelelően erős hitelesítési módot kell választani a programozható rendszer védelmi szintjéhez igazítva, hogy ne lehessen azt könnyen kijátszani vagy feltörni. A hitelesítés leggyakrabban jelszóval történik, ezért a jelszavak létrehozását, közlését és használatát külön szabályozni kell. Cél, hogy elég erős legyen, és csak az ismerje, akihez tartozik, vagyis ne juthasson illetéktelenek tudomására.

A jelszavakon kívül más hitelesítési módot meg lehet határozni, amely helyettesítheti vagy kiegészítheti a jelszavas hitelesítést. Ilyen pl. a biometrikus hitelesítő (retina, ujjlenyomat, írisz, hang), chipkártya és token. Ilyenkor mérlegelni kell az alkalmazás körülményeit és a hitelesítési mód előnyeit, illetve hátrányait. Ha a védelmi szint megköveteli, a hitelesítéshez többfaktorú (multi factor) hitelesítési módot kell előírni. Ilyenkor rendszerint egymás után többféle hitelesítésen kell átesni, és a hitelesítések mindegyikének sikeresnek kell bizonyulni az érvényességhez.

A hitelesítés akár sikeres vagy sikertelen, olyan esemény, amit a programozható rendszereknek naplózni kell, és a rendellenességeket az incidenskezelés keretében ki kell vizsgálni. Személyek mellett sok esetben a programozható rendszereken futó szolgáltatásokat is azonosítani és hitelesíteni kell. Ez hasonló módokon történhet, mint a személyek esetében úgy, hogy itt a hitelesítő adat jellemzően egy kódoltan tárolt jelszó. Fontos, hogy a szolgáltatásokra alkalmazni kell a legkisebb jogosultság elvét.

Ezen kívül az üzenetek és elektronikus dokumentumok hitelességének biztosítására vagy ellenőrzésére lehet szükség. Ilyen esetekben az üzenetet el kell látni digitális aláírással és biztosítani kell a nyilvános kulcsú infrastruktúra (Public Key Infrastructure - PKI) kiépítését a kommunikáló rendszerek között a privát és publikus kulcsok kezeléséhez. Ennek megvalósításhoz megfelelő protokollokat (pl. IP Sec, SSL/TLS, S/MIME) és azokat támogató alkalmazásokat kell felhasználni. A digitális tanúsítványok

Nukleáris létesítmények programozható rendszereinek védelmi követelményei belső kiadását vagy beszerzését, valamint azok védelmét eljárásrendben kell szabályozni.

3.5.2.16. Hordozható eszközök és mobil adathordozók használata

A hordozható eszközök, ideértve a mobil adathordozókat és a saját tulajdonú BYOD (Bring Your Own Device) eszközöket, alkalmasak a bizalmas adatok felfedésére, fertőzött kód programozható rendszerekbe történő bejuttatására és akár rendszerek elindítására a rajtuk tárolható operációs rendszerek segítségével. Emiatt használatukat adminisztratív, fizikai és technikai védelmi kontroll intézkedésekkel korlátozni kell figyelembe véve legalább az alábbiakat:

- a) Minden hordozható eszköz használatát tiltani kell, ami külön nincs engedélyezve (white list). Így meg kell határozni, hogy kinek, mit, hol és mihez szabad használni.
- b) Meg kell tiltani a BYOD-eszközök védett zónákba történő bevitelét.
- c) Meg kell tiltani a hordozható eszközök mozgását a védelmi zónák között.
- d) Monitorozni, naplózni és ellenőrizni kell a hordozható eszközök csatlakozását a programozható rendszerekhez.
- e) Fizikai hozzáférési védelmikontroll-intézkedésekkel korlátozni kell időben és térben (mikor, hol) a hordozható eszközök által történő fizikai adatmozgatást.
- f) A hordozható eszközök integritását és bizalmasságát olyan védeltségi szinten kell biztosítani, mint ami a csatlakoztatott programozható rendszerekre vonatkozik.
- g) Meg kell győződni a csatlakoztatni kívánt hordozható eszközök eredetéről és a rajta lévő adatok sértetlenségéről. Ellenőrizni kell, hogy kitől és honnan származnak az adatok, és az adatforrás azonosságát is ellenőrizni kell, hogy a forrás valóban az-e, akinek állítja magát. Ezen túl ellenőrizni kell, hogy az adatok sértetlenek maradtak-e az esetleges szállítás alatt.
- h) A programozható rendszereken a hordozható eszközök számára biztosított csatlakoztatási pontokat a szükséges minimumra kell csökkenteni és lehetőség szerint korlátozni kell a csatlakoztathatóság idejét.
- i) A programozható rendszereken ki kell kapcsolni vagy meg kell szüntetni a hordozható eszközökről történő elindítás funkcióját (boot).

3.5.2.17. Vezeték nélküli készülékek és hálózatok

A vezeték nélküli készülékek és hálózatok elterjedése programozható rendszerek körében is egyre jelentősebb. A technológia alkalmazása

Nukleáris létesítmények programozható rendszereinek védelmi követelményei bizonyos esetekben előnyös (pl. vezetékes hálózat hiánya, alternatív kommunikációs lehetőség biztosítása), azonban használatát védelmi szempontok szerint mérlegelni kell:

- a) Rádióhullámok kommunikációvesztést okozhatnak.
- b) A csatorna illetéktelen lehallgatása vagy blokkolása veszélyt jelent.
- c) Titkosítás, hitelesítés, behatolás érzékelés alkalmazása szükséges.
- d) A titkosítási mechanizmusok és protokollok gyorsan változnak.
- e) A biztonságra és védelemre gyakorolt minden hatást figyelembe kell venni.
- f) A hálózat elválasztása a vezetékes hálózattól ajánlott.

Ha szükséges a vezeték nélküli hálózatok használata, akkor a vezeték nélküli hálózatokon történő hozzáféréseket védelmi intézkedésekkel korlátozni kell legalább az alábbiak figyelembevételével:

- a) Használatukat a programozható rendszereknél alapvetően meg kell tiltani, és csak bizonyos indokolt esetekben szabad engedélyezni.
- b) A hozzáférési tartományt korlátozni kell a szükséges területre és a rendelkezésre állást a szükséges időre.
- c) A programozható rendszereken a csatlakozási funkciót ki kell kapcsolni, ha nem engedélyezett a használata.
- d) Monitorozni kell a rendelkezésre álló vezeték nélküli hálózatokat.
- e) A hálózatokon történő hozzáféréseknek összhangban kell lennie a mélységi védelemmel.
- f) Ha lehetséges, a vezeték nélküli hálózatokon kriptográfiai eszközökkel kell biztosítani az adatok forrásának hitelességét és az üzenetek tartalmának sértetlenségét az adatátvitel során (pl. védve van man-in-the-middle típusú támadások ellen).

A vezeték nélküli eszközök mint hordozható eszközök létesítményen belüli használatát szabályozni kell.

3.5.3. Folytonos üzemvitel, rendszerek biztonsági mentése

3.5.3.1. Folytonos üzemvitel

A biztonsági szempontból kritikus rendszerek esetében olyan intézkedéseket kell bevezetni, amelyek mind üzemzavari és katasztrófa helyzetekben, mind üzemeltetési és felhasználási problémák, hibák esetében biztosítják a folytonos üzemvitel fenntartását, szükség esetén helyreállítását.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
A folytonos üzemvitel biztosításában alapvető szerepe van a megelőző intézkedéseknek, melyek főbb területei:

- a) Üzemeltetési, karbantartási előírások biztosítása.
- b) Tartalék eszközök biztosítása.
- c) Felkészült üzemeltető, karbantartó személyzet biztosítása.
- d) Biztonsági mentések készítésének szabályozása.
- e) Felelősségek meghatározása.
- f) Külső szerviz, külső tartalékképzési megoldás alkalmazására vonatkozó intézkedések megfontolása.
- g) Fizikai, logikai védelmi rendszerek és intézkedések alkalmazása.
- h) Hibatűrő műszaki megoldások alkalmazása.
- i) A folytonos üzemvitel biztosítása érdekében szükséges szabályozások:
- j) Ki kell dolgozni a rendszereken, berendezéseken végzett hardver-, szoftver-, adat- és paramétermódosítások végrehajtására vonatkozó szabályzást. A módosításokat minden esetben dokumentáltan kell végezni.
- k) Ki kell dolgozni a vírusvédelemre vonatkozó szabályokat.
- l) Ki kell dolgozni a hordozható eszközökre vonatkozó szabályokat.
- m) Helyreállítási tervet kell kidolgozni a bekövetkezett hibák, üzemzavarok tervszerű, gyors és hatékony elhárítása érdekében.

3.5.3.2. Rendszerek biztonsági mentése

Biztonsági mentés készítésének célja

A biztonsági szempontból kritikus berendezés, rendszer, illetve információ sértetlenségének és rendelkezésre állásának fenntartása érdekében az operációs rendszerekről, programokról, adatokról, paramétereikről és dokumentumokról elektronikus másolatot, mentést kell készíteni.

A mentések megléte lehetővé teszi, hogy esetleges meghibásodások esetén a meghibásodott berendezést, a lehető legkisebb kiesés mellett, a meghibásodás előtti működőképes állapotba lehessen hozni.

A fenti célok elérése érdekében a mentések készítésére vonatkozó szabályzásban (nyilvántartásban) tételesen fel kell sorolni a mentendő berendezéseket, meg kell határozni az egyes berendezések esetében készítendő mentések típusait, hogy milyen ciklussal és mely esetekben kell mentést készíteni, illetve a mentések ellenőrzését, tárolását, nyilvántartását hogyan kell végezni.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

A biztonsági mentés szabályrendszerének hatálya

A biztonsági mentési szabályokat úgy kell definiálni, hogy érvényesek legyenek minden olyan berendezésre, rendszerre, amely mentését rendszeresen vagy esetileg kell elvégezni.

A mentendő rendszereket és azok minden mentendő komponensét nyilván kell tartani. A mentésekből az adott rendszerhez tartozó bármely berendezés esetén a teljes programrendszernek előállíthatónak kell lennie. Az előállítás módszerét az adott berendezés érvényes dokumentumainak tartalmaznia kell. A reprodukálásnak az adott berendezésre vonatkozó üzemeltetési előírásokban definiált időkorlátokon belül elvégezhetőnek kell lennie.

Mentési kategóriák meghatározása

A biztonsági mentési szabályokban elő kell írni, hogy a mentést minimálisan az alább definiált két kategóriában kell elkészíteni:

- a) Szakterületi mentés: az ilyen típusú mentéseket a karbantartó, üzemeltető szervezetek napi feladatainak ellátása, váratlan hibák elhárítása, rendszerek, eszköz- és adatvagyonelemek helyreállításának céljából kell készíteni.
- b) Tartalék mentés: a tartalék mentés szintén az esetleges hibák elhárítása, a rendszerek helyreállítása céljából készül, de a szakterületi mentéstől függetlenül kell tárolni. Ennek célja, hogy a szakterületi mentés esetleges problémája – sérülés, stb. – esetén lehetőség legyen a rendszer, az adatvagyonelem, stb. helyreállítására.

Mentések készítésének szabályai

A biztonsági szempontból kritikus rendszerek mentéseinek készítésére vonatkozó szabályozást az alábbi szempontok figyelembevételével kell kidolgozni:

- a) Szükséges-e a biztonsági mentéseket előre meghatározott időközönként, ciklikusan elkészíteni.
- b) Szükséges-e a rendszer tervezett karbantartása, módosítás esetén, a karbantartás, vagy módosítás megkezdése előtt mentést készíteni.
- c) Szükséges-e a karbantartást, módosítást követően ismételten menteni.
- d) Meg kell határozni, hogy módosítást követően elegendő-e a módosítás által érintett terjedelemben (rendszerkomponens, adatbázis, stb.) menteni, vagy a teljes rendszert le kell menteni.

Bármilyen okból történik mentés, annak végrehajtását minden esetben dokumentálni kell. Az elkészült mentéseket egyértelmű azonosítóval el kell látni, majd nyilvántartásba kell venni.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

Mentések tárolása

A biztonsági szempontból kritikus rendszerek mentéseinek készítésére vonatkozó szabályozásban a mentések tárolására vonatkozó előírásokat ki kell dolgozni. Ennek során az alábbi szempontokat kell figyelembe venni.

- a) Az üzemeltetés, karbantartás napi hibajavítási feladatainak ellátásához szükséges mentéseket úgy kell elhelyezni, hogy a folytonos üzemvitel megszakadása esetén a helyreállítás a lehető leghamarabb megtörténhessen. A tárolás helyét úgy kell meghatározni, hogy a mentések elérhetősége bármely időszakban (normál munkaidőben vagy azon kívül) biztosított legyen.
- b) Az egyes rendszerekhez tartozó mentések munkapéldányait rendszerenként elkülönítve kell tárolni, hogy a mentés felhasználása során az esetleges téves felhasználás valószínűsége a legkisebb legyen. További fontos követelmény, hogy az adott munkapéldánynak csak az aktuális verziója legyen a rendszerrel azonos helyszínen.
- c) A tartalék mentések tárolását más, azonos káresemény általi sérüléstől védett helyen kell biztosítani.
- d) A mentések tárolásának szabályait úgy kell kialakítani, hogy a mentésekhez csak az arra jogosult üzemeltető és karbantartó szervezetek illetékes tagjai férhessenek hozzá.
- e) Adathordozó fizikai tárolása esetén gondoskodni kell a tárolóhely megfelelő fizikai védelméről, elektronikus tárolás esetén (pl. erre a célra kijelölt szerver) a megfelelő jogosultsági rendszer kialakításáról.

Mentések ellenőrzése

A biztonsági szempontból kritikus rendszerek mentéseinek készítésére vonatkozó szabályozás a mentések ellenőrzésére vonatkozóan minimálisan az alábbi előírásokat tartalmazza:

- a) Milyen időközönként, illetve mely esetekben kell az ellenőrzést végezni.
- b) Ellenőrizni kell, hogy az előírt példányszámú mentés az előírt tárolóhelyeken megtalálható-e.
- c) Ellenőrizni kell, hogy a mentések azonosítói megegyeznek-e a nyilvántartásban szereplő azonosítókkal.
- d) Össze kell vetni a rendszer aktuális állapotát az adott rendszerről utoljára készített mentéssel. Amennyiben eltérés tapasztalható (módosítás történt a rendszeren), abban az esetben pótolni kell a mentést, illetve aktualizálni kell a mentési nyilvántartást.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

e) Mi a teendő abban az esetben, ha mentés hibája, használhatatlansága igazolódik (sérülés, inkompatibilitás).

Mentések visszatöltése

A mentések készítésére vonatkozó szabályozás mentések visszatöltésére vonatkozó részének kidolgozása során meg kell határozni, hogy

- a) A berendezések dokumentációjában ki kell dolgozni a mentések visszatöltési eljárásait.
- b) Szükséges/lehetséges-e a mentés visszatöltéssel történő ellenőrzése.

Azonosítás, nyilvántartás

A mentések esetleges téves felhasználásának elkerülése érdekében:

- a) Ki kell dolgozni a mentések azonosítási rendszerét. Az azonosítási rendszert úgy kell kialakítani, hogy egyértelműen utaljon a mentett rendszerre, berendezésre, annak helyére, a mentés idejére, illetve a mentés szintjére (teljes rendszer, szoftverkomponens, adatbázis).
- b) Ki kell dolgozni a mentések nyilvántartási rendszerét.
- c) Meg kell határozni a nyilvántartás vezetéséért felelős személyt, szervezetet.

A nyilvántartásról célszerű mentést készíteni arra az esetre, ha a nyilvántartás bármilyen okból hozzáférhetetlenné válik.

3.5.4. Szerződéses partnerek, beszállítók, szolgáltatók, alvállalkozók kiberbiztonsága

Az engedélyes gyakran külső szolgáltatóktól vesz igénybe szolgáltatásokat, vagy felhasználja azok termékeit, amelyek esetenként érzékeny vagy védett információkat, rendszerelemeket tartalmazhatnak. Ilyen esetekben olyan jogi megállapodásokat kell kötni, amik tartalmazzák a megfelelő kiberbiztonsági követelményeket. A megállapodások kidolgozásakor figyelembe kell venni, hogy a szállított termékekkel és szolgáltatásaikkal a beszállítók olyan védett információkhoz juthatnak (pl. sérülékenységek), amik a megállapodás hatályán kívül fejthetik ki hatásukat. Ehhez kapcsolódóan szükséges, hogy az engedélyes olyan kiberbiztonsági intézkedési, felmérési és értékelési folyamatokat alakítson ki, működtessen és dokumentálja azok eredményét, amik eredményeként csökken a szerződéses partnerek, beszállítók, szolgáltatók és alvállalkozók által közvetített, a nukleáris létesítmény programozható rendszerei ellen irányuló rosszindulatú és véletlen károkozások kockázata.

A programozható rendszerek védelmi tervének célszerű tartalmaznia a külső szállítókra vonatkozó követelményeket. Ez magában foglalja a telephelyen belüli és kívüli munkákra érvényes követelményeket, valamint azt az elvárást,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei hogy a külső szállítóknak védelmi intézkedéseket kell fogantatosítaniuk az általuk szállított termék vagy szolgáltatás megfelelő védelme érdekében.

Célszerű, ha az engedélyes belső eljárásrend keretében szabályozza a beszerzés folyamatát. A beszerzés egyes szakaszaira vonatkoztatva ez a következőkből áll:

- a) Előkészítés, elemzés, a projektszintű kockázatok meghatározására: sérülékenységek, fenyegetettségek elemzése; kockázatok meghatározása; intézkedések tervezése (pl. IEC 63096 szerint); maradványkockázat és strukturális kritikusság elemzése (pl. IEC 62645 szerint).
- b) Követelmények meghatározása: az intézkedések és a kritikusság elemzés alapján meghatározhatók az alvállalkozó biztonsági irányítási rendszerére és az általa szállított termékre vagy szolgáltatásra vonatkozó követelmények, amelyek érinthetik a fejlesztés teljes életciklusát, a tervezett funkcionalitást, a beágyazott elemekre vonatkozó biztonsági követelményeket.
- c) Alvállalkozó kiválasztása fázis: pályázati kiírás az alapkövetelmények alapján, tanúsítások beszerzése alapján (pl. ISO 27001 szerint), amik segítenek az alvállalkozó alkalmasságának megítélésében, előzetes auditok szervezése, amikkel ellenőrizhető a követelményeknek való megfelelés.
- d) Alvállalkozó nyomon követése: az alvállalkozó auditálása, a projektet lezáró jelentés; a sebezhetőségek technikai szintű nyomon követése.

Az alvállalkozókra vonatkozó kibervédelmi szabályozásban legalább a következő témakörökre kell kitérni:

- a) A programozható rendszerekhez való hozzáférés és az azokon végzett munka feltételei.
- b) A megállapított programozható rendszerek védelmére vonatkozó követelményeknek való nem-megfelelések szankcionálása.
- c) A programozható rendszerek karbantartására, konfigurálására, frissítésére és tesztelésére vonatkozó rendszabályok, köztük a mobil adathordozókra, hordozható számítógépekre, diagnosztikai- és tesztberendezésekre vonatkozó szabályok kialakítása.
- d) Az alvállalkozó számára kijelölt kapcsolattartási pont meghatározása a kiberbiztonsági kérdések kezelésére, az alvállalkozó által észlelt biztonsági események, incidensek bejelentésére.
- e) Az engedélyes és az alvállalkozó közötti tájékoztatási és együttműködési kötelezettségek, eljárások meghatározása az engedélyes programozható rendszereit érintő kiberbiztonsági

Nukleáris létesítmények programozható rendszereinek védelmi követelményei sérülékenységgé ismertté válása esetében. Ezek magukban foglalhatják a bizalmas és egyéb információk védelmi követelményeit, a tájékoztatási és együttműködési kötelezettségeket stb.

Az alvállalkozók körében kiemelt fontosságú az MSZ/ISO/IEC 27001 szabvány szerint tanúsított információbiztonsági irányítási rendszerrel (IBIR) rendelkező alvállalkozók preferálása, rendszeres auditok és ellenőrzések tervezése és végrehajtása.

A programozható rendszerek védelme érdekében az engedélyeseknek megfelelő szerződéses követelményeket, előírásokat és garanciákat kell érvényesíteniük, beleértve az engedélyes által végzett auditok és ellenőrzések lefolytathatóságát a harmadik fél közreműködési kötelemével annak érdekében, hogy az elvárt kiberbiztonsági színvonal folyamatos fenntartása minden esetben biztosított legyen a saját- és külső munkavállalók esetében egyaránt.

Az engedélyesnek – a megkötött szerződés részeként – valamennyi alvállalkozójától meg kell követelnie, hogy azok a fentiekben kifejtett, a programozható rendszerek védelmére vonatkozó követelményeket a saját al-alvállalkozóikkal szemben is érvényesítsék, beleértve a védelmi szabályozásba történő betekintés és a követelmények teljesülésének ellenőrzési feltételeit.

3.5.5. *A védelemmel összefüggő oktatás, továbbképzés, védelmi kultúra*

3.5.5.1. A védelmi oktatás és továbbképzés céljainak, rendjének meghatározása

A programozható rendszerekkel kapcsolatos védelmi oktatás és továbbképzés célja olyan szintű ismeret megszerzése, hogy a résztvevők legyenek tudatában az általuk használt rendszerek és hálózatok fenyegetettségének, a védelem szükségességének, továbbá hogy mit tehetnek a munkakörükhöz rendelt védelmi szint megtartásáért, illetve növeléséért.

Rendszeresen ellenőrizni kell a munkavállalók végzettsége, képzettsége és/vagy tapasztalata alapján azt, hogy rendelkeznek-e a szerepköreik betöltéséhez szükséges védelmi ismeretekkel. A programozható rendszerek védelmével kapcsolatos alapvető szaktudás-követelményeket kell meghatározni, és ahol lehet ott minősítési és tanúsítási programokat kell felhasználni annak ellenőrzéséhez, hogy azokat naprakészen tartják-e.

A programozható (technológiai és ügyviteli) rendszerek összes felhasználójának (felhasználó, kiemelt felhasználó, rendszergazda) eredményes oktatásához szükséges minden csoport képzési igényének beazonosítása. Emellett e folyamat kiterjed egy, az eredményes képzést, és

Nukleáris létesítmények programozható rendszereinek védelmi követelményei az eredmények mérését szolgáló stratégia meghatározására és végrehajtására.

Minden felhasználói csoport számára egyéni tanrendet kell kidolgozni és rendszeresen aktualizálni.

Az újonnan belépő munkavállalók képzési rendjébe be kell építeni a programozható rendszerek védelmi ismereteit, úgy hogy az belső szabályozási szinten megjelenjen.

3.5.5.2. A kialakított jogosultsági szinteknek megfelelő védelmi oktatási kritériumok a korábban meghatározott védelmi szintek követelményeit figyelembe véve

A meghatározott védelmi szintek követelményeit figyelembe véve ki kell dolgozni egy olyan képzéskritérium-rendszert, mely biztosítja azt a tudásszintet, amellyel biztosítható az adott védelmi szint követelményeinek való megfelelés.

Védelmi szintek/ Felhasználói jogok	Felhasználó	Kiemelt felhasználó	Rendszergazda
5	I.	I.	I.
4	I.	I.	II
3	I.	II	II
2	I.	II	III.
1	II	III.	III.

A táblázatban található „programozható rendszerek védelmi ismeretei” oktatási kategóriákhoz (I., II., III.) ki kell dolgozni a kritériumokat, úgymint képzések rendszeressége, tudásszintje és mélysége valamint a rá fordított idő, a visszamérés metodikája.

3.5.5.3. Speciális oktatások, továbbképzések rendje

Képzési programot kell kidolgozni a programozható rendszerek védelmét érintő minden olyan új technológiai szabványra, eljárásra és termékre vonatkozóan, amelyeket a szervezetnél bevezetnek, még a bevezetés előtt, a bevezetés céljától függetlenül.

A képzésnek testre szabottan kell kiterjednie a vezetői, az üzemeltetői és a karbantartói személyzetre, a védelmi és az üzemeltetői szerepekre. Célszerű a képzéseknek elméleti és gyakorlati elemeket tartalmazniuk. Az

Nukleáris létesítmények programozható rendszereinek védelmi követelményei elsajátított ismereteket (bejelentett vagy eseti) gyakorló tréningek tartásával célszerű elmélyíteni.

A már kialakított képzési rendnek megfelelő oktatásokon túl, amennyiben szükséges rendkívüli képzéseket kell tartani.

3.5.5.4. Védelmi kultúra kialakítása

A programozható rendszerek védelmi kultúrájának megteremtése egy olyan folyamatos és rendszeres tevékenység, melynek során elérhető az a kedvező állapot, ahol az alábbi feltételek teljesülnek:

- a) Az összes felhasználó részesül etikus viselkedéssel és a rendszervédelmi tudatossággal foglalkozó képzésben. Az etikus viselkedés és a rendszervédelmi alapelvek vonatkozásában pozitív hozzáállás tapasztalható.
- b) Az összes felhasználó részesül a rendelkezésre állás, a bizalmasság és a sértetlenség sérülését okozó hibákból származó károk elleni védelemre vonatkozó rendszerbiztonsági eljárások megfelelő szintű képzésében.
- c) A vezetés figyelemmel kíséri ennek megfelelőségét a képzési és oktatási programok és folyamatok folyamatos felülvizsgálata és aktualizálása révén.
- d) Rendszeres időközönként gyakorlati oktatást kell tartani a vezetői, üzemeltetői és karbantartó személyzet számára annak érdekében, hogy mindenki tudatában legyen a programozható rendszerek védelmének fontosságával.

Az ember okozta szándékos vagy szándékolatlan károkozás megelőzésének leghatékonyabb módja a programozható rendszerek védelmi szervezetének létrehozása, szerepek és felelősségek meghatározása és a hozzáférések korlátozása. Ezeket további, a személyzettel vagy a személyzet által kezelt programozható rendszerekkel kapcsolatos védelmi intézkedésekkel kell kiegészíteni, amelyek legalább az alábbiak:

- a) Az alkalmazás feltételeként ajánlott a következő ellenőrzéseket elvégezni: az Atv. 11. §-a szerinti foglalkoztatást kizáró okok (pl. büntetett előélet, meghatározott bűncselekmények elkövetése miatti bírósági elítélés), életrajz helyessége és teljessége, referenciák, pszichológiai viselkedés, valamint interneten és egyéb médiában való megjelenés vizsgálata. Ha a vizsgálathoz az engedélyesnek nincs megfelelő kompetenciája/erőforrása - különösen a pszichológiai viselkedéssel kapcsolatosan - szakértő személy vagy intézmény támogatásának igénybe vétele lehet indokolt.
- b) A magasabb védelmi szintű eszközökkel kapcsolatban álló személyzetet szigorúbban és rendszeresen kell ellenőrizni. Adott esetekben a

Nukleáris létesítmények programozható rendszereinek védelmi követelményei személyiségi jogokkal összeegyeztetve a személyzet viselkedését és munkavégzését figyelni kell a hozzáférési jogosultságok megadása után.

- c) A programozható rendszerek kezelését úgy kell kialakítani, hogy az minél kevesebb lehetőséget adjon az emberi tévedésre és vegye figyelembe az emberi reakció idejét.
- d) Az információbevitelt, ideértve a manuális adatbevitelt és adatbeolvasást, a lehetőségek szerint korlátozni kell és a programozható rendszereknek ellenőrizni kell a bevitt adatok teljességét, pontosságát, érvényességét és hitelességét. Az ellenőrzést minél előbb el kell végezni, így pl. adatbevitelnél a bevétel közben vagy közvetlenül a bevétel után a letárolás, vagy feldolgozás előtt. Ha meg lehet határozni az érvényes értelmezési tartományokat, akkor ezek alapján vizsgálni kell a bevitt adatok érvényességét. Ha lehetséges, a bevitt adatok konzisztenciáját meg kell vizsgálni az éppen beolvasott adatok körében, hogy egymáshoz képest és a már korábban beolvasott adatokhoz viszonyítva konzisztensek-e.
- e) Az információk megjelenítésénél az egyértelműsége és a jól láthatóságra kell törekedni, és csak a szükséges mennyiségű információt szabad kiadni.
- f) A beszállítónak nyilatkoznia kell, hogy hogyan akadályozza meg az alkalmazottak által ismert bizalmas információk felfedését, ami a programozható rendszerek védelmének csökkentéséhez vezethet.
- g) A beszállítónak meghatározott időn belül közölnie kell, ha a programozható rendszerek védelmével kapcsolatos bizalmas információval rendelkező személyzet kilép, vagy beosztása megváltozik.
- h) A beszállítónak részletes dokumentációt kell biztosítani az általa érintett programozható rendszerek védelmének támogatásáról és karbantartásáról, abban az esetben, ha a beszállítóval megszűnik az üzleti kapcsolat.
- i) A beszállítónak minden bizalmas adatot vissza kell szolgáltatnia, ha a leszállított programozható rendszerek karbantartása részéről befejeződik.
- j) A beszállító köteles a neki szolgáltató teljes beszállítói lánc személyzete számára alkalmazott védelmi intézkedéseket dokumentálni, a személyzetet átvilágítani, valamint a viselkedését és a védelmi intézkedéseknek történő megfelelését monitorozni.
- k) A beszerzésekkel érintett beszállítók szerződéseibe egyértelműen és részletesen be kell írni a személyzetre vonatkozó védelmi intézkedéseket.

Ha a megelőzési intézkedések ellenére károkozás történik, az védelmi incidensnek minősül a programozható rendszerekre nézve, és az

Nukleáris létesítmények programozható rendszereinek védelmi követelményei eseménykezelés ajánlásai, folyamata szerint kell eljárni (lásd 3.4.7). Ugyanakkor a támadás és károkozás személyzeti jellege miatt az incidenskezelés számos speciális intézkedéssel járhat. Ilyenek pl. az elszigetelés, a károkozás megállítása vagy bizonyítékokról való gondoskodás szükségessége. Ezek specifikus eljárásokat igényelhetnek, amelyeket dokumentálni kell.

3.5.6. Védelmi felülvizsgálat

A védelmi intézkedések felülvizsgálatának célja a védelmi intézkedések működésének, hatékonyságának, a követelményeknek való megfelelés ellenőrzése.

A felülvizsgálat során a programozható rendszerek védelmi felelőse és a védelmi megbízottak átfogóan és módszeresen ellenőrzik a védelmi tervben megfogalmazott követelmények teljesülését. A felülvizsgálat során általános elemzést készítenek a létesítmény védelmi intézkedéseinek működéséről, javaslatokat fogalmaznak meg a szükséges változtatásokról, fejlesztésekről.

A felső vezetés felelőssége, hogy a felülvizsgálat során készült elemzéseket rendszeresen értékelje, a szükséges változtatásokra intézkedéseket tegyen.

A létesítmény programozható rendszereinek védelmét, a védelmi tervet, a védelmi tervben megfogalmazott védelmi intézkedések teljesítését a hatóság bejelentett és be nem jelentett ellenőrzésekkel rendszeresen felülvizsgálja.

Új nukleáris létesítmények építése esetén kiegészítő ajánlások az alábbi témában:

A védelmi kontrollok megvalósítását úgy kell tervezni, hogy a helyes működésük ellenőrizhető legyen. Ehhez meg kell határozni azokat az eseményeket, amelyekhez auditnaplót szükséges generálni. A naplózás tartalmát meg kell határozni és minden bejegyzéshez időbélyeget kell rögzíteni. Ügyelni kell arra, hogy legyen elég tárolókapacitás az auditfájlok tárolásához és le kell korlátozni a fájlokhoz történő hozzáféréseket. Szükség esetén nem módosítható médiára kell a naplóállományokat írni, és figyelni kell, hogy a naplót adott esetben jogi eljárásokhoz fel lehessen használni bizonyítékként.

A vizsgálatot meg kell tervezni, és a vizsgálati tervben rögzíteni kell a vizsgálat terjedelmét, a célkitűzéseket és az ellenőrzőlistákat. A vizsgálat során felül kell vizsgálni a kapcsolódó dokumentumokat (szabályzatok, eljárások, ajánlások, naplófájlok, hozzáférési listák, konfigurációs fájlok, stb.), interjúkat kell készíteni a személyzettel, és meg kell figyelni a rendszerek működését (konfigurációkezelés, védelmi eljárások, hozzáférési kontrollok, szétválasztott hatáskörök, események monitorozása, hálózati architektúra, stb.). Végül a vizsgálati eredményeket egy jelentésben össze kell foglalni. A nem megfelelést okozó feltárt hiányosságokhoz javítóintézkedéseket kell

Nukleáris létesítmények programozható rendszereinek védelmi követelményei megfogalmazni, azokat tervezett módon végre kell hajtani, és a megvalósítást ellenőrizni kell.

3.5.7. A védelmi terv hatékonyságának ellenőrzésére vonatkozó követelmények

A programozható rendszerek védelmi tervében a védelmi terv hatékonyságát ellenőrző intézkedések ismertetésére ki kell térni. Ilyen lehetőségek a következők:

- a) belső auditok, ellenőrzések,
- b) független auditszervezet által végrehajtott ellenőrzések,
- c) hatósági ellenőrzések,
- d) kibervédelmi gyakorlatok.

A programozható rendszerek védelmi tervének ellenőrzésére vonatkozó intézkedések tartalmazzák

- a) az ellenőrzés/gyakorlat tartásának gyakoriságát,
- b) a feltárt hiányosságok, jó gyakorlatok leírásának követelményét,
- c) a következtetések levonásának, a feltárt hiányosságok kijavításának követelményét.

Az ellenőrzések lebonyolítása során a vonatkozó nemzetközi gyakorlat és szabványok szerint kell eljárni (ISO 27000 szabvány család, Conducting Computer Security Assessments at Nuclear Facilities, IAEA, 2016). A kibervédelmi gyakorlatok tervezéséhez és szervezéséhez ajánlható az FV-21 sz., „A programozható rendszerek védelmi hatékonyságát növelő gyakorlatok tervezése, szervezése és az eredmények értékelése” című útmutató.

3.5.8. A rendszerek védelmével összefüggő változáskezelés, életciklus

A védelmi tervet a programozható rendszerek védelmi felelőse állítja össze, a felső vezetés hagyja jóvá és intézkedik annak végrehajtásáról. A védelmi tervet a programozható rendszerek védelmi felelőse a fizikai védelmi tervvel összhangban 5 évente felülvizsgálja, a szükséges változtatásokról javaslatot tesz a felső vezetésnek.

Események értékelése, a fenyegetettség jelentős változása esetén el kell végezni a védelmi terv rendkívüli felülvizsgálatát.

A programozható rendszerek felülvizsgálata vagy más ok következtében felmerülő átalakításokat előzetesen értékelni kell. A programozható rendszerek védelmi tervének tartalmaznia kell a programozható rendszerek átalakításának értékelésére vonatkozó követelményeket. A programozható rendszerek átalakítására vonatkozó követelményeknek értelemszerűen összhangban kell lenniük

- a) atomerőművek esetében az NBSZ 4.8.2. Az átalakítások belső szabályozása, általános követelmények c. fejezetében,

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

- b) kutatóreaktorok esetében az NBSZ 5.3. Kutatóreaktorok üzemeltetésének szabályzata, de különösen az 5.3.13. Átalakítások végrehajtása c. fejezetében,
- c) a nukleáris létesítmények kiégett üzemanyagának átmeneti tárolóira az NBSZ 6.3.9. Átalakítások c. fejezetében és
- d) a hulladéktárolókra a TBSZ 2.3.13. Az átalakítások belső szabályozása, általános követelmények c. fejezetében leírt általános elvekkel és követelményekkel.

A fokozatosság elvének érvényesítése érdekében az átalakítást a védelmi jelentősége alapján ajánlatos kategorizálni az engedélyes irányítási rendszerébe illeszkedő eljárás alkalmazásával. A kategóriába sorolás egy lehetséges módja a következő:

Szervezeti és irányítási rendszer átalakításánál:

Az A kategóriába kell sorolni azokat az átalakításokat, amelyek esetében az átalakítás

- a) a programozható rendszerek védelmi tervének módosításával jár;
- b) az átalakítás nem kezelhető maradéktalanul a programozható rendszerek védelmi tervében meghatározott működéssel.

A B kategóriába kell sorolni az A kategóriába nem sorolható átalakításokat.

Műszaki átalakításnál:

Az A kategóriába kell sorolni az átalakítást, amennyiben

- a) a programozható rendszerek védelmi tervének módosításával jár;
- b) az átalakítás nem kezelhető maradéktalanul a programozható rendszerek védelmi tervében meghatározott működéssel;
- c) 1. védelmi szintű programozható rendszert vagy annak védelmét érinti;
- d) 2-3. védelmi szintű programozható rendszert vagy annak védelmét érintő, olyan átalakítás, amely hatósági kompetenciába tartozó, NBSZ szerinti műszaki átalakítás része.

A B kategóriába kell sorolni az átalakítást, amennyiben:

- a) nem tartozik az A kategóriába;
- b) az átalakítás csak 4-es vagy 5-ös védelmi szintű programozható rendszereket érint.

A 4. vagy 5. védelmi szintbe tartozó programozható rendszerek vagy azok védelmét érintő műszaki átalakítások B kategóriába sorolását és engedélyezését az engedélyes saját hatáskörben végzi.

A felülvizsgálatokból és az átalakításokból származó változásokat a védelmi tervben követni kell. Az A átalakítási kategóriába sorolt szervezeti és irányítási

Nukleáris létesítmények programozható rendszereinek védelmi követelményei rendszert érintő, valamint műszaki átalakításokat a hatóságnak engedélyeznie kell. A programozható rendszerek védelmi tervének módosításával járó átalakítás esetén az átalakítás engedélyezési terjedelmének tartalmaznia kell a programozható rendszerek védelmi tervének módosított fejezeteit, szövegrészeit, bemutatva ezáltal a hatályos védelmi tervhez képest megvalósuló eltéréseket.

A programozható rendszerek védelmi tervét érintő, engedélyezett átalakítások miatti módosításokat legkésőbb a Fizikai Védelmi Terv felülvizsgálatakor vagy egyéb, külső, belső körülményből (pl. jogszabályváltozás, fenyegetettség jelentős változása) eredő rendkívüli felülvizsgálat alkalmával kell aktualizálni a Programozható Rendszerek Védelmi Tervében.

A programozható rendszerek átalakítására vonatkozóan az engedélyesnek belső eljárásrendet szükséges kialakítania.

3.5.9. Események kezelése

A programozható rendszerek védelmi tervének tartalmaznia kell az események kezelésére, azok osztályozására, megelőzésére, elhárítására vonatkozó szabályokat, az események elkerülése és a bekövetkező események által okozott károk csökkentésére.

A védelmi kontrollokkal ellátott programozható rendszerek viselkedését felügyelni kell a rendellenességek mielőbbi észlelése érdekében.

A védelmi tervben meglévő védelmi eseménykezelés magában foglalja az események összegyűjtését, megszüntetését, osztályozását (rendellenesség, figyelmeztetés, információ), válaszlépések megtételét és tárolását.

A rendellenességeket és figyelmeztetéseket tovább kell elemezni, és ha a védelmi eredmény egy védelmi incidens, akkor a védelmi incidenst kezelni kell.

A védelmi incidenskezelés folyamata magában foglalja az előkészítést, észlelést, elemzést, elszigetelést, felszámolást, helyreállítást és a lezárást. A folyamat célja a szervezett válaszlépések biztosítása a programozható rendszerek működésében fellépő rendellenességek minimalizálása érdekében.

3.5.9.1. A kivizsgálás rendje, kivizsgálást segítő intézkedések

A létesítmény programozható rendszereinek védelmi felelőse intézkedik az események kivizsgálási rendjének elkészítéséről.

Előkészítés:

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
Gyors és szervezett válaszlépések megtétele érdekében incidenskezelési eljárásokat kell kidolgozni. Az eljárásokat az incidenskezelési csoportnak kell végrehajtania meghatározott szerepek betöltésével. Az eljárásokat az egyes incidensek károkozó hatásainak súlyossága szerint kell kidolgozni, dokumentálni és jóváhagyni.

Észlelés:

A védelmi incidensek időben történő felismeréséhez elengedhetetlen az automatikus mechanizmusok alkalmazása. Ezek közül a legfontosabbak a behatolásérzékelő rendszerek (Intrusion Detection System - IDS, Host Intrusion Detection System - HIDS), csapdák (Honeypots, Honeynets) és naplózásokat központosító rendszerek (Security Incident Event Management - SIEM).

A rendszerekben számos jel utalhat rendellenességre, amelyeket figyelni kell. Ilyenek pl. megtelt naplófájl, antivírus vagy IDS-riasztás, kikapcsolt antivírus szoftver vagy egyéb kontrolleszköz, váratlan szoftverfrissítés, külső IP-címre történő csatlakozás, rendszerinformációk iránti érdeklődés, konfigurációs beállításokban váratlan változtatás, váratlan rendszerleállítás, szokatlanul nagy hálózati forgalom, szokatlanul nagy CPU-használat, stb.

Az incidenst észlelés után jelenteni kell. A jelentés módját és útját az incidenskezelési eljárásban dokumentálni kell.

3.5.9.2. Válasz intézkedési terv

Az eseménykezelés részeként a létesítmény programozható rendszereinek védelemi felelőse az egyes eseményosztályok súlyosságának megfelelő intézkedések kidolgozásáról gondoskodik.

Szükséges kialakítani a megfelelő intézkedések végrehajtásához az alábbi lépésekre vonatkozó szabályozásokat, tervezeteket:

Elemzés:

Az incidensek elemzésének feltétele, hogy elegendő információ álljon rendelkezésre. Ezért a naplózásokat és egyéb jelentéseket ennek megfelelően kell konfigurálni. Az elemzés eredménye többek között: az incidens típusa, a megtámadott rendszer védelmi jellemzői, időbeni lefutás, az incidens észlelésének körülményei, támadási vektor, a támadás komplexitása, antivírusadatbázis-minta, fizikai hozzáférés megállapítása, az adatsérülés módja, terjedelme és a károkozások megtörtént és lehetséges következményei.

Elszigetelés:

Nukleáris létesítmények programozható rendszereinek védelmi követelményei
Miután elég információ áll rendelkezésre, az incidenst el kell szigetelni, karanténba kell zárni (containment), hogy ne tudjon tovább terjedni. Az elszigetelés eljárását gondosan ki kell dolgozni, figyelve a következőkre:

- a) Az elszigetelés elrendelésének kritériumait világosan dokumentálni kell, hogy gyorsan lehessen dönteni az elrendeléséről.
- b) Az elszigetelés működésre gyakorolt hatását és következményeit fel kell mérni.
- c) Az elszigetelés módjának megválasztásánál mérlegelni kell az erőforrásokban okozható károkat, a bizonyítékok megőrzésének szükségességét, a rendelkezésre állást (pl. hálózati kapcsolat), a szükséges időt és erőforrásokat, az elszigetelés hatékonyságát (teljes, részleges) és az elszigetelés időtartamát.
- d) Figyelni is kell arra, hogy az elzárt károkozó további károkat okozhat az elzárt rendszerben.
- e) Az elszigetelés megvalósulhat manuális eljárást követve, automatikusan (pl. antivírusprogrammal), szolgáltatások kikapcsolásával vagy kapcsolatok megszakításával.

Felszámolás:

Elszigetelés után a károkozó kódot vagy egyéb káros erőforrást fel kell számolni, és meg kell győződni arról, hogy a károkozás és támadás veszélye tovább nem áll fenn.

Helyreállítás:

A kiaknázott sérülékenységek vizsgálatával meg kell állapítani a hiányosságokat és javításukról, illetve csökkentésükről gondoskodni kell olyan ütemezéssel, hogy a helyreállított rendszer védve legyen, ugyanakkor a helyreállítás minél előbb megtörténjen. A teljes helyreállításig az elszigetelt programozható rendszert részlegesen is helyre lehet állítani, ha az szigetüzemben tud működni és a károkozás felszámolásra került. Javítási intézkedéseknél többek között a következőkre kell gondolni:

- a) A meglévő védelmi intézkedések hiányosságainak pótlása.
- b) Ha olyan eset következett be, ami ellen eddig nem volt védelem, akkor új védelmi intézkedéseket kell bevezetni.
- c) Az eszköz módosítása és újabb eszközök telepítése a hasonló károkozások megakadályozása érdekében.
- d) Eljárások és adminisztratív védelmi intézkedések javítása és további ellenőrzőpontokkal történő kibővítése.

Nukleáris létesítmények programozható rendszereinek védelmi követelményei

e) Az üzemeltetési kézikönyvek és egyéb dokumentumok helyesbítése vagy a hiányosságok pótlása.

f) Személyzet képzése az eseménnyel kapcsolatos témában.

A programozható rendszerek helyreállításához helyreállítási eljárást kell készíteni. A programozható rendszerekről minden adatot menteni kell, ami a helyreállításhoz szükséges, és a helyreállítási eljárásban le kell írni az egyes rendszerekhez szükséges helyreállítási lépéseket. Meg kell győződni a mentett adatok rendelkezésre állásáról, sértetlenségéről és helyreállíthatóságáról, és a bizalmas adatokat ugyanolyan bizalmasan kell kezelni, mintha az üzemi rendszerben lennének.

Az adatokat olyan mentési stratégiával kell menteni, hogy a helyreállításhoz meghatározott helyreállítási időt (Recovery Time Objective - RTO) biztosítani lehessen. Az adatokat olyan gyakorisággal kell menteni, hogy a helyreállításhoz meghatározott adatvesztési szintet (Recovery Point Objective - RPO) biztosítani lehessen. Szükség esetén alternatív adattárolóhelyet kell kialakítani, ami az elsődlegestől megfelelő távolságban van.

A nem, vagy rendellenesen működő programozható rendszert a helyreállítási eljárásnak megfelelően kell helyreállítani a mentett adatok segítségével. A biztonságos és védett állapotba történő helyreállítás során legalább a következőket kell elvégezni:

- a) Az összes rendszerparamétert be kell állítani (alap- vagy meghatározott értékre).
- b) A biztonsági frissítéseket (patch) fel kell rakni és a biztonsági konfigurációkat helyre kell állítani.
- c) Az operációs rendszert és az alkalmazásokat fel kell installálni és megfelelően konfigurálni kell.
- d) A legújabb, rendelkezésre álló adatokat be kell tölteni, és a rendszer megfelelő működését le kell tesztelni.

A helyreállítás után az incidensről és kezeléséről jelentést kell készíteni és el kell küldeni az OAH részére.