Országos Atomenergia Hivatal

N3a.36. sz. útmutató

Új atomerőmű irányítástechnikai rendszerének tervezése

Verzió száma:

2.

2021. május

Kiadta:

---

az OAH főigazgatója

Budapest, 2021

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 radioaktívhulladék-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 üzemen kívül helyezést és a bezárást, radioaktívhulladék-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 fejti 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-e! Az érvényes útmutatókat az OAH honlapjáról (www.oah.hu) töltheti le.

ELŐSZÓ

Az atomenergia békés célú, biztonságos alkalmazására vonatkozó legmagasabb szintű szabályozást az atomenergiáról szóló 1996. évi CXVI. törvény (a továbbiakban: Atv.) tartalmazza.

A nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről szóló rendelkezéseket a 118/2011. (VII. 11.) Korm. rendelet (a továbbiakban: Rendelet) és mellékletei, a Nukleáris Biztonsági Szabályzatok (a továbbiakban: NBSZ) határozzák meg.

A nukleáris biztonsági követelmények és rendelkezések betartása mindazok számára kötelező, akik az Atv. 9. § (2) bekezdése szerinti folyamatos hatósági felügyelet alatt állnak, valamint e törvényben előírt hatósági engedélyhez kötött tevékenységet folytatnak, ilyen tevékenységben közreműködnek, vagy ilyen tevékenység folytatásához engedély iránti kérelmet nyújtanak be. A nukleáris biztonsági követelmények és rendelkezések mellett a követelmények közé tartoznak az egyedi hatósági előírások, feltételek és kötelezettségek, amelyeket az OAH a nukleáris létesítmény nukleáris biztonsága érdekében határozatban vagy végzésben állapíthat meg.

Az NBSZ-ben foglalt követelmények teljesítésére az OAH ajánlásokat fogalmazhat meg, amelyeket útmutatók formájában ad ki. Az útmutatókat az OAH a honlapján közzéteszi. Jelen útmutató az engedélyesek önkéntes alávetésével érvényesül, nem tartalmaz általánosan kötelező érvényű normákat. Az útmutató nem tekinthető hivatalos jogértelmezésnek. A jogértelmezés a jogalkalmazó mindenkori feladata és felelőssége, ezért a jelen útmutatóban leírtak kizárólag szakmai álláspontnak tekinthetők, nem használhatók fel jogértelmezésként peres vagy közigazgatási eljárás során.

A Rendelet 3. § (4) bekezdése alapján, ha a kérelmező a nukleáris biztonsággal összefüggő engedély iránti kérelmét az útmutatókban foglaltak szerint terjeszti elő, továbbá, ha az engedélyes a nukleáris biztonsággal összefüggő tevékenységét az útmutatókban foglaltak szerint végzi, akkor az OAH a választott módszert a nukleáris biztonság követelményei teljesítésének igazolására alkalmasnak tekinti, és az alkalmazott módszer megfelelőségét nem vizsgálja.

Az útmutatókban foglaltaktól eltérő módszerek alkalmazása esetén az OAH az alkalmazott módszer helyességét, megfelelőségét és teljeskörűségét részleteiben vizsgálja, ami hosszabb ügyintézési idővel, külső szakértő igénybevételével és további költségekkel járhat.

Ha az engedélyes által választott módszer eltér az útmutató által ajánlottól, akkor az eltérés indokolása mellett igazolni kell, hogy a választott módszer legalább ugyanazt a biztonsági szintet biztosítja, mint az útmutatóban ajánlott.

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

1.1. Az útmutató tárgya és célja

Az útmutató ajánlásokat tartalmaz az NBSZ 3a.4.5. fejezetében rögzített, a biztonsági irányítástechnikai rendszerekre és rendszerelemekre vonatkozó tervezési követelmények teljesítésének módjára, valamint irányítástechnikai szempontú útmutatást fogalmaz meg a 3a. kötet egyéb releváns követelményeinek teljesítésével kapcsolatban is.

Az útmutató célja, hogy – ajánlásokat adva az atomerőmű irányítástechnikai rendszereinek és rendszerelemeinek tervezési követelményeivel kapcsolatosan – egyértelművé tegye a hatósági elvárásokat, és ezzel elősegítse az érvényes előírásokban meghatározott nukleáris biztonsági kritériumok teljesülését.

1.2. Vonatkozó jogszabályok és előírások

A nukleáris biztonsági követelmények jogszabályi hátterét az Atv. és a Rendelet biztosítja.

2. MEGHATÁROZÁSOK ÉS RÖVIDÍTÉSEK

2.1. Meghatározások

Az útmutató az Atv. 2. §-ában, valamint a Rendelet 10. számú mellékletében ismertetett meghatározásokon kívül az alábbi definíciókat tartalmazza.

Akkreditált szervezet:

Olyan szervezet, amely a megfelelésértékelés végrehajtására tanúsító, ellenőrző, vizsgáló szervezeti felépítést és eljárásokat implementál valamely szakmai területen és rendelkezik a Nemzetközi Akkreditálási Együttműködés (ILAC) vagy az Európai Akkreditálási Együttműködés (EA) valamely tagjának ezen tevékenységre vonatkozó, érvényes akkreditációjával.

„Az akkreditálás annak hivatalos elismerése, hogy egy szervezet, természetes személy alkalmas bizonyos tevékenységek (vizsgálat, kalibrálás, mintavétel, tanúsítás, ellenőrzés stb.) elvégzésére. Az akkreditálás célja az egységes európai elvekre épülő akkreditálási rendszerekben elismerést nyert szervezetek iránti bizalom növelése, a vizsgálati, tanúsítási és ellenőrzési tevékenység megbízhatóságának emelése, a vizsgálati eredmények és tanúsítványok kölcsönös elfogadásának elősegítése, megteremtve ezáltal az ismételt vizsgálatok kiküszöbölését és a kereskedelem műszaki akadályainak elhárítását.” (Forrás: www.nat.hu)

Egyszeres hibatűrés elve:

Amikor egy funkciót redundáns rendszerek, vagy egy rendszeren belül is redundáns rendszerelemek teljesítenek, valamelyik redundáns rendszerben, vagy – a rendszer belső redundanciája esetén – egy rendszerelemében bekövetkező egyszeres meghibásodáskor a funkció még teljesíthető. Az egyetlen hiba eredményeként fellépő további hibák az egyedi hiba részeként kezelendők.

Függetlenség:

A rendszerek, rendszerelemek olyan állapota, jellemzője, amelynek teljesülése esetén az egyes rendszerek, rendszerelemek nincsenek hatással egymásra, azaz valamely rendszer, rendszerelem működése vagy meghibásodása nem képes befolyásolni valamely más rendszer, rendszerelem állapotát, jellemzőjét.

Független szervezet:

A függetlenséget (pártatlanságot) a tanúsító és ellenőrző szervezeteknél meghatározott követelmények alapján definiáljuk; ugyanakkor a függetlenség az alábbiak alapján értelmezhető olyan szervezetekre is, amelyek nem tanúsítói, hanem egyéb szakértői tevékenységet végeznek.

Független az a szervezet, amely teljesíti az MSZ EN ISO/IEC 17065 szabvány („Megfelelőségértékelés. Termékek, folyamatok és szolgáltatások tanúsítását végző szervezetekre vonatkozó követelmények") szerinti pártatlan szervezetre vonatkozó követelményeket; elsődlegesen (idézet a szabvány 4.2, a pártatlanság kezelése című alfejezetéből):

"A tanúsító szervezet és a szervezeti irányítása alatt álló ugyanazon jogi személynek vagy személyeknek egyetlen része sem:

a) lehet a tanúsított termék tervezője, gyártója, üzembe helyezője, forgalmazója vagy karbantartója;

b) lehet a tanúsított folyamat tervezője, megvalósítója, működtetője vagy fenntartója;

c) lehet a tanúsított szolgáltatás tervezője, végrehajtója, szolgáltatója vagy fenntartója;

d) ajánlhat vagy nyújthat tanácsadást (lásd a 3.2. szakaszt) ügyfelei részére;

e) ajánlhat vagy nyújthat az irányítási rendszerrel kapcsolatos tanácsadást vagy belső auditálást ügyfelei részére olyan esetben, ahol a tanúsítási rendszer megköveteli az ügyfél irányítási rendszerének értékelését."

Független szakértő:

Független szervezetre megadott meghatározás értelemszerű alkalmazásával definiált függetlenséget teljesítő szakértő. Az atomenergia alkalmazása körében eljáró független műszaki szakértő esetén figyelembe kell venni az Atv. 19/A. § (1) és (2) pontja, valamint az atomenergia alkalmazása körében eljáró független műszaki szakértőről szóló 247/2011. (XI. 25.) Korm. rendelet előírásait is.

Megbízhatóság (működőképesség):

A rendszer vagy rendszerelem azon tulajdonsága, hogy a tervezett funkcióját (és kizárólag azt) a figyelembe vett üzemeltetési körülmények között megfelelő időn keresztül vagy megfelelő valószínűséggel képes ellátni.

Megengedett elektromágneses zavartatási környezet:

Olyan specifikáció, amely leírja, hogy a tér egy bizonyos pontjában mekkora sugárzott elektromágneses jel lehet jelen (frekvencia függvénye is).

Az adott ponton telepített berendezéseknek igazoltan tűrniük kell a környezetben specifikált zavarok mértékeit (és számukra érdektelen azok forrása, forrásai). Visszafelé: nem telepíthető olyan elektromágneses sugárforrás, amely hatására a korábban specifikált környezeten a tényleges zavarértékek a specifikált zavarok szintje fölé emelkednének.

Rendelkezésre állás:

Annak mértéke, illetve valószínűsége, hogy egy adott rendszer vagy rendszerelem a tervezett funkcióját a figyelembe vett üzemeltetési körülmények között egy kiválasztott időpontban megfelelően képes ellátni. Amennyiben a rendszerben javítást nem alkalmazunk, akkor a rendelkezésre állás megegyezik a megbízhatósággal.

Tanúsító szervezet:

Olyan szervezet, amely az MSZ EN ISO/IEC 17065 szabvány („Megfelelőségértékelés. Termékek, folyamatok és szolgáltatások tanúsítását végző szervezetekre vonatkozó követelmények”) szerinti, terméktanúsítási tevékenységekre alkalmas, az ehhez szükséges tulajdonságokkal/képességekkel (szervezeti struktúra, eljárások, személyzet stb.) rendelkezik. A tanúsítási tevékenységnek a jelen dokumentumban megfogalmazott tanúsítási feladatokra (pl. nukleáris rendszerekben alkalmazható számítástechnikai és irányítástechnikai eszközök megfelelésértékelése) kell irányulnia, és amennyiben az adott területen léteznek nemzetközi szakmai szabványok, azokon kell alapulnia.

A tanúsító szervezetnek vagy magának kell megvalósítania ellenőrző (MSZ EN ISO/IEC 17020 szerint – „Megfelelőségértékelés. Ellenőrzést végző különféle típusú szervezetek működésének követelményei”) és/vagy vizsgálólaboratóriumi (MSZ EN ISO/IEC 17025 szerint – „Vizsgáló- és kalibráló-laboratóriumok felkészültségének általános követelményei”) funkciókat (természetesen a tanúsítás szakmai területével azonos szakmai területen), vagy olyan szervezetet (szervezeteket) kell a feladatmegoldásba bevonnia, amelyik ezen szabványok szerinti ellenőrző és/vagy vizsgáló tulajdonságokkal/képességekkel rendelkezik.

A tanúsító (ellenőrző, vizsgáló) szervezet kérheti akkreditációját, vagyis annak külső, független igazolását, hogy működése megfelel a vonatkozó elveknek és szabályoknak (lásd *Akkreditált szervezet*).

Validáció:

176. Validálás

Annak ellenőrző vizsgálata, hogy a rendszer, rendszerelem, szolgáltatás, módszer, számítási eszköz, számítógépprogram megfelel-e a funkcionális, a teljesítmény- és interfész-követelményeknek az előre meghatározott és írásban rögzített feltételek mellett.

Verifikáció:

184. Verifikálás

Ellenőrző folyamat, mely során megvizsgálják, hogy a rendszer, rendszerelem szolgáltatás, módszer, számítási eszköz, számítógépprogram, fejlesztési, gyártási folyamat minden egyes fázisának terméke kielégíti-e az előző fázis által meghatározott összes követelményt.

2.2. Rövidítések

ABOS	Atomerőművi rendszerek és rendszerelemek biztonsági osztályba sorolása. Az atomerőmű rendszereit és rendszerelemeit biztonsági hatásuk, legmagasabb biztonsági szintbe sorolt funkcióik alapján az NBSZ 3a.2.2.1200.-3a.2.2.2300. pontjainak megfelelően biztonsági osztályokba és nem biztonsági osztályba kell sorolni.
F1A, F1B, F2	A biztonsági funkciók szintjei (biztonsági szintek). A biztonsági funkciók biztonsági szintekbe kell sorolni az NBSZ 3a.2.2.0700. pontja szerint.
FAT	Factory Acceptance Test, gyártóművi végellenőrzési tesztelés
HSI	Human System Interface, ember-gép kapcsolati felület
RAMS	Reliability, Availability, Maintainability and Safety: megbízhatóság, rendelkezésre állás, karbantarthatóság és biztonság
SAT	Site Acceptance Test, üzembe helyezési tesztelés
TA1-TA4	Az atomerőmű tervezési alapjának részeként figyelembe vett üzemállapotok
TAK1, TAK2	Az atomerőmű tervezési alapjának kiterjesztései
V&V	Verifikációs és validációs tevékenységek

3. KAPCSOLAT AZ NBSZ EGYÉB KÖTETEIVEL ÉS ÚTMUTATÓIVAL

Az új atomerőmű irányítástechnikai rendszerének tervezése során az NBSZ 3a. kötetén kívül a következő NBSZ-kötetekben találhatók figyelembe veendő előírások:

a) 1. kötet: Nukleáris létesítmények nukleáris biztonsági hatósági eljárásai. Az irányítástechnikai rendszert úgy kell tervezni, kivitelezni, dokumentálni stb., hogy az engedélyezési eljárások lefolytathatók legyenek.

b) 2. kötet: Nukleáris létesítmények irányítási rendszerei. Az irányítástechnikai rendszer egyes aspektusait, paramétereit úgy kell meghatározni, hogy illeszthető legyen a teljes létesítmény irányítási rendszeréhez, vagy az irányítási rendszerben a szükséges adaptációk elvégezhetők legyenek (pl. humán szakmai követelmények, stb.).

c) 4. kötet: Atomerőművek üzemeltetése. A kötet előírásait az irányítástechnikai rendszer üzembe helyezése és üzemeltetése során be kell tartani; illetve ezen életciklusfázisokon keresztül már a tervezésnél figyelembe kell venni.

d) 8. kötet: Nukleáris létesítmények megszüntetése. Az irányítástechnikai rendszereket úgy kell tervezni, hogy a leszerelésük szabályosan elvégezhető legyen. A leszerelésnél alkalmazandó speciális szabályokat már a tervezés során meg kell adni.

e) 9. kötet: Új nukleáris létesítmény tervezési és létesítési időszakára vonatkozó követelmények.

Jelen útmutató a meglévő atomerőműveknél használt, 3.5 sz. *„Atomerőmű irányítástechnikai rendszereinek és rendszerelemeinek tervezési követelményei”* című NBSZ-útmutatót helyettesíti az irányítástechnikai rendszerek vonatkozásában új atomerőmű tervezése esetén. Jelen útmutató a megújult NBSZ tartalmához, annak 3a. kötete 3a.4.5. fejezetében felsorolt új követelményekhez igazodva készült, amelyek nagyon kevés átfedést mutatnak a korábbi NBSZ kapcsolódó pontjaival és a hozzájuk tartozó útmutatással. Látható, hogy az idők során a hangsúly az irányítástechnika területén a programozható rendszerekre tevődött át, és ma már az NBSZ-követelmények, és ennek megfelelően jelen útmutató is a korábbinál nagyobb arányban koncentrál azokra a módszerekre és megoldásokra, amelyek a programozható rendszerek és az azokban futó szoftver tervezésével és biztonságigazolási folyamatával kapcsolatosak.

Jelen útmutató kapcsolódik a következő NBSZ-útmutatókhoz:

a) Az NBSZ 3a.2. fejezetéhez (N3a.12. *„Általános tervezési elvek atomerőművek és rendszereinek tervezéséhez”*) készült útmutató. Ez az útmutató az erőmű alapvető tervezési elveit, a tervezési alapra vonatkozó követelményeket magyarázza. Bár az ebbe a fejezetbe tartozó követelmények elsősorban a technológiai tervezésnek szólnak, az irányítástechnikának is figyelembe kell vennie őket, hiszen az irányítástechnika tervezési alapját az erőmű tervezési alapjából kell származtatni, és az annak való megfelelést az irányítástechnika szintjén is demonstrálni kell.

b) N3a.37. *„Új atomerőmű blokk- és tartalékvezénylőjének tervezése”* című útmutató. Az irányítástechnikai rendszerek egyik kapcsolódási felületét jelentik az ember-gép kapcsolati felületek (HSI), amelyek közül számos, az erőmű biztonságos üzemeltetéséhez alapvetően szükséges megjelenítő és operátori beavatkozást lehetővé tevő felület a blokk- és tartalékvezénylőkben kerül elhelyezésre. A két útmutató tehát egymáshoz szorosan kapcsolódó rendszerekre vonatkozik, amelyek megfelelő együttműködését a tervezésnek biztosítania kell.

A fenti kötetekkel és útmutatókkal való kapcsolat feltárása mellett az alábbi, 3a. kötetben található, de nem a 3a.4.5. fejezetbe tartozó NBSZ-követelmények esetében indokolt az irányítástechnikai szempontú útmutatás megfogalmazása. Ezen NBSZ-követelménypontokhoz az adott fejezetekhez tartozó specifikus útmutatókban is található útmutatás, jelen útmutató a kapcsolódásokra kívánja felhívni a figyelmet és hangsúlyozza az irányítástechnikai specifikumokat.

a) NBSZ 3a.2. fejezete, 3a.2.2.8500. pont. A meghibásodások figyelembevételét előíró általános követelmény, amelynek számos irányítástechnikai specifikuma van.

b) NBSZ 3a.3. fejezete, 3a.3.1.1100., 3a.3.1.1600., 3a.3.1.1700., 3a.3.2.0400., 3a.3.6.2800. és 3a.3.9.0200. pontok. A biztonsági funkciót ellátó rendszerekre és rendszerelemekre vonatkozó, megbízhatósággal és karbantarthatósággal kapcsolatos követelmények, amelyeket az irányítástechnikai tervezés során, annak teljes vertikumában szem előtt kell tartani.

c) NBSZ 3a.4. fejezete, 3a.4.4.0400. pont. Ez az NBSZ-fejezet a blokk- és tartalékvezénylők tervezésének követelményeit sorolja fel, amelyeket az irányítástechnika és a HSI szoros kapcsolata miatt az irányítástechnikai tervezés során is ajánlott figyelembe venni.

4. AZ ÚTMUTATÓ AJÁNLÁSAI

4.1. Általános ajánlások

4.1.1. Életciklusalapú megközelítés

Az irányítástechnikai rendszer, alrendszerei és rendszerkomponensei tervezését és megvalósítását szigorú életciklus-szemlélettel kell megvalósítani. Az életciklus a rendszer, alrendszer, rendszerkomponens koncepciója kidolgozásának indulásától a teljes fejlesztésen és integráción keresztül, az üzemeltetés és karbantartás fázisán keresztül a rendszer, alrendszer és rendszerelem leszereléséig tart. Külön figyelmet kell fordítani az életciklus módosításokat magába foglaló fázisaira. Ezeket konfigurációmenedzsmenten keresztül úgy kell megvalósítani, hogy az életciklus érintett részére csatol vissza a folyamat, és az életciklus-tevékenységek módosítási igény szerinti elvégzésével kell a módosítási igényre reflektáló változtatásokat kifejleszteni.

Külön hangsúlyozni kell, hogy az irányítástechnikai rendszerek életciklusában több szereplő vesz részt. Egyik ilyen felosztás a tervező/kivitelező és az üzemeltető szerint lehetséges. Igen fontos biztonsági és üzemeltethetőségi kritérium, hogy a rendszerre, alrendszerre vagy rendszerelemre vonatkozó releváns információk áramlása ezen két szereplő között biztosítva legyen: az üzemeltető legyen tisztában a rendszer biztonságos üzemeltetéséhez szükséges összes előírással, utasítással, szabállyal; míg a tervező kapjon visszajelzést a rendszer üzemeltetési tapasztalatairól, és ezáltal ellenőrizni tudja a biztonsági és egyéb teljesítménymutatók teljesülését és döntéseket hozhasson (javaslatokat tehessen) az esetlegesen szükséges módosításokra.

A folyamatalapú fejlesztésnek ma már nagy hagyományai vannak az elektromos, elektronikus és programozott elektronikus rendszerekre vonatkozóan, ezen fejlesztési elvek alkalmazása szükséges. A fő elvek az alábbiak:

a) A rendszer fejlesztésének életciklusfázisokra bontása. A fázisok felosztható lépésekre, amelyek még tovább bonthatók feladatokra. Minden tevékenységhez meghatározandó, hogy mely bemeneti információk jóváhagyott rendelkezésre állása mellett indulhat, mi a tevékenység célja (milyen kimeneti információkat kell előállítani), milyen módszerek alkalmazása szükséges a megfelelő minőségű kimeneti információ előállításához, milyen kritériumok vonatkoznak a tevékenység résztvevőire (végzettség, gyakorlat stb.). Egy tevékenység akkora terjedelmet fogjon át, hogy a bemeneti információk alapján az elvárt

kimeneti eredmény egy lépésben, sorosan alkalmazandó módszerek nélkül, sorosan alkalmazandó több szereplő nélkül előálljon.

b) A fejlesztés többszintű, az adott tevékenységtől független ellenőrzése: az egyes feladatok és lépések eredményeinek felülvizsgálata (verifikáció), valamint az életciklusfázisok és a teljes fejlesztés eredeti követelményrendszernek való megfelelésvizsgálata (validáció).

c) Az életciklusban áramló információk rögzítése, dokumentálása.

d) A személyi függetlenségek, részvételi redundanciák (vö. b) pont) biztosítása.

e) A résztvevők alkalmasságának biztosítása.

Fontos kiemelnünk, hogy az irányítástechnikai rendszer nem öncélú: feladata az erőmű biztonságos és hatékony üzemeltetésének biztosítása. Így feladatait az erőmű tervezése során kell meghatározni az erőművet tervező technológusoknak. Az irányítástechnikai rendszer technológia funkció specifikációja így tartalmazza azokat a funkciókat, amelyeket az erőművi technológusok allokálnak az irányítástechnikai rendszerre, de tartalmazza azokat a műszaki követelményeket is, amelyek magas szintről származnak (mérések megkövetelt helyei, szükséges zavartatás tűrések, fizikai korlátok stb.) és tartalmazza az irányítástechnikai rendszer RAMS (Reliability, Availability, Maintainability and Safety) követelményeit is.

Az irányítástechnikai alapkövetelmény-rendszer bővülhet (de az alapkövetelmény-rendszer egyedi követelményei nem változhatnak meg) az egyéb alrendszerektől (pl. HSI) átadott további követelményekkel. Ehhez hasonlóan, az irányítástechnika tervezése során előállhatnak olyan, más alrendszerekre vonatkozó követelmények (pl. operátori megjelenítések a HSI-n az irányítástechnika állapotára vonatkozóan), amelyeket a más alrendszereknek kezelniük kell. A tervezési folyamatot úgy kell összeállítani, hogy ezeket az egymásra hatásokat biztonságosan kezelni tudja (iterációs tervezés).

4.1.2. A szabványok alkalmazása

A biztonsági funkciót ellátó irányítástechnikai rendszerek és berendezések tervezése során az NBSZ 9.3.7. fejezetéhez készített útmutató (N9.3. *„A szabványok használatának szabályai”*) ajánlásait figyelembe véve célszerű kialakítani a szabványok használatának rendszerét.

A biztonsági funkciót ellátó irányítástechnikai rendszerek és berendezések tervezése során a Nemzetközi Atomenergia Ügynökség és az Európai Unió ajánlásait figyelembe kell venni. A fontosabb ajánlások a következők:

1. **IAEA SSR-2/1**: Atomerőművek biztonsága: tervezésspecifikus biztonsági követelmények. (Safety of Nuclear Power Plants: Design Specific Safety Requirements, Series No. SSR-2/1 (Rev. 1), 2016.)
2. **IAEA SSG-39:** Atomerőművek irányítástechnikai rendszereinek tervezése (Design of Instrumentation and Control Systems for Nuclear Power Plants: Specific Safety Guides, Series No. 39, 2016)
3. **WENRA RHWG Report: Safety of new NPP designs** – Study by Reactor Harmonization Working Group RHWG, March 2013. Új atomerőművek tervezésének biztonsági kérdéseit összefoglaló tanulmány.
4. **WENRA RHWG Reactor Safety Reference Levels**, January 2008. A WENRA biztonsági vonatkoztatási szintjei.
5. **WENRA RHWG Report: Updating WENRA Reference Levels for existing reactors in the light of TEPCO Fukushima Dai-ichi accident lessons learned**, November 2013. A biztonsági vonatkoztatási szintek frissítése a fukusimai baleset tapasztalatai alapján.
6. **WENRA RHWG Report: Safety Reference Levels for Existing Reactors UPDATE IN RELATION TO LESSONS LEARNED FROM TEPCO FUKUSHIMA DAI-ICHI ACCIDENT**, 24th September 2014 A biztonsági vonatkoztatási szintek frissítése a fukusimai baleset tapasztalatai alapján.
7. **European Commission EUR 19265 EN:2000 v11**: Common position of European nuclear regulators for licensing of safety critical software for nuclear reactors. - Az európai nukleáris szabályozó testületek közös álláspontja nukleáris reaktorok biztonságkritikus szoftvereinek engedélyezésével kapcsolatban.

4.2. Tematikus v. specifikus ajánlások

3a.2.2.8500. „A tervezésnél figyelembe kell venni a rendszerelemek meghibásodási módjait, azok lehetséges szándékolatlan működéseit, valamint következményeit.”

Az irányítástechnikai rendszer funkcióinak biztonsági szintjétől függően a funkciókat ellátó rendszerelemeket és rendszereket biztonsági osztályokba és környezetállósági osztályokba kell sorolni. Az egyes biztonsági szintekhez illetve biztonsági osztályokhoz specifikus NBSZ-követelmények tartoznak a meghibásodások figyelembevételével és kezelésével kapcsolatban. Alapvető követelmények az egyszeres hibatűrés elve (lásd NBSZ 3. kötet 3a.3.1.1100. pont), illetve a közös okú hibák elkerülésének elve (lásd NBSZ 3. kötet

3a.3.1.1000. pont). Lásd továbbá NBSZ 3. kötet 3a.4.5.2100. pont, 3a.4.5.4400. pont, és 3a.4.5.4700. pont, valamint a hozzájuk tartozó útmutatás.

3a.3.1.1100. „A tervezésnél alkalmazni kell az egyszeres hibatűrés követelményét. A rendszerelemek szándékolatlan működésének lehetőségét egy lehetséges meghibásodási módként kell kezelni. Passzív tervezési megoldás meghibásodását figyelembe kell venni, hacsak nem igazolható, hogy az nagyon kis valószínűségű, vagy nem befolyásolja az adott funkciót."

Az irányítástechnikai rendszer technológiaifunkció-specifikációjának készítése során az egyszeres hibatűrés követelményének alkalmazásakor a funkcióellátással és a rendszer-üzemállapotokkal kapcsolatos elvárások további definiálása szükséges.

Az egyszeres hibatűrés követelményének betartása az irányítástechnikai rendszer architektúrájának tervezése során a megfelelő mértékű redundancia beépítésével lehetséges. Az egyszeres hibatűrés elérésére alkalmazott tervezési megoldások hatásosságát determinisztikus és valószínűségi elemzésekkel (pl. hibafaelemzéssel) kell igazolni (vö. NBSZ 3a.4.5.4400.).

3a.3.1.1600. „Az atomreaktor automatikus leállítását és az aktív biztonsági funkciót ellátó rendszerek vezérlését végző rendszer megfelelő tervezésével biztosítani kell, hogy az üzemviteli személyzet a kiépített operatív irányítási helyekről ne tudja megakadályozni az automatikus biztonsági működéseket sem TA1 üzemállapot, sem TA2-4 üzemállapotot eredményező események esetén, ugyanakkor a szükséges beavatkozásokat végre tudja hajtani."

Az operátori beavatkozás lehetőségének tiltását aktív védelmi funkció esetén szelektíven, csak az adott védelmi funkcióra vonatkozóan szabad megvalósítani.

Már az irányítástechnikai rendszer funkcionális specifikálása során be kell mutatni, hogy az elindult biztonsági funkciók (aktív biztonsági funkciók) nem szakíthatók meg.

Emellett már az irányítástechnikai rendszer funkcionális specifikálása során biztosítani kell, hogy az aktív védelmi funkciók ne lehetetleníthessék el más, esetlegesen szükséges beavatkozás kézi indítását, kivéve azokat az eseteket, amelyekben a technológiai célok elérése érdekében szükséges egy aktív funkció mellett bizonyos más védelmi funkciók letiltása. Ez utóbbi esetekben viszont tételes elemzéssel kell igazolni a tiltás szükségességét.

Az adott követelmény specifikációban való érvényre jutását szimulációval ellenőrizni/igazolni kell. Az irányítástechnikai rendszer fejlesztése és megvalósítása a specifikációnak megfelelően történik, valamint végső validációjának a specifikáción kell alapulnia, így a végső rendszer e követelménypontnak is meg fog felelni.

3a.3.1.1700. „A biztonsági funkciót ellátó programozott rendszereknek - a programozott rendszerekre vonatkozó általános követelményeken túlmenően - teljesíteniük kell a következő követelményeket:

a) a legszigorúbb minőségbiztosítási követelményeket kielégítő referenciákkal rendelkező hardver és szoftver eszközöket kell használni,

b) a teljes fejlesztési folyamatot, beleértve a tervezési változtatások ellenőrzését, tesztelését és üzembe helyezését szisztematikusan dokumentálni és értékelni kell,

c) a számítógépes alapú rendszerek megbízhatóságának igazolása érdekében a számítógépes alapú rendszereket olyan szakértőkkel kell felülvizsgáltatni, akik függetlenek a tervezőtől és a szállítótól, továbbá

d) amennyiben egy rendszer szükséges megbízhatósági szintje nem igazolható, akkor a hozzárendelt védelmi funkciók teljesítését diverz eszközökkel is biztosítani kell.”

Hardvereszköz alatt az önálló azonosítóval, önálló specifikációval rendelkező, egyedileg cserélhető egységet értjük. Szoftvereszköz alatt az önálló azonosítóval, önálló specifikációval rendelkező, egyedileg cserélhető szoftverkomponenst értjük.

A biztonsági funkciókat ellátó programozott rendszerekben alkalmazott hardver- és szoftvereszközöknek az MSZ EN ISO 9001 szabvány szerinti minőségirányítási rendszerben kell készülniük. A minőségirányítási rendszernek le kell fednie a hardvereszközök vonatkozásában a teljes tervezés és gyártás folyamatát; szoftvereszközök vonatkozásában a szoftvertervezés és -létrehozás fázisait. Amennyiben az eszközök részegységei más gyártótól származnak (beszállító), a beszállító minőségirányítási rendszerének értékelését és illesztését az eszköz gyártójának el kell végeznie.

A minőségirányítás meglétét az adott hardver-/szoftverelemek vonatkozásában egyrészt az alkalmazott minőségirányítási rendszer tanúsítványával, másrészt az adott hardver-/szoftverelemre vonatkozó minőségmenedzsment-jelentéssel kell igazolni. Ez utóbbi jelentés részletesen bemutatja, hogy miként alkalmazták ténylegesen a

minőségirányítási rendszer előíráshalmazát az adott termék vonatkozásában (a) pont).

A tervezési és gyártási folyamat irányíthatósága az alkalmazott módszerek, gyártási technikák és V&V módszerek egyszerűségét és átláthatóságát követelik meg. Ennek biztosítása érdekében célszerű előnyben részesíteni a tipizált és strukturált megoldásokat. Előnyös, ha olyan eszközöket és módszereket alkalmaznak, amelyek támogatják a verifikációt és a követelmény nyomonkövethetőségét mind a hardver, mind a szoftver tervezése és gyártása során.

A fejlesztés során olyan biztonsági életciklustervet (IEC 61513 szerint) kell összeállítani, amely az alábbi kulcselemek segítségével képes a fejlesztés során a szisztematikus és megfelelő szakmai, biztonsági szintű dokumentáció elkészültét biztosítani.

a) A fejlesztés életciklusszakaszokra bontása;

b) Az egyes életciklusfázisok dokumentáltságának előre történő specifikálása és a specifikáció szerinti megvalósítása;

c) A fejlesztésben részt vevők kompetenciájának megkövetelése (végzettség és szakmai tapasztalat);

d) A szakmák aktuálisan kifejlesztett és elfogadott módszereinek és az ismert legjobb gyakorlat alkalmazása;

e) A fejlesztés során személyi redundanciák (verifikáció és validációk, majd biztonságértékelés) alkalmazása;

A biztonsági életciklusterv hatásosságát meggyőzően igazolni kell (b) pont).

A független szakértő felülvizsgálja az adott rendszer fejlesztési folyamatát, a folyamatban végrehajtott tevékenységeket, az alkalmazott tervezési, megvalósítási elveket, a verifikáció és validáció (ideértve a teszteket) terjedelmét és elvégzésének tényét, valamint eredményeit, az alkalmazott minőségmenedzsment- és biztonságmenedzsment-elvek érvényre jutását.

A független szakértőnek meg kell állapítania, hogy a rendszer alkalmas-e az elfogadott, alap funkcionális, műszaki és biztonsági specifikációja teljesítésére. A szakértő sikeres működésének feltétele, hogy a biztonsági funkciókat ellátó rendszer rendelkezzen elfogadott irányítástechnikai rendszer technológiai funkció specifikációval (vö. NBSZ 3a.4.5.3200 pont).

Akkor kell diverz megoldásokat használni, ha a figyelembe veendő közös okú hibák fellépését feltételezve a rendszer szükséges megbízhatósága nem bizonyítható. Közös okú hibaként kell tekinteni szoftveralapú rendszerek

esetén a külső, rosszindulatú támadás miatti, az összes alkalmazott szoftvert egy időben érintő funkcióvesztést vagy téves funkcióvégrehajtást. A rendszer megbízhatósági szintjét diverz megoldás alkalmazásával ismételten demonstrálni kell.

3a.3.2.0400. „Amennyiben a rendszer, rendszerelem élettartama rövidebb, mint az atomerőmű tervezett élettartama, ezek felújíthatóságát, cserélhetőségét biztosítani kell."

A fenti előírás általánosságban vonatkozik az irányítástechnikai rendszerekre, hiszen az irányítástechnikában felhasznált rendszerek és rendszerelemek élettartama tipikusan a töredéke az erőmű tervezett élettartamának. Épp ezért a fenti követelményt specifikusan az irányítástechnikai rendszerekre megismétli az NBSZ, lásd a 3a. kötet 3a.4.5.1900. pontját, és az ahhoz adott útmutatást.

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."

A vonatkozó szabványok alkalmazásával meg kell határozni az irányítástechnikai rendszerek megengedett elektromágneses zavartatási környezetét: meg kell adni, hogy a telepítés helyén a frekvencia (és szükség szerint egyéb paraméterek) függvényében mekkora térerősség engedhető meg a berendezések biztonságos működtetéséhez. Ezt a környezetet a teljes rendszer további tervezői számára nyilvánossá kell tenni; a teljes atomerőművi rendszerben telepítendő sugárzó alrendszerek esetében pedig vizsgálni kell, hogy az irányítástechnikai rendszerek helyén azok összességében milyen térerősséget hoznak létre.

Amennyiben az irányítástechnikai rendszer tervezése során már ismert telepítésre kerülő vagy már létező sugárforrás, a megengedett elektromágneses zavartatási környezetet úgy kell megalkotni, hogy a tervezett vagy létező sugárforrás figyelembevételével biztosított legyen az irányítástechnikai rendszerek biztonságos üzemeltethetősége.

Az irányítástechnikai rendszer zavartatási környezetén definiált megengedhető zavarok melletti biztonságos működését szabványos vizsgálatokkal kell igazolni.

3a.3.9.0200. „A rendszerek, rendszerelemek ember-gép kapcsolatát és ergonómiai kialakítását olyan módon kell megtervezni, hogy - a feltételezett fizikai környezet és a várható pszichikai állapot figyelembevételével - a megfelelően

képzett személyzet szükség esetén az elvárt időtartam alatt legyen képes feladatait sikeresen elvégezni.”

Az irányítástechnikai rendszerekhez tartozó, kimondottan a rendszerre vonatkozó (és nem technológiai) operátori kijelzések és operátori beavatkozások (HSI) tervezésénél lehetőség szerint törekedni kell arra, hogy az erőművi operátorok csak a számukra, az erőmű aktuális állapotában szükséges irányítástechnikai rendszerinformációkat lássák; gyűjtött állapot (státusz) jelzések alkalmazása javasolt.

Ugyanakkor biztosítani kell, hogy az irányítástechnikai rendszer állapotát a rendszer fenntartására szakosított szakszemélyzet részletesen, a szükséges javítások haladéktalan elvégzéséhez szükséges mélységben megismerhesse; az irányítástechnikai rendszer hibamentes állapotában a rendszer paraméterei (pl. teljesítőképesség, belső hőmérséklet stb.) álljanak rendelkezésre.

3a.3.9.0600. „Az ember-gép kapcsolati felületek - vezénylők, képernyők - tervezésének és ellenőrzésének támogatására üzemeltető, irányítástechnikai, informatikai és technológiai szakembereket kell bevonni.”

(A követelmény szövege egyértelmű, ezért a követelményszöveget meghaladó további útmutatás nem szükséges.)

3a.3.9.0700. „Annak érdekében, hogy az üzemeltető személyzet tagjai az atomerőművi blokk minden üzemállapotában - a munkakörüknek megfelelő terjedelemben - teljes és hatékonyan feldolgozható információval rendelkezzenek, az érintett munkaterületeken megfelelően minősített mérőműszereket és hagyományos vagy számítógépes kijelzőket kell elhelyezni. Biztosítani kell, hogy a műszerezés lehetővé tegye minden, a reaktorzóna, a reaktor-hűtőrendszerek és a konténment funkció ellátása szempontjából jelentős paraméter mérését, az atomerőművi blokk megbízható és biztonságos üzemeltetéséhez szükséges információ rendelkezésre állását, valamint a biztonság szempontjából fontos mért vagy származtatott paraméterek automatikus rögzítését.”

Az irányítástechnikai rendszer által szolgáltatandó információk körét (szükséges mérések, azok fizikai jellemzői, szükséges előfeldolgozások, a megjelenítéssel szembeni követelmények stb.) már az irányítástechnikai rendszer funkcionális specifikációjában rögzíteni kell, és azoknak a reaktor technológiai tervezéséből kell származniuk.

Ezeket az elvárt kijelzéseket az irányítástechnikai rendszer csak a saját állapotára vonatkozó információkkal egészítheti ki, és eredeti terjedelmüket nem csökkentheti, vagy nem változtathatja meg.

3a.4.4.0400. „A tartalékvezénylő funkcióképességét rendszeres ellenőrzéssel kell biztosítani.”

A tartalékvezénylő funkcióképességének rendszeres ellenőrzése a manuális kezdeményezéssel indított teszteljárások sorába tartozik. Ennek megfelelően ezen tesztek aktiválási idejének kijelölését tervezési számítások támasztják alá. Az egyes résztesztek átfedhetik egymást, de összességükben a tartalékvezénylő rendszer teljes spektrumának működését ellenőrzik, ezt elemzésekkel igazolni kell. Az ellenőrzés idején az egyszeres hibatűrés követelménye és a szándékolatlan működés(ek) kiváltásának elkerülésére vonatkozó követelmény érvényben van.

3a.4.4.0500. „A blokk- és tartalékvezénylőkben számítógépek - így különösen személyi számítógép és szerverek - nem lehetnek, azok elhelyezését a vezénylőn kívül más helységekben kell megoldani. Ezen helységekbe történő belépést érzékelni, a blokk- és tartalékvezénylőkben jelezni és archiválni kell.”

A követelmény a normál üzemeltetés idejére és az irányítástechnikai célú telepített számítógépekre vonatkozik, nem az üzembe helyezés időszakára, és nem a karbantartás és a normál üzemmenet helyreállítása céljából alkalmazott hordozható számítógépekre.

3a.4.4.0600. „A blokkvezénylőben és a tartalékvezénylőben azonos funkcionalitású önálló baleset-kezelési panelt kell telepíteni. Ezeken a helyeken kell biztosítani a baleset-kezelési útmutató ajánlásainak végrehajtásához TA4 és TAK1-2 üzemállapotokban szükséges információt és a baleset-kezeléskor szükséges beavatkozási lehetőségeket.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

3a.4.4.0800. „A blokk- és a tartalékvezénylőben biztosítani kell a szükséges információk fogadását és megjelenítését, lehetővé téve az atomerőművi blokk állapotának és a kritikus biztonsági funkciók időben történő értékelését TA2-4 és TAK1-2 üzemállapotokban is.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

3a.4.4.0900. „A biztonsági funkciót teljesítő blokk- és tartalékvezénylői rendszerek, rendszerelemek számára folyamatos, szünetmentes villamos betáplálást kell biztosítani.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

4.2.1. Villamos rendszerek és irányítástechnika

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."

A biztonság szempontjából fontos irányítástechnikai rendszerek tervezési alapját az erőmű tervezési alapjából kell levezetni. Az irányítástechnikai rendszerek válaszidejére, teljesítőképességére, rendelkezésre állására és környezetállóságára vonatkozó követelményeknek (azokat a feltételeket és körülményeket ideértve, amelyek üzemzavarok és balesetek során, illetve azokat követően állnak fenn) illeszkedniük kell az erőmű általános tervezési alapjához.

Az irányítástechnikai rendszer funkcionális specifikációjának megvalósításán túl az irányítástechnikai tervezőnek biztosítania kell (akár többlet műszerezés alkalmazásával), hogy a biztonsági funkciók rendelkezésre állásáról, és a biztonsági funkciók indulásáról és működéséről a szükséges információk legyenek elérhetőek. Ezen információkat az irányítástechnikai rendszer belső működésében fel lehet használni, vagy az operátor számára meg lehet jeleníteni.

3a.4.5.1500. „Az elindult F1A és F1B funkciót nem szabad leállítani, annak be kell fejeződnie."

Lásd az NBSZ 3a.3.1.1600. ponthoz adott útmutatást.

3a.4.5.1600. „A programozható ABOS 2. rendszerek és rendszerelemekben futó szoftver működése legyen determinisztikus, a futási ciklusideje nem függhet a bemeneti jelek kombinációjától, vagy változási sebességétől. ABOS 2. rendszerben valós idő, vagy a redundanciák és diverzitások közötti időzítés szinkronizációs mechanizmus nem használható."

Ajánlott magas szintű, formális vagy félformális, grafikus mérnöki specifikációs módszerek és tanúsított automatikus kódgenerátor használata a programozható ABOS 2. rendszerekben és rendszerelemekben futó szoftver futtatható kódjának elkészítéséhez. Az ezen rendszerekben használt kódgenerátor határozza meg a minimális és maximális futási ciklusidőt, processzorkihasználtságot, és a maximális memóriafelhasználást az adott ABOS 2. rendszerre és rendszerelemekre vonatkozóan. A programozható ABOS 2. rendszerek és rendszerelemek hardverében alkalmazott többmagos és többprocesszoros architektúrák esetén a processzorkihasználtságot a kódgenerátor minden magra és processzorra határozza meg. A

kódgenerátor által előállított kód megfelelőségét (a forráskód, illetve kiinduló specifikáció formájára való tekintet nélkül), illetve a számított terhelési és kihasználtsági paraméterek helyességét független akkreditált tanúsító szervezet által kibocsátott bizonylat igazolja.

A dinamikus memóriafoglalás használata kerülendő. Ha mégis elkerülhetetlen a dinamikus memóriafoglalás alkalmazása, akkor formális matematikai analízissel kell meghatározni a maximális memória használatot. Menedzselt futtatókörnyezetek (pl. automatikus szemétgyűjtéssel kiegészített dinamikus memóriakezelés, virtualizáció) használata csak akkor megengedett ABOS 2. rendszerekben és rendszerelemekben, ha a futtatókörnyezet gyártója határozza meg formális matematikai analízissel az adott, ABOS 2. rendszerben vagy rendszerelemben futó kódra a minimális és maximális futási ciklusidőt, processzorkihasználtságot, és a maximális memóriafelhasználást. A beépítendő memória méretét kellő tartalékkal kell meghatározni, hogy a szoftver memóriaigényének a hardver akkor is megfeleljen, ha az eredeti tervekhez képest új, biztonságnövelő funkciók beépítése válik szükségessé.

Az ABOS 2. rendszerben illetve rendszerelemekben futó programoknak szervezésüket illetően kizárólag ciklikus feldolgozásúaknak kell lenniük. Nem tartalmazhatnak valós idejű óra (Real-Time Clock, RTC) által kiváltott szinkronizációt, a redundanciák és diverzitások (ideértve a különböző mélységi védelmi szintekbe tartozó rendszereket) közötti szinkronizációt (pl. hálózati szinkronizációs protokollal megvalósított kapcsolatot redundanciák és diverzitások között) és jelfeldolgozások által kiváltott programmegszakítást sem.

A redundanciák és diverzitások közötti időzítés szinkronizációs mechanizmus hiányát determinisztikus függetlenségi analízissel kell igazolni.

3a.4.5.1700. „Ellenőrző és mérőműszerezést kell biztosítani a radioaktív anyagok előfordulási helyeinek megfigyeléséhez és mennyiségének méréséhez minden olyan helyen, ahol a környezetbe történő kibocsátásuk lehetséges."

Az irányítástechnikai rendszer tervezési alapjának tartalmaznia kell azokat a mérési pontokat és az azokhoz tartozó követelményeket (pl. mérési tartomány, pontosság, mérési gyakoriság, stb.), amelyek a radioaktív anyagok előfordulási helyeinek megfigyeléséhez és mennyiségének ellenőrzéséhez szükségesek.

3a.4.5.1800. „A tudomány és technológiai fejlődés eredményeit alkalmazni kell az irányítástechnikai tervezés során. Korszerű, ugyanakkor megfelelő üzemi tapasztalatokkal rendelkező berendezéseket kell használni. A gyártásból kiszoruló

technológiák alkalmazását kerülni kell. A rendszerek tervezésekor figyelembe kell venni az irányítástechnika viszonylag rövid életciklusát és a későbbi biztonságnövelés lehetőségét is. Ennek megfelelően elegendő tartalék kapacitást kell tervezni az alábbi szempontok szerint:

a) legyen elegendő szabad hely az elektronikai helységekben és a szekrényekben,

b) szabad szabványos csatlakozási lehetőségek későbbi fejlesztésekhez,

c) szabad memória és feldolgozási kapacitás a komputerekben, valamint

d) elegendő tartalék adatátviteli kapacitás."

Tervezéskor vegyék figyelembe és igazolják, hogy az irányítástechnikai helységekben és a szekrényekben elegendő hely és megfelelő mennyiségű szabad szabványos csatlakozási lehetőség áll rendelkezésre, figyelembe véve a szállítás, telepítés, szerelés, karbantartás és bővítés hely- és csatlakozási igényét [a) és b) pont].

Tervezéskor vegyék figyelembe és igazolják, hogy amennyiben a későbbi biztonságnövelési lehetőségekkel kapcsolatban a mennyiségi tartalékok biztosításán túlmenően a nemzetközi szabványok követése olyan bővítéseket igényelne, amelyek strukturális jellegűek (pl. diverz beavatkozási ágak kiépítése) és nem elégíthetők ki csupán a meglévő irányítástechnikai helyiségek/szekrények tartalék kapacitásaival, akkor ezeket a bővítéseket a betervezett tartalékoknak köszönhetően meg lehet valósítani (a) és b) pont).

A processzoralapú programozható rendszerek és rendszerelemek futtatható kódjának kialakítása során a kódgenerátor határozza meg a minimális és maximális futási ciklusidőt, processzorkihasználtságot, és a maximális memóriafelhasználást az adott rendszerre és rendszerelemekre vonatkozóan. Többmagos és többprocesszoros architektúrák esetén a processzorkihasználtságot minden magra és processzorra meg kell határozni. Ennek segítségével lehetséges igazolni a megfelelő mértékű szabad memória- és feldolgozási kapacitás meglétét (c) pont).

Az adatátviteli kihasználtság és a tartalék adatátviteli kapacitás értékét a fejlesztőkörnyezet támogatásával a forráskód vagy a generált futtatható kód alapján matematikai módszerekkel határozzák meg, és a szállító gyártóművi (Factory Acceptance Test, FAT) és üzembe helyezési (Site Acceptance Test, SAT) tesztjei során mérésekkel igazolják (d) pont).

A fenti elemzések elvégzésére a nukleáris biztonság szempontjából fontos rendszer, rendszerelem műszer- és irányítástechnikai konfigurációja, működtető logikája vagy a hozzá tartozó adatok megváltoztatása esetén ismételten kerüljön sor.

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."

A rekonstruálhatósághoz szükséges, hogy az irányítástechnikai rendszerek tervezési alapja és az irányítástechnikai funkcionalitás megfelelően dokumentált legyen. Az irányítástechnikai rendszereknek és rendszerelemeknek részletes specifikációval kell rendelkezniük, ami magában foglalja mind a funkcionális viselkedés leírását, mind a nem-funkcionális tulajdonságok specifikációját (teljesítőképesség, megbízhatóság, hibatűrő képesség, stb.). ABOS 2. rendszerek és rendszerelemek esetén a funkcionális viselkedést félformális vagy formális eszközökkel kell leírni.

Az irányítástechnikai rendszerek és rendszerelemek bemeneti, kimeneti, valamint az együttműködésre szolgáló csatlakozó felületeinek, kommunikációs protokolljainak és adatábrázolási rendszereinek kialakításakor mind fizikai, mind absztrakt szinten törekedjenek a szabványos megoldások használatára. A szabványok kiválasztásakor vegyék figyelembe azok támogatottságát a megvalósító hardver- és szoftverplatformok, valamint a fejlesztő- és tesztelőeszközök terén.

Az irányítástechnikai rendszerekre vonatkozó felújítási stratégia kialakításánál vegyék figyelembe, hogy a technológia elemeihez hasonlóan az idő előrehaladtával az irányítástechnika komponensei degradációs folyamaton mennek keresztül. A felújítás fázisaihoz kapcsolódóan gondoskodjanak az irányítástechnikai rendszerek funkcióellátó képességének szinten tartásáról. A szinten tartás tervezése és megvalósítása során biztosítsák a tartalék kapacitásra vonatkozó követelmények (NBSZ 3a.4.5.1800. pont) felülvizsgálatát és a kor színvonalának megfelelő aktualizálását, hogy a rendszerek bővítésével kielégíthetők legyenek a növekvő biztonsági és gazdaságossági elvárásokból levezethető, folyamatosan szigorodó követelmények is. Demonstrálandó a szinten tartás tervezett módszertana.

3a.4.5.2000. „ABOS 2. és ABOS 3. rendszerek esetén bizonylattal kell igazolni, hogy az alkalmazott irányítástechnikai platformot egy arra szakosodott, független, akkreditált tanúsító szervezet megvizsgálta és hibamentesnek, valamint nukleáris erőművek biztonsági rendszereiben való alkalmazásra megfelelőnek minősítette. Programozható irányítástechnika esetén a tanúsítványnak a szoftver és a hardver platform, valamint a fejlesztő eszközök és kódgenerátorok megfelelőségét is igazolni kell."

ABOS 2. és ABOS 3. rendszerek megvalósítása, üzembe helyezése, módosítása és felújítása esetén rögzíteni kell a minősítés alapjául szolgáló szabványok körét. Jelen útmutató 4.1.2. pontjában hivatkozott szabványjegyzék felsorolja az irányítástechnikai rendszerekre releváns szabványokat, de egy konkrét projekt kapcsán ezektől eltérő szabványok is kiköthetők. A bizonylatnak (a tanúsító szervezet által kiállított tanúsítványnak) az alábbiakra kell kitérnie hardverplatform esetében:

a) A vonatkozó nukleáris előírásokat a hardverplatform létrehozása során betartották;

b) A funkcionális biztonság szabályai szerint alkalmaztak olyan fejlesztési módszereket, amelyek képesek a szisztematikus hiba elfogadható mértékű minimalizálására.

c) Melyek a hardverplatform potenciális hibás állapotai és azok milyen gyakorisággal léphetnek fel;

d) Melyek a hardverplatform alkalmazásának azon feltételei, amelyek megléte szükséges a kellő biztonsági besorolású alkalmazáshoz (pl. konfigurációs szabályok, környezeti elvárások, karbantartásigény stb.)

A bizonylatnak (a tanúsító szervezet által kiállított tanúsítványnak) az alábbiakra kell kitérnie szoftverplatform esetében:

a) A vonatkozó nukleáris előírásokat a szoftver létrehozása során betartották;

b) A funkcionális biztonság szabályai szerint olyan szoftverfejlesztési módszereket alkalmaztak, amelyek képesek a szisztematikus hiba minimalizálására; vagy olyan komponensek esetében, amelyekre ez nem bizonyítható, már kellő tapasztalat gyűlt össze az elfogadható mértékű hibamentesség demonstrálására és bizonyítására.

c) Melyek a szoftverrendszer alkalmazásának biztonsági feltételei, amelyek megléte szükséges a kellő biztonsági besorolású alkalmazáshoz (pl. alkalmazói szoftver létrehozásának szabályai, stb.).

Ugyanakkor a hardver-szoftver platformok megfelelő alkalmazását, az alkalmazás által a ténylegesen elvárt, specifikált biztonság elérését az irányítástechnikai rendszer tervezési életciklusára vonatkozóan szintén bizonyítani és független szakértő szervezettel ellenőriztetni kell.

3a.4.5.2100. „ABOS 2. és ABOS 3. biztonsági osztályba sorolt rendszerek esetén el kell készíteni az alábbi igazoló elemzéseket:

a) determinisztikus elemzés az egyszeres meghibásodás elleni védettség igazolására,

b) a hardver és szoftver meghibásodási módok és hatások elemzése,

c) az ember-gép kapcsolat kialakításához és az automatizáltság szintjének megállapításához funkció és feladat elemzés,

d) közös okú meghibásodási lehetőségek elemzése, így különösképpen a specifikáció-béli, tervezési, gyártási, szoftver és hardver, környezeti hatások, karbantartási problémák, azonos rendszer vagy rendszerelem alkalmazása különböző mélységben tagolt védelmi vonalakban, architektúra, elválasztások, elégséges diverzitás,

e) valószínűségi megbízhatósági elemzés,

f) teszt lefedettség elemzése."

Az egyszeres meghibásodási követelmény (lásd az NBSZ 3a.3.1.1100. pontban foglalt követelményt és a hozzá fűzött útmutatást) teljesülésének igazolása során egy adott funkció ellátásában részt vevő, ABOS 2. és ABOS 3. biztonsági osztályba sorolt rendszerek mindegyikének összes lehetséges egyszeres hardver meghibásodását egyenként meg kell vizsgálni. A vizsgált meghibásodás minden következményét (ideértve a meghibásodás hatásaiként keletkező esetleges kumulált hibákat és azok következményeit) fel kell sorolni, majd ezek alapján igazolni kell, hogy mindezen, egyetlen meghibásodás eredményeként előálló hibák és következmények nem befolyásolhatják sem a vizsgált funkció végrehajtásának képességét, sem a vizsgált funkcióra vonatkozó követelmények (pl. válaszidő, teljesítőképesség, stb.) teljesülését (a) pont).

A hardver és szoftver meghibásodási módok és hatások elemzése során a véletlen meghibásodásokon és a tervezési hibákon kívül a szándékolatlan és szándékos károkozás és a rendszerek elleni kibertámadás (lásd 190/2011. (IX. 19.) Korm. rendelet) lehetőségét és következményeit vegyék figyelembe (b) pont).

A blokk irányítása során az egyik legjelentősebb kockázati tényező az emberi hiba. Akár normál üzemben, de különösen üzemzavari vagy karbantartási időszakban előfordulhat téves parancs kiadása, információ félreértelmezése, elvégzendő műveletek sorrendjének felcserélése vagy időzítésének elhibázása. Az ilyen – tipikusan az idő szorításában vagy a váratlan üzemviteli állapot hatására – elkövethető kezelői hibák előfordulását az operátorok döntéseit támogató, adott esetben megfelelő letiltásokat, procedurális

reteszeléseket tartalmazó rendszer kialakítása legyen része az ember-gép kapcsolat megvalósításának (c) pont).

A közös okú meghibásodási lehetőségek elemzése terjedjen ki a közös okú meghibásodások (ezek között a környezeti hatások, pl. földrengés vagy elárasztás) által előidézett többszörös hibák, valamint azok következményeinek meghatározására is (d) pont).

A valószínűségi megbízhatósági elemzés tartalmazza a kiinduló megbízhatósági paraméterek (valószínűségi paraméterek, valószínűség-eloszlások) forrását és megválasztásának módját (e) pont).

A teszt lefedettség elemzés magában foglalja a beépített öntesztek és a manuálisan kezdeményezhető, automatizált tesztek elemzését, valamint a szállító gyártóművi (FAT) és üzembehelyezési (SAT) tesztek elemzését (f) pont).

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.”

A nukleáris biztonság szempontjából fontos rendszer, rendszerelem műszer- és irányítástechnikai konfigurációja, működtető logikája vagy a hozzá tartozó adatok megváltoztatásával kapcsolatos tevékenységeket független tanúsító szervezet által igazolt minőségbiztosítási rendszer irányítása alatt végzik.

A változtatások szükségességét és a nukleáris biztonság szempontjából fontos rendszer, rendszerelem tervezési specifikációjának való megfelelését igazolják. Meggyőződnek arról, hogy a változtatás tervezése és megvalósítása során az érintett rendszerben nem keletkezett szándékolatlan vagy gondatlan, a kívánt funkciónak nem megfelelő vagy nem szükséges változtatás. Ellenőrzik, hogy minden megvalósított változtatás megfelelően dokumentálásra kerüljön.

Az adminisztratív ellenőrzés részeként egy, a technológiai rendszertől független, az igazolásra alkalmas Reprezentatív Konfiguráción végzik el a változtatások teljes körű tesztelését. A tesztelési eljárásokat a validációs és verifikációs terv (V&V terv) írja le, amelynek tartalmaznia kell a tesztelési eredmények archiválásának módszereit és eljárásait is.

3a.4.5.2300. „Olyan megfelelő veszélyjelzéseket kell alkalmazni, amelyek lehetővé teszik az üzemeltető személyzet beavatkozását, mielőtt az adott paraméterek a biztonságvédelmi rendszerek működését indító beállítási értéket elérnék. A védelmi működésekhez, fontos paraméter-eltérésekhez tartozó

jelzéseket hangjelzéssel kell ellátni a blokk- és tartalékvezénylőben egyaránt. A védelmi működéshez tartozó jelzések a határérték-túllépés megszűnése után is csak az üzemviteli személyzet beavatkozásával lehetnek nyugtázhatóak."

Már az irányítástechnikai rendszer technológiai funkcionális specifikációjának megalkotása során definiálni kell azokat a paramétereket és paraméterszinteket, ahol a veszélyjelzésadás szükséges, megadva egyben a veszélyjelzés adásának módját és a jelzés nyugtázhatóságának és törölhetőségének feltételeit.

Bizonyos esetekben trendek figyelésével lehetséges előjelzések képzése. Az olyan paraméterváltozásokat, amelyeknél operátori beavatkozással megelőzhető a vészjelzések létrejötte, azaz a biztonságot veszélyeztető állapot megközelítése, előjelzéssel kell ellátni, Az előjelzéseket a megjelenítőkön, jelzőpaneleken a vészjelzésektől jól elválasztva, egyértelműen azonosítható módon kell elhelyezni, hogy ne legyenek összetéveszthetők a vészjelzésekkel.

3a.4.5.2400. „A biztonsági paraméterekkel kapcsolatos műszerezésnek biztosítania kell mind a mérés, mind a feldolgozórendszer hibás állapotának felismerhetőségét."

Olyan hibadetektáló és hihetőségvizsgálati algoritmusokat kell létrehozni, amelyek képesek a mérés és a feldolgozás egyes részeinek, fázisainak, illetve az ezeket megvalósító eszközök hibás állapotait detektálni. A hibadetektáló és hihetőségvizsgálati eljárásoknak a figyelembe vett meghibásodási módok hatásait kell feltárniuk. A hihetőség lehet irányítástechnikai kritériumból levezetett, de lehet technológiaiból levezetett is. Irányítástechnikai kritériumból levezetett pl. a morzekontaktus, vagy egyidejű nyitott és zárt helyzet értékelése. Technológiai kritériumból levezetett olyan technológiai paraméter érzékelése, ami fizikailag nem állhat elő. A hibadetektáló és hihetőségvizsgálati eljárások eredményeit státuszinformációként a mérési eredményhez (jelhez) kell rendelni.

3a.4.5.2500. „Megfelelő felügyeleti és szabályozási eszközöket kell alkalmazni az Üzemeltetési Feltételek és Korlátok megsértésének megelőzése érdekében."

Az irányítástechnikai rendszernek biztosítania kell azokat a feltételeket, amelyek szükségesek az Üzemeltetési Feltételek és Korlátok megsértésének megelőzéséhez és kezeléséhez. Ezeket a feltételeket az irányítástechnikai rendszer tervezési alapjában rögzítik.

3a.4.5.2600. „Olyan műszerezést, adatfeldolgozó, megjelenítő és archiváló rendszert kell létesíteni, amely ésszerűen megvalósítható mértékben független, alkalmas arra, hogy információt adjon az atomerőművi blokk állapotáról TAK2

üzemállapot környezeti körülményei között is, az ilyen helyzetre kidolgozott útmutató és belső utasítások terjedelmében.”

Az irányítástechnikai rendszer tervezési alapjának önálló követelményrendszerben tartalmaznia kell az atomerőművi blokk állapotáról a TAK2-üzemállapot környezeti körülményei között szükséges mérések körét és azok műszaki feltételrendszerét. Az irányítástechnikai tervezés feladata biztosítani azt, hogy a kialakított műszerezés, adatfeldolgozó, megjelenítő- és archiválórendszer ezen műszaki feltételek között is működőképes maradjon.

3a.4.5.2700. „Az irányítástechnikai rendszereknek biztosítaniuk kell:

a) az atomreaktor biztonságos automatikus leállítását és a biztonsági rendszerek indítását meghatározott paraméterek elérése esetén,

b) teljes körű, pontos és a szükséges időn belül rendelkezésre álló információt az üzemeltető személyzet számára az atomerőmű állapotáról,

c) beavatkozási és ellenőrzési eszközöket;

ca) az elmaradt automatikus működések pótlására,

cb) az atomreaktor kézi vagy automatikus úton történő biztonságos leállított állapotba viteléhez, és ilyen állapotban tartásához, a TA1-4 és a TAK1 üzemállapotok körülményei között,

cc) azokhoz a biztonsági beavatkozásokhoz, amelyek nem tartoznak az automatikus biztonsági működések körébe, valamint

cd) a baleset-kezeléshez szükséges kézi működtetésű műveletekhez, továbbá

d) megfelelő adattárolási, rögzítési rendszert arra, hogy valamely tranziens és üzemzavar részletei később kivizsgálhatóak legyenek.”

A követelménypontban felsorolt szempontok alapvető tervezési szempontok az irányítástechnika számára. Az irányítástechnikai rendszer tervezési alapjának, ezen belül a technológiai funkcionális specifikációnak a felsorolt szempontok teljesítéséhez szükséges információkat és követelményeket teljes körben tartalmaznia kell. Az NBSZ 3a.4.5.3200. pontja további követelményeket fogalmaz meg a technológiai funkcionális specifikáció összeállítása számára. Az irányítástechnikai tervezésnek ellenőriznie kell, hogy a követelménypontban felsorolt szempontok teljes körben megfogalmazásra kerültek-e az irányítástechnikai rendszer tervezési alapjában.

3a.4.5.2800. „Az irányítástechnikai rendszerek pontosságára, válaszidejére, eseménysorrend-meghatározására, feldolgozási kapacitástartalékára és

kommunikációs kapacitástartalékára vonatkozóan az atomerőmű tervezési alapjával konzisztensen kell a követelményeket meghatározni.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

3a.4.5.2900. „Biztosítani kell, hogy a biztonsági irányítástechnikai rendszer érzékelje a TA1-4 és a TAK1 üzemállapotokat és az állapotnak megfelelően biztosítsa:

a) az atomreaktor leállítását,

b) a megfelelő biztonsági funkciót ellátó rendszerelemek működtetését, és

c) a támogató funkciók indítását.”

A követelménypont egyes kiemelt fontosságú szempontokra nézve specifikusan megismétli az NBSZ 3a.4.5.2700. pontban már megfogalmazott előírásokat. Ezért az útmutatás azonos az NBSZ 3a.4.5.2700. pontjához megfogalmazott útmutatással.

3a.4.5.3000. „A végrehajtó szervhez vezetett, különböző biztonsági szinthez tartozó parancsok esetén a magasabb biztonsági szintű parancsnak prioritást kell biztosítani. Ettől való eltérést elemzéssel kell igazolni. A prioritásképzést megvalósító rendszerelem biztonsági osztályát az általa kezelt legmagasabb szintű biztonsági funkcióhoz tartozó parancs biztonsági szintjéből kell megállapítani.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

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.”

Az irányítástechnikai rendszer tervezése során az archiválásra kijelölt adatok körének meghatározása, az adatok időbélyeggel való ellátásának irányítástechnikai rendszerbeli helye, továbbá az archív fájlok előállításának és megőrzésének a metodikája kerüljön rögzítésre. Az időbélyegek hozzárendelése a teljes rendszerben legyen egyértelmű és ellentmondásmentes. Ennek egyik alapvető feltétele az időbélyegek alapjai együttfutásának biztosítása. Az együttfutás biztosítását úgy kell megoldani, hogy az ne sértse a redundanciák és diverzitások (ideértve a különböző mélységi védelmi szintekbe tartozó rendszereket) közötti szinkronizáció tilalmát (lásd az NBSZ 3a.4.5.1600. pontjában foglalt követelményt és a hozzá fűzött útmutatást), valamint a különböző biztonsági osztályba sorolt

irányítástechnikai rendszerek közötti kapcsolat visszahatásmentes megvalósítását előíró NBSZ 3a.4.5.4200. pontban foglalt követelményt sem. ABOS 2. rendszer esetén pedig a fizikailag egyirányú kommunikációra vonatkozó NBSZ 3a.4.5.3700. pontban foglalt követelményt és a hozzá fűzött útmutatást be kell tartani a tervezés és megvalósítás során. Az időbélyegek hozzárendelésének tervezésekor az esemény-sorrendezés által szolgáltatott követelményeket figyelembe kell venni.

3a.4.5.3200. „Az irányítástechnikai rendszerek technológiai funkció specifikációjának meg kell felelnie a következő követelményeknek:

a) azonosítja az irányítási feladatot a technológiai céloknak és követelménynek megfelelően,

b) minden irányítási feladathoz egyértelmű azonosító kódot rendel,

c) az irányítási feladatokat az adott feladat biztonsági fontossága alapján funkcionális biztonsági szintekbe sorolja és a mélységi védelem megfelelő szintjéhez rendeli,

d) meghatározza a funkciókhoz kapcsolódó függetlenségi kritériumokat, beleértve a diverzitási követelményeket,

e) meghatározza a funkciókhoz tartozó válaszidőket,

f) minden kimenethez meghatározza azt a biztonságos állapotot vagy pozíciót, amit a kimenet detektált hibája esetén fel kell vegyen,

g) meghatározza az operátori beavatkozást igénylő feladatokat az atomerőmű TA1-4 és TAK1 üzemállapotokra vonatkozóan oly módon, hogy az üzemeltető személyzet képes legyen azokat teljesíteni,

h) emberi nyelvű leírás mellett többszintű, megfelelően strukturált, formális nyelvi leírási módot használ,

i) formai ellenőrzésére, verifikálására automatizált rendszert irányoz elő,

j) tartalmazza az operátori feladatok végrehajtásához és az automatikus feladatok ellenőrzéséhez szükséges információkat,

k) működtetési határértékekhez és analóg értékek megjelenítéséhez meghatározza a pontossági követelményeket, továbbá

l) meghatározza az elvárt megbízhatósági követelményeket, továbbá

m) ABOS 2. biztonsági osztályba sorolt programozható irányítástechnikai rendszerek esetén azok funkcionális ellenőrzésére, validálására szimulációs módszereket határoz meg.”

A technológiai funkció specifikációjának részeként a technológiai célok és követelmények teljesítéséhez ki kell dolgozni egyedi irányítástechnikai funkciókat. Az irányítástechnikai funkciók megadásához első lépésként specifikálni kell az irányítástechnikai rendszer interfészeit (mérési vagy bemeneti interfész, beavatkozási vagy kimeneti interfész, és ember-gép kapcsolati interfész, ami kétirányú). Ezen interfészek közötti kapcsolatot írják le az irányítástechnikai funkciók. Az egyedi irányítástechnikai funkciókat egyértelmű technológiai célokhoz és követelményekhez kell rendelni (a) pont).

A kidolgozott irányítástechnikai funkciókhoz létre kell hozni egy olyan, a funkciókat egyértelműen azonosító kódrendszert, amely további információkat biztosít, pl. az összetartozó funkciócsoportba tartozás felismerhetőségét, a technológia azonosíthatóságát stb., és illeszkedik az erőmű egységes azonosítási sémájához. A kódrendszert úgy kell megalkotni, hogy az egy hierarchikusan szervezett adatbázisba illeszthető legyen (b) pont).

A biztonság szempontjából fontos irányítástechnikai rendszerek tervezési alapját az erőmű tervezési alapjából kell levezetni. Ezért elengedhetetlen, hogy már a technológiai tervezés során, az irányítástechnikai rendszer technológiai funkció specifikációjának elkészítésekor definiálni kell az irányítási feladatok azon alapvető tulajdonságait, amelyek az erőmű tervezési alapjával összhangban alapvetően határozzák meg az irányítástechnikai tervezés menetét. Ilyen az adott irányítási feladat funkcionális biztonsági szintje, a mélységi védelem megfelelő szintjéhez rendelése, a feladatra vonatkozó függetlenségi kritériumok, diverzitási követelmények, válaszidők, az elvárt megbízhatósági követelmények és a feladathoz tartozó kimenetek azon biztonságos állapota vagy pozíciója, amit a kimenetnek detektált hiba esetén fel kell venni (c)–f) és l) pont).

Az irányítástechnikai rendszer funkcionális specifikációjának verifikációja során a tervezési alapnak és a technológiai funkció specifikációnak való megfelelésen kívül ellenőrizni kell annak teljességét és ellentmondásmentességét. Ennek támogatására, a funkcionalitás specifikálásának egyértelműsége érdekében azt formalizált, strukturált módon, szakterületi nyelv alkalmazásával kell elkészíteni (h) pont).

A funkcionális specifikáció készítése során a jelek és változók elnevezési konvenciójára vonatkozóan egységes módszertant kell követni. A formális ellenőrzést végző automatizált rendszer legyen képes a teljesség (pl. minden bemenet be van kötve), a konzisztencia (pl. analóg bemenet nem kapcsolódik közvetlenül bináris jelhez), a terheltség (memória, kommunikáció), és további

kritériumok ellenőrzésére. A formai ellenőrzést és verifikációt végző automatizált rendszer rendelkezzen megfelelő ember-gép kapcsolati felületekkel és archiváló rendszerrel. (i) pont).

Amennyiben a nukleáris létesítmény több azonos technológiájú, azonos tervezési alappal rendelkező atomerőművi blokkal rendelkezik, akkor fontos szempont annak biztosítása, hogy a blokkok részletes irányítástechnikai architektúrája és funkcionális specifikációja azonos tervből generálható legyen. Ugyanakkor alapvető szempont a generálás folyamata során a közös okú hibák elkerülése. Ezért automatizált generálási módszerekkel kell biztosítani a blokkok azonos tervből generált architekturális és funkcionális specifikációit. Ezen automatikus generálási módszereknek lehetőséget kell biztosítani arra, hogy a blokkok közti szisztematikus és formalizálható eltéréseket definiálni lehessen, és azokat az automatikus generáló eljárások működésük során figyelembe vegyék, így a definiált eltéréseket a blokkspecifikus generált eredményekbe helyesen beépítsék. Az automatikus generálási módszerek hibamentességét igazolni kell.

A funkcionális specifikáció elkészítése többszintű, megfelelően strukturált, formális nyelvi leírási mód alkalmazásával csak akkor lehet sikeres, ha annak alapját egy számítógéppel támogatott specifikációs eszköz képezi. A specifikációs eszköz a tervezés során használt digitális tervező eszköznek minősül, így vonatkozik rá az NBSZ 3. kötetének 3a.4.5.3400. pontja, és rendelkeznie kell az abban megkövetelt funkcionalitással, többek között szimulációs és tesztelési képességekkel. Az automatizált rendszer 2. biztonsági osztályba sorolt programozható irányítástechnikai rendszerek esetén legyen alkalmas a biztonsággal kapcsolatos funkciók validálására, szimulációval generált jelfelület fogadására és feldolgozására. (m) pont).

3a.4.5.3300. „Az irányítástechnikai rendszerek és rendszerelemek tervezését és kivitelezését az adott biztonsági besorolású rendszerekre és rendszerelemekre vonatkozó kiválasztott szabványoknak megfelelően, differenciált követelmények szerint kell végezni.”

Az irányítástechnikai tervezés elején meg kell határozni azon szabványok körét, amelyek előírásait a tervezés és a kivitelezés (fejlesztés, gyártás, integrálás, telepítés) során betartják, és amelyeknek való megfelelést a megfelelő ellenőrzési fázisokban (tervezési verifikációs ellenőrzések, gyártóművi végellenőrzési tesztek, üzembehelyezési tesztek) demonstrálják. A kiválasztott szabványoknak minden esetben igazodniuk kell a tervezés, fejlesztés, gyártás, szerelés alatt álló rendszerelem biztonsági osztályba sorolásához. Alapelvként szem előtt tartandó, hogy az egyes rendszerelemek

biztonsági osztályát az általuk kezelt legmagasabb biztonsági szintű funkció biztonsági szintjéből kell megállapítani (vö. NBSZ 3a.4.5.3000.)

Általánosságban igaz, hogy a magasabb biztonsági osztályba sorolt rendszerelemekre elfogadott szabályok alkalmazása elfogadható alacsonyabb biztonsági osztályba sorolt rendszerelemek tervezése és kivitelezése során. A differenciált követelmények szerinti tervezés és kivitelezés elve ugyanakkor azt hangsúlyozza ki, hogy a túlzott, nem megfelelően kiválasztott szabványrendszer szerint végzett fejlesztőmunka könnyen túlspecifikált, a követelmények teljesítéséhez szükséges szintnél bonyolultabb felépítésű rendszerelemhez vezethet. Ez számos egyéb elvárásra (pl. fejlesztési idő, élettartam, karbantarthatóság, rekonstruálhatóság stb.) hátrányosan hathat, ezért kerülendő (vö. még NBSZ 3a.4.5.4200.).

Fontos felhívni azonban a figyelmet arra, hogy a szabványoknak való megfelelés nem helyettesíti, csak segíti a jogszabályi előírásoknak (pl. az NBSZ 3. kötete követelményrendszerének) való megfelelést.

A különböző biztonsági osztályokhoz tartozó rendszerek és rendszerelemek vonatkozásában alkalmazandó differenciált követelményrendszerrel kapcsolatban további ajánlásokat önálló útmutató fogalmaz.

3a.4.5.3400. „Az irányítástechnika tervezése során használt digitális tervező eszközök és adatbázisok közötti adatcserét automatizált módon kell végrehajtani. Törekedni kell arra, hogy a konzisztens adatstruktúrában egy adat egy helyen legyen tárolva. Programozható rendszerek és rendszerelemek tervezéséhez olyan korszerű fejlesztő eszközöket kell használni, amelyek az alábbi funkciókkal rendelkeznek:

a) programozás,

b) kódgenerálás,

c) dokumentálás,

d) kód analízis, valamint

e) szimuláció, tesztelés.”

A választott tervezőrendszernek valamennyi, a fentiekben felsorolt funkcióval rendelkeznie kell. A tervezőrendszernek rendelkeznie kell továbbá azzal a képességgel, hogy be tudja fogadni intelligens elektronikus eszközök formális módszerekkel leírt specifikációit. A tervezőrendszer rendelkezzen magas szintű verziókezeléssel, ami lehetővé teszi korábbi módosítások nyomon követését.

Az irányítástechnika tervezése során előállított többszintű, megfelelően strukturált, formális nyelvi leírásból lehetőleg automatikus átalakítási (kódgenerálási) eljárással készüljön el az irányítástechnikai rendszer programozható eszközeiben futtatott szoftverkód. A kódgenerálási eljárás lehet többlépéses, azonban az egyes lépések megfelelőségét és konzisztenciáját igazolni kell (vö. NBSZ 3a.4.5.3500.). Az egyes lépésekben felhasznált adathalmazban az azonos egyedi absztrakt jelentéssel bíró adatoknak felhasználásuk során egy közös forrásból kell származniuk. Ez a közös forrás egy jól definiált egyedi tárolási helyet és egyetlen tárolt példányt jelent, és az azonos egyedi absztrakt jelentéssel bíró adatoknak konzisztensen csak ezt az egy tárolt példányát szabad szükség esetén megváltoztatni.

A tervezőrendszer(ek)hez meg kell adni a verifikáció, validáció és minőségbiztosítás módját leíró eljárásokat és elfogadási kritériumokat.

3a.4.5.3500. „Digitális ABOS 2. és ABOS 3. osztályba sorolt rendszerek esetén dokumentálni kell, hogy a generált felhasználói szoftver kód visszaolvasásra került, majd a visszaolvasott kód analízise igazolta, hogy a kódgenerálási folyamat nem vitt be hibát. A fejlesztési, tervezési, gyártási és létesítési szakasz minden műveletét részletesen dokumentálni kell. Bármely dokumentum hatósági ellenőrzés vagy szakértői értékelés tárgyát képezheti a létesítmény teljes időtartama alatt."

A kódgenerálási folyamat ellenőrzésének preferált módja, hogy a visszaolvasott kódból visszaállítják a funkciók (grafikus) specifikációját, majd igazolják a kiinduló specifikációval való egyezést. A generált kód analízise során szükségessé váló transzlációs átalakítások konzisztenciáját igazolni kell.

A fejlesztési, tervezési, gyártási és létesítési szakasz során készített dokumentumok köre legyen teljes, konzisztens, hozzáférhető és álljon rendelkezésre olyan formában, amely biztosítja a hatékony ellenőrzés elvégezhetőségét.

3a.4.5.3600. „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."

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

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."

A követelménypont elsődleges célja annak biztosítása, hogy az alacsonyabb biztonsági osztályba sorolt rendszer vagy rendszerelem visszahatásmentesen kapcsolódjon a magasabb biztonsági osztályba sorolt rendszerhez vagy rendszerelemhez, azaz sem normál működése, sem meghibásodása ne befolyásolhassa a magasabb biztonsági osztályba sorolt rendszer vagy rendszerelem funkcionalitását és a nem funkcionális követelmények teljesülését. Ez a fizikailag egyirányú kommunikáció alkalmazásával biztosítható, ahol az adatáramlás egyetlen iránya az ABOS 2. rendszer vagy rendszerelem irányából az alacsonyabb biztonsági osztályba sorolt rendszer vagy rendszerelem felé mutat, az egyirányúsítás garanciáját pedig a megvalósítás fizikai elve adja (pl. egyirányú optikai kapcsolat).

A követelménypont másik célja a programozott rendszerek védelme a kibertámadásokkal szemben. A fizikailag garantált egyirányú kommunikációs kapcsolat ugyanis megakadályozza, hogy ezen a kapcsolaton keresztül az alacsonyabb biztonsági osztályba sorolt rendszer vagy rendszerelem felől kibertámadás érhesse az ABOS 2. rendszert vagy rendszerelemet.

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

Alapvető elvárás, hogy a különböző atomerőművi blokkokhoz tartozó, a technológiához kapcsolódó irányítástechnikai rendszer egymástól függetlenek legyenek, azaz többek között ne legyen köztük sem villamos, sem információs kapcsolat. Ha ez mégsem kerülhető el, akkor is gondoskodni kell a visszahatás-mentességről, aminek egyik eszköze a fizikailag garantált egyirányú kommunikációs kapcsolat alkalmazása.

Külső rendszerek (pl. az erőmű területén kívül elhelyezkedő felügyelő, megfigyelő vagy támogató szervezetek) felé a technológiához kapcsolódó irányítástechnikai rendszer csak fizikailag egyirányú adatkapcsolaton keresztül szolgáltathat adatot. Ennek egy lehetséges megvalósítási módja az adatok kicsatolása a technológiához kapcsolódó irányítástechnikai rendszerből fizikailag egyirányú adatkapcsolaton keresztül egy adatkoncentrátorba (on-line archívumba), majd ebből az adatkoncentrátorból szolgáltatni a szükséges adatokat a külső rendszerek felé.

Ha külső rendszerből szükséges adatot juttatni a technológiához kapcsolódó irányítástechnikai rendszerbe, akkor körültekintő tervezéssel kell biztosítani,

hogy a nukleáris biztonság és a számítógépes védettség követelményei maradéktalanul teljesüljenek, és az alkalmazott megoldás hatásosságát elemzéssel és validációs teszteléssel is igazolni kell.

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."

A diagnosztikai és szerviz célú eszközök nem csak adat kicsatolása céljából csatlakoznak az ABOS 2. és ABOS 3. rendszerekhez. A tesztelési és diagnosztikai tevékenységek elvégzése céljából a csatlakoztatott eszköz fizikai (feszültség, áram) vagy logikai (kommunikációs protokoll) alapú tesztjeleket vagy diagnosztikai parancsokat adhat az ABOS 2. és ABOS 3. rendszerek meghatározott bemeneteire. Ilyen esetekben külön elemzésekkel kell igazolni, hogy a szándékolatlan vagy rosszindulatú parancsok bejutása a biztonsági rendszerbe a csatlakoztatott diagnosztikai és szerviz célú eszközök felől 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."

A megkövetelt hibatűrő képességet az irányítástechnikai rendszer technológiai funkció specifikációja határozza meg minden irányítási feladatra. F1A és F1B, valamint F2 funkciók esetében lásd még az NBSZ 3a.4.5.4400. pontjában leírt követelményt és az ahhoz adott útmutatást.

3a.4.5.4100. „Az irányítástechnikai rendszerek architektúrájának illeszkedni kell a mélységben tagolt védelem szintjeihez. A mélységi védelemhez illeszkedő szinteket az ésszerűen megvalósítható legteljesebb mértékben el kell választani egymástól"

A mélységi védelem szintjeit az NBSZ 3a.2.1.1900. pontja alapján kell meghatározni. Az irányítástechnikai rendszerben elválasztott, önálló részrendszerekkel kell megvalósítani a mélységi védelem különböző szintjeit. A szintek közötti elválasztás mértékét és az alkalmazott diverzitás módját az irányítástechnikai rendszer technológiai funkciójának specifikációja

határozza meg. Az elválasztott, önálló részrendszerek egymásra nem hathatnak; közös méréseket nem használhatnak; és beavatkozási szinten is a lehetőségeknek megfelelően el kell egymástól választani őket. Közös mérések alkalmazása sérti a védvonalak elválasztásának elvét, ezért ha alkalmazásuk mégis elkerülhetetlen, akkor egyedileg kell vizsgálni, hogy miért szükséges közös mérést használni, és milyen intézkedéseket használnak a kívánatos megbízhatóság eléréséhez. Ki kell zárni (és bizonyítani kell), hogy alacsonyabb szintű rendszer bármely meghibásodása esetén a magasabb szintű rendszer nem tudja a funkcióit végrehajtani.

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.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

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.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

3a.4.5.4400. „F1A és F1B, valamint F2 funkciók tekintetében biztosítani kell az egyszeres hibatűrő képesség folyamatos fenntartását. F1A, F1B vagy F2 funkcióvesztés még karbantartás vagy kézzel indított tesztelés esetében sem engedhető meg. F1A és F1B funkció esetén az egyszeres meghibásodás téves működést sem okozhat. Igazolni kell, hogy az alkalmazott architektúra megfelel a megbízhatósági követelményeknek.”

F1A és F1B funkciók esetében a redundancia fokát úgy kell megválasztani, hogy a karbantartásban érintetté tehető, vagy egy időben tesztelhető redundáns részek nélkül, további egy hibát feltételezve is teljesüljön mind a funkció-végrehajtás minden biztonsági funkciójára, mind a téves funkcióvégrehajtás elkerülésére. Azt, hogy mekkora rendszerrész tesztelése lehetséges, azaz mekkora degradáció engedhető meg, az többek között az egyszeres meghibásodási kritériumtól függ. Ez praktikusan a

karbantartásban vagy tesztben érintett részek nélkül háromszoros redundanciát igényel; annak függvényében tehát, hogy mekkora részt enged a tervező karbantartani/tesztelni, a teljes rendszer négyszeres vagy magasabb fokú redundanciával rendelkezik.

F2 funkciók esetében, ahol a követelmények hasonlóak, de karbantartás/tesztelés mellett a meghibásodási okú téves működés nem kizárt, a redundancia foka eggyel csökkenthető.

A megbízhatósági elemzésekben szerepeltetni kell a karbantartásban/tesztelésben érintett részrendszereket (pl. hibafa-elemzésben azokat fixen nem rendelkezésre állónak deklarálni) és így bizonyítani a fennmaradó rendszerre az egyszeres hibatűrést és az egyéb megbízhatósági követelmények teljesülését.

3a.4.5.4500. „Az ABOS 2. és ABOS 3. biztonsági osztályba sorolt irányítástechnikai rendszerek összes komponensének automatikus önellenőrző képességgel kell rendelkezni. Az önellenőrzés során feltárt hiba esetén jelzést kell generálni az operátor számára és - ha szükséges -, az alrendszer kimeneteit a 3a.4.5.3200. pont előírásai szerint, előre meghatározott, a biztonság irányába ható állapotba kell vezérelni.”

A hibadetektáló és hihetőségvizsgálati eljárások eredményeit státuszinformációként a mérési eredményhez (jelhez) kell rendelni, lásd az NBSZ 3a.4.5.2400. pontjában foglalt követelményt és a hozzá tartozó útmutatást. Az irányítástechnikai rendszerre vonatkozó specifikációnak, valamint a részrendszerek, alrendszerek és komponensek specifikációinak mind tartalmazniuk kell a kimenetek biztonsági irányát, legyenek azok ténylegesen fizikai kimenetek vagy kommunikációs kimenetek.

Az öntesztek le kell fedniük a fellépő hibák jelentős részét; ugyanakkor az automatikus öntesztek által fel nem fedezett hibák felderítésére további manuális (emberi beavatkozású) tesztek megvalósítása szükséges, ezt az NBSZ 3a.4.5.4600. pontja írja elő.

Az öntesztek hibalefedését és detektálási (ciklus) idejét meg kell adni, és a megbízhatósági elemzéseket ezen detektálási idők figyelembevételével kell elvégezni.

Az operátor számára adott jelzésnek egyértelműnek kell lenni: jelezni kell a hiba keletkezési helyét és jelezni kell az ennek következtében biztonsági állapotba vezérelt kimeneteket [meg kell jelölni a kényszerített biztonságos állapot(ok)at és az érintett alrendszer(eke)t].

3a.4.5.4600. „Az ABOS 2. és ABOS 3. biztonsági osztályba sorolt irányítástechnikai rendszerek önellenőrzés által nem ellenőrizhető meghibásodásainak feltárására, valamint a biztonsági funkciók működőképességének demonstrálására manuális kezdeményezésű automatizált tesztelési lehetőséget kell biztosítani. A manuálisan kezdeményezhető, automatizált tesztelés végrehajtásához beépített eszközöket kell használni. A tesztelési ciklusidő megfelelőségét biztonsági elemzés alkalmazásával kell igazolni.”

A manuálisan kezdeményezhető automatizált tesztelés aktiválására a ciklusidő által meghatározott időpontokban kerül sor. Az ebbe a körbe tartozó teszteljárások manuálisan kezdeményezettek, de végrehajtásuk automatizált. A teszteljárások lefolytatását automatikus működésű eszközök vezérlik, a tesztelés eredményeinek regisztrálása és kiértékelése szintén automatikusan történjen. A generált teszt inputjelek indította jelfolyamok és rendszerállapotok kialakulásának elemezhetőségét biztosítandó a regisztrált adatok legyenek időbélyeggel ellátottak. A tesztelést vezérlő automatikus működésű eszközök dokumentálják a tesztek lefolytatását, a konfiguráció tesztelt területeinek működését, és támogassák a lefolytatott tesztek kiértékelését.

A FAT funkcionális teszteset készlet legyen közvetlen módon elérhető annak érdekében, hogy szükség esetén az üzemeltetők késlekedés nélkül ki tudják választani és le tudják futtatni a kiválasztott teszteljárást.

A tesztek terjedelme legyen oly módon meghatározott, hogy az egyes résztesztek, amelyek átfedhetik egymást, összességükben a teljes rendszer működését ellenőrizzék.

A manuálisan kezdeményezhető tesztek célja az üzemszerűen működő rendszer védelmi funkcióinak tesztelése. A védelmi funkció indításához szükséges kezdeti eseményeket az automatikus tesztelőberendezés által generált inputjelek váltják ki. A manuálisan kezdeményezhető tesztek az irányítási rendszer hibamentes üzemszerű működését ellenőrzik abban az állapotban és konfigurációban, amire az adott teszt vonatkozik, ezért a tesztelés tényéről a tesztelt rendszer nem rendelkezhet információval.

Az egyszeres meghibásodási követelmény betartása a manuálisan kezdeményezhető tesztek előkészítése, lefolytatása és kiértékelése alatt is érvényben marad.

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.”

A diverzitás szükséges mértékének levezetése illetve a közös okú meghibásodások valószínűségének elemzése tartalmazza a diverzitás valamennyi aspektusát (tervezési diverzitás, eszköz szintű diverzitás, funkcionális diverzitás, kezelői szintű diverzitás, jelszintű diverzitás, szoftver diverzitás).

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.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

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, az alábbiak szerint:

a) Az ABOS 2. biztonsági osztályba sorolt számítógépes platformon, mikroprocesszoros platformon, egyéb technológiájú programozható elektronikus rendszerelemekkel vagy komplex elektronikus komponensekkel megvalósított programozott rendszerekre és rendszerelemekre a fejlesztés során verifikációs és validációs, valamint az ezekből következő tesztelési terveket kell kidolgozni. A verifikációs, a validációs, és a tesztelési terveket fejlesztés közben, valamint az üzembe helyezés előtt végre kell hajtani.

b) az első üzembe helyezés után még megváltoztatható programú, vagy megváltoztatható logikájú ABOS 2 biztonsági osztályba sorolt rendszerek és rendszerelemek esetében az üzemeltetési életciklus szakaszban szükségessé váló további fejlesztések és módosítások e rendelet szerinti átalakítások megtervezésekor a verifikációs és validációs, és az ezekből következő tesztelési tervek újra kidolgozandók, és az üzembe helyezés előtt végrehajtandók a tervező, a gyártó, valamint a felhasználó vagy üzemeltető részvételével.

c) Az ABOS 3. vagy alacsonyabb biztonsági osztályba sorolt számítógépes platformon, mikroprocesszoros platformon, egyéb technológiájú programozható elektronikus eszközökkel vagy komplex elektronikus komponensekkel megvalósított programozott rendszerekre és rendszerelemekre az első üzembe helyezést megelőzően, és az üzemeltetési életciklus szakaszban szükséges, e

rendelet szerinti átalakítások fejlesztésekor validációs és ebből következő tesztelési terveket kell kidolgozni, és az üzemeltetés előtt végrehajtani.

d) A biztonsági funkciókat, és az ezeket megvalósító rendszereket a gyártóműben, vizsgáló, vagy minősítő laboratóriumban és a létesítményre jellemző körülmények között kell tesztelni. A tesztek fedjék le az összekapcsolt hardverekből, a szoftverekből és a rendszer integrálásából adódó szempontokat, valamint a tervezés során figyelembe vett és a létesítményre jellemző kezdeti eseményeket, amelyek kezeléséhez a biztonsági és egyéb funkciókra szükség van.

e) A komplex elektronikus komponensekhez kapcsolódó adatgyűjtő, adatfeldolgozó, valamint fejlesztő, programozó és tesztelő informatikai rendszereket a biztonság szempontjából értelmezhető jelentőségük szerint kell tervezni és minősíteni.

f) A verifikáció és a validáció, valamint a tesztelés dokumentálandó, és a dokumentáció az engedélyezési illetve üzembe helyezési eljárásban az üzemeltető és a hatóságok számára felhasználható kell, hogy legyen."

A biztonsági osztályba sorolt irányítástechnikai rendszereket és azok komponenseit az életciklus során több alkalommal kell tesztelni. Tipikusan három fő validációs tevékenység azonosítható. A tervezési és megvalósítási életciklusfázis eredményét (a megvalósított és integrált rendszert) a gyártóművi végellenőrzési tesztek (FAT-tesztek) ellenőrzik, az üzembehelyezési fázis eredményét (a leszállított, szerelt és a technológiához csatlakoztatott rendszert) az üzembehelyezési tesztek (SAT) ellenőrzik, az üzemeltetés alatt pedig a beépített öntesztek és a manuálisan kezdeményezhető, automatizált tesztek ellenőrzik a végleges rendszert.

Minden validációs tevékenységnek előre meghatározott tesztelési tervvel kell rendelkeznie, amely meghatározza a validáció részét képező tesztek körét, a használt tesztkörnyezetet és a környezeti feltételeket. Az adott validációs tervben azonosított minden egyes teszthez részletes tesztelési programot kell kidolgozni, ami definiálja a teszt célját, a tesztelési módszert, a tesztelési lépéseket (a megismételhetőséget biztosító részletességgel), a teszt elfogadásának kritériumait, és a felfedezett eltérések kezelését. Mind a validációs tervet, mind a validációs tervben azonosított minden egyes teszt tesztprogramjait az adott validációs tevékenység megkezdése előtt be kell mutatni. A validációs tervnek és a benne azonosított tesztprogramoknak lehetővé kell tenniük a meghatározott validációs célok és tesztkörnyezet figyelembevételével a teljeskörűség igazolását.

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."

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

3a.4.5.5100. „Kereskedelmi termék alkalmazása esetén a terméknek rendelkeznie kell egyedi- és típus-azonosítással és megfelelő, akkreditált vizsgáló szervezettől származó minősítéssel, annak igazolására, hogy a termék a tervezési alapból levezetett követelményeknek megfelel."

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

3a.4.5.5200. „A műszerezettségnek a TA1-4 és a TAK1-2 üzemállapotok körülményei között is információt kell szolgáltatnia a kritikus biztonsági funkciók, valamint az üzemállapot kezeléséhez szükséges technológiai rendszerek állapotáról."

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

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."

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

3a.4.5.5400. „A tervezésben a programozható rendszerek védelmi szempontjait is figyelembe kell venni. Ha a tervezés során a nukleáris biztonsági és a programozható rendszerek védelmi szempontjai konfliktusba kerülnek, a nukleáris biztonsági szempont prioritást élvez."

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

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 megtervezni."

Meg kell határozni, mely rendszerelemek és rendszerek funkciói változtathatók meg a helyszínen akár a berendezés helyszíni módosításával (fizikai átalakítás, fizikai módosítás vagy rongálás), akár lekapcsolásával, akár átprogramozásával; és melyeknél lehetséges a funkció távolról történő módosítása. Minden egyes esetben fel kell mérni, milyen mértékű és milyen következményű (pl. védelmi funkció indul, redundancia a funkciót átveszi, stb.) lehet a beavatkozás. A beavatkozások eszközigényét szintén fel kell mérni (pl. egyszerű mechanikai eszközök, számítógép, célszoftverek, védett elérésű célszoftverek stb.) és felmérik az eredményes használathoz (funkcióváltoztatás) szükséges ismeretek körét (tervek, általános elvek, általános szaktudás stb.). Ugyancsak figyelembe kell venni annak lehetőségét, hogy a módosítás rejtve marad egy tényleges aktiválásig.

Ezen információkat a védelem (security) tervének kialakításához kell felhasználni.

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.”

A programozható eszközök rendelkezzenek belső hibafeltáró algoritmusokkal. Saját hardvermeghibásodásaikat (ideértve az ellenőrző összegek által felfedett tárterülethibákat, de akár az ellenőrző összeg érvénytelenségét más okból is) lehetőleg detektálniuk és távadniuk kell a kiértékelhetőséghez szükséges és a lehetőségek szerinti felbontásban.

Meg kell oldani, hogy rendszeres időközönként megállapítható legyen, hogy az aktuális szoftververziók megfelelnek a jóváhagyott, érvényes szoftververzióknak; ehhez ellenőrzési listákat és az érvényes szoftververziókról készült másolatokkal történő időszakos összehasonlításokat célszerű alkalmazni.

Az adatfeldolgozás során első lépcsőben a más rendszerekből, külső technológiákból származó jelek hihetőségvizsgálatát (pl. tartomány) kell elvégezni. Érvénytelen jelek esetében meg kell határozni a biztonsági reakciókat (helyettesítő jel értéke vagy végrehajtandó funkció) és a szükséges jelzések szintjét.

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.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)

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

(A követelmény szövege egyértelmű, ezért a követelmény szöveget meghaladó további útmutatást nem szükséges.)

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.”

Az erőmű biztonságos működtetéséhez a működtető és felügyelő személyzetnek információval kell rendelkeznie a rendszerben végzett karbantartási és tesztelési tevékenységekről, valamint az elvégzett karbantartások és módosítások esetleges következményeiről. A kidolgozott adminisztratív rendszernek és az ehhez tartozó belső eljárásnak, és a hozzáférések biztonsági protokolljainak (eljárásainak) támogatniuk kell ezt az átláthatóságot; és biztosítaniuk kell, hogy a karbantartást csak az arra kijelölt személyzet végezhesse el a megfelelő engedélyek birtokában, továbbá a rendszernek csak a karbantartás/módosítás elvégzéséhez szükséges részéhez férhessen hozzá, és csak az engedélyezett tevékenység elvégzéséhez szükséges lehetőségekkel és felhatalmazásokkal rendelkezzen. Ehhez fizikai eszközök (pl. kulccsal zárható irányítástechnikai szekrények, szekrényajtó nyitásérzékelők és jelzők stb.) és számítógépbiztonsági kontrollok (pl. külső adathordozók csatlakoztatásának tiltása, csatlakoztatás naplózása, a használható adathordozók nyilvántartása, azokhoz való hozzáférés adminisztrálása, stb.) is szükségesek lehetnek, erre vonatkozóan az NBSZ 3a.4.5.5100. pontja határoz meg követelményeket. A tevékenység elvégzése után a kiadott jogosultságokat meg kell vonni, a biztonsági rendszereket alaphelyzetbe kell állítani.

Karbantartási programot kell bemutatni, amelynek működtetése hozzájárul a várható meghibásodások megelőzéséhez és biztosítja a rendszerelemek meghibásodási gyakoriságának az előírt korlátok között tartását. A

karbantartási programhoz kapcsolódóan be kell mutatni a karbantartás hatékonyságának folyamatos ellenőrzését támogató módszertant.

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 hardver dokumentációt,

c) a szoftver dokumentáció és kód minden formáját, így többek között a specifikációkat, a tervezési dokumentumokat, a forrás kódokat, a futtatható kódokat, gépi kódokat, könyvtárakat,

d) fejlesztő rendszereket, beleértve a kód generátorokat, fordítóprogramokat, teszt környezeteket és teszt eszközöket,

e) a teszteseteket és eredményeket,

f) a módosításokat és az azokhoz kapcsolódó elemzéseket, valamint

g) az oktatási anyagokat.”

(A követelmény szövege egyértelmű, ezért a követelmény szövegét meghaladó további útmutatás nem szükséges.)