ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM
BOLYAI JÁNOS HADMÉRNÖKI KAR
Hadmérnöki Doktori Iskola

Alapítva: 2002. évben

Neszveda József

APERIODIKUS ALKALMAZÁSÚ KATONAI BERENDEZÉSEK MEGBÍZHATÓSÁGA

Doktori (PhD) értekezés

…….
tudományos témavezető
Dr. Forgon Miklós
nyugállományú okl. mérnök ezredes

2011.

TARTALOMJEGYZÉK

BEVEZETÉS

Az elmúlt évtizedek jellemzője, hogy a mikroelektronika robbanásszerű fejlődése következtében a katonai eszközök egy növekvő csoportjának az a közös sajátossága, hogy elektronikus vagy mechatronikai jellegű, és programozható elektronikát tartalmaz. A Magyar Honvédségnél számos olyan eszköz van rendszerben vagy várható a rendszerbe helyezése, amely így jellemezhető. Ezeket a katonai eszközöket a továbbiakban **katonai berendezés**eknek nevezem. Várható, hogy a katonai berendezések számaránya a jövőben növekszik[1].

A bipoláris világrend megszűnése óta jellemző tendencia a NATO országokban, hogy a nemzeti hadseregek békelétszámai csökkenek. A Magyar Honvédségnél ezt a tendenciát a sorkötelesség eltörlése felerősítette. A kisebb békelétszám kevesebb hadi eszközt működtet, így növekszik azon eszközök száma, amelyek két alkalmazás között, vagy a felhasználást megelőzően **huzamosabb ideig** (hónapokig, esetleg évekig), **üzemen kívül**i állapotban tárolnak.

Ugyanezen időszak jellemzője, hogy gyakoribbá és kiterjedtebbé vált a NATO szerepvállalása a katonai erőt igénylő ENSZ békefenntartó műveletekben. Ezek a műveletek igénylik a raktáron levő eszközök mozgósítását, de értelemszerűen nem évekre előre megtervezettek, vagyis az eszköz használatba vétele **aperiodikus**.

A katonai berendezések egy növekvő csoportjának felhasználása **küldetéses jellegű**: a tényleges feladatvégzés viszonylag rövid időtartamú[2] és a berendezések a feladatvégzést megelőzően vagy két feladatvégzés között több hónapig esetleg évekig **üzemen kívüli** állapotban vannak. A tényleges feladatvégzésre aperiodikusan van igény. A harctevékenységet végző katonai eszköz **biztonság-kritikus** berendezés (SCS[3]), hiszen bármely a feladat végrehajtását akadályozó hiba végzetes lehet és feladatvégzéskor általában nincs mód és/vagy idő a működésbeli hiba elhárítására. A biztonság-kritikus berendezések irányító alapfolyamatait és a vész-, védelmi funkcióit

[1] Az amerikai Védelmi Minisztérium 2007-ben kiadott programjában [1] jelentősen növelte az ember nélküli automatikus vagy fél-automatikus katonai eszközök kifejlesztésére szánt költségvetést.

[2] A küldetéses jellegre a rövid 1 – 10 napos folyamatos üzemelés a jellemző.

[3] SCS: Safety-Critical System: Biztonság-kritikus rendszer. [4], [6], [7]

hardveresen és szoftveresen egybeintegrálva kell megvalósítani. Az ilyen katonai berendezéseket nevezem a továbbiakban **aperiodikus alkalmazású katonai berendezés**eknek[4].

A katonai tervezés részéről egyértelmű igény, hogy **kellő pontossággal lehessen definiálni** a katonai berendezések meghibásodási valószínűségét feladatvégzéskor.

Az automatizált irányító rendszerekben alkalmazott eszközök műszaki megbízhatósága mindig is fontos volt, de az IEC 61508[5] szabvány [2] terjesztette ki a megbízhatóság vizsgálatot a teljes életciklusra (M1 melléklet), vagyis bevonta a megbízhatóság vizsgálatba a berendezés tervezése, a gyártása, és az üzemelése során elvégzendő feladatokat. A nagy megbízhatóságot igénylő folytonos üzemű rendszerek részére fogadták el az IEC 61511 szabvány[6]. Az IEC 61511 amerikai megfelelője az ANSI/ISA-84[7].

Az IEC 61508 és az IEC 61511 szabványok megalkotása az irányító rendszerek komplexitásának növekedése és a megbízhatóság számszerűsítése és ellenőrizhetősége miatt vált szükségessé. Az IEC 61508 és az IEC 61511 szabványok definiálják a **biztonság-sérthetetlenség szint (SIL[8])** fogalmát és a szintek meghatározási módszereit.

Az IEC 61508 előírása szerint: „*Az EUC[9] (irányított berendezés) irányító rendszere el fog különülni és független az E/E/PE vész-, védelmi rendszertől, más technológiák vész-, védelmi rendszertől, és a külső kockázat csökkentő megoldásoktól.*"[2].

Ezen előírást nem lehet betartani a **biztonság-kritikus** (SCS[10]) berendezések vagy rendszerek esetén, ahol az alapfolyamat legkisebb hibája is végzetes lehet.

---

[4] Adott körülmények között ilyen felhasználásúk lehetnek az automata felderítő robotrepülőgépek, a mobilrobotok, az egyszer használatos rádiólokációs zavaró berendezések, illetve a fél-automatikus légvédelmi rakéta komplexumok egyes berendezései, a radarberendezések, a távvezérelt robotok, stb.

[5] Az IEC 61508 szabvány számos iparág és alkalmazás számára egységes nyelvezetet és eljárástechnikát ajánl. Az alapfogalmak bevezetésétől, a szakkifejezések definiálásán keresztül, a számítási és intézkedési eljárások áttekintéséig ad az egyes eszközök, valamint az eszközökből felépített rendszerek megbízhatóságára a szakhatóságok számára ellenőrizhető választ. [2]

[6] Az IEC 61511 szabvány a folytonos technológiák (vegyipar, energia ipar, stb.) és vész-, védelmi rendszereik számára lett kidolgozva. Az első rész az értelmezési területet, a definíciókat, és a hardver és szoftver követelményeket, a második rész az IEC61508 szabvány értelmezését, a harmadik rész a biztonság-sérthetetlenség szint meghatározását tartalmazza. [3]

[7] Az amerikai ANSI/ISA-84. [5] és az IEC 61511 szabvány párhuzamosan fejlődött. A két szabvány közötti eltérés csekély.

[8] Az E/E/PE (elektromos/elektronikus/programozható elektronikus) rendszerhez rendelt biztonsági műveletek sérthetetlenség igényének 4 diszkrét szintje van (egytől négyig). A 4 a legmagasabb, az 1 a legalacsonyabb biztonság sérthetetlenségi szint. [2], [3]

[9] Equipment Under Control

[10] SCS: Safety-Critical System: Biztonság-kritikus rendszer. [4], [6], [7]

Az API 14C[11] [6] és a MIL-STD-882[12] [4] szabványok értelmezik a biztonság-kritikus berendezés fogalmát. Az értekezésemben az amerikai API 14C, és a MIL-STD-882 szabványok biztonság-kritikus berendezésre vonatkozó fogalmait használom.

Az aperiodikusan alkalmazott katonai berendezések megbízhatóság vizsgálatához több szabvány fogalmait kell **összeilleszteni** az alábbi sajátosságok miatt:

- Az IEC 61508 és az IEC 61511 szabvány számos definíciója abból a feltevésből indul ki, hogy a berendezés vagy rendszer meghibásodás hibaaránya az idő függvényében állandó az üzemelési életciklus alatt. Az aperiodikusan alkalmazott berendezésekre ez a feltevés nem igaz.
- Az aperiodikusan alkalmazott katonai berendezések feladat végrehajtása biztonság-kritikus jellegű, azonban az API 14C és a MIL-STD-882 szabványokat a berendezések folytonos üzemelésű illetve batch[13] üzemelésű működtetésre dolgozták ki. Az aperiodikusan alkalmazott berendezések működése nem ilyen, mert az üzemen kívüli állapot jóval hosszabb, mint a tényleges feladatvégzés.
- Az aperiodikusan alkalmazott berendezések esetén az előre tervezhető periodikusan végrehajtott ellenőrző teszt és karbantartás az üzemen kívüli üzemállapotot szakítja meg. A folytonos és a batch üzemeltetés[14] más jellegű ellenőrző tesztet és karbantartást igényel.

A gyártók az általuk szállított eszközhöz természetesen adnak üzemeltetési és karbantartási útmutatót. Ezek jelenleg empirikus tapasztalatokon vagy folytonos, folyamatos üzemeltetést feltételező számításokon nyugszanak. Az általam vizsgált berendezéscsoportra a SIL fogalmához hasonló, akkreditált formula jelenleg nincs.

A PhD értekezésem témája az aperiodikusan alkalmazott katonai berendezések **megbízhatóság** vizsgálatának olyan kialakítása, amely összhangban van a nemzetközi szabványokkal és figyelembe veszi ezen berendezések sajátosságait.

---

[11] Az amerikai API 14C szabvány a különösen nagy biztonság igényű vegyi technológiák számára lett kidolgozva. [6]

[12] A MIL-STD-882 [4] szabvány és előzményei párhuzamosan fejlődött az IEC 61508 szabvánnyal és előzményeivel. Különbség, hogy a MIL-STD-882 szabvány nem vette át a SIL besorolást.

[13] A hosszabb, ismétlődő folyamatos működést rövid karbantartó szünetek szakítják meg.

[14] Az IEC 61508, IEC 61511, ANSI/ISA-84, API 14C, MIL-STD-882 szabványokat erre dolgozták ki.

A munkám során a következő célokat tűztem ki:

1. Az a **hipotézisem**, hogy az általam aperiodikus alkalmazású katonai berendezéseknek elnevezett berendezéscsoport megbízhatóságát nem lehet az eddig kidolgozott módszerekkel vizsgálni[15].
2. Célom a folytonos illetve batch jellegű üzemelésű berendezések SIL mérőszámához hasonlatosan - a szükséges hibavalószínűség számítás **elméleti megalapozás**ával - az aperiodikusan alkalmazott katonai berendezések megbízhatóság számításának kidolgozása és az **MSIL**[16] **osztályozás** definiálása.
3. Hipotézisem szerint az üzemen kívüli üzemmód, periodikus teszt üzemmód, feladatvégzés üzemmód közötti üzemmódváltások a hibavalószínűség állapottér idő-diszkrét leírását igényelik. Az a célom, hogy az átmenet-valószínűség mátrix **konverziójával** modellezhetők legyenek az üzemmódváltások.
4. Az a **hipotézisem**, hogy a hibavalószínűségek megfelelő **korrekciós eljárás**ával modellezhető az üzemen kívüli állapotban elvégzett periodikus tesztek által feltárt és kijavított hibák hatása a hibavalószínűségekre.
5. Célom a megbízhatósági számításokra alkalmas, az aperiodikusan alkalmazott katonai berendezések üzemeltetési sajátosságait kezelő modell **algoritmusának** kidolgozása.
6. Feltevésem szerint az üzemeltetési sajátosságait kezelő modell megalkotásához szükség van az aperiodikusan alkalmazott katonai berendezésekre érvényes **tesztlefedettség** faktor, valamint az **emberi tényező** faktor meghatározására.

---

[15] Az aperiodikusan alkalmazott katonai berendezések feladat végrehajtás üzemmódjának biztonság-kritikus jellege és az üzemeltetésük sajátosságai miatt, az IEC 61508, az IEC 61511, a MIL-STD-882, az ANSI/ISA-84 és az API 14C szabványok számos fogalmát és számítási eljárását **hozzá kell igazítani** az ilyen berendezésekhez.

[16] MSIL: Military Safety Integrity Level: Katonai Biztonság-Sérthetetlenség Szint.

A következő kutatási módszereket alkalmaztam:

1. Tanulmányoztam a megbízhatósággal és a biztonságos működtetéssel kapcsolatos nemzetközi szabványokat és a biztonságos működtetéssel kapcsolatos számítási módszereket. A vizsgálataimat a megfelelő hardverstruktúra kialakítására is kiterjesztettem, mert az elektronikus vagy mechatronikai jellegű berendezések műszaki megbízhatóságát döntően az irányító rendszer elektronikai és elektromechanikai részegységei[17], különösen a végrehajtók határozzák meg.
2. A szakirodalom és az Interneten hozzáférhető publikációk tanulmányozásával, elemzésével bővítettem a kutatási céljaim eléréséhez szükséges elméleti ismereteimet.
3. Összegyűjtöttem és rendszereztem a SIL mérnöki tevékenységgel kapcsolatos hazai és külföldi kutatási tevékenységeket, információkat.
4. A kutatás eredményeit, a felállított téziseket - esettanulmány segítségével - szimulációs vizsgálattal ellenőriztem. Számítógépes szimulációs program futtatásával elemeztem az egyes paraméterek hatását a feladat végrehajtás során várható hibavalószínűségre.
5. A költséghatékony megoldás kiválasztásához tanulmányoztam a biztonság-kritikus kialakításnak eleget tevő hardverstruktúrákat, és ennek figyelembe vételével dolgoztam ki a szimulációs modellt.
6. Kutatási eredményeimet rendszeresen publikáltam szakmai kiadványokban, és tudományos előadásokon.

Az értekezés fejezeteinek tartalma:

I. fejezet

Az aperiodikusan alkalmazott katonai berendezések csoportjának definiálása. A biztonság-sérthetetlenséggel összefüggő tesztlefedettség és az emberi tényező faktorok

[17] A távadók, távadók, és a logikai döntést végző programozható logika áramköri egységei.

hozzáillesztése az aperiodikusan alkalmazott katonai berendezések sajátosságaihoz. A feladatvégzést blokkoló átlagos meghibásodás-valószínűség (PFM_{Bavg}) fogalmának értelmezése és a számítási képletének megadása. Az aperiodikusan alkalmazott biztonság-kritikus katonai berendezések biztonság-sérthetetlenség szint (MSIL) fogalmának értelmezése.

II. fejezet

A kezelhető és a veszélyes hibák viselkedésének vizsgálata a különböző redundáns hardver struktúrákban. A diagnosztika és a hardver redundancia kapcsolatának elemzése. Az aperiodikusan alkalmazott katonai berendezések esetén az irányítási lánc elemeivel és a hardver struktúrával kapcsolatos elvárások áttekintése.

III. fejezet

Az aperiodikusan alkalmazott katonai berendezések műszaki megbízhatóság számítási módszereinek áttekintése. Az üzemeltetés módok átmenet-valószínűség mátrixainak, továbbá az üzemmód-váltások kezelésének levezetése. Az üzemen kívüli állapotot megszakító periodikus ellenőrző teszt hatásának állapot-korrekcióként való értelmezése. Az üzemeléskor érvényes átlagos hibavalószínűség érték számítási algoritmusának és MATLAB programjának megadása.

IV. fejezet

A javasolt számítási módszer alkalmazásának bemutatása a kis-hatótávolságú légvédelmi rakéták TZM berendezésének irányító rendszerén.

Mellékletek:

Életciklus diagramok és kapcsolataik

Meghibásodási ráta szorzófaktorok

Meghibásodási ráta értékek

TESEO modell súlyozó értékei

Végrehajtók

ISA-TR-84.02.00-2002 felépítése

SIF-hez tartozó eszközök, alrendszerek hibatáblázata a Markov gráf szerkesztéséhez

Matlab M fájlok

I. FEJEZET

APERIODIKUSAN ALKALMAZOTT KATONAI BERENDEZÉSEK ÜZEMELÉSÉNEK JELLEMZŐI

Az aperiodikusan alkalmazott katonai berendezéseknek három jellegzetesen eltérő (feladatvégzés, időszakos teszt, üzemen kívüli üzemmód) üzemállapota van. Ez az alkalmazásmód jellegzetesen eltér az elméletileg kellően kimunkált folyamatirányítás, batch irányítás és gyártásautomatizálás alkalmazásoktól.

Ez utóbbi irányító rendszerekben a szabványok által előírt módon, az alapirányítási műveletek és a vész, védelmi rendszer hardveresen és szoftveresen elkülönített, két különálló irányítási rendszer. A két különálló irányítási rendszer eltérő jellegű hibás üzemmódjait sorolja fel [7] szakirodalomból átvett 1. táblázat.

1. táblázat: Hibás üzemmódok

Az alapirányítási rendszer	**A vész, védelmi rendszer**
A beavatkozó eszköz alsó, felső véghelyzetben, vagy kifagyott	Működtetéskor fellépő hiba (Fail-Danger = Veszélyes hiba)
Az irányító kimenet túl alacsony, vagy túl magas szintje (előjelzés)	Késleltetett működés (Fail-Danger = Veszélyes hiba)
A távadó jelének változása, vagy a beavatkozó eszköz reagálása akadozó	Hamis működtetés (Fail-Safe = Kezelhető hiba)
A beavatkozó eszköz reagálása lassú	
A távadó jele alsó, felső véghelyzetben, vagy kifagyott	
A távadó jelének túl alacsony, magas szintje (előjelzés)	
Az irányító kimenet változása túl gyors	

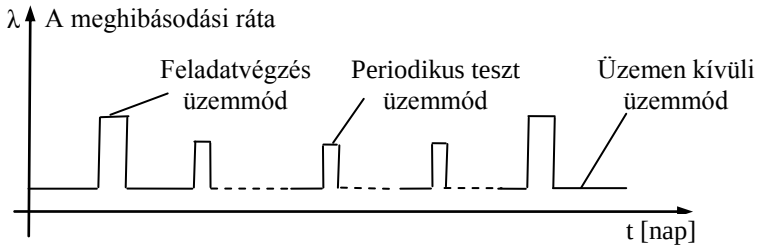
A két különálló irányítási rendszert az indokolta, hogy amíg az alapirányításban a hibajelenséget a kezelőszemélyzet általában azonnal észleli, addig a vész, védelmi rendszerek hónapokig, vagy jó esetben akár több évig sem hajtanak végre beavatkozásokat. A vész, védelmi rendszerek meghibásodása rejtve maradhat, amíg nincs ok a működtetésükre.

Az IEC 61508 és az IEC 61511 szabvány konzekvensen különválasztja és két különböző „időléptékben” tárgyalja a nagy beavatkozás gyakoriságú folytonosan üzemelő alapirányítás és az alacsony beavatkozás gyakoriságú vész, védelmi rendszerek biztonság sérthetetlenség szintjének, és ezen keresztül a műszaki megbízhatóságának fogalmait. Az aperiodikusan alkalmazott katonai berendezésekben nem különül el ez a kétféle üzemmód, mert irányító rendszerük biztonság-kritikusra tervezett. Ugyanakkor eltér a szokásos biztonság-kritikus berendezésektől, mert a feladatvégzés üzemállapot a folytonos technológiák alapirányítási műveleteihez, míg az üzemen kívüli üzemállapot a vész, védelmi rendszer működés módjához hasonló.

Az aperiodikusan alkalmazott katonai berendezések esetén a következő megfontolások alapján nem lehet azonosnak tekinteni az üzemen kívüli, az időszakos teszt, valamint a feladatvégzés üzemállapotok meghibásodás valószínűségét:

- egy-másfél év időintervallumban a szakszerűen tárolt eszközökben az üzemen kívüli üzemállapot, a mechanikai és a hőhatások hiánya miatt, csökkenti a meghibásodás valószínűségét;
- az üzemen kívüli állapotot megszakító teszt üzemmód és a feladatvégzés üzemmód körülményei a végrehajtandó feladatokban és a működési környezetben nem azonosak;
- a berendezés hibáinak javítására, a végrehajtandó feladat időkorlátja miatt, csak nagyon korlátozottan van lehetőség.

Az 1. ábra mutatja a meghibásodási ráta változását a különböző üzemmódokban[18].



1. ábra. A meghibásodás hibaaránya
(Készítette Neszveda József)

A további vizsgálataimban a periodikus teszt üzemmódhoz rendelem a berendezés **normál** üzemelési körülményeihez tartozó λ meghibásodási ráta értéket[19].

[18] Az előbbi felsorolásban szereplő időléptéket csak erősen torzítottan lehetett ábrázolni.

[19] Ezt a berendezés hardver és szoftver összetevőinek meghibásodási rátáiból lehet kiszámítani.

1.1 Aperiodikusan alkalmazott berendezések megbízhatóság vizsgálata és SIL besorolásuk specifikumai

Az aperiodikusan alkalmazott berendezések meghibásodás-valószínűségének változása az idő függvényében indokolja - az IEC 61508, IEC 61511, illetve a MIL-STD-882, API 14C szabványok fogalmaira és módszereire támaszkodva **az** aperiodikusan alkalmazott katonai berendezések **sajátosságainak megfelelően** - néhány fontos fogalom értelmezését.

Az üzembiztos működés szempontjából a legfontosabb kritérium a szűkebb értelembe vett **megbízhatóság**[20]. A megbízhatóság függvény szabványos jelölése R(t). A megbízhatóság az idő függvényében változik. A megbízhatóság komplement fogalma a **hibavalószínűség.** A hibavalószínűség függvény az IEC 61508 szerinti jelölése PF(t). A két fogalom kapcsolata:

$$PF(t) = 1 - R(t) \qquad (1.1)^{21}$$

Egy adott berendezés megbízhatósága, illetve a meghibásodásának valószínűsége közvetlenül méréssel nem határozható meg. Méréssel egy berendezés, vagy a berendezés hardver és szoftver összetevőinek **meghibásodási rátája**[22] határozható meg. A meghibásodási ráta jelölésére a görög kis λ betűt írja elő a szabvány.

A λ meghibásodási ráta meghatározásának mérési eljárásában a vizsgált eszközből N darabot üzemeltetnek folyamatosan. A T_0 időintervallumban a meghibásodott eszközök száma ΔN_{fk}, a továbbra is működő eszközök száma N_{sk}.

A k-adik idő intervallumban λ_k meghibásodási ráta:

$$\lambda_k = \frac{\Delta N_{fk}}{N_{sk}} \left[h^{-1} \right] \qquad (1.2)$$

A fenti mérési eljárást többször végrehajtva egy görbesereg keletkezik, amelyből valószínűség számítási eljárásokkal határozzák meg az eszközre jellemző meghibásodási ráta jelleggörbét. Nagyszámú empirikus tapasztalat alapján a mérés jellegzetes, a 2. ábrán láthatóhoz hasonló, görbét eredményez. A 2. ábrán kezdetben a

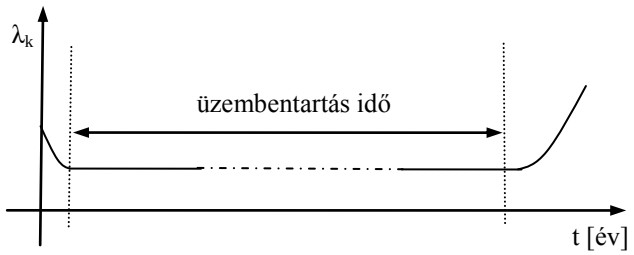
---

[20] Reliability: Megbízhatóság. Az IEC 61508 szerint a megbízhatóság: Egy előre megadott idő intervallumban annak valószínűsége, hogy amikor igény van a tervezett művelet végrehajtására, akkor a rendszer végrehajtja azt, feltéve, hogy a rendszer a megadott határértékeken belül működik. [1]

[21] Probability of Failure: Hibavalószínűség. Az IEC 61508, az IEC 61511, az ANSI/ISA 84, stb. a PF(t) jelölést használja (A magyar szabvány [44] F(t)-vel jelöli.). Az **Értekezésemben nem a magyar, hanem a nemzetközi szabványok** [2], [3], [4], [5], [6], [8], [28], [52] és irodalom [10], [11], [12], [29], [34], [55], stb. jelöléseit alkalmazom. A továbbiakban a közismert képletek forrását **nem jelölöm**.

[22] Failure rate: Meghibásodási ráta (Hibaarány)

hibás alkatrészek és az első üzembehelyezéskor előforduló túlterhelések okozzák a magasabb meghibásodási ráta értéket. Megbízhatóra tervezett berendezések esetén ez a gyártás közbeni minőség-ellenőrzés időszaka. A 2. ábrán a végső magasabb értékeket az anyagfáradás okozza. (Az időlépték torzított.)



2. ábra. A meghibásodási ráta változása
(Készítette Neszveda József)

A λ_k meghibásodási ráta meghatározásának mérési eljárása alapján is kiszámítható az **átlagos meghibásodási idő**[23], amit a szabványok MTTF-el jelölnek: Számos mérés alapján kapott Θ átlagos meghibásodási idő értékekből átlagszámítással határozzák meg az adott eszköz átlagos meghibásodási (MTTF) idejét. Az átlagszámítás módszerére az IEC 61508 szabvány csak a 70%-os statisztikai konfidencia határ betartását írja elő[24], amihez a legtöbb megbízhatóság meghatározásával foglakozó szakkönyv - köztük a [11] is - a Chi-Squared[25] eloszlást és tesztet javasolja.

A meghibásodási ráta különböző átlagszámítási módjai egymástól eltérő eredményt adnak, ezért a λ meghibásodási rátát szolgáltató adatbázisok a meghatározás módja szerint adnak meg értéket. Az 1.5 kifejezés a meghibásodási ráta függvény (2. ábra) jellegzetes formáját alapul véve az MTTF konzervatív [10] számítási módjának megfelelő, ahol az első j időt úgy tekintik, mintha az első j eszköz már az első időintervallumban tönkrement volna.

$$\Theta = \frac{jT_0 + \sum_{i=j}^{j+k} T_i + (N-k-j)T_N}{k} \qquad (1.5)$$

ahol Θ egy konkrét mérés eredménye, $T_0 = 1[h]$ az időalap, az első meghibásodás T_1, a második T_2 időpontban történik, és így tovább T_N-ig, és $T_N > T_{j+k}$.

[23] MTTF: Mean Time To Failure: Átlagos meghibásodási idő.

[24] A hibamódok, és hatásuk analíziséhez elegendő mennyiségű adatra van szükség. A minimum, hogy az egy-oldalas statisztikai konfidencia határ elérje a 70%-ot. [2], [8], [29]

[25] Több exponenciális egymástól független valószínűségi változó négyzet összegének eloszlása.

A végső (N-j-k) működő eszköz T_N működési idejét nagyobbra választják, mint az addig leghosszabban működő eszköz T_{j+k} működési ideje.

Az így számított MTTF érték reciprok értéke a meghibásodási ráta.

$$\lambda = 1/\mathrm{MTTF}\left[\mathrm{h}^{-1}\right] \tag{1.6}$$

Számos adatbázis közli az elektronikus és mechanikus eszközök, berendezések meghibásodási rátáját. Az adatbázisok az üzembenntartás alatti közel állandó[26] meghibásodási ráta értéket adják meg. Az Értekezés a FARADIP[27] [9] adatbázist alkalmazza. A 3. sz. melléklet néhány eszköz λ meghibásodási ráta értékét tartalmazza.

A λ meghibásodási ráta mérési elvéből következik, hogy a további számítások alapját képező λ meghibásodási rátát T_0 időperiódusokban határozzuk meg. A szabványokban a T_0 időperiódus egy óra λ_H=1 [h^{-1}] vagy 1 év λ_L=1 [$year^{-1}$].

$$\lambda_L\left[\mathrm{year}^{-1}\right] = 8{,}76\cdot 10^3 \cdot \lambda_H\left[\mathrm{h}^{-1}\right] \qquad \text{(Egy év 8760 óra.)} \tag{1.7}$$

Az 1 év időperiódussal számított λ_L meghibásodási ráta azonban származtatott mennyiség, vagyis nincs akadálya a λ_H 1 óra értékből kiindulva – 1.7 kifejezéshez hasonlóan átszámítva - tetszőleges időalap használatának.

Az adatbázisok az átlagos gyártási és üzemelési körülményekre adják meg az eszközök, berendezések meghibásodási rátáját. A gyártás közbeni minőségellenőrzést, illetve a különböző üzemelési körülményeket szorzó faktorokkal veszik figyelembe. A szorzófaktorokat a 2. sz. mellékletben tüntettem fel. A hardver és szoftver összetevőinek meghibásodási rátáiból az IEC 61078 [8] szabványban megadott Megbízhatóság blokkdiagram módszerrel határozható meg egy konkrét berendezés meghibásodási rátája.

Minél komplexebb egy rendszer, annál jobban képes elkerülni a teljes leállást, mert redundáns vagy ritkán használt eszközök meghibásodása esetén nem minden hiba juttatja működésképtelen állapotba a rendszert.

A μ javítási ráta a definíció szerint:

$$\mu = 1/\mathrm{MTTR}\left[\mathrm{h}^{-1}\right] \tag{1.8}$$

ahol az MTTR[28]: a meghibásodott berendezéseknek átlagos helyreállítási ideje

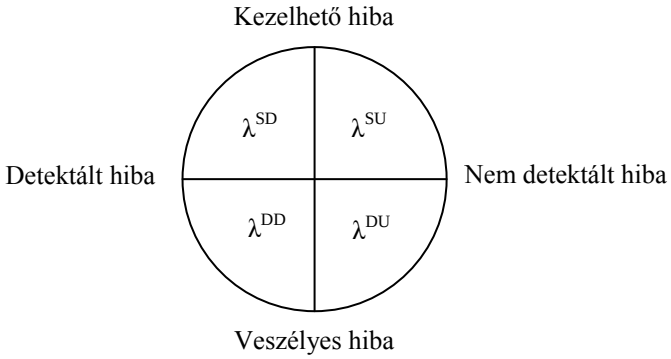
[26] A közel állandó érték exponenciális eloszlásra utal.

[27] FAilure RAte Data In Perspective

[28] MTTR: Mean Time To Repair: Átlagos javítási idő.

A folytonos technológiák üzemelési gyakorlatának megfelelően az MTTR érték helyett, az adott technológiára és üzemvitelre jellemző, a hiba észlelésétől, a helyreállítás befejezéséig terjedő (MDT[29]) értéket szokás alkalmazni. Az MTTR és a MDT értékek szintén valószínűségi változók, amiket helyreállítási kísérletekkel határoznak meg.

Mivel a komplex elektronikus rendszerekben a hibák hatása az üzemelés-megbízhatóságára eltérő, ezért a hibák feloszthatók kezelhető és veszélyes hibákra[30]. Természetesen, hogy egy hiba kezelhető-e, vagy veszélyes-e az a hardver kialakítástól és a működtetés módjától függ. A hibák egy másik csoportosítás szerint - mivel a hibák egy része felszínre kerül az ellenőrző tesztek időpontjaiban, vagy programozható eszközök esetén a diagnosztizáláskor, vagy az előírt karbantartás végrehajtásakor – a hibák lehetnek detektáltak és nem detektáltak.



3. ábra. A meghibásodási ráta felosztása
(Átvéve: [12])

Az előbbi csoportosítás szerint a hibák négyféle típusba, és így a berendezés teljes λ meghibásodási rátája négy részre bontható[31].

$$\lambda = \lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU} \tag{1.9}$$

ahol λ^{SD} a kezelhető és detektált, λ^{SU} a kezelhető és nem detektált, λ^{DD} a veszélyes és detektált, λ^{DU} a veszélyes és nem detektált hibaösszetevő.

---

[29] MDT: Mean Dead Time: Átlagos kiesett idő, ami mindig nagyobb, mint az MTTR, mert magába foglalja a hiba észlelésétől a helyreállítás megkezdéséig tartó időintervallumot is.

[30] Az IEC 61508 definíciói: A kezelhető hiba (safe failure) nem juttatja a rendszert veszélyes vagy működésképtelen állapotba. [1] A veszélyes hiba (dangerous failure) a rendszert veszélyes vagy működésképtelen állapotba juttatja. [1]

[31] Az 1.9 kifejezésben az egyes hibatípusok előfordulási száma van viszonyítva az összes hiba számához, és ez az arány határozza meg a hibatípusok felosztásának arányait, vagyis a 3. ábrától eltérően a hibatípusok előfordulási aránya nem egyenlő.

Az IEC 61508 szabvány elvárása[32], hogy a rendszer meghibásodása **exponenciális eloszlást** kövessen! Ez a feltevés elsődlegesen az analitikus (időben folytonos) analízis szempontjából fontos. A numerikus szimuláció - amit az értekezésben alkalmazok - elvileg megkerülhetővé teszi ezt a megkötést. Azonban az értekezésben használom a Markov-modellt, amely explicite feltételezi az exponenciális eloszlást [13], [34], [45].

A katonai berendezések jól tervezettek, nagyszámú részegységei gyártásközben egyedi ellenőrzésen mennek keresztül, így a teljes életciklus alatt a berendezés bármely részegységének előírásszerű működése nem okozhat hibát egyik részegységben sem. Ebből következően az **exponenciális eloszlás feltevése** megengedhető [2], [45], [46].

A berendezés üzemelés életciklusa alatt (2. ábra) a λ meghibásodási ráta állandó. Időben folytonos vizsgálatakor exponenciális eloszlás esetén [4], [10] a berendezés megbízhatóságának időbeli lefolyása az 1.10. kifejezéssel adható meg:

$$R(t) = e^{-\lambda t} \tag{1.10}$$

Az 1.10 kifejezés felhasználásával a berendezés várható élettartama[33] (T_{LE}) az 1.11 kifejezéssel határozható meg:

$$T_{LE} = \int_0^{\infty} R(t)dt \tag{1.11}$$

Ugyancsak az 1.10 kifejezés felhasználásával a berendezés hibavalószínűsége:

$$PF(t) = 1 - R(t) = 1 - e^{-\lambda t} \tag{1.12}$$

Az **átlagos hibavalószínűség**[34] PF_{avg} számítása a folytonos idejű rendszerekben:

$$PF_{avg} = \frac{1}{T}\int_0^{T} PF(t)\,dt \tag{1.13}$$

Az IEC 61508 szabvány vezette be a megkülönböztetést az alacsony működtetés igényű[35] és a magas működtetés igényű[36] üzemmód között.

---

[32] Jól tervezett rendszerben a részegységek tervezett együttműködése nem okoz hibát, vagyis az egyes részegységek meghibásodása független egymástól. [1]

[33] T_{LE}: lifetime expectancy: várható élettartam

[34] PF_{avg}: average Probability of Failure: átlagos hibavalószínűség

[35] Low Demand Mode: Alacsony működtetés igényű üzemmód, ahol a működtetési igény gyakorisága nem nagyobb, mint évente 1, illetve nem nagyobb, mint az ellenőrző tesztek közötti idő kétszerese években mérve per év. [1]

[36] High Demand Mode: Magas működtetés igényű üzemmód az, ahol a működtetési igény gyakorisága nagyobb, mint évente 1, illetve folyamatos működtetés, valamint ha a működtetés igény nagyobb, mint az ellenőrző tesztek közötti idő kétszerese években mérve per év. [1]

A magas működtetés igényű berendezéseket a kezelőszemélyzet folyamatosan figyeli és intézkedik. Ilyenkor a veszélyes hibák hibavalószínűségének (PF_D [h^{-1}]) átlaga a megbízhatóság mérőszáma. A PF_{Davg}[37] értékének meghatározása:

$$PF_{Davg} = \frac{1}{T}\int_0^T PF_D(t)\,dt \qquad (1.14)\ [3], [5]$$

Az alacsony működtetés igényű berendezés vagy rendszer (pl.: vész-, védelmi rendszerek, vagy ritkán működtetett eszköz) hibás állapota akkor derül ki, amikor igény van a működtetésükre. A hibavalószínűség működtetéskor[38] (PFD [$year^{-1}$]) annak a valószínűsége, hogy az alacsony működtetés igényű rendszer nem működik előírás szerint egy potenciálisan veszélyes helyzetben. Az **átlagos hibavalószínűség működtetéskor** PFD_{avg}[39] az alábbi kifejezéssel adható meg:

$$PFD_{avg} = \frac{1}{TI}\int_0^{TI} PFD(t)\,dt \qquad (1.15)$$

ahol a „TI" a bizonyító erejű tesztek[40] közötti időintervallum.

Ez a két fogalom nem pusztán az időalapban különbözik! A PFD, mint valószínűségi változó, tartalmazza, hogy a hiba sokáig rejtve maradhat. Ennek oka, hogy a magas működtetés igényű irányítási rendszerben (pl.: alapirányítás) fellépő potenciálisan veszélyes helyzet (hazárd) nem igényli automatikusan az alacsony működés igényű irányítási rendszer (pl.: vész-, védelem) a működtetését, vagyis a két esemény egymástól független.

Előfordul, hogy a vész-, védelmi rendszer hibája nem létező veszélyhelyzetet jelez, és ennek hatására feleslegesen működik, ami a berendezés vagy rendszer leállását okozza. A hamis leállás átlagos valószínűsége $PF_{avg}^{spurious}$[41] értéke az alábbi:

$$PF_{avg}^{spurious} = \frac{1}{TI}\int_0^{TI} PFS(t)\,dt \qquad (1.16)$$

A 1.16 kifejezésben az PFS [$year^{-1}$] a hamis leállás valószínűsége[42].

---

[37] PF_{Davg} : average Probability of dangerous Failure: a veszélyes hibák átlagos hibavalószínűsége

[38] PFD: Probability of Failure on Demand: átlagos hibavalószínűség működtetéskor

[39] PFD_{avg}: average Probability of Failure on Demand: átlagos hibavalószínűség működtetéskor

[40] Proof test: bizonyító erejű teszt. A bizonyító erejű teszt a hibák felderítése céljából végrehajtott periodikus teszt a biztonságosra műszerezett rendszerben, amely mintha új lenne, vagy amennyire praktikusan lehetséges állapotba állítja vissza a rendszert. [3]

[41] $PF_{avg}^{spurious}$: Average spurious Probability of failure: Hamis leállás átlagos valószínűsége

Az IEC 61511 és az ANSI/ISA 84 szabványokban a PF_{Davg} és a PFD_{avg} értelmezése feltételezi, hogy az irányítási rendszerben elkülönül az alapirányítás irányítási rendszere és a vész, védelem irányítási rendszere. Ezek a szabványok külön táblázatban adják meg az alacsony (2. táblázat) és a magas (3. táblázat) működtetés igényű üzemmódokhoz tartozó SIL értékeket.

2. táblázat: Alacsony működtetés igényű üzemmód SIL értékei

SIL	Alacsony működtetés igényű üzemmód (Az átlagos hibavalószínűség működtetés igényekor) A T_0 időalap 1 év.
4	$10^{-4} > PFD_{avg} \geq 10^{-5}$
3	$10^{-3} > PFD_{avg} \geq 10^{-4}$
2	$10^{-2} > PFD_{avg} \geq 10^{-3}$
1	$10^{-1} > PFD_{avg} \geq 10^{-2}$

3. táblázat: Magas működtetés igényű vagy folytonos üzemmód SIL értékei

SIL	Magas működtetés igényű vagy folytonos üzemmód (A veszélyes hibák átlagos valószínűsége) A T_0 időalap 1 óra.
4	$10^{-8} > PF_{Davg} \geq 10^{-9}$
3	$10^{-7} > PF_{Davg} \geq 10^{-8}$
2	$10^{-6} > PF_{Davg} \geq 10^{-7}$
1	$10^{-5} > PF_{Davg} \geq 10^{-6}$

Az aperiodikusan alkalmazott katonai berendezések **feladatvégzés üzemmód**jában nem engedhető meg feladatvégzést blokkoló hiba, hiszen katonai művelet végrehajtása közben bármilyen késlekedés vagy üzemzavar végzetes lehet. Ezért az aperiodikusan alkalmazott katonai berendezések irányító rendszerének megbízhatóság vizsgálatakor az alapirányítás átlagos hiba valószínűségét PF_{Davg}, a vész, védelem átlagos működési

[42] PFS: Probability of Failing Safely: Biztonságos leállás valószínűsége.

igénykor fellépő hiba valószínűségét PFD_{avg}, és a hamis leállás átlagos valószínűségét $PF_{avg}^{spurious}$ **együttesen** kell figyelembe venni.

A hamis leállás feladatvégzés üzemmódban veszélyes. Nem lehet a két hibaok valószínűséget ($PF_{avg}^{spurious} + PF_{Davg}$) együtt integrálni a 1.14 kifejezés szerint akkor sem, ha ez csak a feladatvégzés időtartamára terjed ki. Ennek oka, hogy a feladatvégzés megkezdésekor érvényes kezdeti meghibásodási ráta érték meghatározásához a periodikus tesztekkel megszakított üzemen kívüli időszak meghibásodás valószínűségének **időbeli változás**át is figyelembe kell venni. Ezt az értéket a tárolási idő hossza és az üzemen kívüli állapotot megszakító teszt gyakorisága, valamint az időszakos tesztek hiba felderítési hatékonysága befolyásolja.

Ezért azt javaslom:

- az aperiodikusan alkalmazott katonai berendezések átlagos meghibásodás valószínűségének meghatározásba **vonjuk be** a feladatvégzés kezdetéig az utolsó teszt óta eltelt időt;
- az IEC 61511 és az ANSI/ISA 84 szabványok a 2. és 3. táblázat alkalmazásához csatolt kiegészítő megjegyzései közül az 5. számú kiegészítő megjegyzés **küldetési idő**[43] fogalmát felhasználva a feladatvégzés kezdetéig az utolsó teszt óta eltelt idő és a feladatvégzési idő legyen az aperiodikusan alkalmazott katonai berendezések küldetési ideje.

A PF_{Davg} és a PFD_{avg} számítása egybevonható és elvégezhető akár a 1.14 akár az 1.15 kifejezéssel [14]S[44]. Ennek feltételei:

- az 1 óra, illetve az 1 év helyett egy közös időalapot kell választani, és a közös időalapnak megfelelő értékkonverziót kell végrehajtani;
- az 1.14 kifejezésben szereplő T, illetve az 1.15 kifejezésben szereplő TI időállandók helyett, összhangban a hamis leállás átlagos valószínűségét $PF_{avg}^{spurious}$ figyelembe vételével, az aperiodikusan alkalmazott katonai berendezések küldetési idejére kell elvégezni az integrálást;
- figyelembe kell venni, hogy az üzemen kívüli állapot periodikus tesztekkel

[43] Egy megbízhatóra és korlátozott idejű küldetésre tervezett E/E/EP berendezés, amely nem javítható a küldetés alatt, SIL értékének meghatározása a következő: Meg kell határozni a küldetési idő alatti hibavalószínűségek átlagértékét, majd ezt kell osztani a küldetési idővel. Ezután az óránkénti hibavalószínűséget definiáló táblázatot (esetünkben az 3. táblázat) kell alkalmazni. [1]

[44] Az „S” betű itt és a továbbiakban a saját cikket, illetve kifejezést jelöli.

történő megszakítása más jellegű, mint a működésre kész, de igény híján nem működő vész-, védelmi rendszerek periodikus tesztekkel történő ellenőrzése.

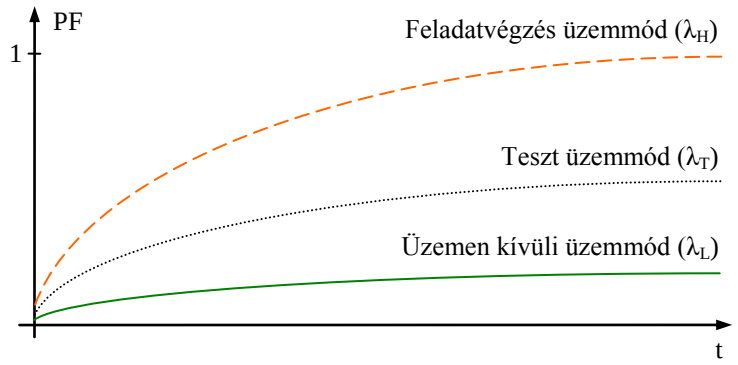
Az aperiodikusan alkalmazott katonai berendezések nemcsak az üzemmódok váltogatásában, az eltérő időalapú hibavalószínűségek együttkezelésében, és a „hamis" leállás figyelembevételében térnek el az IEC 61508, IEC 61511 és az ANSI/ISA 84 szabványok definícióitól. További különbségek:

- A feladat végrehajtásának körülményei folytán még redundáns hardver architektúra esetén **sincs mód**, vagy idő[45] feladatvégzés üzemmódban a javításra.
- Az IEC 61508 tesztlefedettség (DC) fogalma nem alkalmazható[46], ezért a **szabványtól eltérően** kell értelmezni a tesztlefedettség fogalmát.

Az előbbi okok következtében, a **hipotézisemnek megfelelően**, az aperiodikusan alkalmazott katonai berendezések sajátosságait figyelembe véve kell értelmezni a biztonság-sérthetetlenség szint és az átlagos meghibásodás valószínűség fogalmait.

1.2 Meghibásodási ráta ugrások hatása

A 4. ábrán a valós arányokat erősen torzítva, egy koordináta rendszerben ábrázoltan látható, hogy folyamatos feladatvégzés üzemmód (szaggatott vonal), folyamatosan végzett teszt (pontozott vonal), és állandó üzemen kívüli állapot (folytonos vonal) esetén hogyan változnak a berendezés hibavalószínűség görbéi[47].



4. ábra. Üzemmódváltás hatása
(Készítette Neszveda József)

[45] A kezelő személyzettől fizikailag távol telepített eszköz, amelynek a távvezérelhető funkciói korlátozottak.

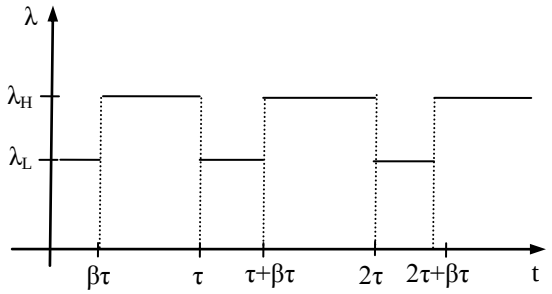
[46] A DC a szabvány definíciója szerint a detektált és az összes veszélyes hiba aránya.

[47] A 4. ábra görbéihez állandó λ_H, λ_T, és λ_L hibaarány értékek tartoznak a berendezés életciklusa alatt.

A 4. ábrán nem látható, hogy teszt üzemmód után, vagyis a hibák felderítése és kijavítása után, a meghibásodás valószínűség javul. A 4. ábra azt a mindennapi (kvalitatív) tapasztalatot tükrözi, hogy az erősebb igénybevétel hamarabb vezet hibához.

Az üzemmód-váltásokat az aktuális hibavalószínűségben történő **ugrásszerű változás**ként lehet figyelembe venni. A 1.12 kifejezésből adódóan az aktuális hibavalószínűségben történő ugrásszerű változás visszavezethető λ meghibásodási ráta ugrásszerű változására.

A λ meghibásodási ráta szezonálisan történő ugrásszerű változásainak analitikus kezelésére a [15] tanulmány közöl javaslatot. A megközelítés hasznos a szezonálisan váltakozó terhelésű berendezések, például a vízcsőhálózatok, fűtési rendszerek, stb. meghibásodás valószínűségének elemzésére.



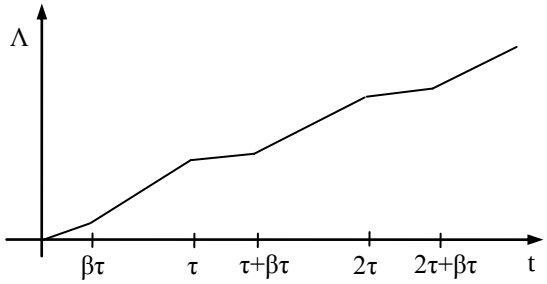
5. ábra. Váltakozó meghibásodási ráta
(Átvéve: [15])

Az 5. ábrán a τ a periódus idő (pl.: 1 év), a β az eltérő meghibásodási rátájú szezon (pl.: tél) aránya a teljes periódus időn belül, a λ_H a nagyobb és a λ_L a kisebb igénybevételhez tartozó meghibásodási ráta.

A tanulmány bevezeti a meghibásodási ráta integrált értékét:

$$\Lambda = \int_0^t \lambda(t)dt \qquad (1.17)\ [15]$$

A meghibásodási ráta integrált értékének grafikus megjelenítése a 6. ábrán látható.



6. ábra. A váltakozó meghibásodási ráta integrált értéke
(Átvéve: [15])

Így az 1.11 kifejezésbe behelyettesítve az 1.10 kifejezés 1.17 kifejezéssel módosított értékét a T_{LE} várható élettartam:

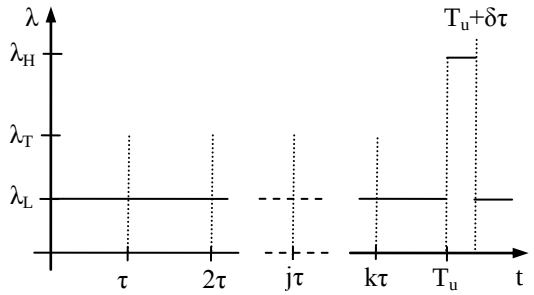
$$T_{LE} = \int_0^{\infty} e^{-\Lambda t} dt \qquad (1.18)\ [15]$$

Bevezetve az $A = \exp\ -\tau\ \lambda_H + \beta(\lambda_L - \lambda_H)$ segédváltozót, amit alkalmazva a várható élettartam zárt képlete:

$$T_{LE} = \frac{1}{1-A}\left\{\frac{1-\exp\ -\lambda_L \beta\tau}{\lambda_L} - \frac{1-\exp\ -\lambda_H \beta\tau}{\lambda_H}\left[\exp\ -\lambda_L \beta\tau\ \right]\right\} \qquad (1.19)\ [15]$$

A szezonális meghibásodási ráta változások analitikus vizsgálata során feltételezzük, hogy a berendezés várható T_{LE} élettartama alatt a λ_L, és a λ_H értékek állandók, valamint a $\beta\tau$, és a τ állandó időtartamok.

A λ_L, és λ_H állandó értékének feltételezése az 2. ábra életciklus fogalma, és a 4. ábra alapján természetes. A $\beta\tau$, és a τ értékek természetes szórása azonban csak akkor elhanyagolható, ha a $\beta\tau$, illetve a τ idők viszonylag nagyok a T_0 időalaphoz képest, ami vízcsőhálózatok, fűtési rendszerek, stb. megbízhatóság vizsgálatakor, amikor több hónap aránylik az egy órához teljesül.



7. ábra. Aperiodikusan alkalmazott katonai berendezések váltakozó meghibásodási rátája
(Készítette: Neszveda József)

A 7. ábrán a τ a periodikus tesztek közötti időtartam, a T_u a feladatvégzés kezdete, a λ_H a feladatvégzéshez, a λ_T a tesztekhez, és a λ_L az üzemen kívüli állapothoz tartozó meghibásodási ráta.

Az aperiodikusan alkalmazott katonai berendezések meghibásodási ráta váltakozása (7. ábra) lényegesen eltér a szezonális meghibásodási ráta változásoktól (5. ábra), aminek következtében:

- nincs figyelembe véve, hogy feladatvégzés üzemmód kezdő időpontja nem illeszkedik a periódusba, azaz $T_u \neq (k+1)\tau$;

- a várható élettartam (1.19 kifejezés) „A” segédváltozójának alkalmazásakor kerekítési problémát vet fel, hogy a teszt üzemmód időtartama rövid a periodikus teszt gyakoriságához képest $\beta \approx 1$, és $\beta\tau \approx \tau$;
- nincs figyelembe véve, hogy a teszt üzemmód eredménye csökkenti a hibavalószínűséget.

Az előbbiek miatt az **analitikus** vizsgálat **nem alkalmazható** az aperiodikusan alkalmazott katonai berendezések műszaki megbízhatóság vizsgálatához. Mint azt feltételeztem **időben diszkrét numerikus** vizsgálati módszert célszerű alkalmazni.

A fentieken kívül az is az időben diszkrét numerikus vizsgálati módszer alkalmazását veti fel, hogy az átlagos hibavalószínűség üzemen kívüli időszakban és az átlagos hibavalószínűség feladatvégzéskor kiszámítása eltérő időalapon történik, és hogy az aperiodikusan alkalmazott katonai berendezések műszaki megbízhatóság vizsgálatában egyidejűleg mindkét értéket figyelembe kell venni. Az időben diszkrét numerikus vizsgálati módszer hátránya, hogy nem adható meg zárt képlettel.

Az időben diszkrét vizsgálatkor[48] a megbízhatóság kT_0 időperiódusban:

$$R(k) = PS^k \qquad \{ PS = R(1) \} \tag{1.20}$$

ahol: PS a sikeres működés valószínűsége[49].

Miután a berendezés üzemelés életciklusa alatt a λ meghibásodási ráta állandó, a meghibásodás valószínűség eloszlása exponenciális [13], és $\lambda \ll 1$:

$$R(1) = e^{-\lambda T_0} = 1 - \lambda T_0 + \frac{1}{2}\lambda^2 T_0^2 - \frac{1}{6}\lambda^3 T_0^3 + \cdots \approx 1 - \lambda T_0 \tag{1.21}$$

Ebből adódóan a $PS = R(1) = 1 - \lambda T_0$.

Az időben diszkrét vizsgálatkor az egyes időperiódusokban a hibavalószínűség:

$$PF(k) = 1 - R(k) \tag{1.22}$$

$$PF(1) = 1 - R(1) = 1 - 1 + \lambda T_0 = \lambda T_0 \tag{1.23}$$

Az 1.21 kifejezéssel számítható a PF_{avg} **átlagos hibavalószínűség** a diszkrét idejű, exponenciális eloszlású rendszerekben:

$$PF_{avg} = \frac{1}{kT_0}\sum_{i=1}^{k} PF(i) = \frac{1}{kT_0}\sum_{i=1}^{k} 1 - \left(1 - \lambda T_0\right)^i \tag{1.24}$$

---

[48] Az 1.20 kifejezéssel a megbízhatóság értéke gyorsabban csökken az idő függvényében, mint az 1.10 analitikus kifejezés alkalmazásakor. Ezáltal a diszkrét idejű vizsgálat szigorúbb feltételeket szab.

[49] PS: Probability of Successful operation: Sikeres működés valószínűsége

1.3 Aperiodikusan alkalmazott katonai berendezések biztonság-sérthetetlenség szintje

Az 1.1 fejezetben kifejtett üzemmód-váltásból és üzemmód-jellegből eredő eltérések miatt az aperiodikusan alkalmazott katonai berendezések átlagos meghibásodás valószínűségének megállapítása az általam definiált **PFM_{avg}**[50] értékből történik [16]S.

A **PFM_{avg}** definiálása a következő:

Legyen T_u a feladatvégzés megkezdődéséig eltelt idő:

$$T_u = n \cdot m \cdot T_0 + k \cdot T_0 \qquad (1.25)S$$

ahol: $T_0 = 1\ h$, „n” a periodikus tesztek száma, „mT_0” két teszt közötti üzemen kívüli állapot időtartama, és „kT_0” az utolsó teszt és a feladatvégzés kezdete közötti időintervallum.

A PFM_{avg} számításában figyelembe vett PF meghibásodás valószínűségek egyaránt tartalmazzák a veszélyes és a kezelhető hibákból származó leállásokat.

Az utolsó teszt és a feladatvégzés kezdete közötti átlagos hibavalószínűség:

$$PF_{Lavg} = \frac{1}{kT_0} \sum_{i=n\cdot m}^{n\cdot m+k} PF_L(i) \qquad (1.26)S$$

Feladatvégzéskor átlagos hibavalószínűség, ahol j az üzemórák száma:

$$PF_{Mavg} = \frac{1}{jT_0} \sum_{i=n\cdot m+k}^{n\cdot m+k+j} PF_M(i)\,. \qquad (1.27)S$$

Az 1.26 kifejezés alkalmazásához elengedhetetlen a kezdeti hibavalószínűségének $PF_L(n \cdot m)$ meghatározása. Az üzembehelyezés kezdetétől a vizsgált időintervallum kezdetéig $(n \cdot m \cdot T_0)$ üzemen kívüli állapotban romlik a berendezés megbízhatósága. Ugyanezen időintervallumban végzett tesztek viszont növelik a megbízhatóságot. Ezek a tesztek azonban költség- és időkorlátok miatt nem **bizonyító erejű teszt**ek, vagyis a berendezés nem kerülhet majdnem új állapotba.

A $PF_L(n \cdot m)$ meghatározáshoz szükség van annak ismeretére, hogy a teszt milyen mértékben deríti fel a hibákat. Az üzemen kívüli állapotot megszakító ellenőrző teszt során a detektált hibák kijavításra kerülnek, ezért az ellenőrzött részegységek, és a műveletek aránya befolyásolja a teszt által detektálható hibák arányát. Ennek mértékét a C_M **tesztlefedettség** határozza meg.

---

[50] PFM_{avg}: average Probability of Failure in Mission: Aperiodikusan alkalmazott berendezés átlagos hibavalószínűsége feladat végrehajtáskor

Az IEC 61508, IEC 61511 és az ANSI/ISA 84 szabványok a tesztlefedettség (DC[51]) értékét a berendezés minden részegységére, a tesztre rendelkezésre álló időtartam[52] alatt detektált, veszélyes λ_{DD} meghibásodási ráta és az összes veszélyes λ_{Dtotal} meghibásodási ráta arányaként definiálja.

Hipotézisemnek megfelelően ez nem alkalmazható az aperiodikusan alkalmazott katonai berendezésekre, mert a periodikus tesztnek nincs szoros időkorlátja, és mert a hamis leállás is veszélyes hiba.

Értekezésemben az aperiodikusan alkalmazott katonai berendezések tesztlefedettségét az irányítási rendszer ellenőrzött részegységei és műveletei, valamint az összes részegység és művelet hányadosaként határoztam meg:

$$C_M = \frac{\sum \lambda_{0D}(\text{ellenőrzött részegység} + \text{ellenőrzött művelet})}{\sum \lambda_0(\text{részegység} + \text{művelet})} \qquad (1.28)S$$

ahol a részegység a rendszer közös hibajellemzőkkel leírt része; a művelet a berendezés által a feladatvégzés üzemmódban megkívánt feladatsor; a λ_{0D} meghibásodási ráta az összes (kezelhető és a veszélyes) detektált hiba mérőszáma; a λ_0 meghibásodási ráta az összes (detektált és nem detektált) hiba mérőszáma.

Amennyiben $PF_{BL}(i)$ azon állapotok valószínűségének összege[53], amelyek a feladatvégzés kezdetekor azonnal meghiúsítják a berendezés működését, úgy az 1.26 kifejezés a következőképpen módosul:

$$PF_{BLavg} = \frac{1}{kT_0} \sum_{i=n\cdot m}^{n\cdot m+k} PF_{BL}(i). \qquad (1.29)S$$

Amennyiben pedig a $PF_{BM}(i)$ azon állapotok valószínűségének összege, amelyek feladatvégzés közben meghiúsítja a berendezés működését, vagy veszélyeztetik a kezelő személyzetet, akkor az 1.27 kifejezés a következőképpen módosul:

$$PF_{BMavg} = \frac{1}{jT_h} \sum_{i=n\cdot m+k}^{n\cdot m+k+j} PF_{BM}(i). \qquad (1.30)S$$

---

[51] DC: Diagnostic Coverage [2], [3], [5] $DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$

[52] diagnostic test interval [2], [3], [5]

[53] A kritikus üzembiztonságú irányítórendszerek redundáns architektúrájúak, mert a redundáns architektúra lehetővé teszi az irányítórendszer csökkentett üzemmódú működését. A csökkentett üzemmódú működés nem hiúsítja meg a feladat végrehajtását, mert ha a redundáns részegységből az egyik meghibásodik, a másik elegendő a feladat végrehajtásához. Egy redundáns rendszer az i-edik időperiódusban különböző valószínűséggel üzemel a lehetséges állapotai közül az egyikben.

Az aperiodikusan alkalmazott katonai berendezések üzemmódja változik a vizsgált időintervallumban, és ebből adódóan az átlagos hibavalószínűség vizsgálata két időintervallumra bontható. Üzemmódváltáskor (T_u időpontban) a λ meghibásodási ráta értékben ugrásszerű változás van, ezért:

$$PF_{BLavg}(n \cdot m + k) < PF_{BMavg}(n \cdot m + k) \qquad (1.31)S$$

A 1.32 kifejezés az $(nm+k)T_0$ időperiódusban a nagyobb (az 1.31 relációnak megfelelően a PF_{BMavg}) értéket tartalmazza:

$$PFM_{Bavg} = \frac{\sum_{i=n \cdot m}^{n \cdot m+k-1} PF_{BL}(i)}{kT_0} + \frac{\sum_{i=n \cdot m+k}^{n \cdot m+k+j} PF_{BM}(i)}{jT_0} \qquad (1.32)S$$

ahol a PFM_{Bavg} az üzemelést blokkoló átlagos hibavalószínűség[54].

Az MSIL érték bevezetését a következő megfontolások indokolják:

- Az eltérő időalapú hibavalószínűségek együttkezelése és a „hamis" leállás figyelembevétele sokkal szigorúbb feltételt szab, mint az IEC 61508 és az IEC 61511 szabványok.
- A feladat végrehajtás körülményei okán az **összes** (alapirányítási és vész-, védelmi) **funkció**ra együttesen kell megállapítani a meghibásodás valószínűség értéket. Ez azt jelenti, hogy az összes távadó, a logikai döntéshozó, és valamennyi végrehajtó a megbízhatóság vizsgálat része. Az IEC 61508 és IEC 61511 szabványok SIL értelmezése szerint csak a vész-, védelmi láncban **egy konkrét** biztonsági funkcióra[55] (SIF) kell megállapítani a SIL értéket.
- A katonai berendezéseknek feladatvégzéskor általában tucatnál több funkciót kell ellátniuk és ezek együttes megbízhatósága számít.

Az általam javasolt **MSIL** értékhatárokat a 4. táblázat tartalmazza. A 4. táblázat határértékei úgy lettek megválasztva, hogy ha a 10 - 30 végrehajtót[56] működtető aperiodikusan alkalmazott katonai berendezés egy-egy művelete a 2. vagy a 3. táblázat

---

[54] PFM_{Bavg}: average Probability of Balk Failure: az üzemelést blokkoló átlagos hibavalószínűség. A PFM_{Bavg} érték magába foglalja a PFD_{avg}, a PF_{Davg} , és a $PF_{avg}^{spurious}$ értékeket.

[55] Egy biztonsági funkciót általában 1 végrehajtó, 1 – 3 távadó, és a logikai döntéshozó néhány csatornája valósítja meg.

[56] A $PFM_{Bavg} = 5 \cdot 10^{-5}$ értelmezhető úgy, hogy 2000 alkalommal végrehajtott egy hét időtartamú feladatvégzés esetén egy hiba fordulhat elő az irányító rendszerben.

szerint SIL-2, akkor ez a berendezés a javaslatom szerinti eljárással az MSIL-2 kategóriába kerüljön.

4. táblázat: Az aperiodikusan alkalmazott katonai berendezések MSIL értékei

MSIL	Aperiodikus működtetés igényű üzemmód (Az üzemelést blokkoló hibák átlagos valószínűsége) A T_0 időalap 1 óra.
4	$10^{-6} > \mathrm{PFM}_{\mathrm{Bavg}} \geq 10^{-7}$
3	$10^{-5} > \mathrm{PFM}_{\mathrm{Bavg}} \geq 10^{-6}$
2	$10^{-4} > \mathrm{PFM}_{\mathrm{Bavg}} \geq 10^{-5}$
1	$10^{-3} > \mathrm{PFM}_{\mathrm{Bavg}} \geq 10^{-4}$

1.4 Emberi tényező

Az emberi tevékenység okozta hiba[57] modellezésére számos, ugyanarra a helyzetre eltérő eredményt szolgáltató eljárás terjedt el. Az emberi hibák jelentős része következmény nélküli. A nem kívánatos hatást előidéző emberi hiba csak a hibásan működtetett vagy működni hagyott eszközök komplex hibavalószínűség analízisével (pl.: hibafa analízis, Markov-modell, stb.) állapítható meg. **Összességében** az emberi tényező **növeli** a hibavalószínűséget. A jól felépített vész-, védelmi rendszer és a jól kidolgozott kezelői taszkok az emberi tényező hatását vagy semlegesítik, vagy jelentősen csökkentik.

A HEART[58] az embert a rendszer egységeként kezeli. Előnye, hogy az emberi meghibásodási rátát a determinisztikus megbízhatóság számítási eljárásokba lehet illeszteni. Az UK-ban és az USA-ban számos tanulmány kísérelte meg számszerűsíteni az ember okozta hibát. Elsődlegesen a nagy folytonos technológiák (erőművek, különös figyelemmel a nukleáris erőművekre, vegyi üzemek, stb.) kezelőszemélyzetének

[57] Az ember okozta hiba IEC 61508 szerinti definíciója: Olyan emberi beavatkozás, vagy a beavatkozás elmaradása, amely nem tervezett hatással jár. [1]

[58] HEART: Human Error Assessment and Reduction Technique. Emberi hibák mérésének és csökkentésének technikája [50], [51], [58].

tevékenységét elemezve alkottak egy kezelői tevékenység listát. Ezeket az adatbázis értékeket a HEART módszer alkalmazza. Az emberi hiba adatbázisok a tevékenységi listákhoz (taszkokhoz) rendelnek emberi hiba gyakoriságot. Egy adott taszk előfordulási gyakorisága technológiáról technológiára változik, így az adatbázisban szereplő adatokból csak részletes tevékenység elemzéssel lehet meghatározni az adott taszkhoz tartozó emberi hibaarányt. Az ember okozta hiba szintén felosztható kezelhető és veszélyes hibára.

A THERP[59] a körülményeket vizsgálja, hogy javaslatot tehessen azok javítására, és így növelje a megbízhatóságot. Az ember szubjektív objektum. Ezért, ha konkrét körülmények között működő berendezés esetén kell meghatározni az emberi hiba valószínűségét, akkor a THERP eljárás szellemében az adatbázisok által publikált adatokat az alábbi befolyásoló tényezőkkel célszerű módosítani:

- a fizikai környezet, munkaszervezési környezet, személyes kapcsolati környezet;
- a kezelőszemélyzet kiválogatásának módja, kiképzése és továbbképzése;
- személyes vagy külső körülmények okozta stressz.

Az emberi hibához vezető okokat empirikusan elemezve a hibavalószínűség növekedésének mértékére a TESEO[60] módszer szorzófaktorokat definiál.

A már felsoroltakon kívül a megbízhatóság számításban széleskörűen alkalmazott eljárás még: SLIM[61], API[62], IDA[63], HCR[64]. Az ember okozta hiba figyelembe vételére kidolgozott modellek egymástól szemléletükben és céljaikban is különbőznek.

Egyes vélemények vitatják azt, hogy az ember okozta hibát független hibaként lehet kezelni, mert véleményük szerint a kezelőszemélyzet leggyakrabban abban hibázik, hogy az irányítórendszerben fellépő hibára későn vagy rosszul reagál. „*A körülményeket változtasd, ne az embert*” [17] mottóval írt könyv a környezeti, kiképzési, stb. feltételeket nyolc csoportba sorolva azt vizsgálta, hogyan növeli meg az eredendően

---

[59] THERP: Technique for Human Error Rate Prediction: Az emberi hibaarányt előrebecslő technika [34], [51].

[60] TESEO: Empirical Technique To Estimate Operator Error: Empirikus eljárás a kezelői hiba meghatározására. [17], [58].

[61] SLIM: Success Likelihood Index Method. A siker valószínűsége index módszer.

[62] API: Absolute Probability Judgment: Abszolút valószínűség megítélése.

[63] IDA: The Influence Diagram Approach. Hatásdiagram közelítés.

[64] HCR: Human Cognitive Reilability Correlation: Emberi észlelés megbízhatóság korreláció.

berendezés vagy rendszer hibát, illetve szervezési vagy kiképzési hiányosságot a kezelőszemélyzet tévedése. Ezen iskola által vizsgált nyolc csoport:

- egyszerű kihagyás, emberi figyelmetlenség okozta balesetek;
- balesetek, amelyek jobb képzéssel és instrukciókkal talán elkerülhetők;
- a fizikai vagy mentális képességek hiánya okozta balesetek;
- balesetek a nem megfelelő utasítások követése következtében;
- balesetek, amelyek jobb menedzsmenttel megelőzhetők lettek volna;
- balesetek, amelyek jobb karbantartással megelőzhetők lettek volna;
- balesetek, amelyek jobb berendezés konstrukcióval megelőzhetők lettek volna;
- balesetek, amelyek jobb üzemeltetési technikával megelőzhetők lettek volna.

Miután az aperiodikusan alkalmazott katonai berendezések üzemmódváltásait amúgy is a meghibásodási ráta ugrásszerű változásával képezem le, ezért az ember okozta hiba vizsgálható úgy, hogy a **h_A emberi hibatényező** faktorral szorozva megnő a λ meghibásodási ráta ugrásszerű változásának mértéke[65].

A küldetés végrehajtás körülményeinek **négy** jellegzetes esetére dolgoztam ki a súlyozó tényezőket[66]. A négy jellegzetes esetet önkényesen, de az aperiodikusan alkalmazott katonai berendezések alkalmazásmódját figyelembe véve alakítottam ki. A hozzájuk tartozó súlyozó tényezőket az 5. táblázat tartalmazza.

Az 5. táblázatban a jól motivált és kiválóan felkészített kezelőszemélyzet meghatározás azt feltételezi, hogy az aperiodikusan alkalmazott katonai berendezések kezelőszemélyzete az alkalmasságot figyelembe vevő kiválogatáson és hatékony kiképzésen ment keresztül, valamint folyamatos továbbképzésen vesz részt. A munkaszervezés katonás és a katonai parancsok - a megfelelő csoportmunka érdekében - úgy alakítja ki az együttműködő csoportokat, hogy a személyes emberi kapcsolatokban sem legyen feszültség. Az 5. táblázatban a nem kiválóan, de kellően felkészített személyekkel kiegészített kezelőszemélyzet azt jelenti, hogy nem volt lehetőség a legszigorúbb alkalmassági vizsgára és nem volt elegendő idő a csoport összeszoktatására.

---

[65] Az ember okozta hiba meghibásodási ráta változásként való figyelembe vétele a TESEO eljárás szemléletét alkalmazza.

[66] Az 5. táblázatban feltüntetett h_A hibaarány növelő tényező értékek a TESEO eljárás súlyozó értékei (4. sz. melléklet) felhasználásával készültek.

5. táblázat: A küldetés végrehajtás körülményei

A kezelőszemélyzet és az eszköz alkalmassága	h_A
Jól motivált és kiválóan felkészített kezelőszemélyzet, valamint optimálisan felkészített eszköz.	1,112
Jól felkészített eszköz, és személyes konfliktussal nem terhelt, jól felkészített kezelőszemélyzet	1,224
Nem kiválóan, de kellően felkészített személyekkel kiegészített kezelőszemélyzet, és elvárhatóan felkészített eszköz	1,640
Nem kiválóan, de a feladat végrehajtására képes kezelőszemélyzet és elvárhatóan felkészített eszköz.	3,560

Az aperiodikusan alkalmazott berendezések esetében **csak feladatvégzés üzemmódban kell figyelembe venni az ember okozta hibát.** Feladatvégzéskor az emberi hibák növelik a hibavalószínűséget, viszont az üzemen kívüli üzemállapotban nincs ember által okozott hiba. Periodikus tesztek alkalmával előfordulhat emberi hiba, azonban többnyire következmény és időkorlát nélkül[67] javítható, ezért a további vizsgálatokban emberi hibától mentesnek tekintem a periodikus teszt üzemmódot.

1.5 Összefoglalás és következtetések

A fejezetben rámutattam, hogy megbízhatóság számítási szempontból az elmúlt évtizedek tendenciai szükségessé tették egy speciális katonai berendezéscsoport definiálását az alábbi módon:

Az aperiodikusan alkalmazott katonai berendezések **küldetéses** feladatvégzésű, katonai célú és ezért valamennyi hibaokot **együtt kezelő**, **biztonság-kritikus**ra tervezett, programozható elektronikus vagy mechatronikai jellegű eszköz.

A definíció kifejtése:

- az aperiodikusan alkalmazott katonai berendezések tényleges feladatvégzése viszonylag rövid (1 – 10 nap) időtartamú és folyamatos üzemmódú;

[67] Ha ez nem okoz komoly anyagi vagy személyi sérülést.

- két feladatvégzés között az eszköz hónapokig nem működik, az irányító berendezése üzemen kívüli állapotban van.
- a feladatvégzések között periodikusan végzett 1 – 2 napos ellenőrző teszt célja a műszaki megbízhatóság növelése;
- feladatvégzéskor bármilyen a feladat végrehajtását gátló ok végzetes lehet ezért az alapirányítás irányító rendszerének átlagos veszélyes hiba valószínűséget PF_{Davg}, a vész, védelem átlagos működési igénykor fellépő hiba valószínűséget PFD_{avg}, és a hamis leállás átlagos valószínűségét $PF_{avg}^{spurious}$ **együttesen** kell figyelembe venni;
- a feladatvégzés küldetéses jellegű és csak a feladatvégzéskor előforduló hibák kritikusak, mert a periodikus teszt üzemállapotokban keletkező hibák nem veszélyeztetik a küldetés végrehajtását.

Az eltérő üzemmódok következménye, hogy az aperiodikusan alkalmazott katonai berendezések **meghibásodási rátája nem állandó** az üzembenntartás életciklus alatt. Megállapítottam, hogy az aperiodikusan alkalmazott katonai berendezések **üzemmód-váltás**ai az aktuális hibavalószínűségben történő **ugrásszerű változás**ként vehető figyelembe. Ugyancsak a hibavalószínűség ugrásszerű változásaként kezelhető az **emberi tényező okozta** hiba.

Bemutattam, hogy e sajátosságokból adódóan az aperiodikusan alkalmazott katonai berendezések megbízhatóságának mérőszámaként nem lehet alkalmazni az IEC 61508 és az IEC 61511 szabványok definiált SIL értékeket és az ehhez szükséges PF_{Davg} és PFD_{avg} fogalmakat.

Az aperiodikusan alkalmazott **katonai célú** berendezések hibavalószínűség mértékére bevezettem a $\mathbf{PFM_{Bavg}}$ fogalmat.

A PFM_{Bavg} számításakor az alábbi peremfeltételek érvényesek:

- az aperiodikusan alkalmazott katonai berendezéseket **küldetéses működésre tervezett** rendszernek tekintjük. A küldetési idő magába foglalja az utolsó teszt óta eltelt időt és a feladatvégzési időt;
- a PFM_{Bavg} tartalmazza **valamennyi hibaok** hibavalószínűségét, amely blokkolja a feladatvégzés üzemmódot és így megakadályozhatja a katonai tevékenység sikeres végrehajtását, vagyis magába foglalja a PFD_{avg}, a PF_{Davg} , és a $PF_{avg}^{spurious}$ értékeket és figyelembe veszi az üzemen kívüli üzemállapotban végzett periodikus tesztek hatását és az ember okozta hibát;

- az aperiodikusan alkalmazott katonai berendezések **biztonság-kritikusra** tervezettek, ezért valamennyi műveletének együttes meghibásodás valószínűségével kell számolni.

Az **1.32 kifejezés**sel **megadtam** a PFM_{Bavg} számítási képletet. A számításokban szereplő hibavalószínűségek magukba foglalják a tesztlefedettség és az emberi hiba tényezőket.

Rámutattam, hogy a folytonos technológiák üzemelés közbeni ellenőrző tesztje és az aperiodikusan alkalmazott katonai berendezések üzemen kívüli állapotát megszakító ellenőrző tesztje közötti különbségek miatt nem lehet alkalmazni az IEC 61508, IEC 61511 és az ANSI/ISA szabványok μ javítási ráta és DC tesztlefedettség fogalmait.

Az üzemen kívüli üzemállapotot megszakító ellenőrző teszt hatékonyságának definiálására megalkottam és **az 1.28 kifejezéssel definiáltam** a PFM_{Bavg} kezdeti értékének kiszámításához szükséges $\mathbf{C_M}$ **tesztlefedettség** fogalmat.

Definiáltam a λ meghibásodási ráta ugrásszerű változásaként figyelembe vehető, és így a PFM_{Bavg} számítási módszerébe illeszthető **emberi tényező** faktorokat.

Az aperiodikusan alkalmazott katonai berendezések alkalmazásmódjához illeszkedve a berendezés műszaki állapotának és a kezelőszemélyzet kiképzettségének figyelembe vételére **négy** feladat végrehajtás helyzetet definiáltam az **5. táblázat**ban, és meghatároztam a négy feladat végrehajtás helyzetet jellemző $\mathbf{h_A}$ tényezőt.

A $\mathbf{PFM_{Bavg}}$ számítási módszere indokolja az aperiodikusan alkalmazott katonai berendezések megbízhatóságának mérőszámaként az **MSIL** érték bevezetését. Az általam javasolt és a **4. táblázat**ban megadott MSIL határértékek összhangban vannak az IEC 61508, IEC 61511 és az ANSI/ISA szabványok SIL érték határértékeivel.

II. FEJEZET
APERIODIKUSAN ALKALMAZOTT KATONAI BERENDEZÉSEK HARDVER STRUKTÚRÁJA

A berendezések megbízhatóságát redundáns hardver kialakítással szokás növelni. Számos szakkönyv és értekezés a „megbízhatóság blokkdiagram RBD[68]" módszerrel vizsgálja a passzív redundancia hatását a megbízhatóságra. Az RBD nem tesz különbséget a hibatípusok között, emiatt nem alkalmazható a diagnosztikai képességgel rendelkező redundáns hardverstruktúra vizsgálatára.

A hardver redundancia elemzésekor abból a felismerésből kell kiindulni, hogy a redundáns rendszerek nem egyformán reagálnak a kezelhető (Safe), és a veszélyes (Dangerous) hibákra. Vizsgálataim alapján, amit a cikkemben [31]S már publikáltam, a redundáns rendszerekben a kezelhető[69] és a veszélyes[70] hiba valószínűségének számszerűsítésére **kontaktus logikát** alkalmazhatunk. A 6. táblázat[71] a redundancia nélküli és a leggyakrabban alkalmazott redundáns rendszerekre tartalmazza ezt a kontaktus logikát[72].

A 6. táblázatban a redundancia hatásának számszerűsítése okán abból a feltevésből indultam ki, hogy a résztvevő eszközök meghibásodási rátája: $\lambda = 0{,}02$ és a kezelhető meghibásodási ráta[73] SFF = 0,9.

---

[68] RBD: Reliability Block Diagram: Megbízhatóság blokkdiagram.

[69] A berendezésben fellépő kezelhető (Safe) hibát alaphelyzetben zárt kontaktus reprezentálja. Ha bekövetkezik a hiba, akkor a kontaktus bont és a létraágban megszűnik a gerjesztés. A létraág nem működteti az eszközt, így nincs közvetlen veszély és a működés hiány azonnal megjelenik a kezelőszemélyzet vagy automatikusan működő berendezés esetén a diagnosztizáló hardver számára, így kezelhető.

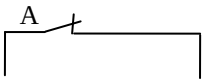
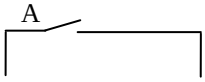
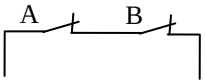
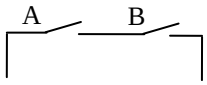
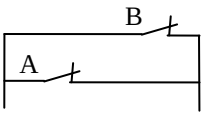
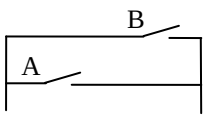
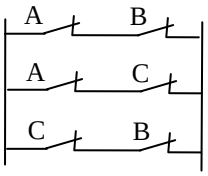
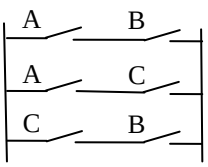
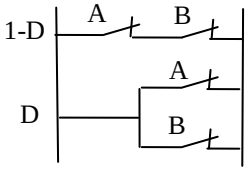
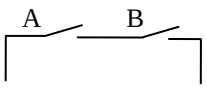
[70] A berendezésben fellépő veszélyes (Dangerous) hibát alaphelyzetben nyitott kontaktus reprezentálja. Amikor bekövetkezik a hiba a kontaktus zár, ami gerjeszti a létraágat és így azonnal veszélyes helyzetet teremt, amit csak a berendezés azonnali vészleállításával lehet elkerülni.

[71] Megjegyzés: A 6. táblázatban a λ és az MTTF értékek valószínűségváltozók. Az MTTF nem azt jelenti, hogy az eszköz várhatóan a táblázatban megadott időtartamig nem hibásodik meg! Példaképpen: annak kockázata (λ [year^{-1}]), hogy egy egészséges 20 éves fiatal a következő három napban meghal, olyan csekély, hogy reciprok (MTTF) értéke több ezer évre jön ki. Természetesen senki sem él több ezer évig.

[72] A kiinduló ötletet a [7] szerzőpárosától vettem át. A rajzokat magam készítettem, és a számértékeket én határoztam meg.

[73] SFF: Save Failure Fraction: Biztonságos hibaarány (a 2.1 fejezetben található 2.1 kifejezés definiálja.)

6. táblázat: A kezelhető és a veszélyes hiba viselkedése redundáns rendszerekben

Kezelhető hiba		Veszélyes hiba	
1001 (Egy válasz az egyre)			
	$\lambda_E=\lambda_A$ =0,02 MTTF=1/ λ_E = 50 év		$\lambda_E=\lambda_A$ =0,02 [74]MTTF=1/ λ_E = 50 év
1002 (Egy közös válasz kettőre)			
	$\lambda_E=\lambda_A+\lambda_B$ =0,04 MTTF=1/ λ_E = 25 év		$\lambda_E=\lambda_A*\lambda_B$ =0,0004 MTTF=1/ λ_E = 2500 év
2002 (Válasz bármelyik a kettő közül)			
	$\lambda_E=\lambda_A*\lambda_B$ =0,0004 MTTF=1/ λ_E = 2500 év		$\lambda_E=\lambda_A+\lambda_B$ =0,04 MTTF=1/ λ_E = 25 év
2003 (Válasz, ha háromból kettő)			
	$\lambda_E=$ $(\lambda_A+\lambda_B)*(\lambda_A+\lambda_C)*(\lambda_C+\lambda_B)$ =0,000064 MTTF=1/ λ_E = 15625 év		$\lambda_E=$ $\lambda_A*\lambda_B+\lambda_A*\lambda_C+\lambda_C*\lambda_B$ =0,0012 MTTF=1/ λ_E = 833 év
1002D (Egy közös válasz kettőre diagnosztikával)			
	$\lambda_E=(1\text{-SFF})(\lambda_A+\lambda_B)$ +SFF* $\lambda_A*\lambda_B$ MTTF=1/ λ_E = 227,2 év		$\lambda_E=\lambda_A*\lambda_B$ =0,0004 MTTF=1/ λ_E = 2500 év

A vizsgált struktúrák közül az 1001 struktúra jellemzi a nem redundáns berendezést.

[74] Indoklás az 1.1 fejezetben

Az 1002 redundáns struktúrában az egyik eszköz hibája vagy hibajelzése leállítja a berendezést. Ez veszélyes hiba esetén hasznos, de kezelhető hibánál a felesleges leállás a nem redundáns berendezéshez képest rontja a megbízhatóságot.

A 2002 redundáns struktúrában mindkét eszköz egyidejű meghibásodása vagy hibajelzése állítja le a rendszert. Ez kezelhető hiba esetén hasznos, de veszélyes hiba bekövetkezésekor megengedhetetlen, mert a jelzőeszköz hibája végzetes lehet.

A 2003 redundáns struktúrában két eszköznek kell meghibásodnia vagy hibajelzést küldenie, hogy leálljon a rendszer. Ez kiegyensúlyozott megbízhatóságot eredményez, de nagyon költséges megoldás.

A 6. táblázatból kiolvasható, hogy az előbb felsorolt, huzalozott logikával is megvalósítható, redundáns struktúrák közül a kezelhető és a veszélyes hibákra egyaránt csak a 2003 redundancia javítja a megbízhatóságot.

Az elmúlt 30 évben a mikroelektronikai eszközök effektív teljesítménye több nagyságrenddel nőtt, miközben áruk jelentősen csökkent. A hardveres és szoftveres **diagnosztikai** kártyával bővített redundáns működésre képes programozható elektronikák alkalmazása költség-hatékony megoldást eredményez. Az 1002D redundáns struktúrában a diagnosztizáló kártya felismeri a kezelhető hibákat és engedi a megmaradt rendszert működni [24]. A 6. táblázatban foglalt számszerűsített értékek egyértelműen reprezentálják, hogy a nem redundáns struktúrához képest az 1002D redundáns struktúra a veszélyes hibákra az egyik leghatékonyabb és a kezelhető hibák esetén is jelentősen javítja a megbízhatóságot.

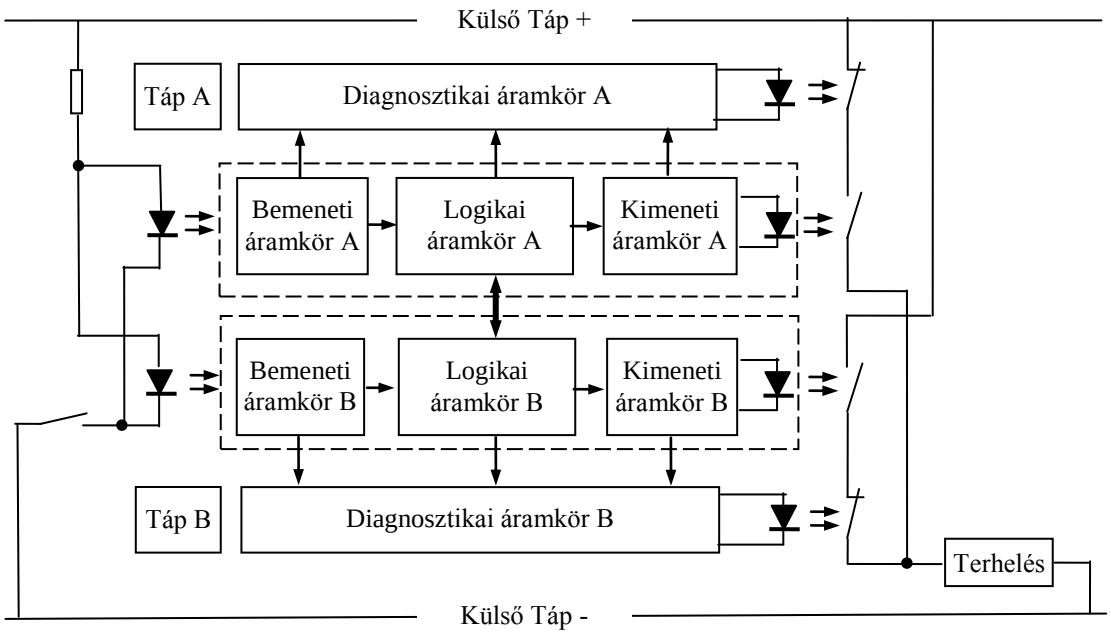
Az 1002D struktúra alkalmazására a 90-es évek közepén hívták fel a SIL mérnökök figyelmét. Egy FMEDA[75] technikát alkalmazó vizsgálatban [18] - alkatrész szintig lebontva - demonstrálták az eljárás alkalmasságát. Az 1002D struktúra nagy előnye, hogy a mikroelektronika fejlődésével egyre költséghatékonyabbá válik.

2.1 1002D hardverstruktúra

A 8. ábrán egy kétállapotú érzékelő kontaktusa működtet egy kétállapotú végrehajtót egy 1002D hardver elrendezésű logikai vezérlőn keresztül. Az „A” és a „B” csatorna áramkörei párhuzamosan működnek. A logikai funkciót végző CPU-k összehangoltan mindig azonos utasítást futtatnak, vagyis az „A” és a „B” csatorna is aktív. A

[75] FMEDA: Failure Mode Effect and Diagnostic Analysis: Hibahatás és diagnosztika analízis

legfontosabb hibákat (pl.: tápkimaradás) minden ipari kivitelű vezérlőben áramkör figyeli. A hibák közötti kölcsönhatások elemzéséhez, vagyis a veszélyes hibák kiszűréséhez intelligens (CPU-t, memóriát tartalmazó) diagnosztikai áramkör kell. A diagnosztikai áramkörök folyamatosan figyelik a bemeneti, logikai, kimeneti áramköröket és amennyiben veszélyes hibát észlelnek valamely áramkörükben, akkor blokkolják a saját csatornájuk kimenetét, miközben a hibátlan csatorna tovább működhet. Ha eltérő eredmény van az azonos funkciót végző be- vagy kimeneten, akkor az egyik biztos hibás, amit a megfelelő diagnosztika dönt el.



8. ábra. 1002D hardverstruktúra egy csatornára
(Készítette: Neszveda József)

A diagnosztikai áramkör képességét az SFF arányszám[76] adja meg. Az SFF biztonságos meghibásodási ráta függ a diagnosztikai kártya, és a vele együttműködő CPU képességeitől. Az SFF értéke a λ hibaaránnyal kifejezve:

$$SFF = \frac{\lambda^{SU} + \lambda^{SD} + \lambda^{DD}}{\lambda^{Total}} \qquad (2.1)$$

Az IEC 61511 szabvány a megbízhatóság mérőszámaként kezelt SIL besoroláshoz hozzárendeli a hardverhiba tolerancia minimum táblázatot (7. táblázat).

[76] Az IEC 61511 definíciója: Egy berendezés összes véletlen hardver hibáinak azon része, amely kezelhető vagy veszélyes, de detektált hiba. [3]

7. táblázat: Programozott elektronikák hardverhiba tolerancia minimuma [3]

SIL	**Hardverhiba tolerancia minimum**		
	SFF < 60%	60% < SFF < 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Különleges előírások (lásd: IEC 61508)		

A 7. táblázat azt mutatja meg, hogy milyen mértékű hardver redundancia szükséges a kívánt SIL érték eléréséhez:

„0”: Nem redundáns a rendszer.

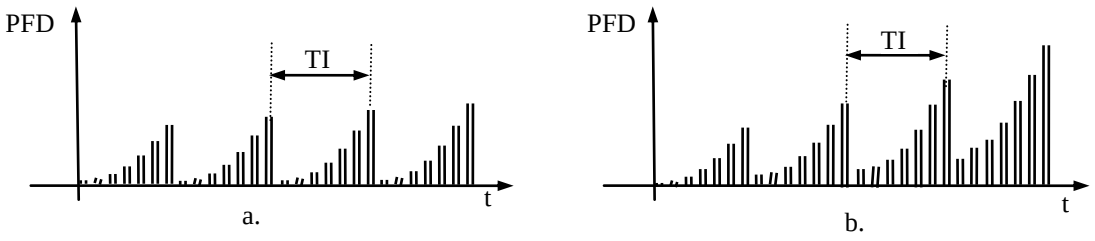
„1”: Redundáns 1002 struktúra. Kettő azonos érték kell a működtetéshez.

„2”: Redundáns 1003 struktúra. Legalább kettő azonos érték kell a működtetéshez.

„3”: Redundáns 1004 struktúra. Legalább három azonos érték kell a működtetéshez.

A 7. táblázat nem különbözteti meg a programozható és a huzalozott kialakításokat, de értelemszerűen az intelligencia nélküli eszközök, valamint az alsó kategóriás vezérlők (mikrokontroller, vezérlő relé, stb.) SFF szintje 60% alatti [53].

A hardverhiba tolerancia minimum fogalom bevezetésére azért volt szükség, mert az alacsony működtetés igényű rendszer SIL értékének meghatározásakor a PFD_{avg} definíciójában (1.15 kifejezés) szereplő „TI” periodikus teszt intervallumra a szabvány nem tesz megkötést.



9. ábra. A hibavalószínűség változása az időben
(Készítette: Neszveda József)

Tökéletes és gyakori tesztet feltételezve elérhető a 9.a. ábrán látható „mintha új lenne” hibavalószínűség. Az öregedés, kopás, rejtett anyaghibák, stb. következtében ez a valóságban nem realizálható, továbbá a túl gyakori teszt (a „TI” mértékének csökkentése) elfogadhatatlan költségnövekedést okoz. A valósághoz jobban közelít a 9.b. ábra, ahol a teszt nem képes helyreállítani a kezdő állapotot.

A közepes 60% < SFF < 90% érték közepes és nagy teljesítményű kereskedelmi forgalomban levő kommersz logikai vezérlőkkel döntően a logikai vezérlő egységben futó szoftveres megoldásokkal teljesíthető[77]. Nagy SFF > 90% érték eléréséhez azonban intelligens **diagnosztizáló áramkör**re, van szükség.

2.2 Biztonságosra műszerezett rendszer

Egy biztonságosra műszerezett rendszer[78] (SIS) felbontható irányítási láncokra. Legegyszerűbb esetben az irányítási lánc távadó, logikai feladatmegoldó és beavatkozó soros kapcsolata. Az irányítási lánc ezen összetevői komplett készülékek. A teljes rendszer megbízhatósága függ összetevőinek megbízhatóságától és a rendszer struktúrától. Az alkalmazott készülékek bármelyike lehet redundáns.

A biztonságosra műszerezett rendszerben alkalmazott készülékek hibaállapotai:

- kezelhető hibaállapot[79]: Ez nem teljesen azonos az IEC 61508 kezelhető hiba jelentésével, mert nem a veszélyes hiba komplement párja. A SIL mérnökök több részre bontották a kezelhető hibát. A kezelhető hibaállapot, amikor a hibás vagy a hamis riasztás miatt leállna a rendszer, de a biztonság architektúra megakadályozza ezt. Rendszer szinten a készülékek kezelhető hibaállapot arányát célszerű meghatározni;
- következmény nélküli hibaállapot[80]: Előfordulhat olyan meghibásodás a készüléken belül, ami nem akadályozza annak működését. Ezt a hibaállapotot a kezelhető és nem detektált hibák közé sorolják, mert nem veszélyes, sőt nem is észleli a rendszer;
- bejelentés hibaállapot[81]. Ebben a hibaállapotban nem működik az automatikus diagnosztika, és erről berendezéstől függően küld, vagy nem küld jelzést[82];

---

[77] Ennek figyelembe vételével igaz a következő állítás: Nem szükséges egyedi fejlesztésű vezérlő berendezés, mert a kereskedelmi forgalomban levő ipari kivitelű PLC-k alkalmasak nagy megbízhatóságot igénylő katonai eszközök (pl.: mobilrobotok) irányítására. [19].

[78] SIS: Safety Instrumented System: biztonságosra műszerezett rendszer. Az IEC 61511 szabvány szerint Egy biztonságosra műszerezett rendszer távadó(k), logikai feladatmegoldó-(k), végrehajtó(k) kombinációiból áll. A SIS egy vagy több biztonsági funkciót hajt végre. [3].

[79] Fail-Safe: Kezelhető hibaállapot

[80] No effect: Következmény nélküli hibaállapot

[81] Annunciation: Bejelentés hibaállapot

- veszélyes hibaállapot. Ez megegyezik az IEC 61511 szabvány veszélyes hiba fogalmával.

Vizsgálataim alapján egyértelmű kritérium, hogy az aperiodikusan alkalmazott katonai berendezések irányító rendszere biztonság-kritikus kialakítású legyen. Ezért valamennyi távadóját, beavatkozóját és a vezérlő berendezést úgy kell megválasztani, hogy biztonsági funkció megvalósítására is alkalmas legyen.

2.2.1 Távadók

Ha egy távadót biztonsági funkcióra is javasol a gyártója, akkor az FMEDA jegyzőkönyvet, amely tartalmazza a megbízhatóság számításához szükséges meghibásodási ráta értékeket, elérhetővé kell tenni a felhasználók számára[83]. A készülékgyártók az FMEDA jegyzőkönyvet vagy saját maguk készítik el, vagy valamely minősítő szervezettel készíttetik el. A jegyzőkönyv a 2 – 3 oldalas, és az adatközlésen túl a vizsgálat fontos körülményeit, és a távadó alkalmazásának megkötéseit is közli.

Az első példa a [20] internet címen elérhető Rosemount 3051S nyomástávadó FMEDA jegyzőkönyve (készült 2003. szeptember, készítette: Exida).

A Rosemount 3051S nyomástávadó egy kétvezetékes C generációs (HART-os[84], 4 – 20 mA-es) távadó. A jegyzőkönyv állítása szerint a Rosemount 3051S nyomástávadó - annak ellenére, hogy egy összetett, sok alrendszerből álló készülék - önmagában is képes a SIL2 megvalósítására. A Rosemount 3051S nyomástávadókat redundáns párban alkalmazva[85] a SIL3 is elérhető.

A jegyzőkönyv a 10. ábrán látható blokkdiagramot, a hibatáblázatot (8. táblázat) és a hibapartíciók kiosztását (9. táblázat), valamint megkötéseket tartalmazza.

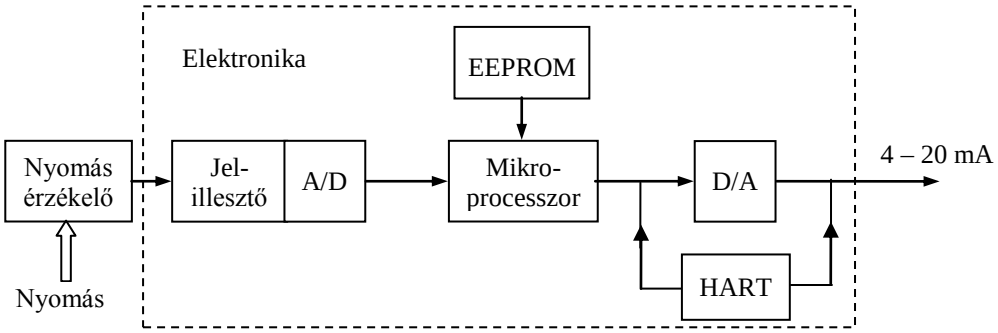
---

[82] Az a hibaállapot ritka. De a diagnosztika hiánya lehet veszélyes hatású. Ezért meg kell fontolni, hogy a vizsgált berendezés esetében a kezelhető, vagy a veszélyes hibaállapotok közé legyen sorolva. A legkorrektebb megoldás, ha külön hibaállapotként modellezik.

[83] A „Safety Equipment Reliability Handbook, Volume 1.” [23] több száz távadó hibaarány adatát tartalmazza.

[84] (HART: Highway Addressable Remote Transducer): Ráültetett jellel távolról címezhető távadó.

[85] Számos biztonság-mérnök állítja: Az ok, amely miatt két azonos típusú, önmagában is összetett rendszert alkotó, készülék meghibásodik, nagy valószínűséggel közös ok, ami rontja a megbízhatóságot [21], ezért ellenzik, hogy ugyanazon gyártótól származzon az azonos feladatot ellátó, redundáns párt alkotó készülékek. A Szerző osztja ezt a véleményt.



10. ábra. Rosemount 3051S blokkdiagramja [20]
(Átrajzolta: Neszveda József)

8. táblázat: A Rosemount 3051S nyomástávadó hibatáblázata [20]

Hiba kategória	fit[86]	$\lambda = \text{fit} \cdot 10^{-9}$
Magas érték hiba (PLC detektálta)	55	$55 \cdot 10^{-9}$
Alacsony érték hiba (PLC detektálta)	228	$228 \cdot 10^{-9}$
Nem detektált veszélyes hiba[87]	101	$101 \cdot 10^{-9}$
Következmény nélküli	198	$198 \cdot 10^{-9}$
Bejelentés, nem detektált	29	$29 \cdot 10^{-9}$

Megkötések [20]:

- *a HART kommunikáció nem vesz részt biztonsági funkcióban;*
- *ha az analóg kimenet < 3,6 mA, akkor alacsony érték hiba;*
- *ha az analóg kimenet < 21,5 mA, akkor magas érték hiba;*
- *a távadó jele intelligens eszközbe (PLC, DCS, stb.) kerül, ami az alacsony és a magas érték hibákat érzékeli;*
- *bármely komponens hibája, hibás üzemállapotba hozza a nyomástávadót;*
- *a tápfeszültség pontatlanságot okozó csökkenésekor a kimenetet alacsony érték hibára állítja a távadó mikrokontrollere;*
- *a meghibásodási ráta érték állandó.*

[86] A 8. táblázatban a fit jelentése: a 10^9 üzemóra alatt bekövetkező hibák száma.

[87] Megjegyzés: A logikai feladatmegoldó (pl.: PLC) által nem detektált, de vizsgálat által mért veszélyes hiba például a távadó kimenetének „kifagyása” (a mért nyomástól független állandó értéket mutat) vagy csúszása.

A 8. táblázat értelmezése az alkalmazástól függ. A hibapartíciók kiosztása egyrészt attól függ, hogy a magas vagy az alacsony nyomás indítja-e a vész-, védelmi funkciót. Másrészt függ a távadó jelét fogadó logikai vezérlő diagnosztizáló képességétől, azaz hogy csak az alacsony vagy csak a magas érték hibát detektálja, vagy mindkettőt.

A 9. táblázat a hibapartíciók kiosztásához szükséges.

9. táblázat: A hibapartíciók kiosztása

	PLC diagnosztika képessége	Hibaállapot	
		< 4 mA	> 20 mA
Alacsony nyomás indítja a biztonsági funkciót	Csak a < 4 mA detektálja	λ^{SD}	λ^{DU}
	Csak a > 20 mA detektálja	λ^{SU}	λ^{DD}
	Egyaránt detektálja a < 4 mA és > 20 mA	λ^{SD}	λ^{DD}
	Nem detektál	λ^{SU}	λ^{DU}
Magas nyomás indítja a biztonsági funkciót	Csak a < 4 mA detektálja	λ^{DD}	λ^{SU}
	Csak a > 20 mA detektálja	λ^{DU}	λ^{SD}
	Egyaránt detektálja a < 4 mA és > 20 mA	λ^{DD}	λ^{SD}
	Nem detektál	λ^{DU}	λ^{SU}

Példaképpen, ha a 9. táblázat szürke sorának felel meg a nyomástávadó biztonsági alkalmazása, akkor az alábbi meghibásodási ráták olvashatók ki a 8. táblázatból:

Magas érték hiba (PLC detektálta) $\lambda^{DD} = 55 \cdot 10^{-9} \left[h^{-1} \right]$

Alacsony érték hiba (PLC detektálta) $\lambda^{SD} = 228 \cdot 10^{-9} \left[h^{-1} \right]$

Nem detektált veszélyes hiba $\lambda^{DU} = 101 \cdot 10^{-9} \left[h^{-1} \right]$

Következmény nélküli $\lambda^{SU} = 199 \cdot 10^{-9} \left[h^{-1} \right]$

Bejelentés, nem detektált $\lambda^{AU} = 14 \cdot 10^{-9} \left[h^{-1} \right]$

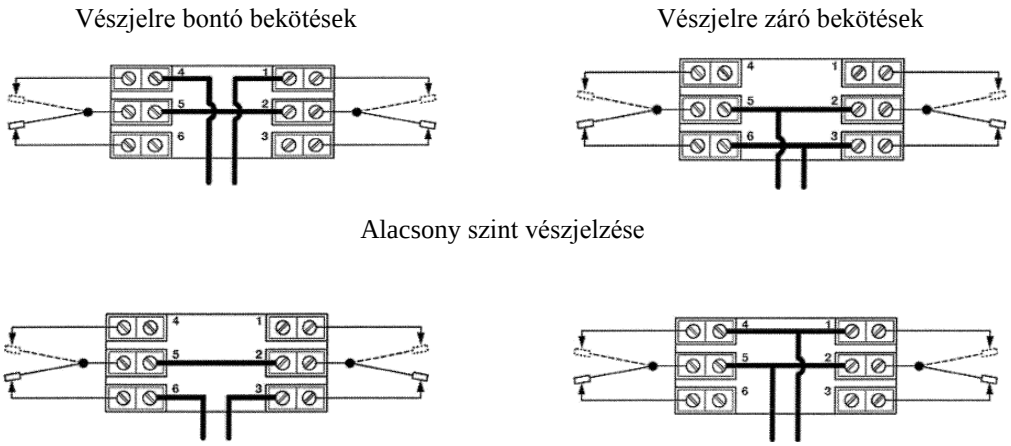
Az előbbieken túl a jegyzőkönyv tartalmazza az SFF értéket (83,3%), amit a 2.1 kifejezés átrendezésével az alábbi képlettel számol ki.

$$SFF = 1 - \frac{\lambda^{DU}}{\lambda^{Total}} \tag{2.2}$$

Ha a HART kommunikációt is bevonjuk a biztonsági funkcióba, akkor növelhető az SFF érték. Ez a megoldás azonban a fogadó oldal, vagyis a PLC-vel szemben támaszt nagyobb követelményeket.

A második példa a Magnetrol DPDT redundáns, mechanikus szintkapcsoló. A FMEDA jegyzőkönyve [22] (készült 2006. július, készítette: Magnetrol).

A Magnetrol DPDT redundáns, mechanikus szintkapcsoló olyan készülék család, amelynél a különböző tokozás nem befolyásolja a meghibásodás valószínűséget. A bontó vagy záró kontaktus kimenet választás szintén nem befolyásolja a meghibásodás valószínűséget. A lehetséges négy bekötési módot mutatja a 11. ábra.



11. ábra. Magnetrol DPDT szintkapcsoló bekötései [20]
(Átmásolta: Neszveda József)

A redundáns mechanikai érzékelők bekötésének egyik lehetősége, hogy a PLC két külön bemeneti moduljába külön-külön van bevezetve a két szintkontaktus. A másik lehetőség, amikor mindkét kontaktus jel ugyanazon bemeneti modulba kerül. Ez eltérő hibadiagnosztizáló eljárást[88] eredményez.

A jegyzőkönyv a következő megkötéseket tartalmazza:

- *Ha a kontaktus alacsony szinten ragad, akkor az alacsony érték hiba.*
- *Ha a kontaktus magas szinten ragad, akkor magas érték hiba.*
- *A távadó jele intelligens eszközbe (PLC, DCS, stb.) kerül.*
- *Bármely komponens hibája, hibás üzemállapotba hozza a szintkapcsolót.*
- *A meghibásodási ráta érték állandó*

[88] A diagnosztizálást a logikai feladatmegoldó (pl.: PLC) végzi.

- *A mechanikai kialakítás miatt az alacsony és a magas szint jelzését külön kell választani.*

10. táblázat: Szintkapcsoló hibatáblázata [22]

Hiba kategória	**Meghibásodási ráta [**fit]	
	Alacsony szint jelzése	Magas szint jelzése
Detektált veszélyes hiba	71	98
Magas szint hiba (PLC detektálta)	0	98
Alacsony szint hiba (PLC detektálta)	71	0
Nem detektált veszélyes hiba	40	28
Következmény nélküli	15	0

A 10. táblázat alapján attól függően, hogy az alacsony vagy a magas szint váltja ki a biztonsági funkciót különböző meghibásodási ráta értékekkel kell számolni.

11. táblázat: Szintkapcsoló meghibásodási ráta értékei [22]

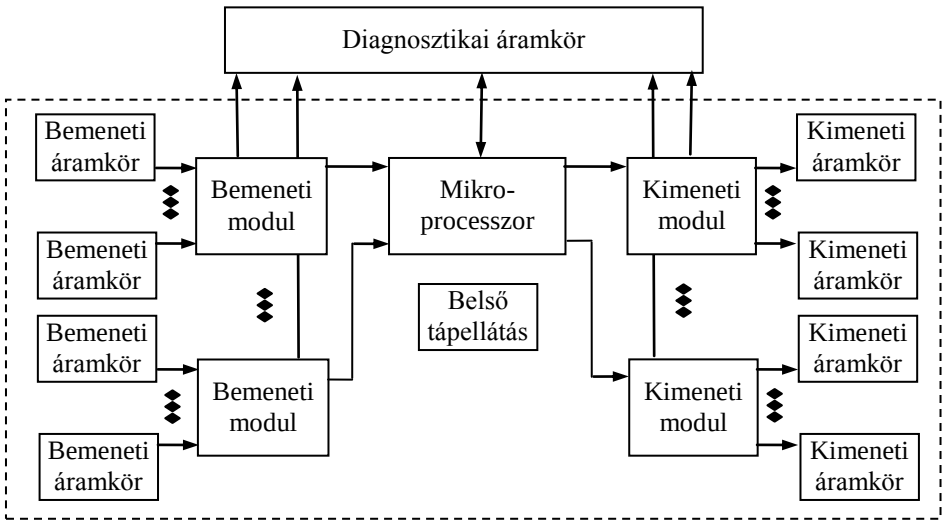
	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	SFF
Alacsony szint indítja a biztonsági funkciót	0	15	71	40	68,2%
Magas szint indítja a biztonsági funkciót	0	0	98	28	77,7%

A 10. és 11. táblázatok alapján előnyösebb, ha a magas szint indítja a biztonsági funkciót. A jegyzőkönyv azonban értelemszerűen nem tartalmazza a vezérlő berendezés és a távadó közötti vezeték meghibásodását. A vezeték szakadás, ami veszélyes hiba, alacsony szintként jelenik meg a vezérlő berendezés bemenetén, ezért a biztonsági funkció szempontjából javallott, hogy azt az alacsony szint indítsa.

2.2.2 Logikai feladatmegoldó eszközök

Napjainkban jellemző tendencia, hogy a katonai fejlesztések zömmel minősített gyártók által szállított, de a kereskedelmi forgalomban is elérhető eszközökre épülnek. Az is jellemző, hogy egyedi tervezésű logikai feladatmegoldó eszközt[89] csak olyan beszállítóktól fogadnak el, amelyek vállalják, hogy hitelesített minőségbiztosítási eljárás alkalmazásával gyártják az eszközeik.

A 12. ábrán egyberajzolva látható 1001 (szaggatott vonallal határolt) és 1001D (diagnosztikai kártyával kiegészített teljes ábra) hardver struktúra több be-, és kimeneti csatornára.



12. ábra. Az 1001 és az 1001D hardverstruktúra több csatornára.
(Készítette: Neszveda József)

A 12. ábrán a mikroprocesszor és a be-, és kimeneti áramköröket tartalmazó be[90]-, és kimeneti[91] modulok elrendezése látható.

---

[89] A „Safety Equipment Reliability Handbook, Volume 2." [23] több tucat nagy megbízhatóságú és biztonsági PLC CPU modulja, és ezek be-, ki-, valamint interfészmoduljaik hibaarány adatát tartalmazza, köztük a 12. táblázat adatait is.

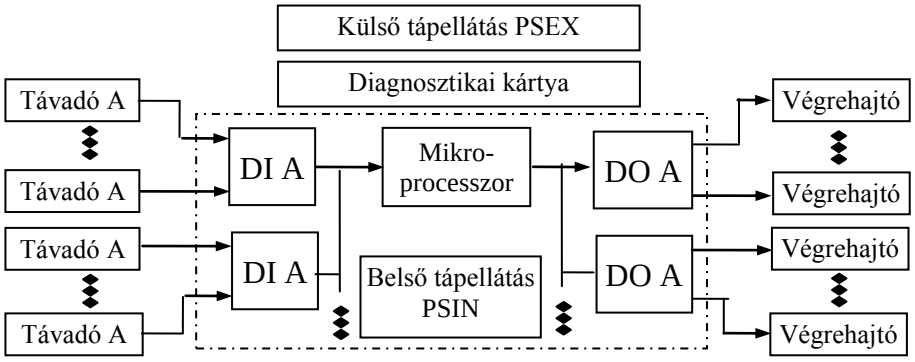
[90] A kereskedelmi forgalomban levő ipari irányító berendezésekben az analóg bemeneti modulok jellemzően 4 – 20 mA-esek. Típusai: 4, 8 vagy 16 csatornás. A digitális bemeneti modulok 0 – 24 V_{DC}-esek. Típusai: 8 vagy 16 csatornás. Az analóg bemeneti áramkörök és a digitális bemeneti áramkörök egységes kialakításúak.

[91] Az analóg kimeneti modulok jellemzően 4 – 20 mA-esek. Típusai: 2, 4 vagy 8 csatornás. Az analóg kimeneti áramkörök egységesek kialakításúak. A digitális kimeneti modulok 0 – 24 V_{DC}-esek. A kimenetek vagy tranzisztoros, vagy kontaktus kialakításúak. Típusai 4, 8 vagy 16 csatornás.

12. táblázat: Generic SIL3 PLC eredmény táblázata [29]

Komponens	**Meghibásodási ráta** [1/óra]			
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Tápellátás (belső)	2,25E-06	-	2,50E-06	-
CPU modul	7,43E-06	7,50E-08	2,38E-06	1,25E-07
Analóg bemeneti modul (8)	9,90E-07	1,00E-08	9,00E-07	1,00E-07
Analóg bemeneti áramkör	4,80E-08	3,00E-09	4,80E-08	3,00E-09
Digitális bemeneti modul (16)	5,70E-07	3,00E-08	3,80E-07	2,00E-08
Digitális bemeneti áramkör	1,24E-07	7,00E-09	6,70E-08	4,00E-09
Analóg kimeneti modul (8)	1,43E-06	7,50E-08	4,75E-07	2,50E-08
Analóg kimeneti áramkör	-	-	9,50E-08	5,00E-09
Digitális kimeneti modul (16)	7,60E-07	4,00E-08	1,90E-07	1,00E-08
Digitális kimeneti áramkör	1,39E-07	1,00E-09	5,70E-08	3,00E-09

A 13. ábra[92] a 8. ábrán látható elrendezés „A” csatornáját mutatja több be-, és kimeneti jel esetén.



13. ábra. Irányító rendszer struktúra
(Készítette: Neszveda József)

[92] Megjegyzés: A 13. ábrán a DI: digitális bemeneti modul a digitális áramkörökkel együtt, a DO: digitális kimeneti modul a digitális áramkörökkel együtt összevont blokkok, hisz a modul bármelyik áramkörének kiesése kritikus.

Vizsgálataim alapján az 1002D hardverstruktúrát javaslom az aperiodikusan alkalmazott katonai berendezések irányító rendszerének úgy, hogy a vezérlő berendezés és a veszélyes állapotot detektáló távadók **redundáns**, a végrehajtók és a többi távadó **egyszeres** kialakításúk, és a diagnosztikai lefedettség $SFF \geq 0,95$. Modellkísérletekből (6. táblázat) kiderül az 1002D struktúra, nagy diagnosztikai lefedettség esetén, kiegyensúlyozottan hatásos a kezelhető és a veszélyes hibákra egyaránt.

A struktúraválasztásnak következménye van, mert mint a 90-es évek közepén végzett vizsgálatok [24] kimutatták: „*Lényegi a különbség az 1002 architektúrájú és a 1002D architektúrájú PLC-k esetén a PLC-k meghibásodás-valószínűség modelljeinek hatékonysága között.*"

A PLC gyártók nagy megbízhatóságú és biztonsági PLC-i diagnosztikai áramkörrel készülnek, mert így redundancia nélkül is elérhető a SIL2, illetve 1002D kialakítással a SIL3 is. Ennek megfelelően a gyártók nagy megbízhatóságú (H vagy HR jelzésű) és/vagy biztonsági (S jelzésű) PLC-i alkalmasak az aperiodikusan működtetett katonai berendezések logikai döntéshozói funkcióinak ellátására. A nagy megbízhatóságú és biztonsági PLC-k között az a különbség, hogy amíg a biztonsági PLC-k programozása csak kész gyári funkcióblokkokból és függvényekből, előírt programozás technikai előírások szerint történhet, addig a nagy megbízhatóságú PLC-k bármely szabványos irányítástechnika programnyelven programozhatók. E különbségből adódóan:

- a biztonsági (Safety) PLC-kre garantálják a szoftverbiztonságot, viszont ezek programozhatósági lehetősége korlátozott és nehézkes, de egyszerű logikai állítások programozására azonban tökéletesen megfelel;
- a nagy megbízhatóságú (H) PLC bármely szabványos irányítástechnikai programnyelven programozható, viszont ha biztonsági funkcióra is alkalmazzák, akkor a felhasználói szoftvert az 1. sz. melléklet 3 ábrájának megfelelő szoftver életciklus diagram szerint kell megírni és validálni[93].

Az aperiodikusan működtetett katonai berendezések logikai döntéshozói funkcióinak ellátására - amennyiben a feladat végrehajtás nagymennyiségű és rendkívül gyors számítási műveletet igényel - az ipari kivitelű számítógép bázisú PAC[94] rendszer is alkalmas lehet, amint piacra kerül a már bejelentett „H" jelű sorozat.

---

[93] Bárki által ellenőrizhetően igazolni az elvárt működést.

[94] PAC: Programmable Automation Control: Programozható automatizálás irányító A PAC rendszer ismertetése a [25] internet címen részletesen megtalálható.

Az aperiodikusan működtetett katonai berendezések logikai feladatmegoldói funkcióinak ellátására a **kereskedelmi forgalom**ban is elérhető, **nagy megbízhatóságú és/vagy biztonsági PLC** kialakítást javaslom. A választás indokai:

- bár önmagukban a nagy megbízhatóságú és biztonsági PLC-k drágábbak a normál kivitelnél, de ha távadó vagy végrehajtó, és főleg ha logikai feladatmegoldó redundanciát váltanak ki, akkor költséghatékonyabbak;
- a gyártók megadják a nagy megbízhatóságú és/vagy biztonsági PLC-ék SIL besorolását. Saját fejlesztésű eszköz SIL besorolását, ha a fejlesztőnek nincs erre a célra saját akkreditált laboratóriuma, hivatalos minősítőkkel kell elvégeztetni.

2.2.3 Végrehajtók

A végrehajtó meghibásodása megakadályozza a biztonsági funkció végrehajtását, ezért a végrehajtó minden hibája veszélyes hiba. Ráadásul a végrehajtók működtetéséhez általában nagy energia szükséges, ezért külön figyelmet érdemel a tápellátásuk, ami lehet villamos, pneumatikus, vagy hidraulikus. A végrehajtó[95] és szerelvényei (tápellátás, rögzítés, stb.) a biztonsági funkció (SIF) része.

Előzetes méretezéskor és eszköz kereséskor a gyakorlati SIL mérnökök abból indulnak ki, hogy ha a teljes irányítási láncban a veszélyes hiba valószínűségét szétosztjuk a távadó, a logikai megoldó, és a végrehajtó között, akkor a veszélyes hibák valószínűségének több mint 60% a végrehajtóra és ennek szerelvényeire jut. Ha a logikai megoldó redundáns és diagnosztizáló kártyával rendelkezik, akkor ez az arány 85% felettire becsülhető.

Számos eszközt alkalmaznak végrehajtóként. A végrehajtó némelykor nagyon egyszerű eszköz (például: relé, mágneskapcsoló, stb.), de gyakran összetett berendezés (például a kinetikus energia gyors elnyelésére tengelykapcsolóval és fékkel szerelt motorvezérlő, ahol a motorvezérlő lehet frekvenciaváltó, lágyindító, stb.) Leggyakrabban villamosmotor, pneumatikus munkahenger, vagy hidraulikus munkahenger a végrehajtó eszköz.

A pneumatikus, illetve hidraulikus munkahenger nagy, illetve nagyon-nagy energiasűrűségű (elvégzett munka/térfogat) eszközök. Kialakításukból adódóan egyenes

[95] A „Safety Equipment Reliability Handbook, Volume 3.” [23] több száz végrehajtó hibaarány adatát, köztük a 13.a és 13.b táblázatok adatait is, tartalmazza.

vonalú mozgást végeznek. A véghelyzetük stabil állapot, ezért véghelyzetükben tehermentesítést nem igényelnek. A pneumatikus, illetve hidraulikus munkahengerek önmagukban megbízható eszközök, az átlagos meghibásodási rátáikat az 5. sz. melléklet tartalmazza. A munkahengerek és a PLC közötti kapcsolathoz elektro-pneumatikus, illetve elektro-hidraulikus átalakítóra van szükség, amit szintén be kell vonni a megbízhatósági számításba.

A gyártó által SIL2 besorolású, komplex berendezésként figyelembe veendő végrehajtóra példa az ABB TZIDC/TZIDC-200 intelligens helyzetbe-állító. A használat közbeni és FMEDA hibaanalízis jegyzőkönyve (készült 2004. február, készítette: Exida) a [26] Internet címen elérhető.

A jegyzőkönyv a következőket deklarálja [26]:

- *a TZIDC / TZIDC200 intelligens* helyzetbe-*állító kétféle funkcióval lehet biztonsági végrehajtóként alkalmazni. Egyrészt gyors lezáróként, másrészt folytonos helyzetbe- állítóként. Mindkét esetben a bemeneti 4 – 20 mA áramot konvertálja a megfelelő nyomásértékké;*
- *gyors lezáróként alkalmazva az* eszköz*, mint alrendszer nem intelligens és nem tartalmaz lényegi redundanciát, vagyis a hardver hiba tolerancia értéke 0. Intelligens helyzetbe-állítóként alkalmazva, mint alrendszer a hardver hiba tolerancia értéke 1, és a biztonságos meghibásodási ráta 60%< SFF < 90%;*
- *a TZIDC / TZIDC200 használat* közbeni *bizonyítása az ABB Automation Products GmbH. által összegyűjtött és analizált folyamatadatokkal történt. A bizonyítási eljárás, Chi-Squared eloszlást feltételezve, az IEC 61508-nak megfelelően az egy-oldalas konfidencia határ 70%-ig történt. A használat közbeni bizonyítási eljárásnak nem volt része a beavatkozó elem, azt a végfelhasználónak kell figyelembe vennie;*
- *feltételezzük, hogy a* PFD_{avg} értékében *legalább 50% súlyú a végrehajtó. Továbbá mivel a TZIDC / TZIDC200 csak része a teljes végrehajtónak, ezért a ráeső rész a* PFD_{avg} *értékének legfeljebb 20%-a. Ez azt jelenti, hogy alacsony működés igényű üzemmódban a SIL2 számára megengedett 1,00E-02 értékből TZIDC / TZIDC200 csak 2,00E-03 részt fed le.*

13.1. táblázat: Az ABB TZIDC/TZIDC200 helyzetbe-állító hibatáblázata [26]

Hiba kategória	fit
Kezelhető, detektált hiba	45
Kezelhető, nem detektált hiba	845
Veszélyes, detektált hiba	47
Veszélyes, nem detektált hiba	172
Következmény nélküli	70
Bejelentés, nem detektált	4

A 13.1. táblázat alapján az IEC 61508 szerinti meghibásodási ráták:

Veszélyes, detektált $\lambda^{DD} = 47 \cdot 10^{-9}$

Kezelhető, detektált $\lambda^{SD} = 45 \cdot 10^{-9}$

Veszélyes, nem detektált $\lambda^{DU} = 172 \cdot 10^{-9}$

Kezelhető, nem detektált $\lambda^{SU} = 919 \cdot 10^{-9} = (845 + 70 + 4)10^{-9}$

13.2. táblázat: Az ABB TZIDC/TZIDC200 gyors lezáró hibatáblázata [26]

Hiba kategória	fit
Kezelhető, detektált hiba	0
Kezelhető, nem detektált hiba	695
Veszélyes, detektált hiba	0
Veszélyes, nem detektált hiba	40
Következmény nélküli	23
Bejelentés, nem detektált	0

A 13.2. táblázat alapján az IEC 61508 szerinti meghibásodási ráták:

Veszélyes, detektált $\lambda^{DD} = 0$

Kezelhető, detektált $\lambda^{SD} = 0$

Veszélyes, nem detektált $\lambda^{DU} = 40 \cdot 10^{-9}$

Kezelhető, nem detektált $\lambda^{SU} = 718 \cdot 10^{-9} = (695 + 23)10^{-9}$

Fontos tapasztalat, hogy *„Az alacsony működés igényű üzemmódban a periodikus teszt az egyik hatékony eszköz a végrehajtó megbízhatóságának növelésére.”* [27] Mindemellett kevés végrehajtó rendelkezik SIL2 elérésére alkalmas paraméterekkel.

2.3 Összefoglalás és következtetések

Vizsgálataim alapján bizonyítottam, hogy a gyakorlatban a redundancia nem mindig hasznos. A hamis riasztás, ami a berendezés felesleges blokkolását okozza, a polgári gyakorlatban többnyire költségnövekedéssel jár, de **katonai művelet közben végzetes** is lehet. A szakirodalom alapján rámutattam, hogy a problémát leghatékonyabban a diagnosztika hatékonyságának növelésével lehet megoldani, ami intelligens diagnosztikai áramkör alkalmazását igényli.

Elemzésemben bizonyítottam, hogy pusztán a **karbantartás és ellenőrző teszt gyakoriságának növelésével** a megbízhatóság nem javítható korlátlanul. A megbízhatóság redundanciával és **intelligens diagnosztikai** kártya alkalmazásával növelhető. A diagnosztikai kártyával kialakított irányító rendszerben **már egyszeres redundancia** alkalmazása is elérhetővé teszi a SIL3 fokozat elérését. Ennek alapján az 1002D hardver struktúrát **javaslom** az aperiodikusan alkalmazott katonai berendezések logikai feladatmegoldó hardverstruktúrájának.

A kereskedelmi forgalomban kapható nagy megbízhatóságú és biztonsági PLC-k jelentős része ilyen hardver kialakítású. Amennyiben nemcsak egyszerű vezérlési feladatot kell megvalósítani, akkor az aperiodikusan alkalmazott katonai berendezések logikai feladatmegoldója a kereskedelmi forgalomban kapható **nagy megbízhatóságú PLC** lehet.

Példákon keresztül bemutattam, hogyan lehet meghatározni az irányítási rendszer konkrét eszközeinek meghibásodási ráta értékeit.

Gyakorlati tapasztalat, hogy az 1002D hardverstruktúrájú, nagy megbízhatóságú vagy biztonsági PLC és legalább SIL1 besorolású távadó választás esetén a PFD_{avg} értékének számításakor a végrehajtó meghibásodásának részaránya 85% feletti. Ebből következik, hogy az aperiodikusan alkalmazott katonai berendezések PFM_{Bavg} számításakor a **végrehajtó meghibásodásának részarányára** szintén 85% feletti érték várható. Ez a tény felhívja a figyelmet a **periodikus teszt** fontosságára, mint az egyik leghatékonyabb eszközre, ami a végrehajtók megbízhatóságát növeli.

III. FEJEZET

APERIODIKUSAN ALKALMAZOTT KATONAI BERENDEZÉSEK MŰSZAKI MEGBÍZHATÓSÁGA

A megbízhatóság számítási módszerekkel számos szakkönyv foglakozik. Az Értekezés az ISA-TR84.0002-2002 technikai riport sorozatra [28] hivatkozik. A technikai riport sorozat felépítése a M6 melléklet M6.1 ábráján látható. A 14. táblázat a három megbízhatóság számítási módszer képességeinek összehasonlítását tartalmazza.

14. táblázat: A megoldási eljárások összehasonlítása [28][96]

	Egyszerűsített egyenletek[97]	Hibafa analízis[98]	Markov analízis[99]
	Tipikus modellezett rendszer		
A megbízhatóság számítási módszerek jellemzői	Egyszerű SIF	SIF komplex környezetével	SIF komplex környezetével, vagy PE logikai feladatmegoldó
A redundáns elemek különböző javítási időinek kezelése	Nem alkalmas	Igen	Igen
Eltérő technológiai feladatot ellátó redundáns elemek kezelése	Nem alkalmas	Igen	Igen
Sorozat függő hibák kezelése	Nem alkalmas	Nehéz	Igen
Számítási eljárás	Egyszerű matematika	Egyszerű matematika vagy Boolen algebra	Mátrix algebra
A hibaútvonal grafikus megjelenítése	Gyakorlatilag csak egyszerű SIF esetén	Igen	Nehéz

Az aperiodikusan alkalmazott katonai berendezések irányító rendszerének biztonság-kritikus megvalósítása során többször előfordul, hogy egy folyamatjellemzőt az alapirányítás számára és a vész-, védelem számára is mérni kell. A mérést tiltott

[96] [28] Part1: Framework, definitions, system, hardware and software requirements, Table 6.1.

[97] Simplified Equitations: Egyszerűsített egyenletek

[98] FTA: Fault Tree Analysis: Hibafa analízis

[99] Markov Analysis: Markov analízis

egyetlen eszközzel megvalósítani. Két eszközt alkalmazva viszont célszerű a redundanciában rejlő előnyöket kihasználni. A redundáns kialakítás kizárja az „Egyszerűsített egyenletek” alkalmazását.

A II. fejezetben már bemutattam, hogy a diagnosztizáló kártya a PLC áramkörein kívül képes a távadók és a végrehajtók bizonyos hibáinak felismerésére is. Ezt az FTA vagy a Markov analízis is képes kezelni, de a Markov analízis rugalmasabb.

Minthogy az aperiodikusan alkalmazott katonai berendezések üzemmód-váltásait a meghibásodási ráta ugrásszerű változásával modellezem, ezért a diszkrét idejű matematikai módszer a kézenfekvő matematikai eljárás. Ez a mátrix-algebrát alkalmazó Markov analízisnél rendelkezésre áll. A Markov analízis az aperiodikusan alkalmazott katonai berendezésekre következő feltételek mellett alkalmazható:

- az üzemen kívüli állapotot megszakító tesztek gyakoriságának időintervalluma jóval kisebb, mint a berendezés MTTF ideje;
- a T_0 időalapot úgy kell megválasztani, hogy reális legyen az a feltételezés, hogy egy periódusban csak egy SIF komponens hibásodik meg;
- ha a rendszer egy SIF komponense valamely hibatípusnak megfelelő állapotba jut, akkor a meghibásodott rendszerkomponens - a jól működő állapot helyreállítása előtt - nem juthat egy másik hibatípusnak megfelelő állapotba.

A [28] meghatározását a szerző is vallja: „A Markov analízis fő előnye a rugalmassága. A Markov-modell lehetővé teszi a rendszer komponensek eltérő hiba típusainak, a rendszer diagnosztikai képességének kezelését, valamint a hibaarány az idő függvényében történő változásának figyelembe vételét, továbbá a nem tökéletes teszt és helyreállítás, valamint a közös hiba-ok vagy szisztematikus hiba kezelését. A Markov analízis fő hátránya a nagy számítási igény[100] és a modellalkotás idő igénye.”

Mindezek miatt az aperiodikusan alkalmazott katonai berendezések megbízhatóság vizsgálatához az **idő-diszkrét állapotterű Markov analízis** módszert[101] választottam.

---

[100] Manapság, amikor a modellalkotást és a számításokat személyi számítógépen futtatható programok segítik, akkor az előnyök mellett a hátrányok elhanyagolhatok.

[101] A hibátlan működés és a hibás állapotok valószínűségeinek időbeli változása folytonos, azonban a folytonos idő T_0 időintervallumokra van felosztva. A vizsgálati módszer a mintavételezi eljárásokhoz hasonló. A modell állapottere diszkrét időközönként módosul, miközben a T_0 időintervallumokban alatt a hibátlan működés és a hibás állapotok valószínűségértéke nem változik. Ha a T_0 időintervallum elegendően kicsi, akkor az idő-diszkrét állapotterű modell állapotterének időbeli változása közel azonos a folytonos idejű modelléhez, mert az idő kvantálásból származó hiba elhanyagolható. Ráadásul a hiba iránya olyan, hogy a hibás állapotok valószínűsége nagyobb, és így a hibátlan működésé kisebb értéket ad idő-diszkrét esetben! Így szigorúbb kritériumot jelent, mint a folytonos eset.

3.1 A Markov-modell

A Markov-modell a hibaállapotaival írja le a biztonságosra műszerezett rendszert. Értelemszerűen a valóságban egy rendszer egy adott pillanatban, egy konkrét állapotban van. A Markov-modell azt írja le, hogy a lehetséges állapotok közül az adott pillanatban **milyen valószínűséggel** van a rendszer egy **konkrét** állapotban. A Markov-modell olyan gráf, amelynek csomópontjai (S_k: States) a rendszer állapotai, és a Markov-modell élei/átmenetei (T: Transition) pedig a soron következő T_0 időperiódus végén az egyik állapotból a másikba kerülés valószínűsége.

Az átmenetek meghatározását tünteti fel a 15. táblázat:

15. táblázat: A Markov-modell átmenetei

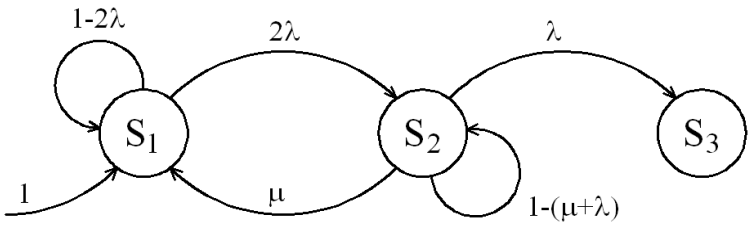
T mátrix átmenetei		Állapotba				
		1	2	3	-	n
Állapotból	1	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$	-	$t_{1,n}$
	2	$t_{2,1}$	$t_{2,2}$	$t_{2,3}$	-	$t_{2,n}$
	3	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	-	$t_{3,n}$
	-	-	-	-	-	
	n	$t_{n,1}$	$t_{n,2}$	$t_{n,3}$	-	$t_{n,n}$

A Markov-modell kialakítását a következő egyszerű példa mutatja be. Álljon egy redundáns rendszer mindössze két azonos komponensből. A lehetséges állapotok:

S_1: A rendszer hibátlanul működik.

S_2: Az egyik komponens meghibásodik, a másik hibátlanul működik.

S_3: Mindkét komponens meghibásodik



14. ábra. Három állapottal jellemzett redundáns rendszer Markov-modellje
(Készítette: Neszveda József)

A 14. ábrán az azonos komponensek meghibásodási rátája egyaránt λ. Az azonos komponensek javíthatóságának valószínűsége (javítási rátája) egyaránt μ.

Szokásos feltételezés, hogy a rendszer kezdetben hibátlan, így a kiinduló állapot 1, az összes többi 0. Az állapotokat **s** sorvektorként felírva:

$$\mathbf{s}(0) = s_1 \quad s_2 \quad s_3 = 1 \quad 0 \quad 0 \tag{3.1}$$

A 14. ábrán az állapotok és az élek felrajzolása után az élek meghatározásának menete a következő: Bármely komponens kezdeti hibavalószínűsége $PF=\lambda T_0$ (1.23 kifejezés). A rendszer S_1 állapotából S_2 állapotába $t_{1,2} = 2\lambda T_0$ valószínűséggel jut, mert vagy az egyik komponens hibásodik meg, vagy a másik. Annak valószínűsége, hogy a rendszer S_2 állapotából S_3 állapotába jut $t_{2,3} = \lambda T_0$, mert ehhez a második komponensnek is meg kell hibásodnia. Annak valószínűsége, hogy a rendszer S_2 állapotából S_1 állapotába jut $t_{2,1} = \mu T_0$.

Az 1.21 kifejezés alapján a sikeres működés valószínűsége, vagyis hogy a rendszer az S_1 állapotában marad $t_{1,1} = 1\text{-}2\lambda T_0$. Annak valószínűsége pedig, hogy a rendszer az S_2 állapotában marad $t_{2,2} = 1\text{-}(\lambda+\mu)T_0$. Az S_3 állapot megszakítja a folyamatos működést. Az ilyen jellegű állapotokat „nyelő" állapotnak is nevezik. A modell az ebből való visszatérést nem vizsgálja. Amennyiben a rendszer az S_3 állapotba kerül, akkor a modell szerint annak valószínűsége, hogy ott is marad 1. A gyakorlatban ez nem feltétlenül van így, sőt a legtöbb esetben a leállás utáni helyreállítást követően a rendszer újra indul. A modell azonban kifejezi azt a célt, hogy az ilyen jellegű állapotokat akarjuk elkerülni.

A szöveges leírás és/vagy a gráf alapján a **T** átmenet-valószínűségmátrix[102].

$$\mathbf{T} = \begin{pmatrix} 1-2\lambda T_0 & 2\lambda T_0 & 0 \\ \mu T_0 & 1-(\lambda+\mu)T_0 & \lambda T_0 \\ 0 & 0 & 1 \end{pmatrix} \tag{3.2}$$

T átmenet-valószínűségmátrix szabályrendszere:

- minden sor a vele azonos sorszámú állapothoz tartozik;
- a főátló elemeit úgy kell meghatározni, hogy a sor elemeinek összege 1 legyen;
- a sor többi eleme, a sorral azonos sorszámú állapotból kiinduló és az elemen végződő átmenet(ek)et tartalmazza.

A rendszer a kezdeti **s**(0) állapotból T_0 időköz elteltével **s**(1) állapotba jut[103], ekkor

$$\mathbf{s}(1) = \mathbf{s}(0)\mathbf{T} \tag{3.3}$$

---

[102] A második és harmadik sorok azt tartalmazzák, hogy ha a rendszer ebbe a hibaállapotba kerül, akkor milyen valószínűséggel marad ebben az állapotban vagy jut egy másikba.

[103] Feltételezzük, hogy a T_0 időköz elegendően kicsi és így a meghibásodás valószínűség közel állandónak tekinthető. Az idő-diszkrét modellben a meghibásodás valószínűség értékek ugrásszerűen a kT_0 időpontokban változnak meg.

A kT_0 időköz elteltével a vizsgált rendszer **s**(k) állapotba jut:

$$\mathbf{s}(k) = \mathbf{s}(0)\mathbf{T}^k \tag{3.4}$$

A 3.4 kifejezésben az **s**(k) sorvektor első eleme $s_1(k)$ mutatja annak valószínűségét, hogy a rendszer sikeresen működik a k-adik időperiódusban, a többi $s_i(k)$ $(i \neq 1)$ eleme azt mutatja meg, hogy milyen valószínűséggel tartózkodik kT_0 időköz elteltével valamelyik hiba-állapotában, vagyis az adott típusú meghibásodásnak mekkora a valószínűsége[104].

A **T** átmenet-valószínűség mátrixból az **I** egységmátrixot kivonva a főátlóban negatív előjellel az adott sorhoz tartozó állapot meghibásodás ($PF_{i,i}$) valószínűsége kerül. Az így kapott **P** mátrix - ha nem tartalmaz μ javítási rátát[105] - **minden eleme** λT_0 jellegű, és így konstans értékkel szorozható.

Amennyiben a λ meghibásodási ráta **ugrásszerű változását** egy $\mathbf{T}_1$ átmenet-valószínűség mátrix elemein akarjuk érvényesíteni, akkor az **I** egységmátrixot kivonva a $\mathbf{T}_1$ átmenet-valószínűség mátrixból a $\mathbf{P}_1$ mátrixot kapjuk, ami konstans értékkel (h) szorozható. Az így kapott új $\mathbf{P}_2$ meghibásodás-valószínűség mátrixhoz az **I** egységmátrixot hozzáadva megkapjuk az új $\mathbf{T}_2$ átmenet-valószínűség mátrixot.

$$\mathbf{T}_2 = \mathbf{T}_1 - \mathbf{I} \cdot h + \mathbf{I} \tag{3.5}$$

A 3.5 kifejezéssel, ahol az **I** az egységmátrix, **érvényesíthető** a λ meghibásodási ráta ugrásszerű változása az átmenet-valószínűség mátrixban.

3.1.1 1002D struktúra Markov-modellje

Az 1002D struktúrájú irányító rendszernek az egyik lehetséges Markov-modellje az állapotok hibatípusok szerinti összevonása [30]S, [52], [61].

A 15. ábrán látható az ennek megfelelő Markov-modell. A sötétszürke színnel jelzett S_6 vészleállás, és S_7 hamis leállás nyelő[106] állapotok. A világosszürke színnel jelzett S_2, S_3, S_4, S_5 állapotok a redundáns elemekhez (távadók, PLC) tartoznak. A

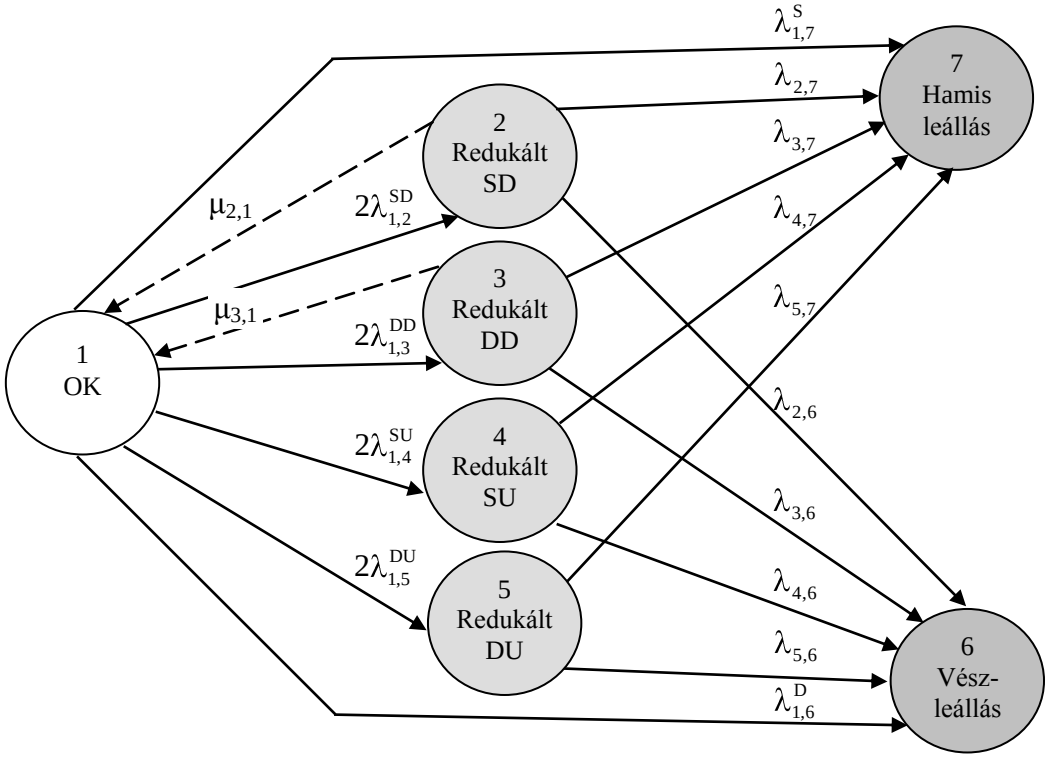
---

[104] A mátrix-algebra szabályainak megfelelően, ha az $\mathbf{s}(0)$ a 3.1 kifejezéshez hasonlóan olyan sorvektor, amelynek első eleme 1 és a többi 0, akkor $\mathbf{s}(k)$ és a $\mathbf{T}^k$ mátrix első sora azonos.

[105] Ha figyelembe kell venni a μ javítási rátát, akkor az **I** egységmátrix helyett egy olyan **N** mátrixot kell alkalmazni, amelynek főátlója csupa 1-es és a megfelelő pozíciókban tartalmazza a μ javítási rátát.

[106] A modell terjedelme itt befejeződik. Az ezekből való visszatérést a modell nem tárgyalja.

kiinduló S_1 állapotból ide tartó élek 2-es szorzó faktora azt fejezi ki, hogy a redundáns elempároknak azonos a λ meghibásodási rátája.



15. ábra. Az 1002D struktúra egyszerűsített (összevont) Markov-modellje
(Készítette: Neszveda József)

Működtetéskor az S_6 a veszélyes állapot. A PFD_{avg} értékét- amennyiben nem volt bizonyító erejű teszt a kT_0 időköz alatt - a 3.6 kifejezés adja meg[107].

$$PFD_{avg} = \frac{1}{kT_0}\sum_{i=1}^{k} s_6(i) \tag{3.6}$$

A hamis leállás (STR[108]) eredményeként az S_7 állapotba kerül a rendszer. A hamis leállás átlagos valószínűsége kT_0 időköz alatt:

$$STR_{avg} = \frac{1}{kT_0}\sum_{i=1}^{k} s_7(i) \tag{3.7}$$

A hamis leállás várható ideje ($MTTR^{spurious}$[109]) egyre gyakrabban optimalizált[110] érték egy biztonságosra műszerezett rendszerben.

---

[107] A tudományos köznyelvnek számító angolszász szakirodalomnak és a [44] között van némi eltérés.

[108] STR: Spurious Trip Result: Hamis leállás eredménye.

[109] $MTTF^{spuriuos}$: Mean Time To spurious Failure: Hamis leállást okozó hiba átlagos ideje

[110] A hamis leállás ugyan nem jelent veszélyt, de különösen nagy folytonos technológiák esetén jelentős anyagi kárt okoz, ezért a valószínűségének csökkentése feladata egy jól működő rendszernek.

$$MTTR^{Spurious} = \frac{1}{STR_{avg}} = \frac{1}{\frac{1}{kT_0}\sum_{i=1}^{k} s_7(i)} \tag{3.8}$$

Az s_6 és s_7 kivételével a többi állapotban a rendszer működik. Így a rendszer megbízhatósága kT_0 idő elteltével:

$$R(k) = \sum_{j=1}^{5} S_j(k) \tag{3.9}$$

A 3.10 kifejezés a 15. ábra alapján felírt **T** átmenet-valószínűség mátrix.

$$\mathbf{T} = \begin{vmatrix} 1-\sum_{j=2}^{7}\lambda_{1,j} & 2\lambda_{1,2}^{SD} & 2\lambda_{1,3}^{DD} & 2\lambda_{1,4}^{SU} & 2\lambda_{1,5}^{DU} & \lambda_{1,6}^{D} & \lambda_{1,7}^{S} \\ \mu_{2,1} & 1-\mu_{2,1}-\sum_{j=6}^{7}\lambda_{2,j} & 0 & 0 & 0 & \lambda_{2,6}^{D} & \lambda_{2,7}^{S} \\ \mu_{3,1} & 0 & 1-\mu_{3,1}-\sum_{j=6}^{7}\lambda_{3,j} & 0 & 0 & \lambda_{3,6}^{D} & \lambda_{3,7}^{S} \\ 0 & 0 & 0 & 1-\sum_{j=6}^{7}\lambda_{4,j} & 0 & \lambda_{4,6}^{D} & \lambda_{4,7}^{S} \\ 0 & 0 & 0 & 0 & 1-\sum_{j=6}^{7}\lambda_{5,j} & \lambda_{5,6}^{D} & \lambda_{5,7}^{S} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix} \tag{3.10}$$

A SIL mérnökök kedvelt fogalma a meghibásodás várható ideje, amit az MTTR értékkel határoznak meg. Ez kiszámítható a megbízhatóság R(k) értékeiből is:

$$MTTR = \frac{1}{\frac{1}{kT_0}\sum_{i=1}^{k}\sum_{j=1}^{5} S_j(i)} \tag{3.11}$$

Az MTTR analitikusan számítható a **T** átmenet-valószínűség mátrixból is. Ehhez először át kell alakítani a **T** átmenet-valószínűség mátrixot úgy, hogy töröljük a nyelő állapotokhoz tartozó sorokat és oszlopokat. A 3.10 kifejezésben ez a S_6, és S_7. Az így kapott **Q** mátrix segítségével létrehozható az **N** mátrix az alábbi módon:

$$\mathbf{N} = (\mathbf{I} - \mathbf{Q})^{-1} \tag{3.12}$$

Az átlagos meghibásodási idő az **N** mátrix első sor elemeinek összege:

$$MTTR = \sum_{j=1}^{5} n_{1,j} \tag{3.13}$$

ahol az $n_{1,j}$ értékek az **N** mátrix első sorának elemei.

3.1.2 Átmenet valószínűségi értékek meghatározása a Markov-modellben

A 3.5 … 3.12 kifejezésekben felírt összefüggések kiszámításához szükség van a **T** átmenet-valószínűség mátrix elemeinek ismeretére. A modell **T** átmenet-valószínűség mátrix elemeit az alábbi munkafázisok szisztematikus - szükség esetén iteratív - végrehajtásával lehet meghatározni:

1. Valamennyi biztonsági funkciót (SIF) a biztonsági igényekhez és az előírásokhoz illesztve definiálni kell. Egy távadó, illetve végrehajtó csak egy biztonsági funkcióhoz tartozzon, kivéve a logikai feladatmegoldót, ami több biztonsági funkciónak lehet eleme.
2. Fel kell sorolni a biztonsági funkciókat megvalósító eszközöket (távadókat, végrehajtókat, továbbá a hozzátartozó szerelvényeket, PLC-t, tápellátást.) és ezek hiteles - a hibatípusok szerint csoportosított - meghibásodási rátáit.
3. A távadókat és szerelvényeiket egy alrendszerként, azaz egy egységként kell kezelni. Szükség esetén FAT vagy Markov-modellel meg kell határozni együttes meghibásodási rátáikat és hibatípusaikat.
4. A végrehajtókat és szerelvényeiket (a PLC kimeneti áramkörétől a beavatkozó szervig) egy alrendszerként, azaz egy egységként kell kezelni. Szükség esetén meg kell határozni együttes meghibásodási rátáikat és hibatípusaikat.
5. Meg kell határozni a redundáns eszközök működés közbeni javítási eljárását, az észleléstől a készre jelentésig. Definiálni kell a MTTR (átlagos javítási idő) és a μ javítási ráta értékeket.
6. Minden egyes biztonsági funkcióhoz (SIF) fel kell sorolni a hozzátartozó eszközöket, alrendszereket, és részletes meghibásodási rátáikat, és ha van, akkor a javítási ráta értéket. (Az így létrehozott táblázatra egy hipotetikus példa az M7 mellékletben látható.)
7. A meghibásodási ráta típusok elemzésével eldönthető, hogy minimálisan hány hibaállapottal jellemezhető a biztonságosra műszerezett (SIS) rendszer és hogy milyen állapotok között van átmenet. Ezek alapján már kidolgozható a Markov gráf szerkezete.
8. Egy konkrét biztonsági funkcióra a biztonsági funkcióban résztvevő eszközök meghibásodási rátáiból meghatározhatók a gráf éleinek értékei. Az átmenet-valószínűség értékek ismeretében definiálható a **T** átmenet-valószínűség mátrix.

3.2 Aperiodikusan alkalmazott katonai berendezések Markov-modellje

Az aperiodikusan alkalmazott katonai berendezések sajátosságait – az üzemmód-váltásokat, a folytonos technológiáktól eltérő teszt üzemmódot – figyelembe kell venni a biztonság-valószínűség idő-diszkrét állapotterű Markov-modelljében.

Legyen a normál terhelést jelentő teszt üzemmód átmenet-valószínűség mátrixa **T**. Legyen $\mathbf{T}_L$ az üzemen kívüli és $\mathbf{T}_M$ a feladatvégzés üzemmódokhoz tartozó átmenet-valószínűség mátrix. Az 1.2 fejezetben leírt módon a meghibásodás-valószínűség értékek ugrásszerű változásával modellezem az üzemmód-váltásokat. A λT_0 meghibásodás-valószínűség értékek ugrásszerű változása a 3.5. kifejezésnek megfelelően változtatja meg a **T** átmenet-valószínűség mátrix elemeit. Ezért **üzemmód-váltások** a **T**, $\mathbf{T}_L$, és $\mathbf{T}_M$ átmenet-valószínűség mátrixok a 3.14 kifejezés szerinti egymásba konvertálásával kezelhetők.

A **T** átmenet-valószínűség mátrix átkonvertálásához $\mathbf{T}_L$, vagy $\mathbf{T}_M$ átmenet-valószínűség mátrixszá, illetve vissza csak a megfelelő „h” konstanst kell meghatározni.

$$\begin{vmatrix} 1-h\sum_{j=2}^{7}\lambda_{1,j} & h2\lambda_{1,2}^{SD} & h2\lambda_{1,3}^{DD} & h2\lambda_{1,4}^{SU} & h2\lambda_{1,5}^{DU} & h\lambda_{1,6}^{D} & h\lambda_{1,7}^{S} \\ h\mu_{2,1} & 1-h\mu_{2,1}-\tau\sum_{j=6}^{7}\lambda_{2,j} & 0 & 0 & 0 & h\lambda_{2,6}^{D} & h\lambda_{2,7}^{S} \\ h\mu_{3,1} & 0 & 1-h\mu_{3,1}-h\sum_{j=6}^{7}\lambda_{3,j} & 0 & 0 & h\lambda_{3,6}^{D} & h\lambda_{3,7}^{S} \\ 0 & 0 & 0 & 1-h\sum_{j=6}^{7}\lambda_{4,j} & 0 & h\lambda_{4,6}^{D} & h\lambda_{4,7}^{S} \\ 0 & 0 & 0 & 0 & 1-h\sum_{j=6}^{7}\lambda_{5,j} & h\lambda_{5,6}^{D} & h\lambda_{5,7}^{S} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix} \tag{3.14}$$

Az üzemmód-váltások figyelembe vétele az alábbiak szerint módosítja a 3.4 kifejezést.

$$\mathbf{s}(p+q+p+q+\cdots+r)=\bar{S}(0)\mathbf{T}_L^p\mathbf{T}^q\mathbf{T}_L^p\mathbf{T}^q\ldots\mathbf{T}_M^r \tag{3.15}$$

A 3.15 kifejezésben a p az üzemen kívüli, q a teszt, és r a feladatvégzés üzemmódok diszkrét idejű, egybefüggő időintervallumainak számai.

3.2.1 Aperiodikusan alkalmazott katonai berendezések teszt üzemmódjának beillesztése a Markov-modellbe

Az aperiodikusan alkalmazott katonai berendezések üzemen kívüli állapotát megszakító teszt vizsgálatakor az alábbiakat feltételezzük:

- a periodikus teszt üzemmódban a kezelőszemélyzet előírt műveletsort hajt végre. Amikor a kezelőszemélyzet hibát észlel, akkor sor kerül a berendezés javítatására. A javítás eredményét az előírt műveletsor végrehajtásával ellenőrzi;
- a műveletsor végrehajtására normál - nem a harci helyzetet imitáló körülmények között - történik (Az M3 mellékletben található eszköz meghibásodás alapértékek normál körülményeket feltételeznek);
- a teszt üzemmód kezdetekor a berendezés irányító rendszere nyugvó állapotból aktív állapotba kerül. Ez a meghibásodás-valószínűség érték jelentős növekedésével jár (M2 melléklet).
- a műveletsor elsődlegesen az irányítási rendszer **végrehajtóinak működését** ellenőrzi. A műveletsor időtartama rövid, legfeljebb néhány óra;
- a kezelőszemélyzet csak a detektálható, vagy leállást okozó hibaállapotokat képes észlelni, az összes többi állapotot sikeres működésként észleli, és ennek megfelelően jegyzőkönyvezi;
- a feltárt hibák javítási időtartama eltérő, ezért nem lehet átlagos értéket definiálni, ezért a nyugvó állapotot megszakító periodikus teszt üzemmódban a μ helyreállítás valószínűség **nem értelmezhető!** A nyugvó állapotot megszakító periodikus teszt tesztlefedettség C_M fogalmát az 1.28 kifejezés adja meg;
- a feltárt S_k hibaállapotok állapot-valószínűségét - a javítás eredményeként - legfeljebb a teszt üzemmód kezdeti $S_k(1)$ állapot-valószínűség értékekre állíthatók vissza, de ezt a mértéket is csökkenti a C_M tesztlefedettség értéke;
- a teszt üzemmód befejezésekor a berendezés irányító rendszere ismét nyugvó állapotba kerül. Ez a meghibásodás-valószínűség érték jelentős csökkenésével jár.

A teszt üzemmódra tett előbbi feltételezések mellett a teszt üzemmódra előírt műveletsor végrehajtásakor - a 15. ábra szerinti modellt alkalmazva - a kezelőszemélyzet a teszt üzemmód qT_0 időtartama alatt 3.16 kifejezéssel megadott valószínűséggel észlel hibát.

$$s_x = \frac{1}{qT_0} \sum_{i=1}^{q} s_2(i) + s_3(i) + s_6(i) + s_7(i) \tag{3.16}$$

Ugyanazon előírt műveletsor végrehajtása közben a kezelőszemélyzet a 3.17 kifejezéssel megadott valószínűséggel nem észlel hibát:

$$s_s = \frac{1}{qT_0} \sum_{i=1}^{q} s_1(i) + s_4(i) + s_5(i) \qquad (3.17)$$

Periodikus teszt üzemmód célja a hiba észlelése és javítatása. A 3.15 kifejezésben ezt az **állapot-valószínűségek korrekció**ival kell figyelembe venni. A valószínűségállapotok korrekciójára az egyik tanulmányomban [30]S már a következő javaslatot tettem:

A detektálható hibás **állapotok korrekciója** a hibaállapotok **előfordulás valószínűségével súlyozottan** történjen. Mivel csak statisztikai valószínűség adható meg, hogy melyik hibaállapot milyen valószínűséggel következik be, ezért a sikeres működés valószínűsége a hibaelhárítás okozta **átlagos javulás** mértékével emelkedjen meg és ennek megfelelően a hibás állapotok valószínűsége együttesen az átlagos javulás mértékével csökkenjen.[111]

Matematikailag ez a következőképpen valósítható meg: Tételezzük fel, hogy egyetlen időperiódusban végrehajtható a teszt és a javítás. Legyen az $\mathbf{s}_x$ sorvektor elemei azon állapotok, amelyekben a kezelőszemélyzet a kT_0 időtartam eltelte után végrehajtott teszt közben hibát észlelhet. Ennek megfelelően a 15. ábrán látható összevont 1002D hardver struktúrájú irányítási modell esetén a kezelőszemélyzet által kT_0 időtartam eltelte után végrehajtott teszt során észlelt $\mathbf{s}_x$ hibaállapot sorvektor a következő:

$$\mathbf{s}_x(k) = s_2(k) \quad s_3(k) \quad s_6(k) \quad s_7(k) \qquad (3.18)S$$

A maximális javíthatóság sorvektora $\mathbf{v}_x$ a hibaállapotok kT_0 időpontban és a berendezés első üzembehelyezéskor létező hibavalószínűségük különbségei, vagyis:

$$\mathbf{v}_x(k) = s_2(k) - s_2(1) \quad s_3(k) - s_3(1) \quad s_6(k) - s_6(1) \quad s_7(k) - s_7(1) \qquad (3.19)S$$

Egyszerűbben:

$$\mathbf{v}_x(k) = v_{x1}(k) \quad v_{x2}(k) \quad v_{x3}(k) \quad v_{x4}(k) \qquad (3.20)S$$

[111] Megjegyzés: Az elvégzett teszt alatt csak egy konkrét hibaállapotba kerülhet az eszköz. A fenti javaslat ezt úgy veszi figyelembe, hogy a hibaállapotok az előfordulásuk valószínűségének megfelelően vannak súlyozva, vagyis azt a trivialitást feltételezi, hogy az üzemelési élettartam alatt a hibavalószínűségeknek megfelelő gyakorisággal fordulnak elő a hibák. [31], [31]

A kT_0 időintervallumban végrehajtott teszt által feltárt hibák kijavítását követően következik be a berendezés átlagos javulása. A $\mathbf{v}_x$ sorvektor x darab elemének átlagértékét meghatározva a kT_0 időintervallumban az $v_{xavg}(k)$ átlagos javulás mértéket kapjuk meg. Az átlagos javulás mértéke a kezdeti állapot helyreállítását feltételezi, ezért az értékét módosítja a C_M tesztlefedettség.

$$v_{xavg}(k) = \frac{C_M}{x} \text{Sum } \mathbf{v}_x(k) \qquad (3.21)S$$

ahol az x azon állapotok száma, amelyben a kezelőszemélyzet hibát észlelhet.

Tekintve, hogy az irányítási rendszer üzemen kívüli állapotát megszakító periodikus teszt rövid, a sikeres működés illetve az állapotok hibavalószínűségének korrekciója **egyetlen időintervallum** bekövetkező változásként vehető figyelembe. A kT_0 időintervallumban végrehajtott teszt által feltárt hibák kijavítása következtében az állapotok hibavalószínűségének változásait egyetlen időperiódusként kezelve az alábbi egyenletek definiálják a korrigált állapot-valószínűség értékeket:

$$s_1(k+1) = s_1(k) + v_{xavg}(k) \qquad (3.22.a)S$$

$$s_2(k+1) = s_2(k) - v_{xavg}(k)\frac{s_2(k)}{s_2(k)+s_3(k)+s_6(k)+s_7(k)} \qquad (3.22.b)S$$

$$s_3(k+1) = s_3(k) - v_{xavg}(k)\frac{s_3(k)}{s_2(k)+s_3(k)+s_6(k)+s_7(k)} \qquad (3.22.c)S$$

$$s_4(k+1) = s_4(k) \qquad (3.22.d)S$$

$$s_5(k+1) = s_5(k) \qquad (3.22.e)S$$

$$s_6(k+1) = s_6(k) - v_{xavg}(k)\frac{s_6(k)}{s_2(k)+s_3(k)+s_6(k)+s_7(k)} \qquad (3.22.f)S$$

$$s_7(k+1) = s_7(k) - v_{xavg}(k)\frac{s_7(k)}{s_2(k)+s_3(k)+s_6(k)+s_7(k)} \qquad (3.22.g)S$$

A 3.22.a kifejezés a sikeres működés átlagos javulását tartalmazza.

A 3.22.d és a 3.22.e kifejezésekből következik, hogy az S_4 és S_5 állapot-valószínűség értékek nem változnak.

A 3.22.b, 3.22.c, 3.22.f, és 3.22.g kifejezések tartalmazzák a meghibásodás valószínűségek súlyozott csökkenését. Ezekben a kifejezésekben szerepel az $\mathbf{s}_x(k)$ sorvektor sorösszege. Ezért a további számításokhoz célszerű ezt meghatározni:

$$s_x(k) = \text{Sum } \mathbf{s}_x(k) \qquad (3.23)S$$

Behelyettesítve az $s_x(k)$ értékét azon 3.22 kifejezésekbe, amelyek a korrekció következtében változnak, majd rendezve azokat a következő sorvektor elemeket kapjuk:

$$s_1(k+1) = s_1(k) + v_{xavg}(k) \qquad \text{(3.24.a)S}$$

$$s_2(k+1) = s_2(k)\left\{1 - \frac{v_{xavg}(k)}{s_x(k)}\right\} \qquad \text{(3.24.b)S}$$

$$s_3(k+1) = s_3(k)\left\{1 - \frac{v_{xavg}(k)}{s_x(k)}\right\} \qquad \text{(3.24.c)S}$$

$$s_6(k+1) = s_6(k)\left\{1 - \frac{v_{xavg}(k)}{s_x(k)}\right\} \qquad \text{(3.24.d)S}$$

$$s_7(k+1) = s_7(k)\left\{1 - \frac{v_{xavg}(k)}{s_x(k)}\right\} \qquad \text{(3.24.e)S}$$

Az algoritmizálhatóság érdekében vezessük be a sikeres működés valószínűségének átlagos növekedését tartalmazó $\mathbf{v}(k)$ vektor-változót.

$$\mathbf{v}(k) = \begin{bmatrix} v_{xavg} & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad \text{(3.25)S}$$

A periodikus teszt állapot-konverzióját leíró 3.24.b … 3.24.e kifejezésekhez most vezessük be a hibaállapotban maradás csökkenő valószínűségét tartalmazó $\mathbf{w}(k)$ vektorváltozót:

$$\mathbf{w}(k) = 1 \quad wa(k) \quad wa(k) \quad 1 \quad 1 \quad wa(k) \quad wa(k) \qquad \text{(3.26)S}$$

ahol a wa(k) változó a 3.24 kifejezésekben szereplő $1 - \frac{v_{xavg}(k)}{s_x(k)}$ érték.

A végrehajtott teszt során észlelt hibák kijavítása után bekövetkező állapotkorrekció utáni $\mathbf{s}_{korr}(k+1)$ állapotvalószínűség vektor az alábbi vektorművelet formulával számítható:

$$\mathbf{s}_{korr}(k+1) = \text{Diag}\left[\mathbf{w}^T(k)\mathbf{s}(k) + \mathbf{v}^T(k)\right]^T \qquad \text{(3.27)S}$$

Amennyiben $(i-1)T_0$ üzemen kívüli állapot után az ellenőrző teszt a iT_0 időperiódusban normál körülmények között történik és nem detektálódik hiba, majd újra üzemen kívüli állapot következik, akkor az $(i+1)T_0$ időperiódusban az állapotvektor a 3.15 kifejezéssel megadott algoritmus szerint a következő:

$$\mathbf{s}(i+1) = \mathbf{s}(0)\mathbf{T}_L^{(i-1)} \cdot \mathbf{T} \cdot \mathbf{T}_L \qquad \text{(3.28)}$$

A 3.27 kifejezés voltaképpen azonos a 3.22 kifejezésekkel. A 3.27 kifejezés $\bar{S}_{korr}(k+1)$ állapotvalószínűségei a 15. ábra Markov-modelljének megfelelő hét állapot kT_0 időtartam eltelte utáni értéke, ahol feltételezzük, hogy kT_0 időtartam alatt lezajlott a teszt és a javítás. Ehhez a periodikus tesztekkel megszakított üzemen kívüli üzemállapot vizsgálatához **megfelelő T_0 időalapot** (pl.: két napot) kell választani!

Az üzemen kívüli állapotot megszakító tesztek célja a hibák felderítése, kijavítása, és így a meghibásodás-valószínűség csökkentése. Ezért az $(i \cdot m)T_0$ időperiódusban az **s** állapotvektor meghatározása a 3.28 kifejezés alkalmazása helyett a 3.27 kifejezésnek megfelelő **állapot-korrekcióval** valósul meg.

Bár a végső vizsgálatokhoz elegendő az **s**(k) állapotvektorok diszkrét idejű sorozata, a 3.28 kifejezés korrekt folytatása érdekében mégsem elegendő, hogy az $\mathbf{s}(i \cdot m)$ állapotvektort lecseréljük az $\mathbf{s}_{korr}(i \cdot m)$ állapotvektorra. Ahogy az a 3.15 kifejezésből következik az $\mathbf{s}(i \cdot m) = \mathbf{s}(0)\mathbf{T}_{korr}(i \cdot m)$ művelet az algoritmizálható eljárás.

A $\mathbf{T}_{korr}(i \cdot m)$ átmenet-valószínűségmátrix időben változó érték és minden $i \cdot m \cdot T_0$ időintervallumban meg kell határozni. Ellenőrző tesztekkor a következő műveletsort kell végrehajtani:

$$\mathbf{s}(i \cdot m - 1) = \mathbf{s}(0)\mathbf{T}_L^{(i \cdot m - 1)} \qquad (3.29.a)S$$

$$\mathbf{s}(i \cdot m) = \mathbf{s}_{korr}(i \cdot m) = \mathbf{s}(0)\mathbf{T}_{korr}(i \cdot m) \qquad (3.29.b)S$$

$$\mathbf{s}(i \cdot m + 1) = \mathbf{s}(0)\mathbf{T}_{korr}(i \cdot m) \cdot \mathbf{T}_M \qquad (3.29.c)S$$

A $\mathbf{T}_{korr}(i \cdot m)$ sorainak meghatározása:

- A $\mathbf{T}_{korr}(i \cdot m)$ mátrix első sorának és a 3.27 kifejezésnek megfelelő $\mathbf{s}_{korr}(i \cdot m)$ állapotvektornak azonosnak kell lenniük.

  Az, hogy a $\mathbf{T}_{korr}(i \cdot m)$ állapotvalószínűség mátrix első sora megegyezik a $\mathbf{s}_{korr}(i \cdot m)$ állapotvektorral következik a 3.3 és a 3.29.b kifejezésekből.

- A $\mathbf{T}_{korr}(i \cdot m)$ mátrix második és harmadik sorai az eredeti $\mathbf{T}_L$ állapotvalószínűség mátrix megfelelő sorai, de a tesztlefedettség tökéletlensége miatt az adott sornak megfelelően korrigálni kell a 3.5 kifejezés szerint.

  A teszt során vagy az derül ki, hogy nincs ebben a hibaállapotban a rendszer, vagy ha mégis akkor a hiba kijavításra kerül. A tesztlefedettség tökéletlensége miatt nem áll helyre az eredeti állapot. A hibavalószínűségeket a kiindulási állapothoz képest konstans $1+(1-C_M)$ tényezővel kell felszorozni. A második sorhoz szükség van az

$\mathbf{i}_2 = 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0$, a harmadik sorhoz az $\mathbf{i}_3 = 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0$ segédvektorokra.

2. sor: $\mathbf{T}_{\text{korr}}\ 2,: = (\mathbf{T}_{\text{L}}\ 2,: - \mathbf{i}_2)\cdot(2 - \text{C}_{\text{M}}) + \mathbf{i}_2$ (3.30.a)S

3. sor: $\mathbf{T}_{\text{korr}}\ 3,: = (\mathbf{T}_{\text{L}}\ 3,: - \mathbf{i}_3)\cdot(2 - \text{C}_{\text{M}}) + \mathbf{i}_3$ (3.30.b)S

- A $\mathbf{T}_{\text{korr}}(\text{i}\cdot\text{m})$ mátrix negyedik és ötödik sorai megegyeznek a $\mathbf{T}_{\text{L}}^{(\text{i}\cdot\text{m})}$ mátrix negyedik és ötödik sorával.

A 3.15. ábra szerinti modellben a negyedik és az ötödik állapot a kezelőszemélyzet számára felderítetlen marad, ezért a $\mathbf{T}_{\text{L}}^{(\text{i}\cdot\text{m}-1)}\cdot\mathbf{T}_{\text{L}}$ mátrixszorzat és a $\mathbf{T}_{\text{korr}}$ korrigált állapotvalószínűség mátrix negyedik és az ötödik sora **nem különbözhetnek** egymástól.

- A $\mathbf{T}_{\text{korr}}(\text{i}\cdot\text{m})$ mátrix hatodik és hetedik sorai az eredeti $\mathbf{T}_{\text{L}}$ állapotvalószínűség mátrix megfelelő soraival egyeznek meg.

A 3.15. ábra szerinti modellben a hatodik és hetedik állapotok nyelő típusúak. Ha az ellenőrző teszt közben a rendszer ezek az állapotok valamelyikébe kerül, akkor működésképtelené válik, vagyis a hiba nem maradhat rejtve! Ezért a javítás utáni állapot az eredeti $\mathbf{T}_{\text{L}}$ állapotvalószínűség mátrixnak megfelelő.

3.2.2 PFM_{Bavg} számítása

A PFM_{Bavg} érték számításához ismerni kell a **T** átmenet-valószínűségmátrixot. Az irányítási rendszer eszközeinek hibatípusonként megadott, normálállapothoz tartozó λ meghibásodási ráta értékeiből a hardver elrendezés ismeretében a **T** átmenet-valószínűségmátrix meghatározható.

Az üzemen kívüli állapot a λ meghibásodási rátákat egy h_L konstans szorzótényezővel (M2 melléklet) csökkenti. Ez befolyásolja a sikeres működés és a hibavalószínűség értékeket, vagyis a **T** átmenet-valószínűségmátrix elemeit. A szorzótényező hatását a 3.5 kifejezés szerint kell figyelembe venni és így felírható az üzemen kívüli állapotra jellemző $\mathbf{T}_{\text{L}}$ átmenet-valószínűségmátrix.

A teszt üzemmódban a normál üzemi körülményekre megadott **T** átmenet-valószínűségmátrixszal kell számolni. Az üzemen kívüli állapotból a 3.5 kifejezés szerint $1/h_L$ szorzótényezővel lehet visszatérni a teszt üzemmódra jellemző **T** átmenet-valószínűségmátrixhoz.

Az aperiodikusan alkalmazott katonai berendezések feladat-végrehajtáskor a normál üzemi körülményekhez képest nagyobb megterhelésnek vannak kitéve. A nagyobb megterhelés, valamint a kezelőszemélyzet, mint hibaforrás megnöveli a λ meghibásodási rátákat, ami egy konstans $h_M = h_C \cdot h_A$ szorzótényezővel vehető figyelembe. A 3.5 kifejezés szerint figyelembe véve a konstans h_M szorzótényezőt, jutunk a feladatvégzés üzemmódra jellemző $\mathbf{T}_M$ átmenet-valószínűségmátrixhoz.

A PFM_{Bavg} számításához az utolsó teszt óta eltelt idő, valamint a feladatvégzés alatt az **s** állapotvektor iT_0 időtartományonként meghatározott értékeire van szükség. Katonai szempontból a berendezés üzemelése az elsődleges, ami amennyiben a 15. ábrán látható modellt alkalmazzuk, akkor a működés az s_1 …, s_5 állapotokban egyaránt biztosított. Viszont a berendezés leállását okozó s_6 és s_7 állapotok egyaránt elkerülendők. A PFM_{Bavg} a következő összefüggéssel határozható meg:

$$PFM_{Bavg} = \frac{\sum_{i=n\cdot m}^{n\cdot m+k-1} s_6(i)+s_7(i)}{(k-1)T_0} + \frac{\sum_{i=n\cdot m+k}^{n\cdot m+k+j} s_6(i)+s_7(i)}{(j+1)T_0} \qquad (3.31)S$$

ahol: T_0 az időalap, „n” a periodikus tesztek száma, „mT_0” az üzemen kívüli állapot hossza két teszt között, „kT_0” az utolsó teszt és a feladatvégzés kezdete közötti időtartam hossza, „jT_0” a feladatvégzés időtartam hossza.

Az üzemmód váltások miatt a 3.31 kifejezés több lépésben számítható ki:

- Először meg kell határozni az $s_6(n\cdot m)$ és $s_7(n\cdot m)$ értékeit. Ehhez szükségesek a **T** és $\mathbf{T}_L$ átmenet-valószínűségmátrixok, valamint mT_0 időközönként a $\mathbf{T}_{korr}(i\cdot m)$ meghatározására.
- Ezután kell meghatározni a PFM_{LBavg} értéket. Ehhez a 3.31 kifejezés első összetevőjét kell meghatározni.

$$PFM_{LBavg} = \frac{1}{(k-1)T_0} \sum_{i=n\cdot m}^{n\cdot m+k-1} s_6(i)+s_7(i) \qquad (3.31.a)S$$

- Ez követően kell meghatározni a PFM_{MBavg} értéket. Ehhez 3.31 kifejezés második összetevőjét kell kiszámítani.

$$PFM_{MBavg} = \frac{1}{(j+1)T_0} \sum_{i=n\cdot m+k}^{n\cdot m+k+j} s_6(i)+s_7(i) \qquad (3.31.b)S$$

- Végül összegezni kell a 3.31.a és 3.31.b kifejezéseket.

$$PFM_{Bavg} = PFM_{LBavg} + PFM_{MBavg} \qquad (3.31.c)S$$

3.3 Számítási algoritmusok

A számítási eljáráshoz ismerni kell a **T** átmenet-valószínűségmátrixot. Az aperiodikusan alkalmazott katonai berendezések esetén a 3.1.2 fejezetben leírt eljáráshoz képest - a biztonság-kritikusra tervezés következtében - a **T** átmenet-valószínűségmátrix meghatározása annyiban módosul, hogy valamennyi alapirányítási és vész, védelmi műveletet definiálni kell (3.1.2 fejezet 1. pont) és azonos szerkezetű Markov gráfot kell minden művelethez rendelni (3.1.2 fejezet 6. pont). Annak betartása érdekében, hogy egy eszköz csak egy művelethez tartozzon, összetett műveleteket kell definiálni (pl.: a munkahenger kitol, és a munkahenger behúz két művelete helyett egy összetett munkahenger mozog műveletet). Ezután az N darab összetett művelethez tartozó átmenet-valószínűségmátrixot összegezni[112] kell.

$$\mathbf{T} = \mathbf{I} + \sum_{i=1}^{N} (\mathbf{T}_i - \mathbf{I}) \qquad (3.32)S$$

Ez alapján a számítási algoritmus számára kiválasztjuk az állandó tartalmú $t = \mathbf{T}\ 7,7$ [7,7] dimenziójú mátrixváltozót. A 3.5 kifejezés felhasználásával deklaráljuk az üzemen kívüli üzemállapothoz tartozó $tl = \mathbf{T}_L(7,7)$ és a feladatvégzés üzemállapothoz tartozó $tm = \mathbf{T}_M(7,7)$ állandó tartalmú mátrixváltozókat.

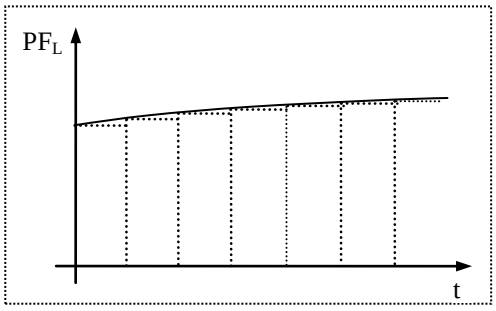
A periodikus tesztekkel megszakított, üzemen kívüli üzemállapot több hónapig, esetleg évekig tart. A T_0 [h^{-1}] időalap alkalmazásával több ezer $\mathbf{s}(k)$ állapot-vektort kell kiszámítani úgy, hogy a $\mathbf{T}_L$ átmenet-valószínűségmátrix értékei nagyon kicsik. A kerekítési problémák miatt a $\mathbf{T}_L$ átmenet-valószínűségmátrix elemeit duplaszó formátumúra kell választani. A duplaszó formátumú, nagyon-nagyméretű mátrixszal végzett műveletek komoly számítási erőforrást igényelnek.

Az üzemen kívüli állapotban nagyjából egy nagyságrenddel csökken a λ meghibásodási ráta a folytonos üzemelés üzemmódhoz képest, ezért $PF_L(t)$ időbeni változása lassúbb, ennek következtében egy vagy két napos időalapra történő **időkonverzió** okozta hiba elhanyagolható.

---

[112] A 3.31 kifejezések magukba foglalják az összes leállást okozó hibatípust, nem csak a veszélyes hibákat, a 3.32 kifejezés összegzi az összes SIF művelet meghibásodás valószínűségét. Így a leírt eljárás által számított meghibásodás-valószínűség értékek körül belül két nagyságrenddel nagyobbak, mint amire az IEC szabványok által egyetlen SIF műveletre definiált SIL mérőszámot illesztették. Ez az oka, hogy az MSIL mérőszám bevezetését javaslom.

A PF_{Lavg} hibavalószínűség diszkrét idejű kiszámítása analóg kerekítési problémát jelent, mint a numerikus integrálszámítás (16. ábra). Az időalap megnövelése az üzemen kívüli állapot és az időszakos teszt meghibásodás valószínűségeinek diszkrét idejű számításakor egyrészt csökkenti a túlságosan kis számértékeknél fellépő kerekítési problémát. másrészt összhangban van a 3.27 kifejezéssel definiált időszakos teszt **egyetlen időperiódusban** végrehajthatott állapot-korrekcióként kezelésével.



16. ábra. Az időalap konverzió hibája
(Készítette: Neszveda József)

Legyen a megnövelt időalap két nap[113], mert két nap még modulcserével megvalósítható kisebb javításokkal együtt is elegendő az időszakos teszt végrehajtására. Ezért vezessük be a két napos (T_N = 48 [h]) időegységet a periodikus tesztekkel megszakított üzemen kívüli állapot vizsgálatára. Az időegység-váltás hatása a meghibásodási rátára:

$$\lambda_N\left[\frac{1}{48}h^{-1}\right] = h_N \cdot \lambda_H\left[h^{-1}\right] \qquad (h_N = 48.) \qquad (3.33)S$$

A számítási algoritmusban az időlépték konverzióhoz az üzemen kívüli üzemállapothoz tartozó „tl” átmenet-valószínűség mátrixváltozó elemeit a 3.5 kifejezésnek megfelelően kell az új időléptéknek megfelelőre átkonvertálni, majd az így kapott „tln” mátrix-változóval elvégezni a számításokat.

A PFM_{Bavg} kiszámítása az időben egymást követő **s**(k) állapot-vektorok felhasználásával történik. Mint már szó eset róla a 3.28 kifejezés számítógépes erőforrás igénye nagy, ezért a 3.29 kifejezésekhez hasonló rekurzív formuláját célszerű alkalmazni az **s**(k) állapot-vektorok kiszámításához.

---

[113] Az időszakos teszt 2 napos időalapja nem igényli azt a feltevést, hogy ebben az időperiódusban csak egy hiba történhet, mert a 3.24 kifejezéseknek megfelelően a hibaállapotok az átlagos statisztikai valószínűségnek megfelelően változnak, vagyis az eseti változások az üzemelés-életciklus alatt a statisztikai valószínűséghez simulnak.

A 17. ábra a PFM_{Bavg} kezdeti értékének meghatározásának folyamatábrája. A 3.28 helyett a 3.34 kifejezésekkel megadott rekurzív formula alkalmazásával nagymértékben csökkenti a számítási kapacitásigényt.

$$\mathbf{s}(\mathrm{i}) = \mathbf{s}(0)\mathbf{T}^{\mathrm{i}} \qquad 3.34.a$$

$$\mathbf{T}(\mathrm{i}) = \mathbf{T}^{\mathrm{i}} \qquad 3.34.b$$

$$\mathbf{T}^{\mathrm{i}} = \mathbf{T}(\mathrm{i})\mathbf{T} \qquad 3.34.c$$

A 3.34 kifejezésben megadott rekurzív formula alkalmazásához a számítási algoritmusban deklarálni kell az „s0” (ahol $s0 = 1 \quad 0 \quad \cdots \quad 0$) vektorváltozót, ami az állapotvektor kiinduló állapota. Továbbá meg kell határozni a változó tartalmú „t0” és „t1” mátrixváltozókat, amelyek mindhárom üzemmódban alkalmazhatók.

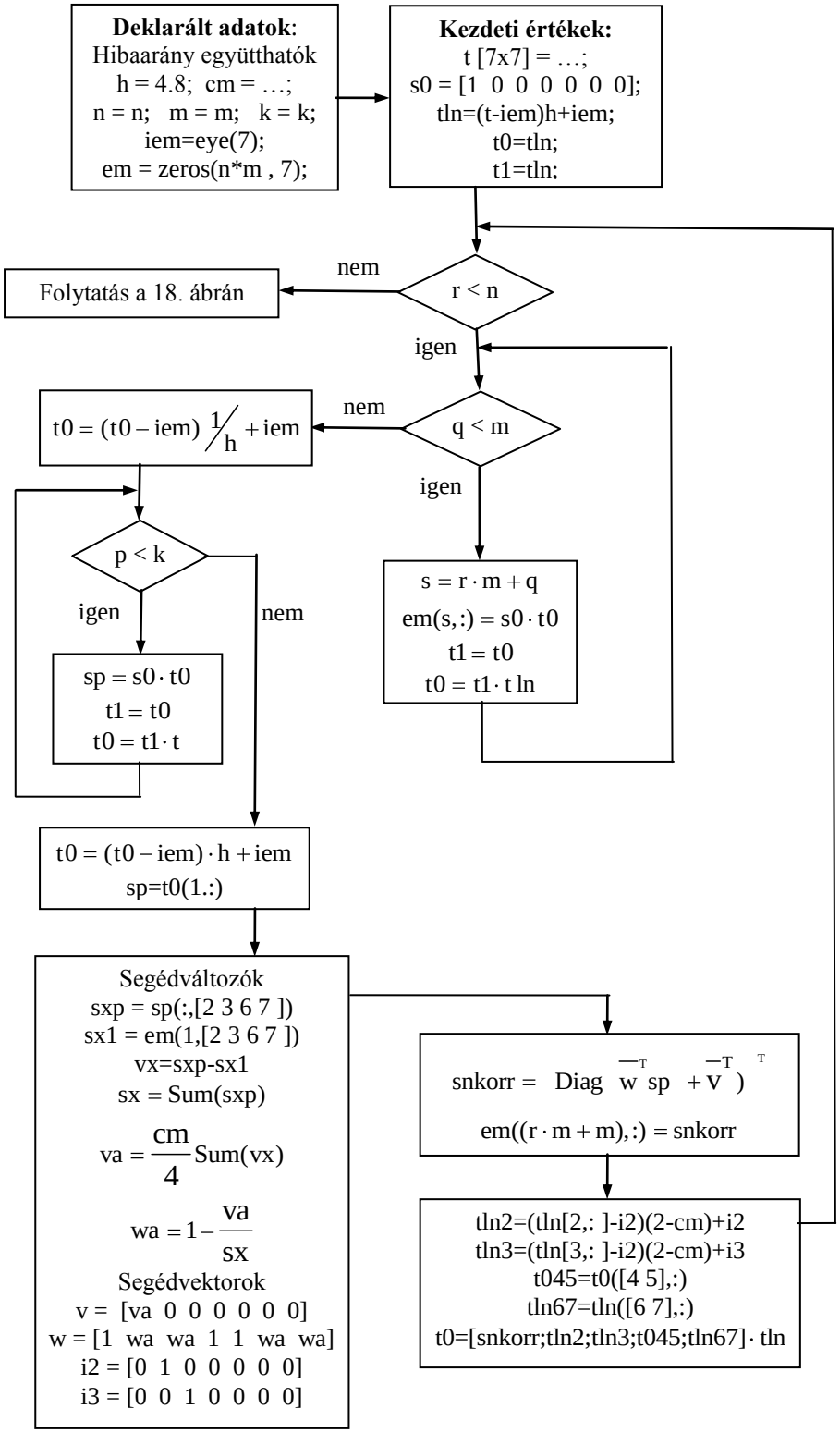
A 3.34 kifejezések algoritmizálásakor a „t0” mátrixváltozó az aktuális $\mathbf{T}^{\mathrm{i}}$, a „t1” mátrixváltozó a $\mathbf{T}(\mathrm{i})$. A „t0” és „t1” mátrixváltozók kezdeti (i=1) értékei az üzemen kívüli üzemállapothoz tartozó, időkonvertált $\mathbf{T}_{\mathrm{LN}}$ átmenet-valószínűségmátrix $\mathrm{t0}_{\mathrm{i=1}} = \mathrm{t1}_{\mathrm{i=1}} = \mathrm{t\,ln}$.

Az algoritmusban a periodikus tesztekkel megszakított, üzemen kívüli üzemmódhoz tartozó állapotvektorokat ($\mathbf{s}(1)$-től $\mathbf{s}(\mathrm{n}\cdot\mathrm{m})$-ig) helyezzük el egy $\mathrm{n}\cdot\mathrm{m},7$ dimenziójú „em” eredménymátrixba. Az „em” eredménymátrixnak a tesztgyakoriság és tesztlefedettség vizsgálatában van szerepe. Az MSIL besoroláshoz elegendő az $\mathbf{s}(\mathrm{n}\cdot\mathrm{m})$ állapotvektor, valamint az $\mathrm{n}\cdot\mathrm{m}\cdot\mathrm{T}_0$ időtartományban a „t0” változó tartalmú mátrixváltozó ismerete.

A 18 ábra az utolsó teszt és a feladatvégzés kezdete közötti állapotvektorokat kiszámító algoritmus folyamatábrája. Az utolsó teszt és a feladatvégzés kezdete közötti állapotvektorokat egy $(\mathrm{k}-1),7$ dimenziójú „eml” eredmény-mátrixba helyezzük el. Az „eml” eredménymátrix a PFM_{LBavg} érték kiszámításához kell.

A 19. ábra a feladatvégzés üzemmód algoritmus folyamatábrája. A feladatvégzés üzemmód állapotvektorait egy $(\mathrm{j}+1),7$ dimenziójú „emm” eredmény-mátrixba helyezzük. Az „emm” eredménymátrix a PFM_{MBavg} érték kiszámításához szükséges.

3.3.1 Periodikus tesztekkel megszakított, üzemen kívüli üzemmód állapotvektorait meghatározó algoritmus



17. ábra. A periodikus tesztekkel megszakított, üzemen kívüli állapot folyamat ábrája
(Készítette: Neszveda József)

Az 17. ábra folyamatábrájához tartozó Matlab[114] M fájlok programjai az M8. melléklet 1a (deklaráció), és 1b (rekurzív számítási algoritmus).

A 17. ábrán látható folyamatábra szöveges leírása:

Deklarált adatként be kell gépelni a konkrétan vizsgált berendezés **T** átmenet-valószínűség mátrixnak megfelelő „t" mátrixváltozó értéket, valamint a h_N időalap konverziót és a 0,1 üzemen kívüli állapot konverziót együttesen tartalmazó „h" konverziós konstans értéket. Esetünkben $h = 0{,}1 \cdot h_N = 4{,}8$. Ugyancsak deklaráljuk az üzemen kívüli állapot hosszát kifejező „m", a periodikus tesztek számát „n" és időtartamát „k" megadó konstansokat.

A számításokhoz továbbá deklaráljuk a [7x7] dimenziójú **I** egységmátrixnak megfelelő az „iem" és a [$(n \cdot m)$x7] dimenziójú eredménymátrixnak az „em" mátrixváltozókat.

Ezután megadásra kerül a kezdeti értéket kifejező „s0" vektorváltozó és az algoritmus meghatározza a kezdeti „tln", „t0", és „t1" mátrixváltozókat.

A periodikus tesztekkel megszakított üzemen kívüli üzemállapothoz tartozó, T_N időközönként meghatározott egymást követő $\mathbf{s}_N(q)$ (ahol q=1÷(m-1)) állapotvektorok a 3.34 kifejezés rekurzív formulája szerint vannak meghatározva és az „em" eredmény-mátrix megfelelő soraiban tárolva.

Az mT_N időszakonként elvégzett periodikus teszt aktív eszközön történik és időtartama néhány óra, emiatt az $(m-1)T_N$ időperiódust követően vissza kell térni a tesztet jellemző normál üzemi körülmények közé és a T_0 [h^{-1}] időléptékre. Ez a „t0" mátrixváltozó - 3.5 kifejezés szerint 1/h konstanssal - normál üzemi körülményekre és T_0 [h^{-1}] időléptékre történő konvertálásával valósítható meg. A teszt üzemmódot a 3.34 kifejezéssel megadott rekurzív formula néhányszor (k=2÷5) végrehajtása modellezi. **Ilyenkor** az így kapott „$sp(r \cdot m + p)$" vektorváltozó értékek (p=1÷ k-1) **nem kerülnek** az „em" eredmény-mátrixba. A 3.22 kifejezések szerinti egyetlen időperiódusban megvalósuló állapot-korrekció kiinduló értékek az „$sp(r \cdot m + k)$" vektorváltozó érték. Az algoritmus ezt úgy állítja elő, hogy először a „t0" mátrixváltozót a 3.5 kifejezés szerint h konstanssal az „em" eredménymátrix soraival azonos időalapra konvertálja. Így a „t0" mátrixváltozó első sora azonos az „$sp(r \cdot m + k)$" vektorváltozóval.

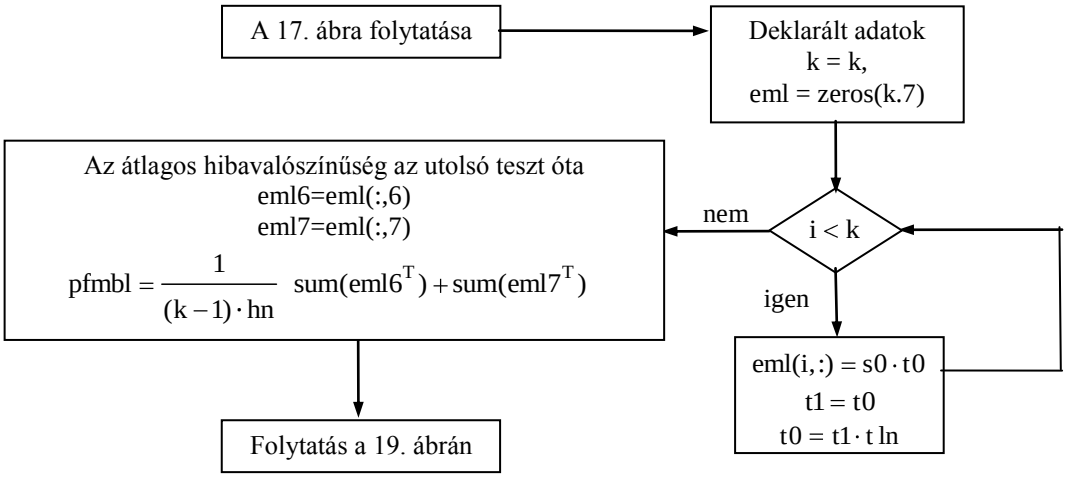
[114] Az értekezés a Matlab program [32], [33] függvényeit alkalmazza a folyamatábra és az algoritmusok megadásakor.

A 3.20 kifejezésnek megfelelő $\mathbf{s}_x(r \cdot m + k)$ állapotvektor az „sxp” vektorváltozó és az **s**(1) állapotvektor az „sx1” vektorváltozó, ami az „em” eredmény mátrix első sorával azonos. A 3.21 kifejezésnek megfelelő $\mathbf{v}_x(r \cdot m + k)$ állapotvektor a „vx” vektorváltozó. Ezt követően a 3.23 kifejezésnek megfelelő s_x érték az „sx” vektorváltozó, a 3.21 kifejezésnek megfelelő $v_{xavg}(i \cdot m + k)$ az „va” vektorváltozó, és végül a „wa” vektorváltozót határozza meg az algoritmus.

A következő lépés, hogy a periodikus teszt állapotkonverzióját leíró 3.27 kifejezés végrehajtásához deklaráljuk 3.25 kifejezésnek megfelelő **v** és a 3.26 kifejezésnek megfelelő **w** vektorváltozókat. Az „em” eredmény-mátrix minden m-edik sora az „$snkorr(i \cdot m)$” vektorváltozó, amit a 3.29.b kifejezéssel lehet meghatározni. Ehhez ismerni kell a $\mathbf{T}_{korr}(i \cdot m)$ mátrixot, vagyis a „t0” mátrixváltozón végre kell hajtani a 3.2.1 fejezetben leírt konverziót.

3.3.2 Az utolsó teszt és a feladatvégzés üzemmód kezdete közötti állapotvektorokat meghatározó algoritmus

Az algoritmushoz tartozó Matlab M fájl az M8. melléklet 2 programja. Ilyenkor az aperiodikusan alkalmazott katonai berendezés üzemen kívüli állapotban van, ezért a hibavalószínűségeket úgy kell értelmezni, hogy üzembehelyezéskor, vagyis a k-dik T_N időintervallumban ilyen valószínűséggel jelenik meg a hiba.



18. ábra. Az utolsó teszt és a feladatvégzés kezdete közötti üzemen kívüli állapot folyamat ábrája (Készítette: Neszveda József)

Az algoritmus szöveges magyarázata:

Az $n \cdot m - dik$ T_N időintervallum az utolsó teszt a szimulációs vizsgálatban. Rendelkezésre áll az $n \cdot m - edik$ „t0” mátrixváltozó, valamint a „h” állapotkonverzió és időlépték váltó konstans.

Az algoritmus számára deklarálni kell a „k” konstanst, ami az utolsó teszt és a feladatvégzés közötti T_N időintervallum száma. Továbbá egy új „eml” [(k-1),7] dimenziójú eredménymátrixot, mert a további számítás egyszerűsítése céljából az $\mathbf{s}(n \cdot m + i)$ állapotvektorokat, ahol (i=1÷k-1) külön célszerű elhelyezni. A feladatvégzés kezdetéig csak (k-1)T_N időintervallum kiszámítására van szükség, mert a k-dik időintervallumnak a feladatvégzés előtti üzembe-helyezést tekintjük.

Az $\mathbf{s}(n \cdot m + i)$ állapotvektorok kiszámítása a 3.34 kifejezések rekurzív formulája szerint történik. A PFM_{LBavg} érték a 3.31.a kifejezés alapján az „eml” eredménymátrix 6. (veszélyes leállás) és 7. (hamis leállás) oszlopainak sorösszegeként számítható.

Az „eml” eredménymátrixban az üzemen kívüli állapothoz tartozó állapotvalószínűségek értékek 48 órás időléptékűek. A PFM_{MBavg} érték két összetevőjét (3.31 kifejezés) azonos időléptékben kell összegezni, ezért az eredménymátrix megfelelő oszlopain állapot és időlépték konverziót kell végrehajtani. Az állapot és időlépték konverzió elvégezhető az oszlopvektorok sorösszegének 1/h konstanssal történő szorzásával, mert a 6. és 7. oszlopok elemei hibavalószínűségek. Így a 15. ábra szerinti Markov-modellhez tartozó időkonvertált PFM_{LNBavg} érték:

$$PFM_{LNBavg} = \frac{1}{(k-1)T_0}\left\{\frac{Sum\ \ eml\ :,6\ ^{T}}{h} + \frac{Sum\ \ eml\ :,7\ ^{T}}{h}\right\} \qquad (3.35.a)S$$

3.3.3 Feladatvégzés üzemmód állapotvektorait meghatározó algoritmus

Az algoritmushoz tartozó Matlab M fájl az M8. melléklet 3 programja tartalmazza.

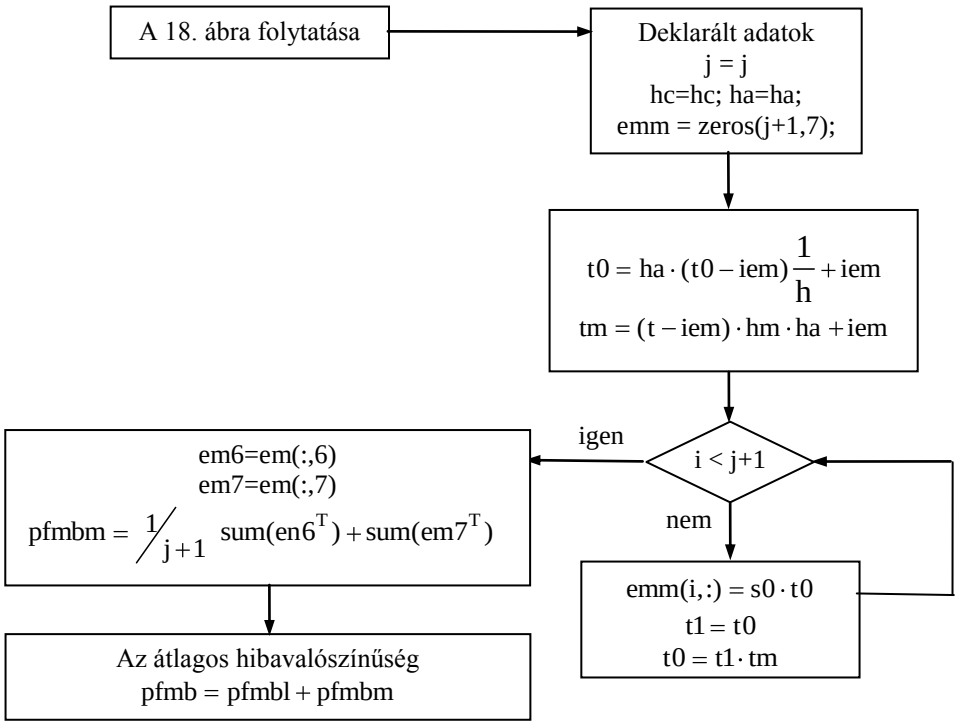
Rendelkezésre áll az $(n \cdot m + k - 1) - edik$ „t0” mátrixváltozó T_N időléptékhez és üzemen kívüli állapothoz tartozó értékekkel, továbbá a h állapotkonverzió és időlépték váltó konstans. Az algoritmus számára deklarálni kell a „j” konstanst, ami az üzemelési órák száma, és a h_A emberi tényező „ha” változóját, valamint a h_M az üzemelés körülményeinek nehézségét kifejező konstansnak megfelelő „hm” változót.

A könnyebb kezelhetőség végett a feladatvégzés üzemmódhoz tartozó állapotvektorokat egy új „emm” [(j+1),7] dimenziójú eredménymátrixba célszerű

elhelyezni. A PFM_{MBavg} érték az „emm” eredménymátrix 6. (veszélyes leállás) és 7. (hamis leállás) oszlopainak sorösszegeként lesz számítható:

$$PFM_{MBavg} = \frac{1}{(j+1)T_0} \text{ Sum emm :,6 }^{T} + \text{Sum emm :,7 }^{T} \qquad (3.35.b)S$$

Az $(n \cdot m + k - 1)T_N$ időintervallumot követően az $(n \cdot m + k)T_0$ időintervallummal folytatódik a vizsgálat, ami a berendezés üzembehelyezése. Ebben az algoritmusban vesszük figyelembe az üzembehelyezést, valamint a „j” órányi üzemelési időt. A feladatvégzés üzemmód folytonos jellegű, ezért az $\mathbf{s}(n \cdot m + i)$ állapotvektorok - ahol (i=1÷j+1) - kiszámításához vissza kell térni a T_0 [h^{-1}] időalapra. Ehhez az $(n \cdot m + k - 1) - edik$ „t0” mátrixváltozón, a 3.5 kifejezés szerint $1/h$ értékkel beszorozva, idő és állapotkonverziót kell végrehajtani.



19. ábra. A feladatvégzés üzemmód folyamat ábrája
(Készítette: Neszveda József)

Az aperiodikusan alkalmazott katonai berendezések általában nehéz körülmények között, és/vagy mobil szerkezetre szerelten működnek. A 3.34 kifejezésben megadott rekurzív formulához képest, a normál körülményekre jellemző „t” mátrix-változó helyett, az üzemelés körülményeire jellemző „tm” mátrix-változót kell alkalmazni, amit

a feladatvégzés körülményeinek nehézségétől függő h_M (M2 melléklet) konstans változó figyelembe vételével kapunk.

A 19. ábrán látható folyamatábra olyan üzemeltetési gyakorlatot szimulál, amikor az üzembehelyezést követően nem azonnal, hanem fokozatosan kerül a berendezés nehéz üzemelési körülmények közé (pl.: légvédelmi rakétaüteg szállító-töltő gépkocsi), és a működtetés félautomatikus, vagyis van kezelőszemélyzet. A 19. ábrán látszik, hogy a 3.34 rekurzív formula alapján számított „emm" eredménymátrix első sora a normál üzemi körülmények szimulálására konvertált „t0" mátrixváltozó első sorával azonos. Ez jól szimulálja azt, hogy az üzembehelyezés általában normál körülmények között zajlik. Van kezelőszemélyzet, tehát az üzembe-helyezéskor és feladatvégzés közben előfordulhat ember okozta hiba, amit a „ha" változó reprezentál.

$$t0 = h_A \cdot (t0 - iem)\frac{1}{h} + iem \qquad (3.36.a)S$$

$$tm = (t - iem) \cdot h_M \cdot h_A + iem \qquad (3.36.b)S$$

A feladatvégzés üzemmód 19. ábrán látható kialakítása következtében a kezelőszemélyzet kiképzettségét reprezentáló „h_A" konstans hatása azonnal, a feladatvégzés körülményeinek nehézségét reprezentáló „h_M" konstans hatása viszont fokozatosan érvényesül. A legelső ciklusban (órában) egyáltalán nem, majd fokozatosan növekedve számos ciklus (óra) után érvényesül teljes mértékben a „tm" mátrix-változóban figyelembe vett „h_M" konstans.

Amennyiben a berendezés automatikus (nincs kezelőszemélyzet) és az üzembehelyezést követően azonnal nehéz üzemelési körülmények közé kerül (pl.: az ellenség vonala mögé dobható autonóm rádió-lokációs zavaró eszközök), akkor a „t0" és a „tm" mátrixváltozókat a következő kifejezésekkel kell konvertálni:

$$t0 = h_M \cdot (t0 - iem)\frac{1}{h} + iem \qquad (3.37.a)S$$

$$tm = (t - iem) \cdot h_M + iem \qquad (3.37.b)S$$

A 3.31 kifejezéseknek megfelelően a PFM_{Bavg} érték a 3.35.a és a 3.35.b kifejezések összege. Az így kapott érték alapján lehet a konkrét alkalmazás mellett (tárolási idő, tesztek sűrűsége, az üzemelés időtartama, stb.) az aperiodikusan alkalmazott katonai berendezést MSIL osztályba (4. táblázat) sorolni.

3.4 Összefoglalás és következtetések

Vizsgálataim alapján az aperiodikusan alkalmazott katonai berendezések irányítórendszer megbízhatóság analízisét az **idő-diszkrét állapotterű Markov analízis módszer**rel célszerű elvégezni.

Ehhez kidolgoztam a hét összevont állapotot tartalmazó Markov gráfot (**15. ábra**), az átmenet-valószínűségek meghatározásának szempont-rendszerét (**3.2.1 fejezet**), és a biztonság-kritikusra tervezett berendezés összes műveletét együttesen tartalmazó **T** átmenet-valószínűség mátrix meghatározását (**3.32 kifejezés**).

Az üzemmód-váltásokból adódó λ meghibásodási ráta ugrások kezelésére kidolgoztam az átmenet-valószínűség mátrix **konverziós szabály**át (**3.5 kifejezés**). Ez a konverziós szabály alkalmas az **üzemelési körülmény** faktorok figyelembe vételére.

A kidolgozott Markov-modellhez megállapítottam az üzemen kívüli állapotot megszakító ellenőrző **teszt üzemmód beillesztés**ének szabályait (3.2.1 fejezet) és levezettem az ehhez szükséges **hibaállapot-vektor korrekció** algoritmusát.

Ehhez kidolgoztam a hibaállapot-vektor korrekció szabályát a következőképpen:

- A sikeres működés valószínűsége a v_x az **átlagos javulás** mértékkel növekszik és a detektált hibaállapotok **együttes mértéke** a v_x átlagos javulás mértékével **csökken** a teszt eredményeként. A detektált hibaállapotok a **korrekciója**, a hibaállapotok **előfordulás valószínűségével súlyozottan** kell, hogy történjen.
- Megadtam az $\mathbf{s}_{korr}$ korrigált hibaállapot-vektor meghatározásához szükséges matematikai kifejezéseket: A 3.27 kifejezéssel **végrehajtható** a fenti szabály szerinti hibaállapot valószínűség korrekció, és a 3.18, 3.19, 3.21, 3.23 kifejezések szolgáltatják a 3.27 kifejezés paramétereit.
- Levezettem, hogy a hibaállapot-valószínűség korrekció kezelése **szükségessé teszi** a $\mathbf{T}_{korr}$ **korrigált átmenet-valószínűség mátrix** meghatározását is.

Kimunkáltam a $\mathbf{T}_{korr}$ átmenet-valószínűség mátrix meghatározásának módszerét. A $\mathbf{T}_{korr}$ korrigált átmenet-valószínűség mátrix időfüggő, ezért minden teszt időperiódusban újra meg kell határozni a következő szabályrendszer szerint:

- A $\mathbf{T}_{korr}(i \cdot m)$ mátrix első sorának és a 3.27 kifejezésnek megfelelő $\mathbf{s}_{korr}(i \cdot m)$ állapotvektornak azonosnak kell lenniük.

- A $\mathbf{T}_{korr}(i \cdot m)$ mátrix második és harmadik sorai az eredeti $\mathbf{T}_L$ állapotvalószínűség mátrix megfelelő sorai, de a tesztlefedettség tökéletlensége miatt az adott sornak megfelelően korrigálni kell.
- A $\mathbf{T}_{korr}(i \cdot m)$ mátrix negyedik és ötödik sorai megegyeznek a $\mathbf{T}_L^{(i \cdot m)}$ mátrix negyedik és ötödik sorával.
- A $\mathbf{T}_{korr}(i \cdot m)$ mátrix hatodik és hetedik sorai az eredeti $\mathbf{T}_L$ állapotvalószínűség mátrix megfelelő soraival egyeznek meg.

Az üzemen kívüli állapot számításához szükséges számítástechnikai erőforrásigény rekurzív formula alkalmazásával (3.34 kifejezés) és időalap konverzióval (3.33 kifejezés) jelentősen mérsékelhető.

Kidolgoztam a 15. ábra szerinti Markov-modell esetére a PFM_{Bavg} érték meghatározásának képletét (**3.31 kifejezés**). A 3.31 kifejezés két összetevőjének $\bar{S}$ állapotvektorait, az eltérő időalap miatt külön eredménymátrixokban kell tárolni. A két összetevő a PFM_{LBavg} (3.35.a kifejezés) és a PFM_{MBavg} (3.35.b kifejezés).

Megállapítottam, hogy üzemen kívüli állapothoz tartozó $\bar{S}$ állapotvektorok ismerete alkalmas a **tesztgyakoriság** és **tesztlefedettség** vizsgálatára.

Megadtam a számításokhoz szükséges algoritmusok folyamatábráit (17., 18., és 19. ábra) és forrásprogramjait (M8 melléklet).

IV. FEJEZET

LÉGVÉDELMI RAKÉTÁK RÁEMELŐ BERENDEZÉSÉNEK MSIL ÉRTÉK MEGHATÁROZÁSA

Az esettanulmány célja az MSIL érték meghatározására szolgáló algoritmus alkalmasságának igazolása, vagyis hogy meghatározható általa az aperiodikusan alkalmazott katonai berendezések bevetéskori megbízhatósága, valamint **tervezhető** az üzemen kívüli állapotot megszakító tesztek gyakorisága és tesztlefedettsége és vizsgálható a kezelőszemélyzet kiképzettségének hatása a megbízhatóságra.

Esettanulmányként a KUB légvédelmi rakétaüteg szállító-töltő gépkocsijának[115] jelenleg kézzel vezérelt, hidraulikus munkahengerekkel működtetett ráemelő szerkezetének irányítórendszerét választottam. A választásom indokai:

- A KUB légvédelmi rakétaüteg szállító-töltő gépkocsija hetekig üzemen kívüli állapotban tartózkodik a hangárban, a kialakult gyakorlat szerint kéthavonta legalább egyszer tartanak működés ellenőrzést, és egy-két éves gyakorisággal vesz részt körül-belül egy hetes éles gyakorlaton, vagyis az üzemeltetési módja megfelel az aperiodikusan alkalmazott katonai berendezésekre az első fejezetben megfogalmazottaknak.
- A KUB légvédelmi rakétaüteg több évtizedes technika és így a gépészeti kialakítása valós katonai titkot nem tartalmaz. Nincs automatizálva, így konkrét irányítóberendezés hiányában a valós hiba-valószínűség meghatározás nem lehetséges, de ez amúgy is kellően kielemzett mérnöki tevékenység. Viszont egy feltételezett irányítórendszer vizsgálata alkalmas az általunk bevezetett MSIL érték meghatározására.
- A KUB légvédelmi rakétaüteg szállító-töltő gépkocsijának fél-automatikus töltési művelete húsznál kevesebb összetett irányítási funkcióval leírható és így megfelel az MSIL értékhatárok definiálásakor tett kritériumoknak.

A KUB légvédelmi rakétaüteg szállító-töltő gépkocsijának teljes automatizálása nagyon költséges megoldás. Ezért az olyan bonyolult művelet, mint a szállító-töltő gépkocsi és a daruszerkezet navigálása ember által irányított, vagyis az irányítás fél-

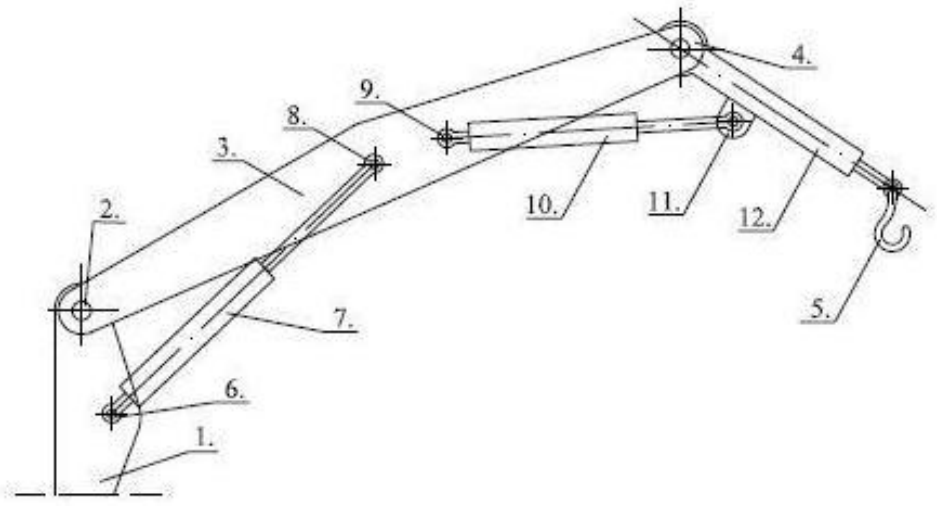
[115] Részletes leírás:[35], [37], [38]

automatikus. A félautomatikus irányítórendszer költséghatékony, de szükség van kezelőszemélyzetre.

4.1 Irányított berendezés

A KUB légvédelmi rakétaüteg szállító-töltő gépkocsijának töltő mechanikáját három egyenes vonalú és egy forgómozgást végző hidraulikus munkahengerből álló daruszerkezet mozgatja. A forgómozgást végző hidraulikus henger alaphelyzetéből jobbra is, balra is 95°-t képes elforogni. A szállító-töltő gépkocsi két oldalán elhelyezett talpak – a rugózás kioldó hidraulikus hengerekkel a két oldalt külön-külön vezérelve - eltávolítják a daruszerkezetet tartó gépkocsi platót a szállító-töltő gépkocsitól, és közel vízszintesen rögzítik. A hidraulikus munkahengerek működtetéséhez szükséges olajnyomást elektromosan vezérelt szivattyú biztosítja. Az olaj nyomása az előrevezető ágban és hőmérséklete a visszatérő ágban mutatós műszerrel van kijelezve. A teher rögzítésére szolgáló horgot a kezelőszemélyzet kézzel rögzíti. A hidraulikus munkahengerek mozgását a kezelőszemélyzet szemmel követve botkarokkal irányítja. A botkarok mechanikusan kapcsolják a hidraulikus munkahengerek útszelepeit.

A daruszerkezet egyenes vonalú mozgást végző hidraulikus munkahengereinek mechanikai elrendezését a 20. ábra mutatja.

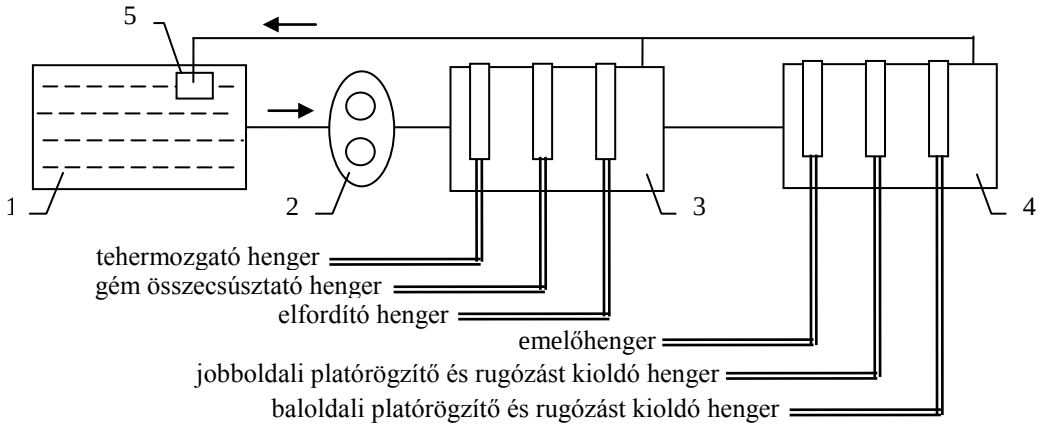


20. ábra. Az emelő berendezés elvi rajza
(Készítette: Neszveda József a [35] alapján)

A 20. ábrán 1. a forgó oszlop váza; 2. az emelőváz alsó csapja, 3 az emelőváz, 4 az emelőváz felső csapja, 5 a horog, 6 az emelőhenger tengelye, 7 az emelőhenger, 8 az

emelő henger csapja, 9 a darugém összecsúsztató henger tengely, 10 a darugém összecsúsztató henger, 11 a darugém összecsúsztató henger csapja, 12 a tehermozgató henger.

A hidraulikus tápellátás blokkvázlatát mutatja a 21. ábra, ahol az 1 az olajtartály, a 2 a szivattyú, a 3 és a 4 a hidraulikus elosztó az útszelepekkel, az 5 a szűrő.



21. ábra. A daruszerkezet munkahengereinek mechanikai elrendezése
(Készítette: Neszveda József a [35] alapján)

4.2 Irányítórendszer

A biztonság-kritikusra tervezett rendszert minél kevesebb irányítási funkcióból és minél kevesebb eszközből célszerű megalkotni, mivel az összes funkció megbízhatósága együttesen szabja meg az elérhető biztonsági szintet.

22. ábra. Hordozható mobilpanel
(Siemens [36])

A fél-automatikus üzemmódban a kezelő irányítja a ráemelést kézben hordozható, szállító-töltő gépkocsi körbejárását nem akadályozó, a gépkocsin elhelyezett irányítóberendezéssel WLAN-os kapcsolatot tartó, a 22. ábrán láthatóhoz hasonló mobilpanel segítségével.

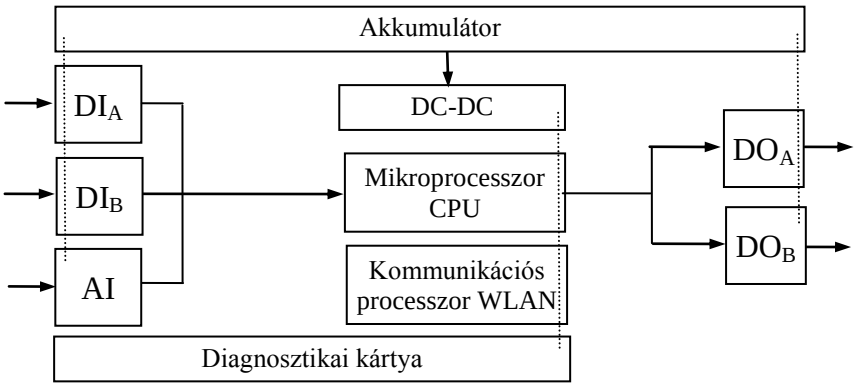
Ilyen mobilpaneleket az ipari automatizálásban már elterjedten alkalmaznak. A 22. ábra a Siemens cég Simatic Mobile Panel 277F WLAN típusát mutatja. A Simatic Mobile Panel 277F WLAN az első olyan eszköz, amely SIL3-mas biztonsági funkcióba illeszthető. Az érintőképernyőre tetszőlegesen konfigurálható ábra, üzenet, működtető nyomógomb. Igényelhető mechanikus nyomógombokkal kiegészített változat is. A mechanikus nyomógombokat célszerű a vészleállítás, illetve az alaphelyzetbe állítás funkciókhoz rendelni.

Irányító berendezésnek választható a 2. fejezetben tárgyalt és kereskedelmi forgalomban kapható „H” jelű nagy megbízhatóságú, vagy az egyszerű vezérlési funkciók miatt lehet „S” jelű biztonsági PLC. A PLC hardver konfiguráció CPU modulból, WLAN kommunikációs modulból, és I/O modulokból alakítható ki. A PLC 24 V_{DC} tápellátása akkumulátorról történik. A CPU és WLAN kommunikációs modul, valamint a diagnosztikai kártya tápellátása DC-DC csatolóval van leválasztva a be és kimeneti csatornák tápellátásától. Az akku figyelőáramköre kétállapotú jelet szolgáltat, ha a töltöttség a kívánt szint alá esik.

A hidraulikus munkahengereket – a két irányuknak megfelelően – két-két jellel kell vezérelni. Ehhez 12 PLC kimenetre és 12 elektro-hidraulikus átalakítóra van szükség. A hidraulikus olajnyomást biztosító szivattyú egy-egy jellel indítható (magas jelszint) és leállítható (alacsony jelszint), azonban a megbízhatóság növelése érdekében célszerű duplikálni a szivattyút. A redundáns kimeneteket különböző kimeneti modulon keresztül célszerű működtetni. A párhuzamos ágakban elhelyezett szivattyúk közül a nem működő tolózárként viselkedik, vagyis zárva tartja az ágát, így további szelepre és így működtető elemre nincs szükség, Az összes többi kijelzés WLAN-on keresztül a Mobil Panel képernyőjén jelenik meg. Így két 8 csatornás kétállapotú kimenetet tartalmazó PLC kimeneti modult kell alkalmazni.

Az olajszivattyúk bármely hibás állapotát egy-egy kétállapotú hibajel jelzi. Az olajszivattyúk hibajeleit különböző bemeneti modulra célszerű vezetni. Az akkutöltöttség alacsony voltát jelző jelet célszerű mindkét modulra bevezetni. A hidraulikus munkahengerek sajátossága, hogy a vezérlő jelüket nem szükséges a végállapotaikban levenni, így működtethetők végállás érzékelők nélkül is. Az

alaphelyzet érzékelésére azért van szükség, mert csak ebben az alaphelyzetben szállítható biztonságosan a daruszerkezet. Az alaphelyzet érzékelésére használható a 2. fejezetben tárgyalt és kereskedelmi forgalomban kapható redundáns mechanikus kapcsoló. A redundancia akkor a leghatékonyabb, ha külön bemeneti modulra vezetjük a redundáns végállás-kapcsolók összetartozó két jelét. Ez két 8 csatornás kétállapotú bemeneti modult igényel.



23. ábra. Irányító berendezés moduljai
(Készítette: Neszveda József)

A hidraulikus olajnyomás és hőmérséklet analóg jel, ezért szükség van még egy 2 csatornás analóg bemeneti modulra is.

4.3 Irányítási funkciók

A biztonság-kritikusra tervezett rendszerben az alapirányítás is a biztonsági rendszer része és az eszköz[116] megbízhatóságát az összes műveletre együttesen kell vizsgálni. A biztonság-kritikusra tervezett rendszerben a hidraulikus munkahengerek mindkét mozgásirányát együttesen egy funkcióként[117] kell vizsgálni, hogy egy eszköz csak egy irányítási funkcióban vegyen részt.

A szállító-töltő gépkocsi irányítási funkcióinak leírásakor veszélyes hibának tekintjük, ami a szállító-töltő gépkocsi manőverező képességét korlátozza vagy megakadályozza, és kezelhető hibának tekintjük, ami a rátöltés műveletét megakadályozza, de a szállító-töltő gépkocsi manőverező képes marad.

---

[116] Az irányítási funkciók leírásában az érzékelőkre az E, a végrehajtókra a V, és a modulokra a 23. ábrán alkalmazott betűkóddal hivatkozom.

[117] Az IEC 61508 szabványban megadott biztonsági funkció fogalma egy eszköz egy műveletét - esetünkben például a hidraulikus munkahenger behúzását - vizsgálja, mint biztonsági funkciót.

1. A jobboldali platórögzítő és rugózást kioldó henger mozgatása. Kezelhető hiba, ha nem lehet kitolni. Veszélyes hiba, ha nem áll vissza az alaphelyzetébe. Az egyidejű vezérlést szoftveresen blokkolni kell. Az irányítási funkció elemei: A mechanikus végállás érzékelők $E1_A$, $E1_B$ kontaktusai; a DI_A és DI_B digitális bemeneti modulok; az DO_A digitális kimeneti modul; a $V1_A$, $V1_B$ elektro-hidraulikus átalakítók; és a mozgatott hidraulikus munkahenger.
2. A baloldali platórögzítő és rugózást kioldó henger mozgatása. Kezelhető hiba, ha nem lehet kitolni. Veszélyes hiba, ha nem áll vissza az alaphelyzetébe. Az egyidejű vezérlést szoftveresen blokkolni kell. Az irányítási funkció elemei: A mechanikus végállás érzékelők $E2_A$, $E2_B$ kontaktusai; a DI_A és DI_B digitális bemeneti modulok; a DO_A digitális kimeneti modul; a $V2_A$, $V2_B$ elektro-hidraulikus átalakítók; és a mozgatott hidraulikus munkahenger.
3. Az elforgató henger mozgatása. Kezelhető hiba, ha nem lehet elforgatni. Veszélyes hiba, ha nem áll vissza az alaphelyzetébe. Az egyidejű vezérlést szoftveresen blokkolni kell. Az irányítási funkció elemei: A mechanikus végállás érzékelők $E3_A$, $E3_B$ kontaktusai; a DI_A és DI_B digitális bemeneti modulok; a DO_A digitális kimeneti modul; a $V3_A$, $V3_B$ elektro-hidraulikus átalakítók; és a mozgatott hidraulikus munkahenger.
4. Az emelőhenger mozgatása. Kezelhető hiba, ha nem lehet kitolni. Veszélyes hiba, ha nem áll vissza az alaphelyzetébe. Az egyidejű vezérlést szoftveresen blokkolni kell. Az irányítási funkció elemei: A mechanikus végállás érzékelők $E4_A$, $E4_B$ kontaktusai; a DI_A és DI_B digitális bemeneti modulok; a DO_B digitális kimeneti modul; a $V4_A$, $V4_B$ elektro-hidraulikus átalakítók; és a mozgatott hidraulikus munkahenger.
5. A gém összecsúsztató henger mozgatása. Kezelhető hiba, ha nem lehet kitolni. Veszélyes hiba, ha nem áll vissza az alaphelyzetébe. Az egyidejű vezérlést szoftveresen blokkolni kell. Az irányítási funkció elemei: A mechanikus végállás érzékelők $E5_A$, $E5_B$ kontaktusai; a DI_A és DI_B digitális bemeneti modulok; a DO_B digitális kimeneti modul; a $V5_A$, $V5_B$ elektro-hidraulikus átalakítók; és a mozgatott hidraulikus munkahenger.
6. A tehermozgató henger mozgatása. Kezelhető hiba, ha nem lehet kitolni. Veszélyes hiba, ha nem áll vissza az alaphelyzetébe. Az egyidejű vezérlést szoftveresen blokkolni kell. Az irányítási funkció elemei: A mechanikus végállás érzékelők $E6_A$, $E6_B$ kontaktusai; a DI_A és DI_B digitális bemeneti

modulok; a DO_B digitális kimeneti modul; a $V6_A$, $V6_B$ elektro-hidraulikus átalakítók; és a mozgatott hidraulikus munkahenger.

7. Az olajszivattyúk működtetése. Az egyidejű vezérlést szoftveresen blokkolni kell. Veszélyes hibának célszerű tekinteni, mert olajnyomásra a hidraulikus munkahengerek mozgatásakor van szükség, és ha nincs nyomás, akkor nem képes visszaállni alaphelyzetbe a daruszerkezet. Az irányítási funkció elemei: A DI_A és DI_B digitális bemeneti modulok; az DO_A és DO_B digitális kimeneti modul; és a működtetett olajszivattyúk.
8. Az olajnyomás a vészminimum érték alá esik. Veszélyes hiba. Az irányítási funkció elemei: A nyomástávadó; az AI analóg bemeneti modul.
9. Az olajhőmérséklet a vészmaximum érték fölé nő. Veszélyes hiba. Az irányítási funkció elemei: A nyomástávadó; az AI analóg bemeneti modul.
10. Akkutöltöttség alacsony jelzés. Kezelhető hiba, mert akkor jelez, amikor az eszköz még működőképes, és mód van a gépkocsi motort aggregátorként használva az akkut tölteni. Az irányítási funkció elemei: Az akkutöltöttség figyelő áramkör; az DI_A és DI_B digitális bemeneti modulok.
11. A szállító-töltő gépkocsi motorikus hibái, amelyek a gépkocsi manőverező képességét megakadályozzák. Veszélyes hiba.

A CPU, a WLAN kommunikáció, és a CPU-ba épített diagnosztikai áramkör minden irányítási funkciónak része, ezért ezek nincsenek a felsorolásban.

4.4 Meghibásodási ráta összetevők

A meghibásodási ráták meghatározása [28] csak a konkrét mechanikai kialakítás, műszerezési és irányítási berendezések ismeretében lehetséges[118]. Viszont 4.3 fejezetben tárgyalt irányítási funkciók alapján ezek a meghibásodási ráták becsülhetők. A 15. ábra Markov-modellje szerint vizsgált konkrét[119] berendezéshez tartozó értékekre bármikor lecserélhetők az M8 melléklet M8.1a. deklarációs Matlab M fájlban a vizsgálathoz használt becsült értékek.

[118] Ennek terjedelme messze meghaladja a jelen Értekezés terjedelmét és nem elengedhetetlenül szükséges az Értekezésben tárgyalt új fogalmak vizsgálatához.

[119] Feltétezve, hogy a konkrét berendezés és részegységei kellően összetettek, hogy az exponenciális eloszlású legyen a berendezés meghibásodási rátája.

Ellenőrző tesztekkor a [40], [41], [57], megfontolásai alapján elsődlegesen a hidraulikus és elektromos tápellátást, valamint terhelési próbával a hidraulikus munkahengerek működését ellenőrzik. Az érzékelő eszközök, és a be- és kimeneti áramköri modulok, valamint a CPU és a kommunikációs processzor hibáit az elektronika jelzi. A hidraulikus munkahenger működésének hibája az üzemen kívüli állapotok ellenőrző tesztjeikor, illetve működés közben azonnal detektálódik. A mechanikus végállás-kapcsolók, valamint a nyomás és a hőmérséklet távadók meghibásodása úgyszintén. Ugyanígy felszínre kerül a töltöttség jelző áramkör kontaktusának és az egyéb hibák többsége. Ezért a detektált hibák arányát a 95%-kosnak feltételezhetjük. Ebből adódóan az 1.28 kifejezéssel definiált C_M tesztlefedettség legfeljebb 90%-osra becsülhetjük. A tesztlefedettséget vizsgálatokban ennél kisebb értékek hatását is elemezzük.

Az irányítási funkciók alapján a veszélyes hibák száma kismértékben meghaladja a kezelhető hibák számát. Ezt a tényezőt a továbbiakban 0,6 értékűnek becsüljük.

A bekapcsoláskor az azonnali leállás valószínűtlen, ezért az ilyen hibák aránya aligha haladja meg a 0,1 értéket, ezért válasszuk ezt, mint legrosszabb esetet.

A vészhelyzet és a hamis leállások aránya a PFM_{Bavg} számítási módja miatt érdektelen[120], csak a 15. ábra szerinti modell alkalmazása miatt kell definiálni, ezért legyen az értéke alaphelyzetben és csökkentett üzemmódban egyaránt 0,5.

Ezek alapján a 15 ábra. gráfjának élei egyszerűen meghatározhatok, amint az a M8 melléklet M8.1a. deklarációs Matlab M fájljának megfelelő soraiban jól nyomon követhető. A 15. ábrához tartozó **T** átmenet-valószínűség mátrixban a λ_{12}, λ_{13}, λ_{14}, és λ_{15} meghibásodási ráták kettes szorzó faktorral vannak figyelembe véve. Ez a magyarázata az M8 melléklet M8.1a. deklarációs Matlab M fájljának megfelelő soraiban szereplő egykettedes szorzótényezőnek.

Mint a 2. fejezetben tárgyaltuk, minden biztonsági funkció leggyengébb láncszeme a mechanikai mozgást végző végrehajtó. A hidraulikus henger, mint mechanikus végrehajtó üzembiztonsága – a robosztus és egyszerű mechanikai kialakítás miatt - meglehetősen jó (M5 melléklet M5.2 táblázat). Így SIL2-es és SIL3-mas biztonsági funkcióba is illeszthetők.

[120] Ha feladatvégzéskor figyelembe vesszük a μ javítási rátát, akkor van jelentősége, mert a hamis leállást általában gyorsabb megszüntetni, mint egyéb hibaokokat.

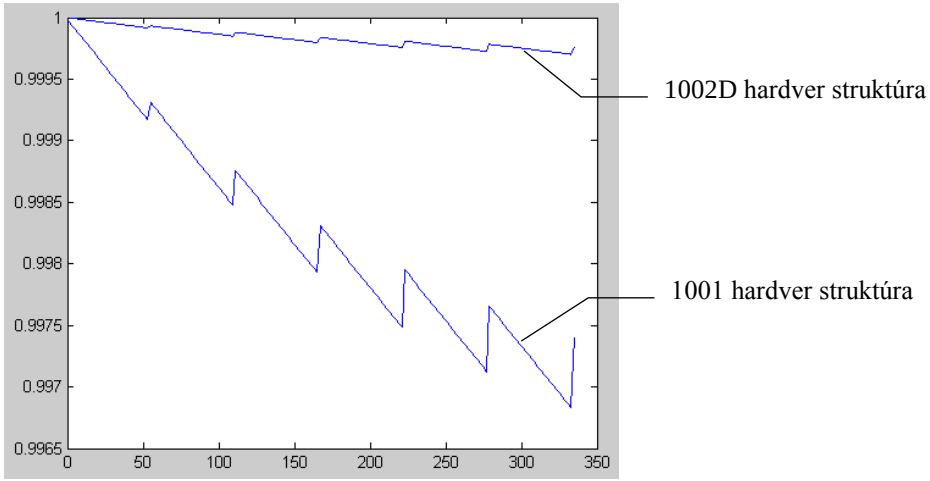
Biztonság-kritikusra tervezett rendszer esetén azonban a 4.3 fejezetben tárgyalt irányítási funkciókat együttesen kell figyelembe venni, ezért egy gyenge/közepes SIL1 érték az, ami jelenleg költséghatékonyan elérhető. Ennek megfelelően a vizsgálatainkban[121] legyen a $\lambda_0 = 6,4 \cdot 10^{-6}$ értékű.

4.5 Számítógépes szimulációk

A vizsgálatokban a 2. fejezetben tárgyaltaknak megfelelően az 1002D irányító berendezés struktúrát feltételezzük úgy, hogy minden művelet a 8 ábra modelljét alkalmazza. Ha egy légvédelmi rakétaüteg szállító-töltő járműve ilyen irányítóberendezéssel rendelkezik, akkor mechatronikai jellegű eszköznek tekinthető.

A periodikus tesztekkel megszakított üzemen kívüli állapot vizsgálatakor a M8 melléklet M8.1b Matlab M fájlja által képzett „em” eredménymátrix első oszlopa úgy értelmezhető, hogy mi a valószínűsége, hogy bekapcsoláskor az irányítórendszer hibátlan. Ez egy redundancia nélküli 1001 hardver-struktúrának felel meg.

A 24. ábra periodikus teszttel 8 hetente (56 naponta) megszakított, közel egy éves (336 napos) üzemen kívüli állapotot feltételezve készült. A vízszintes tengelyen a napok száma, a függőleges tengelyen a berendezés megbízhatósága van ábrázolva.



24. ábra. Az 1001 és a 1002D eszköz működésének valószínűsége
(Matlab programmal készítette: Neszveda József)

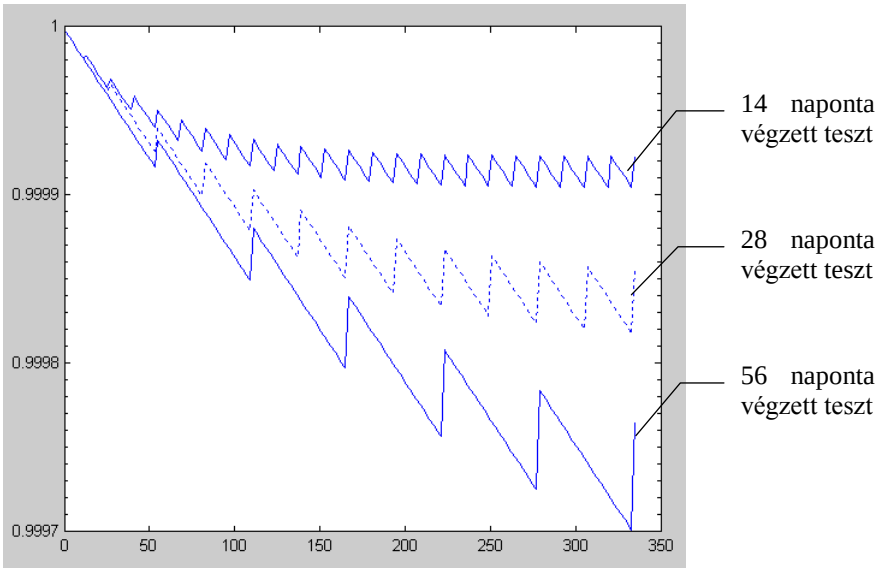
[121] A tesztlefedettség, tesztgyakoriság, kezelőszemélyzet kiképzettség vizsgálatokban a tendenciák szempontjából a kiindulási λ_0 hibaaránynak nincs jelentősége.

Az 1002D hardverstruktúra 15. ábra szerinti Markov-modelljében az „em” eredménymátrix első, második, harmadik, negyedik, ötödik oszlopai olyan állapotok valószínűségeit tartalmazzák az idő függvényében, amelyekben a berendezés még működőképes. A 24. ábra jól mutatja, hogy a redundanciával és diagnosztikával rendelkező 1002D hardverstruktúra.

A sűrűbb mintavétel javítja a megbízhatóságot, de a költség korlátokon túl a hardver tolerancia minimum (7. táblázat) műszaki korlátot is szab. A diagnosztikával rendelkező a 1002D hardverstruktúra műszaki és költségek szempontjából is jobb, mint a nagyon sűrű teszt.

4.5.1 Periodikus tesztsűrűség

A 25. ábra azt mutatja, hogy nagyjából egy év alatt a 4.4 fejezetben definiált meghibásodási ráták esetén, hogyan változik az idő és a különböző sűrűségű periodikus teszt függvényében a megbízhatóság (az üzemelés valószínűsége) feladat végrehajtáskor.



25. ábra. A működés valószínűsége bekapcsoláskor
(Matlab programmal készítette: Neszveda József)

A 25. ábrán a 2 hetente végrehajtott teszt függvénye mutatja legjobban, hogy a periodikusan végrehajtott teszt, a teszt sűrűségétől függő időállandóval, állandósult értékhez közelíti a berendezés megbízhatóságát. [34]. A vizsgálat a 4.4 fejezetben megadott meghibásodási rátákat alkalmazta.

A 25. ábra alapján a 4 hetente végrehajtott teszt esetén egy év alatt állandósul a bekapcsoláskor várható sikeres működés valószínűsége. Az ellenőrző teszteket követően ugrásszerűen megnő a sikeres működés valószínűsége, majd az idő múlásával folyamatosan csökken. A 25. ábra azt is jól reprezentálja, hogy azonos tesztlefedettség esetén is, a ritkább tesztgyakoriság nagyobb amplitúdójú ingadozási sávot alakít ki.

Költségmegfontolásból[122] a tesztgyakoriságot úgy célszerű meghatározni, hogy a raktározás kezdete és a bevetés, vagy a két feladatvégzés közötti időtartam alatt **már állandósuljon a sikeres működés valószínűsége** bekapcsoláskor.

A tesztek gyakoriságának tervezésekor – a legrosszabb esetet feltételezve – az ingadozási sáv alsó (az ellenőrző tesztek előtti) értékeinek burkológörbéjét kell figyelembe venni, mint a sikeres működés valószínűségét bekapcsoláskor.

4.5.2 Tesztlefedettség

A teszt célja a végrehajtó eszközök, érzékelők, és a kiegészítő berendezések működőképességének ellenőrzése.

A [37], [38] által előírt eljárás szerint a szállító-töltő tesztelését, legalább kéthavonta és a tervezett éles gyakorlatok előtti időszakban végzik el:

- szemrevételezés, hitelesítések ellenőrzése;
- a hidraulikus szivattyú nyomásellenőrzése. A szivattyú által továbbított folyadék és gázelvezető rendszer ellenőrzése;
- a hidraulikus munkahengerek végállásig történő mozgatása, a végállás-kapcsolók ellenőrzése;
- próbasúlyemelés és előírt ideig tartás;
- működtetés utáni karbantartás.

Ez a kézi irányításra kidolgozott eljárás egy mechatronikai jellegű automatizált rendszerben az irányítási funkciók és eszközök nagyjából 80%-t fedi le.

A 90-95%-os tesztlefedettség eléréséhez programozható irányítórendszer szükséges, ezért a fenti protokollt az alábbi módon célszerű bővíteni:

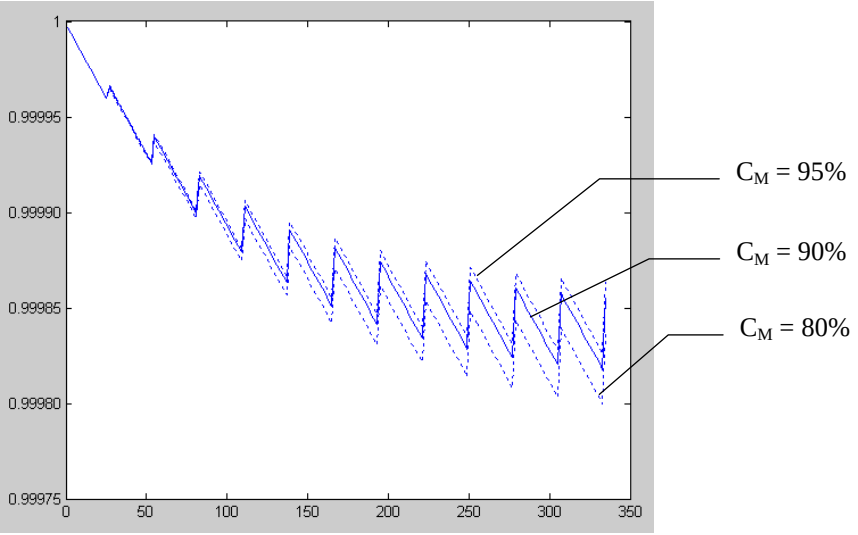
- szemrevételezés, hitelesítések ellenőrzése.

[122] A szakirodalomban számos [39], [40], [41] tanulmány foglalkozik a folytonos technológiák vész-, védelmi rendszerének üzemvitel közbeni ellenőrző tesztek és karbantartás költsége, és az ellenőrző tesztek és a karbantartás által a leállási órák csökkenéséből származó nyereség együttes optimalizálásával. A periodikus teszt üzemmódok különbözősége miatt ezek a módszerek módosítás nélkül az aperiodikusan alkalmazott berendezésekre nem alkalmazhatók.

- az akkumulátor töltöttség és a töltési folyamat ellenőrzése.
- a szivattyú indítása és az általa továbbított folyadék nyomásának, valamint a gázelvezető rendszer ellenőrzése.
- próbasúlyemelés és előírt ideig tartás.
- a hidraulikus munkahengerek végállásig történő mozgatása súllyal együtt, a végállás-kapcsolók ellenőrzése.
- a szivattyú folyadék hőmérsékletének ellenőrzése a munkavégzés alatt és után.
- a CPU és a kommunikációs processzor diagnosztikai üzeneteinek naplózása és hibaelemzése.
- működtetés utáni karbantartás.

Magasabb 95%-os feletti tesztlefedettség eléréséhez a protokollt további eljárásokkal szükséges kiegészíteni:

- rövididejű, de még megengedett mértékű súly túlterheléssel mozgatáskor;
- a csökkentett üzemmód ellenőrzésével[123], ami a bemeneti kapcsok időleges lekötésével megoldható érhető el.



26. ábra. A C_M tesztlefedettség hatása
(Matlab programmal készítette: Neszveda József)

A 26. ábrán az üzemelés valószínűsége látható[124] az idő függvényében. A tesztlefedettség növelése értelemszerűen növeli a tesztre fordított időt és költséget. A kidolgozott szimulációs eljárás éppen ennek optimalizálását teszi lehetővé.

[123] A sorkapcsok lekötése is hibaforrás, ezért ezt az akku töltöttség és a töltési folyamat ellenőrzése után célszerű beiktatni és a hidraulikus munkahengerek súllyal együtt történő mozgatását már visszakötött sorkapcsokkal kell végrehajtani.

4.6 A kezelőszemélyzet kiképzettségének és a berendezés műszaki állapotának komplex elemzése

A feladatvégzés igénye bármikor felmerülhet a két teszt közötti időtartamban, ezért ez is valószínűségi változó. Statisztikai szórást alkalmazva, vagyis a két teszt közötti időtartam **két harmad** részével számolva, az előforduló esetek több mint 90%-át lefedi a vizsgálat[125]. A 16. táblázatban[126] a PFM_{LBavg} annak az átlagos valószínűsége, hogy üzembe-helyezéskor a berendezés működésképtelen, a PFM_{MBavg} annak az átlagos valószínűsége, hogy a berendezés 24 órás folytonos üzemelés közben működésképtelené válik.

16. táblázat: A tesztgyakoriság, a kezelőszemélyzet képzettsége és a berendezés műszaki állapotának hatása a működésképtelenség valószínűségére

	A periodikus teszt gyakorisága							
	Kéthetente		Négyhetente		Nyolchetente		Tizenhat hetente	
	10^{-5}							
h_A	PFM_{LBavg}	PFM_{MBavg}	PFM_{LBavg}	PFM_{MBavg}	PFM_{LBavg}	PFM_{MBavg}	PFM_{LBavg}	PFM_{MBavg}
1,112	1,92435	9,29655	3,64568	15,42346	6,17406	24,93640	9,21054	37,90600
1,224	1,92435	9,55474	3,64568	15,68177	6,17406	25,19490	9,21054	38,16474
1,640	1,92435	10,51376	3,64568	16,64127	6,17406	26,15509	9,21054	39,12586
3,560	1,92435	14,94124	3,64568	21,07082	6,17406	30,58784	9,21054	43,56289

A 16. táblázatban a h_A az 5. táblázat meghatározott, a kezelőszemélyzet kiképzettségét és a berendezés műszaki állapotát együttesen tartalmazó tényező, ami a meghibásodási rátát módosítja. A h_A csak a PFM_{MBavg} értékét befolyásolja, míg a tesztgyakoriság növelése a PFM_{LBavg} és PFM_{MBavg} értékére egyaránt hat, vagyis a PFM_{Bavg} mindkét összetevőjét befolyásolja. Egyik hatás sem lineáris, és a vizsgált értéktartományokban a lineárisnál kevésbé erőteljes. Regressziós görbe keresésének azért nincs értelme, mert a kezdeti meghibásodási rátáktól is függnek a PFM_{LBavg} és a

---

[124] Négyhetente végrehajtott ellenőrző teszt esetén,

[125] A PFM_{LBavg} kiszámításakor a két teszt közötti időtartam több mint 66%-lékát - azaz két hét esetén 10, négy hét esetén 20, nyolc hét esetén 40, és 16 hét esetén 80 napot – vesz figyelembe az algoritmus.

[126] Az üzemképtelenség valószínűségének Matlab programokkal számolt értékei 5 értékes jegy pontosságúra vannak kerekítve a 16. táblázatban.

PFM_{MBavg} értékei. A daruszerkezet és irányító rendszere nem fixen telepített, de működtetéskor fixen rögzített helyzetben van. Ezért 16. táblázatban számolt értékekben a M2 melléklet szerinti üzemelési környezet faktor értéke 3. A 16. táblázat értékei 90%-os tesztlefedettség mellet lettek kiszámítva.

Az esettanulmány kiinduló feltételezései mellett a meghibásodás valószínűség nem lineárisan, hanem a tesztgyakoriság csökkenésével a **lineárisnál erőteljesebben** változik. A tesztgyakoriság csökkenésével a PFM_{Bavg} meghibásodás valószínűség jelentősen nő, de a kezelőszemélyzet kiképzettségének **jelentősége csökken.**

A 16. táblázat alapján – a becsülhető költségtényezőket[127] is figyelembe véve - a szürke színnel kiemelt $h_A = 1{,}224$ (jól felkészített eszköz, és személyes konfliktussal nem terhelt, jól felkészített kezelőszemélyzet) és négyhetente végrehajtott teszt tekinthető optimálisnak.

Az ilyen optimálisnak tekinthető körülmények között számolt $PFM_{Bavg} \approx 1{,}933 \cdot 10^{-4}$ MSIL2-es meghibásodás valószínűség érték úgy értelmezhető, hogy az első napon 5173 bevetésenként legfeljebb egy - a feladat végrehajtás akadályozó - meghibásodás[128] történik az irányító rendszer hibájából.

Az aperiodikusan alkalmazott katonai berendezések küldetéses üzemelésűek. A 16. táblázatban szürke színnel kiemelt esetére a 17. táblázat az üzemelési idő függvényében ábrázolja a teljes küldetési időre a szállító-töltő gépkocsi meghibásodás valószínűségeit.

17. táblázat: A PFM_{Bavg} időbeli változása

Napok száma	1	2	3	4	5	6	7
10^{-4} PFM_{Bavg}	1,93274	2,21508	2,49750	2,77999	3,06257	3,34521	3,62794

A 17. táblázatból kiolvasható, hogy a PFM_{Bavg} érték nem lineárisan növekszik a napok számával. Az esettanulmányban vizsgált paraméterek és üzemeltetési körülmények esetén az MSIL2-es kategória teljesül az irányító rendszere még egyhetes időtartamú feladatvégzéskor is.

[127] A periodikus tesztek költséghatékonyság elemzése külön tanulmányt igényel, de addig is becsülhetők.

[128] A valóságos érték azonban ennél jobb, hisz a PFM_{Bavg} tartalmazza a hamis leállásokat is. Harchelyzetben az erre feljogosított kezelő engedélyezheti az automatika olyan speciális üzemmódját, amelyben a kezelőszemélyzet kézi üzemmódban felülbírálhat bizonyos hibajelzéseket, ezért a hamis leállások egy részében sikerülhet a feladatot végrehajtani.

4.7 Összefoglalás és következtetések

Valamely konkrét irányítórendszer elemeinek vannak biztonsági tanúsítványai, ami az eszközgyártótól igényelhető. Ezek ismeretében meghatározható az irányítórendszer 15. ábra szerinti modelljében szereplő meghibásodási ráták. A meghibásodási ráták meghatározásának módszere a szakirodalomból ismert, a kereskedelmi forgalomban kapható kész szoftverek segítik, vagy az erre szakosodott intézménynél megrendelhető egy konkrét rendszer előírt modell szerinti meghibásodási ráta értékeinek kiszámítása.

Az elvégzett vizsgálatok igazolták, hogy a meghibásodási ráták ismeretében, az általam kidolgozott algoritmusok (M8 melléklet) **alkalmasak** az üzemen kívüli állapotokat megszakító tesztek **gyakoriság**ának, a **tesztlefedettség** mértékének és a személyzet **kiképzettség**ének optimalizálására.

Az algoritmussal igazoltam, hogy minden tesztgyakorisághoz tartozik egy **beállási idő**, ami után az üzemen kívüli berendezés sikeres működésének valószínűsége bekapcsoláskor már állandósult érték. Az elvégzett modellkísérletekből következik, hogy a beállási idő annál **kisebb** és a sikeres működés valószínűsége annál nagyobb minél sűrűbb a tesztgyakoriság.

Költségmegfontolásból a raktározás kezdete és a bevetés (felderítő, zavaró elektronikus eszközök, stb.), vagy a két feladatvégzés (mobil robotok, szállító-töltő légvédelmi rakéta rátöltő gépkocsi, stb.) közötti időtartamot célszerű **beállási időnek választani** és ebből meghatározni a tesztgyakoriságot.

A tesztekkel ellenőrzött működés és a feltárt hibák következtében az ellenőrző teszteket követően **ugrásszerűen megnő** a sikeres működés valószínűsége, majd az idő múlásával folyamatosan csökken. Ez **ingadozási sáv**ot alakít ki. A feladatvégzés igénye bármikor felmerülhet a két teszt közötti időtartamban, ezért célszerű a statisztikai eloszlást figyelembe venni, vagyis a két teszt közötti időtartam **két harmad** részével számolni.

Bemutattam, hogy az általam kidolgozott algoritmussal vizsgálható a **tesztlefedettség hatása** a sikeres működés valószínűségének időbeli változására.

A személyzet kiképzettsége és a berendezés műszaki állapota, mint az várható volt, jelentősen befolyásolja a bevetés hatékonyságát. Bemutattam, hogy az általam kidolgozott algoritmus **számszerűsíti** a kapcsolatot a sikeres működés valószínűsége és személyzet kiképzettsége, valamint a berendezés műszaki állapota között.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Az üzemeltetés sajátosságai következtében az aperiodikusan alkalmazott katonai berendezések **önálló csoportot alkotnak**, amit az alábbi módon definiáltam: az aperiodikusan alkalmazott katonai berendezések **küldetéses** feladatvégzésű, katonai célú és ezért valamennyi hiba okot **együtt kezelő**, **biztonság-kritikus**ra tervezett, programozható elektronikus vagy mechatronikai jellegű eszköz.

Az előbbi definícióból következően az aperiodikusan alkalmazott katonai berendezéseknek **három** jellegzetesen **eltérő** üzemállapota van: a feladatvégzés üzemállapot, az üzemen kívüli állapot és az üzemen kívüli állapotot megszakító ellenőrző teszt üzemállapot. Az eltérő üzemmódok következménye, hogy az aperiodikusan alkalmazott katonai berendezések λ meghibásodási rátáj**a** az **üzemben-tartás életciklus** alatt **nem állandó**.

Megállapítottam, hogy az aperiodikusan alkalmazott katonai berendezések **üzemmód-váltás**ai az aktuális **PF** hibavalószínűségben - ezen belül az üzemelési életciklus alatt a λ meghibásodási rátában[129] - történő **ugrásszerű változás**ként vehetők figyelembe. Ennek kezelésére kidolgoztam az átmenet-valószínűség mátrix **konverziós szabály**át, és e szabályba építve definiáltam az **üzemelési körülmény** tényezők figyelembe vételét.

Bizonyítottam, hogy amennyiben a T átmenet-valószínűség mátrix elemein akarjuk érvényesíteni a λ meghibásodási ráta **ugrásszerű változását**, akkor a 3.5 kifejezés szerinti **konverziós egyenlet**et kell alkalmazni. Igazoltam, hogy a 3.5 kifejezés alkalmas az üzemelési körülmények okozta λ meghibásodási ráta ugrásszerű változást és az emberi hiba faktort figyelembe venni. Ehhez:

- **levezettem**, hogy az üzemelési körülmények jelentős, ugrásszerű változása ugyancsak a λ meghibásodási ráta ugrásszerű változását okozzák, ami így a 3.5 kifejezéssel ugyancsak figyelembe vehetők;
- **négy** küldetés végrehajtás helyzet megkülönböztetését **definiáltam** az 5. táblázatban úgy, hogy az emberi tényező és a berendezés műszaki állapota okozta hibát a hibavalószínűségben ugrásszerű változást okozó $\mathbf{h_A}$ **tényező**ként lehessen figyelembe venni.

[129] Exponenciális eloszlású meghibásodást feltételezve a PF hibavalószínűség arányos a λ hibaaránnyal, ami az üzemelési életciklus alatt állandó.

Vizsgálataimhoz kidolgoztam az 1002D hardverstruktúrájú irányítórendszer hét összevont állapotot tartalmazó **Markov gráf**ot (15. ábra), az átmenet-valószínűségek meghatározásának **szempont-rendszer**ét (3.2.1 fejezet), és a biztonság-kritikusra tervezett berendezés **összevont átmenet-valószínűség**eit meghatározó 3.32 kifejezést.

Rámutattam, hogy az IEC 61508, az IEC 61511, és az ANSI/ISA 84 szabványok PF_{Davg}, PFD_{avg} definíciója **nem alkalmas** az aperiodikusan alkalmazott katonai berendezések megbízhatóságának meghatározására, a következők miatt:

- a jellegzetes alkalmazási terület és körülmények okán az aperiodikusan alkalmazott katonai berendezések irányítórendszerében az alapirányítás átlagos veszélyes hiba valószínűséget PF_{Davg}, a vész, védelem átlagos működési igénykor fellépő hiba valószínűséget PFD_{avg}, és a hamis leállás átlagos valószínűséget $PF_{avg}^{spurious}$ **együttesen** kell figyelembe venni;
- a feladat végrehajtását akadályozó valamennyi művelet megbízhatóságát nem egyenként, mint a fenti szabványok SIF definíciója teszi, hanem együttesen kell meghatározni;
- az üzemen kívüli üzemállapotot megszakító tesztek hatékonyságának meghatározására nem alkalmas a fenti szabványok tesztlefedettség fogalma.

Az aperiodikusan alkalmazott **katonai célú** berendezések hibavalószínűség mértékére, az alább felsorolt sajátosságokkal bevezettem a $\mathbf{PFM_{Bavg}}$ fogalmat, megadtam a PFM_{Bavg} kiszámításának képletét (1.32 kifejezés) és definiáltam a PFM_{Bavg} fogalomhoz tartozó **tesztlefedettség** tényezőt. A PFM_{Bavg} sajátosságai:

- a PFM_{Bavg} tartalmazza **valamennyi hibaok** hibavalószínűségét - akár tényleges veszélyelhárítás, akár téves parancs okozta - amely blokkolja a feladatvégzés üzemmódot és így megakadályozhatja a katonai tevékenység sikeres végrehajtását;
- az aperiodikusan alkalmazott katonai berendezéseket **küldetéses működésre tervezett** rendszernek tekintjük úgy, hogy az **utolsó teszt óta eltelt** időtartamot és a **feladatvégzés** időtartamát együtt kell **küldetési idő**ként figyelembe venni az átlagos hibavalószínűség számításakor;
- Az üzemen kívüli üzemállapotot megszakító tesztek hatékonyságának meghatározására az általam alkotott és az 1.28 kifejezéssel definiált $\mathbf{C_M}$ **tesztlefedettség** tényezőt kell alkalmazni.

Megadtam az aperiodikusan alkalmazott **katonai célú** berendezések megbízhatóságának számszerűsítésére szolgáló, a $\mathbf{PFM_{Bavg}}$ fogalomra épülő **MSIL** besorolás határértékeit.

Rámutattam, hogy a gyakorlatban a redundancia nem mindig hasznos. Bemutattam, hogy a redundancia problémát leghatékonyabban a diagnosztika hatékonyságának növelésével lehet megoldani, ami intelligens diagnosztikai áramkör alkalmazását igényli. Indokoltam az **1002D** hardverstruktúra előnyeit.

Az általam kidolgozott Markov-modellhez megállapítottam az üzemen kívüli állapotot megszakító ellenőrző **teszt üzemmód beillesztés**ének szabályait (3.2.1 fejezet) és levezettem az ehhez szükséges **hibaállapot-vektor korrekció** algoritmusát.

Ehhez kidolgoztam a hibaállapot-vektor korrekció szabályát a következőképpen:

- A sikeres működés valószínűsége a v_x az **átlagos javulás** mértékkel növekszik és a detektált hibaállapotok **együttes mértéke** a v_x átlagos javulás mértékével **csökken** a teszt eredményeként. A detektált hibaállapotok a **korrekciója**, a hibaállapotok **előfordulás valószínűségével súlyozottan** kell, hogy történjen.
- Megadtam az $\mathbf{s}_{korr}$ korrigált hibaállapot-vektor meghatározásához szükséges matematikai kifejezéseket: A 3.27 kifejezéssel **végrehajtható** a fenti szabály szerinti hibaállapot valószínűség korrekció, és a 3.18, 3.19, 3.21, 3.23 kifejezések szolgáltatják a 3.27 kifejezés paramétereit.
- Levezettem, hogy a hibaállapot-valószínűség korrekció kezelése **szükségessé teszi** a $\mathbf{T}_{korr}$ **korrigált átmenet-valószínűség mátrix** meghatározását is.

Kimunkáltam a $\mathbf{T}_{korr}$ átmenet-valószínűség mátrix meghatározásának módszerét. A $\mathbf{T}_{korr}$ korrigált átmenet-valószínűség mátrix időfüggő, ezért minden teszt időperiódusban újra meg kell határozni a következő szabályrendszer szerint:

- A $\mathbf{T}_{korr}(i \cdot m)$ mátrix első sorának és a 3.27 kifejezésnek megfelelő $\mathbf{s}_{korr}(i \cdot m)$ állapotvektornak azonosnak kell lenniük.
- A $\mathbf{T}_{korr}(i \cdot m)$ mátrix második és harmadik sorai az eredeti $\mathbf{T}_L$ állapotvalószínűség mátrix megfelelő sorai, de a tesztlefedettség tökéletlensége miatt az adott sornak megfelelően korrigálni kell.
- A $\mathbf{T}_{korr}(i \cdot m)$ mátrix negyedik és ötödik sorai megegyeznek a $\mathbf{T}_L^{(i \cdot m)}$ mátrix negyedik és ötödik sorával.

- A $\mathbf{T}_{\text{korr}}(i \cdot m)$ mátrix hatodik és hetedik sorai az eredeti $\mathbf{T}_{\text{L}}$ állapotvalószínűség mátrix megfelelő soraival egyeznek meg.

Igazoltam, hogy megfelelő időalap konverzióval az állapotkorrekció **egyetlen időperiódusban** hajtható végre, anélkül, hogy ez számítási hibát okozna. Rámutattam, hogy üzemen kívüli állapotban a **két nap**, mint a diszkrét analízis periódus (mintavételi) ideje megengedhető és még modulcserével megvalósítható kisebb javításokkal együtt is elegendő az időszakos teszt végrehajtására.

Levezettem a PFM_{Bavg} kiszámításához szükséges összefüggést (3.31 kifejezés), és **megadtam** a számításokhoz szükséges algoritmusok folyamatábráit (17., 18., és 19. ábra) és forrásprogramjait (M8. melléklet).

Rámutattam, hogy az üzemen kívüli állapot számításához szükséges számítástechnikai erőforrásigény rekurzív formula alkalmazásával (3.34 kifejezés) és időalap konverzióval (3.33 kifejezés) jelentősen mérsékelhető.

Megállapítottam és esettanulmánnyal demonstráltam, hogy az algoritmusok **alkalmasak** az üzemen kívüli állapotokat megszakító tesztek **gyakoriság**ának, a **tesztlefedettség** mértékének, és a személyzet **kiképzettség**ének optimalizálására. Bemutattam, hogy az általam kidolgozott algoritmussal vizsgálható a **tesztlefedettség hatása** a sikeres működés valószínűségének időbeli változására. Bemutattam, hogy az általam kidolgozott algoritmus, a paraméterek függvényében, **számszerűsíti** a sikeres működés valószínűségét, ami hasznos információ a katonai akció tervezői számára.

Mindezek alapján hasznos, ha intelligens elektronikát tartalmazó új katonai berendezések beszerzésekor, nemcsak a berendezés részegységeinek megbízhatóság mértékét igazoló tanúsítványokat, hanem az ehhez tartozó **részletes jegyzőkönyveket** is megkövetelik a beszállítóktól. E jegyzőkönyvek ismerete folyamatosan üzemelő berendezések esetén az üzembentartás alatt segítik a módosítások és javítások szakszerű felügyeletét (M1. melléklet), az Értekezés tárgyát képező aperiodikusan alkalmazott katonai berendezések esetén pedig lehetővé teszik a **meghibásodási ráták meghatározását**, ami az általam javasolt módszerek alapja.

Ugyancsak előny a katonai vezetés számára, hogy az ellenőrző tesztek hatékonyságát és a feladatvégzés megbízhatóságát **számszerűsítve** lehet elemezni, és ha szükséges az ezeket befolyásoló körülményeket megváltoztatni.

ÚJ TUDOMÁNYOS EREDMÉNYEK

1. Definiáltam az **aperiodikusan alkalmazott katonai berendezés** fogalmát, és megadtam az aperiodikusan alkalmazott katonai berendezések megbízhatóságának mértékét számszerűsítő **MSIL** besorolás határértékeit.

2. Az aperiodikusan alkalmazott **katonai célú** berendezések hibavalószínűség mértékének (MSIL) kiszámításához bevezetem a $\mathbf{PFM_{Bavg}}$ fogalmat, és definiáltam a PFM_{Bavg} fogalomhoz tartozó **tesztlefedettség** tényezőt és **emberi tényező** faktort.

3. Kidolgoztam az aperiodikusan alkalmazott katonai berendezések üzemmód-váltásai okozta meghibásodás-valószínűség érték változások kezelésére az átmenet-valószínűség mátrix **konverziós szabály**át.

4. Kidolgoztam az aperiodikusan alkalmazott katonai berendezések üzemen kívüli állapotát megszakító teszt-üzemmód **állapot-korrekció**ként való kezelését és ehhez az átmenet-valószínűség mátrix **korrekciós szabály**át.

FELHASZNÁLÁSI LEHETŐSÉGEK

A katonai vezetés számára fontos, hogy a katonai berendezések feladat végrehajtás megbízhatósága ismert legyen. Ezért a fejlett elektronikát tartalmazó új katonai berendezések beszerzésekor, nemcsak a berendezés részegységeinek megbízhatóság mértékét igazoló tanúsítványokat, hanem az ehhez tartozó **részletes jegyzőkönyveket** is célszerű megkövetelni a beszállítóktól. A jegyzőkönyvek ismerete alkalmas egy konkrét berendezés meghibásodási ráta összetevőinek meghatározására.

A kidolgozott algoritmusok és programok – a konkrét berendezés meghibásodási ráta összetevőit tartalmazó módosításokkal – alkalmas az aperiodikusan alkalmazott katonai berendezés MSIL értékének meghatározására és így a feladatvégzés sikeres valószínűségének számszerűsítésére, továbbá a rendszeresítésre kerülő katonai berendezés részegységei SIL értékének előírására. Ezért alkalmazásuk szakszerűbbé teszi az új elektronikus haditechnikák beszerzési eljárását.

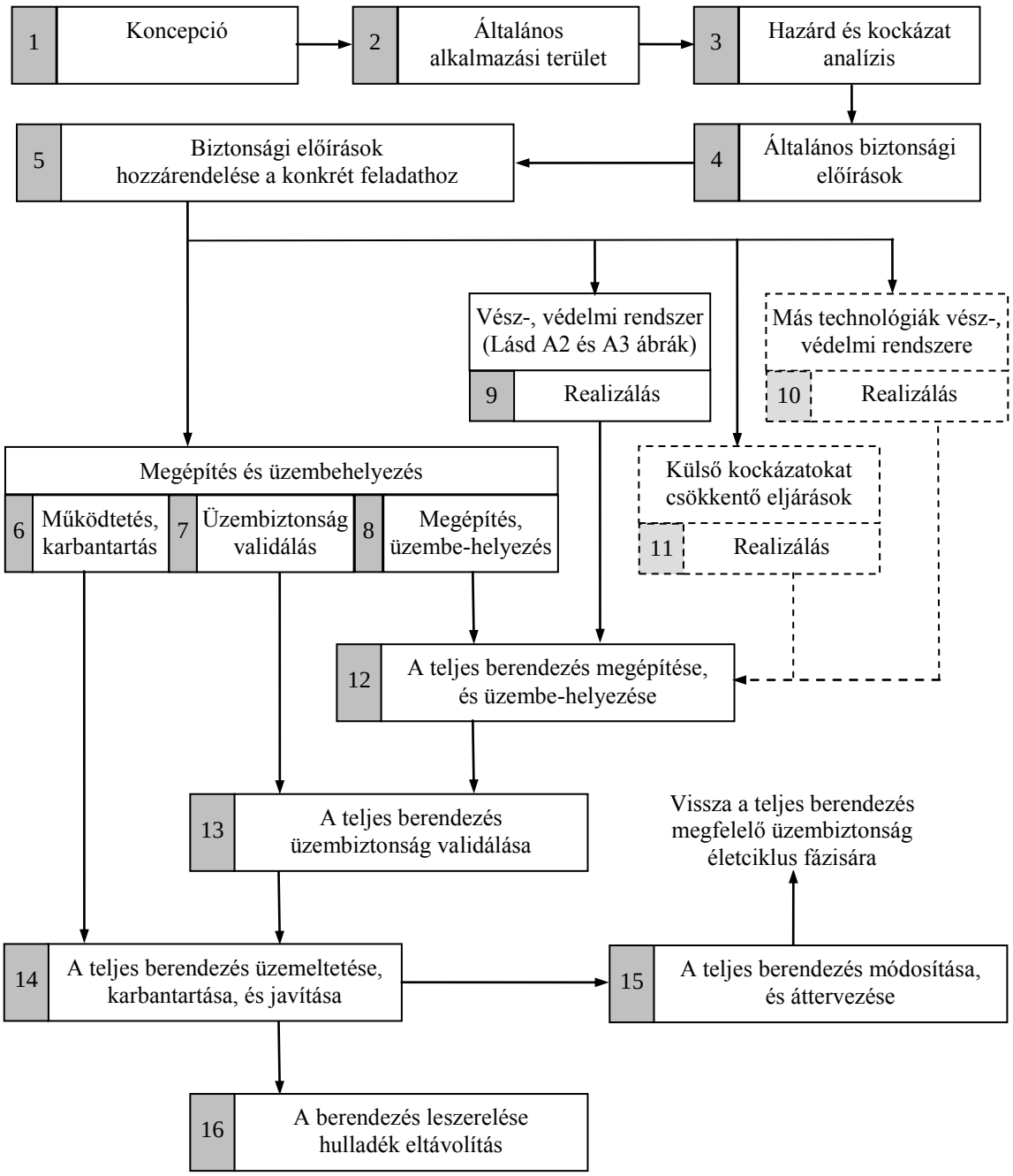
Célszerű a katonai fejlesztéssel foglalkozó cégek számára a megbízhatóságot igazoló számításokhoz útmutatást átadni.

Budapest, 2011-04-20

Neszveda József

MELLÉKLETEK

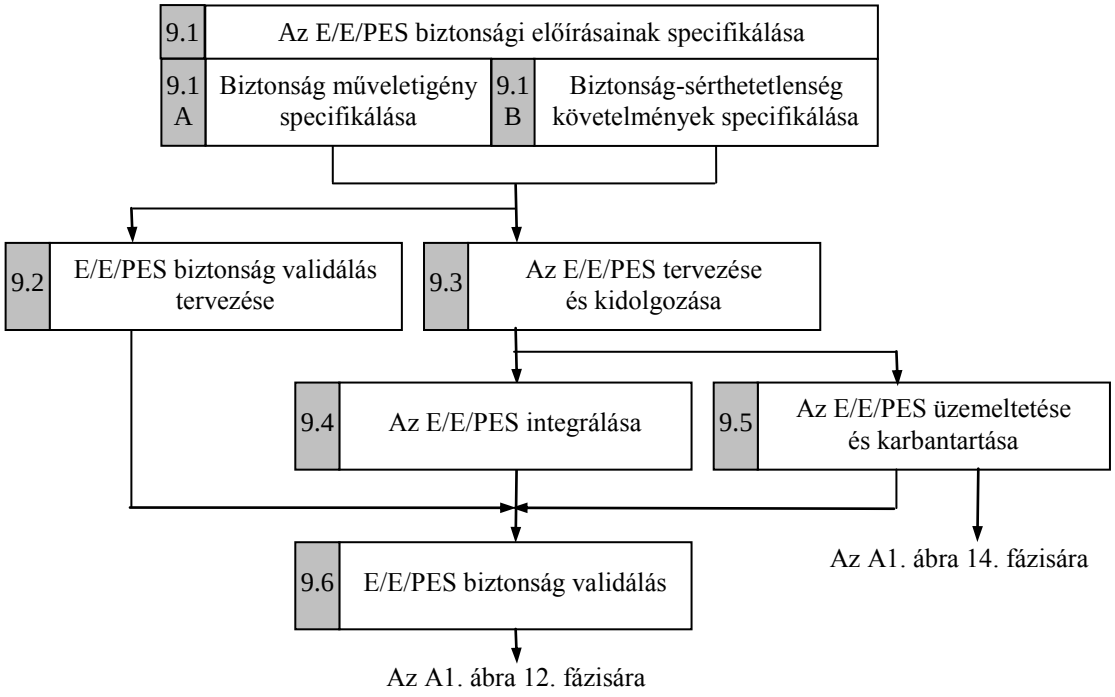
M1 Életciklus diagramok és kapcsolataik



M1.1. ábra. A teljes berendezés életciklus diagramja
(Az IEC 61508 1. Rész 2. ábráját [1] átrajzolta Neszveda József)

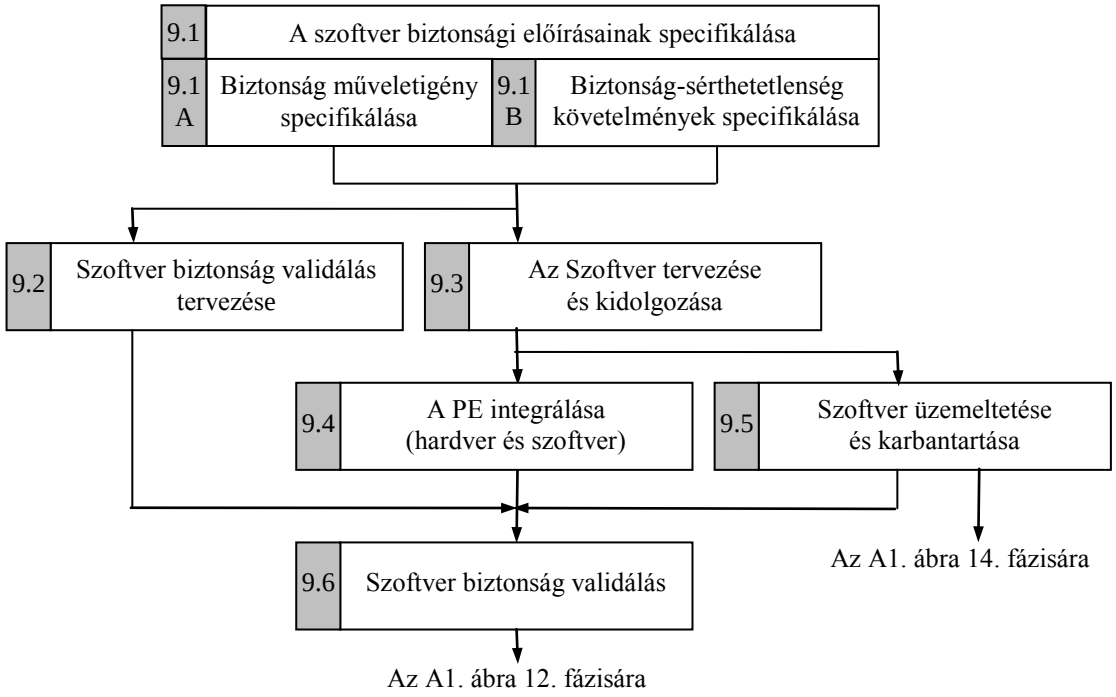
Megjegyzés: A 10. és 11. fázisok leírását az IEC 61508 szabvány nem tartalmazza.

Megjegyzés: Az IEC 61508-2 és az IEC 61508-3 részleteiben tartalmazza a 9. fázis realizálását.



M1.2. ábra. A vész-, védelmi rendszer (A1 ábra, 9. fázis) életciklus diagramja
(Az IEC 61508 1. Rész 3. ábráját [1] átrajzolta Neszveda József)

Amennyiben a berendezés irányítórendszere programozható, akkor a szoftver biztonság életciklus realizálása (I./3. ábra) szinkronizáltan történik a hardver biztonság életciklus realizálásával (I./2. ábra).



M1.3. ábra. A vész-, védelmi rendszer (M1 melléklet M1.1 ábra, 9. fázis) szoftver életciklus diagram
(Az IEC 61508 1. Rész 4. ábráját [1] átrajzolta Neszveda József)

M2 Meghibásodási ráta szorzófaktorok

	SZORZÓ FAKTOROK
MINŐSÉG MENEDZSMENT	
Normál kereskedelmi beszerzés	2
Megbeszélt specifikáció és minőség menedzsment	1
100%-os alkatrész ellenőrzés és beégetés	0,4
KÖRNYEZET	
Nyugvó állapot	0,1
Kellemes (Pl.: légkondicionált)	0,5
Fixen telepített (Nincs kellemetlen vibráció, hőmérsékletingadozás, stb.)	1
Hordozható, mobil	4

M3 Meghibásodási ráta értékek

(FARADIP.THREE [9] normál kereskedelmi beszerzés)

M3.1. táblázat: Érzékelők, távadók

Eszköz	Szorzó faktor: $\text{hiba}/10^{-6}$ óra **Környezet**			
	Kellemes	Fix	Mobil	Nyugvó
Antenna	1	1	5	0,1
Hőmérséklet távadó	0,2	2	8	0,02
Áramlástávadó	1	5	10	0,05
Nyomástávadó	2	2	10	0,2
Nyomáskapcsoló	1	5	40	0,1
Szinttávadó	5	5	10	0,5
Szintkapcsoló	2	5	20	0,2
I/P konverter	2	2	10	0,2
Nyomógomb	0,1	0,5	10	0,1
Váltó kapcsoló	0,03	0,03	1	0,01
Forgó kapcsoló	0,05	0,05	0,5	0,02

M3.2. táblázat: Berendezések

Eszköz	Szorzó faktor: $\text{hiba}/10^{-6}$ óra **Környezet**			
	Kellemes	Fix	Mobil	Nyugvó
Áramforrás (motor, generátor, akku)	-	100	200	2
Elektromos kompresszor	10	100	300	3
Hidraulikus tápkompresszor	20	200	300	2
PLC	20	20	50	2
Mikrokontroller	30	30	100	3
Villamosmotor (a.c.)	1	5	20	0,1
Centrifugál szivattyú	10	50	100	1

M3.3. táblázat: Végrehajtók

Eszköz	Szorzó faktor: $\text{hiba}/10^{-6}$ óra **Környezet**			
	Kellemes	Fix	Mobil	Nyugvó
Mágneskapcsoló DIL	0,03	0,5	1,8	0,01
Hidraulikus munkahenger	1	1	-	-
Teljesítmény relé	1	2	16	0,1
Léptető motor	0,5	0,5	5	0,05
Gömbszelep	0,2	3	10	0,1
Pillangószelep	1	20	30	0,5
Együlékes szabályozó szelep	1,5	20	30	1
Mágnesszelep	1	1	8	0,2

M3.4. táblázat: Egyéb eszközök

Eszköz	Szorzó faktor: $\text{hiba}/10^{-6}$ óra **Környezet**			
	Kellemes	Fix	Mobil	Nyugvó
Tápkábel csatlakozás	0,05	0,05	0,4	0,04
Pneumatikus, hidraulikus csatlakozás	1	1	8	0,8
Mikrohullámú adó/vevő	0,2	1	2,5	0,05

M4 TESEO modell súlyozó értékei.

Az értékek a [20]-ből átvéve

	SZORZÓ FAKTOROK
TEVÉKENYSÉG	
Egyszerű	0,001
Figyelmet igényel	0,01
Nem rutinszerű	0,1
A RENDELKEZÉSRE ALLÓ MÁSODPERCEK	
„A” 2 (rutinszerű műveletre), vagy 3 (nem rutinszerű műveletre)	10
„B” 10 (rutinszerű műveletre), vagy 30 (nem rutinszerű műveletre)	1
„C” 20 (rutinszerű műveletre)	0,5
”D” 45 (nem rutinszerű műveletre)	0,3
„E” 60 (nem rutinszerű műveletre)	0,1
KEZELŐSZEMÉLYZET KÉPZETTSÉGE	
Kiváló	0,5
Átlagos	1
Gyengén képzett	3
VESZÉLYÉRZET	
Veszélyes	3
Potenciálisan veszélyes	2
Normál	1
A BERENDEZÉS KEZELHETŐSÉGE	
Kiváló	0,7
Jó	1
Átlagos	3 - 7
Nagyon szegényes	10

A TESEO arányszámot úgy kezelem, mint kockázat növelő tényezőt, és a feladat végrehajtása közben taszkokat az adott szempont szerinti csoportokba osztva, egy feltételezett eloszlás szerint súlyozva alkotok átlagértéket. Összeszorozva a súlyozó tényezőket, és a folytonos üzemmód 10^{-5} értékével osztva a kapott értéket, az eredményt százalékos növekedésnek tekintem.

A fenti eljárás nélkülöz minden tudományos megalapozottságot, de alkalmas szorzószámokat generál az általános célú, nem egy konkrét alkalmazáshoz rendelt, vizsgálathoz, és jól tükrözi a csoportok egymáshoz viszonyított arányait.

- Jól motivált és kiválóan felkészített kezelőszemélyzet, valamint ideálisan felkészített eszköz.

  Tevékenység 0,005, idő stressz 0,04, képzettség kiváló 0,5, veszélyérzet 1,6, berendezés kezelhetősége kiváló 0,7. A szorzat értéke: 0,000112

  h_A=1,112
- Jól felkészített eszköz, és személyes konfliktussal nem terhelt, jól felkészített kezelőszemélyzet

  Tevékenység 0,005, idő stressz 0,04, képzettség jó 0,7, veszélyérzet 1,6, berendezés kezelhetősége jó 1. A szorzat értéke: 0,000224

  h_A=1,224
- Nem kellően felkészített személyekkel kiegészített kezelőszemélyzet, és elvárhatóan felkészített eszköz

  Tevékenység 0,005, idő stressz 0,04, képzettség átlagos 1, veszélyérzet 1,6, berendezés kezelhetősége jó átlagos 2. A szorzat értéke: 0,00064

  h_A=1,640
- Nem kellően felkészített, de a feladat végrehajtására képes, kezelőszemélyzet és eszköz.

  Tevékenység 0,005, idő stressz 0,04, képzettség átlagosnál gyengébb 2, veszélyérzet 1,6, berendezés kezelhetősége átlagos 4. A szorzat értéke: 0,00256

  h_A=3,560

M5 Végrehajtók

Az V./1. táblázat a [7] szakkönyvből lett átvéve, amelynek szerzői a táblázat forrásának a [23] internet címről megrendelhető (495 $) a „Safety Equipment Reliability Handbook, Volume 3” (Biztonsági eszközök megbízhatósága Kézikönyv, 3. Rész) jelölték meg, ami több száz végrehajtó meghibásodási ráta adatát tartalmazza.

M5.1. táblázat: Pneumatikus munkahenger hibafrakció arányai [h^{-1}]

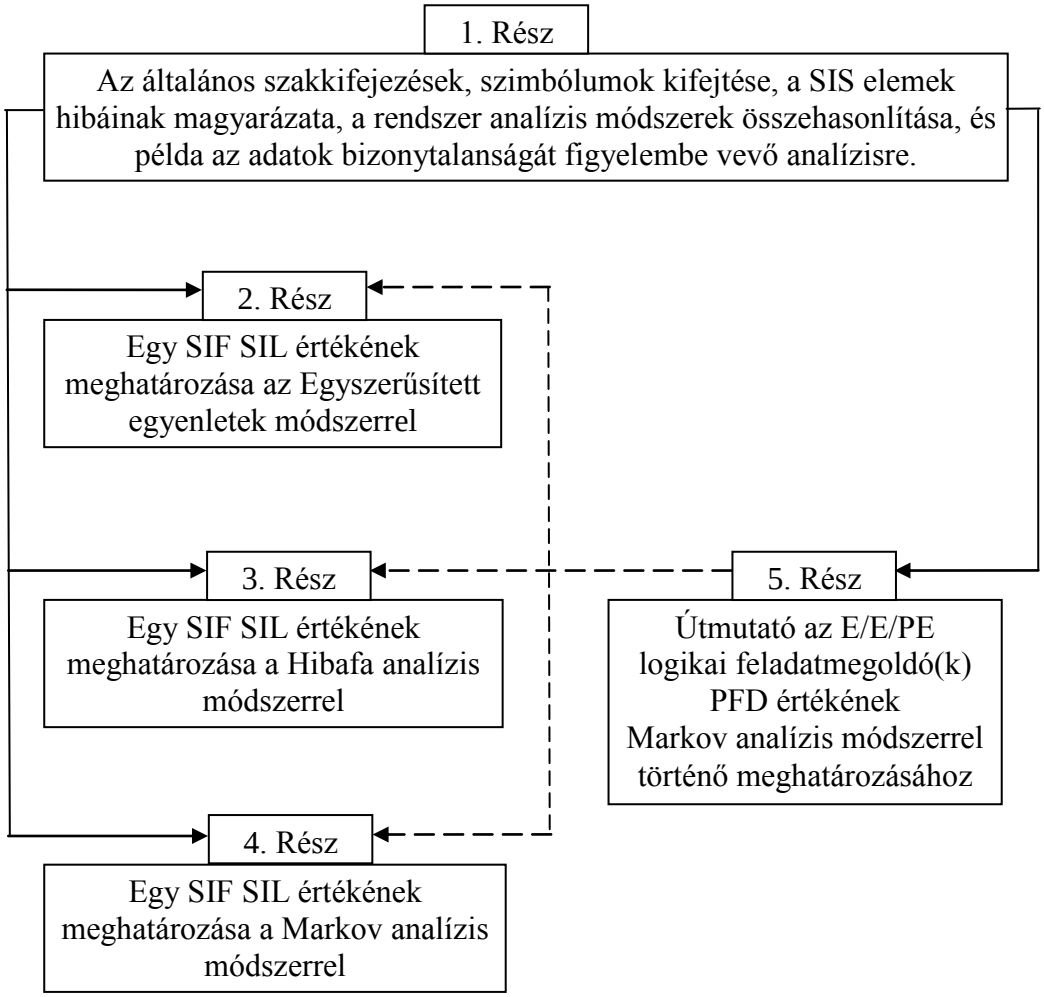
Komponens	**Hiba ok**	λ_{DD}	λ_{DU}
Munkahenger lefogó	A deformációja akadályozza a tengely visszahúzását	1,00E-09	-
Henger	Rongálódása akadályozza a tengely visszahúzását	2,50E-09	-
Dugattyú	Rongálódása / deformációja akadályozza a tengely visszahúzását	1,50E-08	-
Dugattyú csapágyazása	Rongálódása / deformációja akadályozza a tengely visszahúzását	4,00E-08	-
Hengerpersely	Rongálódása / deformációja akadályozza a tengely működtetését	3,60E-08	-
Dugattyúfej	Rongálódása akadályozza a tengely működtetését	1,00E-08	-
Dugattyúrúd csapágyazása	A deformációja akadályozza a tengely visszahúzását	2,00E-08	-
	Együttes érték:	1,24E-07	-

M5.2. táblázat: Hidraulikus munkahenger meghibásodási rátái [h^{-1}]

Komponens	**Hiba ok**	λ_{DD}	λ_{DU}
Munkahenger lefogó	A deformációja akadályozza a tengely visszahúzását	1,00E-09	-
Henger	Rongálódása akadályozza a tengely visszahúzását	2,50E-09	-
Dugattyú	Rongálódása / deformációja akadályozza a tengely visszahúzását	1,50E-08	-
Dugattyú csapágyazása	Rongálódása / deformációja akadályozza a tengely visszahúzását	4,00E-08	-
Tengelyrúd megvezetése	Repedése / törése akadályozhatja a tengely visszahúzását	-	1,20E-08
Dugattyútömítés	Rongálódása akadályozza a tengely visszahúzását	1,00E-08	-
Hengerfedél	A deformációja akadályozza a tengely visszahúzását	2,50E-09	-
	Együttes érték:	7,1E-08	-1,20E-08

A pneumatikus munkahengerek esetén a maximális teszthatékonyság: 100%, hidraulikus munkahengerek esetén a maximális teszthatékonyság: 85,5%,

M6 ISA-TR-84.02.00-2002 felépítése



M6.1. ábra. Az ISA-TR-84.00.02-2002 felépítése [28]
(Átrajzolta: Neszveda József)

Az ábrán szaggatott vonal jelzi, hogy a hagyományos módszerekbe a programozható elektronikát úgy lehet beilleszteni, hogy a programozható elektronika meghibásodási rátáit, PFD értékét külön kell meghatározni.

M7 SIF-hez tartozó eszközök, alrendszerek hibatáblázata a Markov gráf szerkesztéséhez

Az hipotetikus SIF példában két nyomástávadó együttes magas jelére zárják le a tolózárak a csőszakaszt.

M7. táblázat: Hibafajták és értékeik

Eszköz, alrendszer	Hibafajták és értékei [Fits]		Egy hibás a kettőből	Helyre-állítás		Mindkettő hibás
1002D PLC (L1, L2)	SCP		FS	-		FS
	DCP		FD			FD
	SD		DD	μ_L		FD
	DD		DD			FD
	SU		DU			FD
	DU		DU			FD
Nyomástávadók (P1, P2)	SCP		FS	-		FS
	DCP		FD			FD
	SD		SD	μ_P		FS
	DD		DD			FD
	SU		SU	-		FS
	DU		DU			FD
Hidraulikus munkahengerrel működtetett tolózár végrehajtó (V1, V2)	SCP		FS	-		FS
	DCP		FD			FD
	SD		SD	μ_V		FS
	DD		DD			FD
	SU		SU	-		FD
	DU		DU			FD
Stb.						

A M7 melléklet M7.1. táblázatban a szürkén jelzett mezőbe a konkrét gyári vagy számított meghibásodási ráta, illetve javítási ráta értékek kerülnek. Az stb. a további figyelembe veendő elemeket, például a külső elektromos és hidraulikus tápellátást, jelképezi.

A táblázatban szerelő rövidítések:

SCC	Azonos eszköz közös részének, szerelvényének kezelhető hibája
DCC	Azonos eszköz közös részének, szerelvényének veszélyes hibája
SD	Kezelhető, detektált hiba
DD	Veszélyes, detektált hiba
SU	Kezelhető, nem detektált hiba
DU	Veszélyes, nem detektált hiba
FS	Hamis leállás
FD	Vészleállás
μ	Javítási ráta

Megjegyzés: Azonos eszközök esetén a meghibásodásnak lehetnek közös okai. A β faktort, ami a hibák közös részarányát adja meg, az eszközgyártók a jegyzőkönyveikben általában definiálják.

A két azonos feladatot ellátó, λ_A és λ_B meghibásodási rátájú eszköz meghibásodását független eseménynek tekintve a gráf él meghatározásakor az eredő

$$\lambda_{i,j} = \lambda_A + \lambda_B .$$

Ha az eszközök, vagy szerelvényük azonos gyártótól származnak, akkor definiálni kell egy β faktort. A gráf él meghatározásakor az eredő

$$\lambda_{i,j} = \lambda_A + \lambda_B + \beta(\lambda_A + \lambda_B) .$$

ahol a β faktor szokásos értékei 1 – 5%.

M8 Matlab M fájlok.

M8.1a Matlab deklar.m M fájl:

A meghibásodási ráta összetevők, az átmenet-valószínűség mátrixok, és a tesztlefedettség definiálása

```
% Kiindulási paraméterek deklarálása
%Veszélyes hibák aránya
edang=0.6
%Detektált hibák aránya
edect=0.9
%A leállást okozó hibák aránya
estop=0.1
%A hamis leállás aránya alaphelyzetben
espurn=0.5
%A hamis leállás aránya csökkentett üzemmódban
espurr=0.5
%Hibaarányok meghatározása
%Az aperiodikusan alkalmazott berendezés hibaaránya
format long e
lambda0=6.4e-06;
lambda17=lambda0*estop*espurn;
lambda16=lambda0*estop*(1-espurn);
lambda15=(lambda0*(1-estop)*edang*(1-edect))/2;
lambda14=(lambda0*(1-estop)*(1-edang)*(1-edect))/2;
lambda13=(lambda0*(1-estop)*edang*edect)/2;
lambda12=(lambda0*(1-estop)*(1-edang)*edect)/2;
lambda26=lambda12*(1-espurr);
lambda27=lambda12*espurr;
lambda36=lambda13*(1-espurr);
lambda37=lambda13*espurr;
lambda46=lambda14*(1-espurr);
lambda47=lambda14*espurr;
lambda56=lambda15*(1-espurr);
lambda57=lambda15*espurr;
%Az átmenet valószínűség-mátrix kiinduló értéke
format long e
t=[(1-lambda0),2*lambda12,2*lambda13,2*lambda14,
2*lambda15,lambda16,lambda17;
    0 (1-lambda12),0,0,0,lambda26,lambda27
    0 0 (1-lambda13),0,0,lambda36,lambda37
    0 0 0 (1-lambda14),0,lambda46,lambda47
    0 0 0 0 (1-lambda15),lambda56,lambda57
    0 0 0 0 0 1 0
    0 0 0 0 0 0 1]
%Az egységmátrix
iem=eye(7);
%Üzemen kívüli állapot, és időkonverzió szorzótényezői: 0,1 és 48.
h=4.8;
%Üzemen kívüli állapot időkonvertált átmenet-valószínűség mátrixa
tln=(t-iem)*h+iem
%A tesztlefedettség periodikus tesztekkor
cm=0.9;
```

M8.1b Matlab nyugalmi.m M fájl:

A periodikus tesztekkel megszakított üzemen kívüli állapot

```
%Ciklusváltozók értékadása
n=10;m=15;k=3;
%Kezdeti értékek és az Eredménymátrix
format long e
s0=[1 0 0 0 0 0 0];
i2=[0 1 0 0 0 0 0];
i3=[0 0 1 0 0 0 0];
t0=tln;
t1=tln;
em=zeros(n*m,7);
%Az eredmény mátrix feltöltése
for r=0:n-1
    format long e
    for q=1:m
        %A tesztek közötti értékek
        if q<m
            s=r*m+q;
            em(s,:)=s0*t0;
            t1=t0;
            t0=t1*tln;
        else
            %t0 konverzió a teszt kezdetekor
            t0=((t0-iem)/h)+iem;
            %A tesztüzem állapotváltozása
            for p=1:k
                sp=s0*t0;
                t1=t0;
                to=t1*t;
            end
            %t0 konverzió, és az állapot-vektor a teszt befejezésekor
            t0=((t0-iem)*h)+iem;
            sp=t0(1,:);
            %Az állapotkorrekció segédváltozói
            sx1=em(1,[2 3 6 7]);
            sxp=sp(:,[2 3 6 7]);
            vx=sxp-sx1;
            sx=sum(sxp);
            va=cm*sum(vx)/4;
            wa=1-(va/sx);
            %Segédvektorok
            v=[va 0 0 0 0 0 0];
            w=[1 wa wa 1 1 wa wa];
            %A korrigált állapot számítása
            snkorr=(diag(w'*sp)+v')';
            %A korrigált átmenet-valószínűség mátrix részei
            tln2=(tln([2],:)-i2)(2-cm)+i2;
            tln3=(tln([3],:)-i3)(2-cm)+i3;
            t045=t0([4 5],:);
            tln67=tln([6 7],:);
            t0=[snkorr;tln2;tln3;t045;tln67];
            %Az eredménymátrix korrigált sora = s0*t0 = snkorr
            s=r*m+m;
            em(s,:)=snkorr;
            t1=t0
            t0=t1*tln;
        end
    end
end
```

M8.2 Matlab utolso.m M fájl:

Az utolsó teszt és a feladatvégzés kezdete közötti állapot

```
%Az átlagos hibavalószínűség számítása az utolsó tesztet követően
%Ciklusváltozó értékadása
k=7;
%Eredménymátrix
eml=zeros(k-1,7);
%Ciklus
for i=1:(k-1)
    eml(i,:)=s0*t0;
    t1=t0;
    t0=t1*tln;
end
%Veszélyes hiba okozta leállás
eml6=eml(:,6);
%Hamis leállás
eml7=eml(:,7);
%Az átlagos hibavalószínűség az utolsó tesztet követően
pfmbl=(sum(eml6')+sum(eml7'))/(k-1);
%Az 1/óra dimenzióra történő konvertálás
pfmbl=pfmbl/h;
```

M8.3 Matlab uzemeles.m M fájl:

A feladatvégzés állapotvektorai

```
%Az átlagos hibavalószínűség számítása üzemeléskor
%Ciklusváltozó értékadása
j=24;
%Megnövekedett igénybevétel tényezője
hc=2;
%Emberi tényező
ha=1.224;
%Eredménymátrix
emm=zeros(j+1,7);
%Az T0 átmenet-valószínűség mátrix állapot időkonverziója,
%Az emberi tényező figyelembe vételével
t0=ha*(t0-iem)/h+iem;
%Az T átmenet-valószínűség mátrix konvertálása
%a megnövekedett igénybevétel figyelembe vétele,
%és az emberi tényező figyelembe vétele
tm=(t-iem)*hc*ha+iem;
%Ciklus
for i=0:j+1
    emm(i,:)=s0*t0;
    t1=t0;
    t0=t1*tm;
end
%Veszélyes hiba okozta leállás
emm6=emm(:,6);
%Hamis leállás
emm7=emm(:,7);
%Az átlagos hibavalószínűség üzemeléskor
pfmbm=(sum(emm6')+sum(emm7'))/(j+1);
%Az aperiodikusan alkalmazott berendezések
%átlagos hibavalószínűsége 1/óra dimenzióban
pfmb=pfmbl+pfmbm;
```

PUBLIKÁCIÓS JEGYZÉK

Hazai megjelenésű jegyzetek

Neszveda, J. Automatika I. Klasszikus szabályozáselmélet, BMF KVK 2044, 2007

Neszveda, J. Automatizálás eszközei, BMF KVK 2054, 2009

Gecsey, L. Neszveda, J. Automatika I. laboratórium, BMF KVK 2042, 2006

Kucsera, P. Neszveda, J. Automatizálás, BMF KGK 2017, 2009

Gecsey, L. Harkay, T. Neszveda, J. Vajda, A. Automatizálás a gyakorlatban, BMF KVK 2048, 2008

Lektorált hazai cikkek:

Neszveda, J. Redundáns struktúrák és a biztonság sérthetetlenség szint kapcsolata ZMNE, Hadmérnök II. évf. 1. szám, 2007, p. 186-196. ISSN 1788-1919

Forgon, M. Neszveda, J. 1002D struktúrájú, kritikus üzembiztonságú rendszer elemzése diszkrét-diszkrét Markov-modellel, Hadmérnök II évf. 3. szám, 2007, p. 198-205. ISSN 1788-1919

Neszveda, J. Időszakosan használt harctéri eszközök megbízhatóság szintjének elemzése diszkrét-diszkrét Markov-modellel, Robothadviselés 7. Tudományos konferencia 2007, ZMNE, Hadmérnök, 2008, különszám, p. 1-8. ISSN 1788-1919

Neszveda, J. Numerikus modell IMET eszközök megbízhatósági szintjének vizsgálatára ZMNE, Hadmérnök, 2008 III. évf. 4. szám, p. 165-172. ISSN 1788-1919

Neszveda, J. Az aperiodikusan alkalmazott katonai berendezések ellenőrző tesztjeinek hatása a megbízhatóság állapotvektorra, ZMNE, Hadmérnök, 2010 V. évf. 2. szám, p. 322-329. ISSN 1788-1919

Lektorált idegen nyelvű cikkek:

Neszveda, J. Safety Lifecycle of Intermittently Operated Device, Academic and Applied Research in Military Science, Volume 8, Issue 2, 2009, p. 203-2011 ISSN 1588-8789

Konferencia kiadványok:

Neszveda, J. Üzemen kívüli, időszakosan működtetett eszközök megbízhatóság szintjének elemzése, II. Tudományos Szimpózium 2007, ISBN 978-963-7154-61-4

Neszveda, J. Investigating reliability in time-domain, using MATLAB program, XXIV. Nemzetközi Kandó Konferencia 2008, ISBN 978-963-7154-74-4

Neszveda, J. Meghibásodás-valószínűség nem folytonos változásának kezelése állapot korrekcióként, XXV. Nemzetközi Kandó Konferencia 2009, ISBN 978-963-7154-92-8

Neszveda, J. Az aperiodikusan alkalmazott berendezések megbízhatósága, XXVI. Nemzetközi Kandó Konferencia 2010, ISBN 978-963-7158-04-9

FELHASZNÁLT IRODALOM

[1] Sharkey, N. Cassandra or False Prophet of Doom: Ai Robots and War, IEEE Intelligent Systems, 2008. 08

[2] IEC 61508. Functional safety of Electrical/Electronic/Programmable electronic Safety-Related Systems, IEC
Part 1: General requirements, 1998
Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, 2000
Part 3: Software requirements, 1998
Part 4: Definitions and abbreviations, 1998
Part 5: Examples of methods for the determination of safety integrity levels, 1999
Part 7: Overview of techniques and measures, 2000

[3] IEC 61511, Functional safety – Safety integrated systems for the process industry sector, IEC
Part1: Framework, definitions, system, hardware and software requirements, 2002
Part2: Guidelines in the application of IEC 61511-1-Informative, 2002
Part3: Guidelines for determination of safety integrity levels, 2002

[4] MIL-STD-882D, Standard Practice for System Safety, Department of Defense AMSC N/A, 2000

[5] ANSI/ISA-84, Application of safety instrumented system for the process industries, Research Triangle Park, ISA, 2006, ISBN: 1-55617-590-6

[6] API 14C, Recommended Practice for Analysis, Design, Installation and Testing of Basic Surface Safety System for Offshore Production Platforms, 7th edition, D.C. Washington, American Petroleum Institute, 2001

[7] Goble, W. M. Cheddie, H. L. Safety Instrumented System Verification. Practical Probabilistic Calculation, NC: Research Triangle Park, ISA, 2006, ISBN: 1-55617-909-X

[8] EN IEC 1078. Analysis techniques for dependability Reliability block diagram method, 1993

[9] http://www.technis.org.uk/, 2009-07-22

[10] Goble, W. M. Control System Safety Evaluation and Reliability, 2th edition, NC: Research Triangle Park, ISA, 1998, ISBN: 1-55617-636-17

[11] Mood, A. Franklin, A. Graybill, D. Boes, C. Introduction to the Theory of Statistics, 3th Edition, McGraw-Hill. 1974, ISBN 0-07-042864-6.

[12] Grun, P. Cheddie, H. L. Safety Instrumented Systems: Design, Analysis and Justifications, NC: Research Triangle Park, ISA, 2006, ISBN: 1-55617-956-1

[13] Zsigmond, Gy. Folytonos idejű rendszerek megbízhatóság vizsgálata, Automatizálás, 1985 5. szám

[14] Neszveda, J. Numerikus modell IMET eszközök megbízhatósági szintjének vizsgálatára, ZMNE, Hadmérnök, 2008 III. évf. 4. szám, p. 165-172. ISSN 1788-1919

[15] Ermoli, Y. A., Reliability calculation under seasonally varying failure rate, ISA Transaction 46, available online Science Direct 2007

[16] Neszveda, J. Az aperiodikusan alkalmazott berendezések megbízhatósága, XXVI. Nemzetközi Kandó Konferencia 2010. ISBN 978-963-7158-04-9

[17] Kletz, T. A. An Engineers View of Human error, 3th edition NC: Research Triangle Park, ISA, 2001, ISBN: 0852954301

[18] Goble, W. M., Bukowski, J. V, Brombacher, A. C. How Diagnostic Coverage improves safety in programmable electronic system, IEEE Transaction of Reliability Vol. 36, No. 4, New York, 1998

[19] KUCSERA P. Szárazföldi autonóm mobil robotok vezérlőrendszerének kialakítási lehetőségei, Robothadviselés 8. Tudományos konferencia

[20] http://www.emersonprocess.com/rosemount/solution/FMEDA_Rosemount_3051S_v210.pdf. Letöltve: 2009-08-06

[21] Rutledge, P. J. Mosleh, A., Dependent-Failures in Spacecraft Root Causes, Coupling factors, Defenses and Design Implication. "Proceeding of the Annual Reliability and Maintainability Symposium" IEEE, New York, 1995

[22] http://www.magnetrol.com/v2/pdf/MII/FMEDA_Analysis_report_Displacer_Switches.pdf Letöltve 2009-08-06

[23] http://www.isa.org

[24] Goble, W. M., The Safety 1002D PLC – How it works. "Proceeding of the Spring ISA Symposium" New Orleans, ISA, 1997

[25] http://zone.ni.com/devzone/cda/tut/p/id/3755 Letöltve: 2009-08-07

[26] http://library.abb.com/global/scot/scot211.nsf/veritydisplay/1719aad439693429c125723b00406875/$File/CE_TZIDC_TZIDC-200_SIL_FMEDA_EN.pdf Letöltve:2009-08-10.

[27] Bukowski, J. V. Modeling and Analyzing the Effects of Periodic Inspection on the Performance of Safety-Critical Systems, IEEE Transaction of Reliability Vol. 50, No. 3, New York, 2001

[28] ISA-TR84.00.02-2002, Safety Instrumented Function (SIF) – Safety integrated Level (SIL) evaluation techniques, IEC
Part1: Framework, definitions, system, hardware and software requirements, 2002
Part2: Determining the SIL of a SIF via Simplified Equations, 2002
Part3: Determining the SIL of a SIF via Fault Tree Analysis, 2002
Part4: Determining the SIL of a SIF via Markov Analysis, 2002
Part5: Determining the PFD of SIS Logic Solvers via Markov Analysis, 2002

[29] Smith, D. J. Reliability, Maintainability, and Risk: Practical Methods for Engineers, 6th edition. Butterworth-Heinemann, 2001, ISBN: 978-0-7506-6694-7

[30] Forgon, M. Neszveda, J. 1002D struktúrájú, kritikus üzembiztonságú rendszer elemzése diszkrét-diszkrét Markov-modellel, Hadmérnök II évf. 3. szám, 2007, p. 198-205. ISSN 1788-1919

[31] Neszveda, J. Redundáns struktúrák és a biztonság sérthetetlenség szint kapcsolata, ZMNE, Hadmérnök, 2007 II. évf. 1. szám, p. 186-196. ISSN 1788-1919

[32] http://www.mathworks.com/academia/ Letöltve 2009-08-24
Matlab 7 Getting Started Guide
Matlab 7 Programming Fundamentals
Matlab 7 Programming Tips
Matlab 7 Graphics

[33] MATHWORKS, INC: Matlab 2008b HELP, 2008.

[34] Lewis, E. E. Introduction to Reliability Engineering, John Wiley & Sons, New York, 1987

[35] Sb/73. Ábraalbum a 2T7M szállító-töltő gépkocsi műszaki leírásához és üzemelési utasításához, HM., Budapest, 1975

[36] http://www.automation.siemens.com/mcms/human-machine-interface/en/operator-interfaces/mobile-panel/Pages/Default.aspx Letöltve: 2010-01-14

[37] Klé 10. Utasítás a csapatlégvédelmi rakétaalegységek részére (KUB légvédelmi rakéta üteg), HM., Budapest, 1976

[38] Sb/72. A 2T7M szállító-töltő gépkocsi műszaki leírása és üzemelési utasításai, HM., Budapest, 1975

[39] Rouvroye, J. Wiegerinck, E. Jan, A. M. Minimizing cost while meeting safety requirements: Modeling deterministic (imperfect) staggered test using standard Markov models for SIL calculation, ISA Transactions Vol. 45 Num. 4, 2006.

[40] Torres-Echeveria, A. C. Martorell, S. Thompson, H. A. Modeling and optimization of proof testing policies for safety instrumented systems, Elsevier Journal: Reliability Engineering and System Safety, 2009

[41] Bucher, C. Frangopol, D. M. Optimization of lifetime maintenance strategies for deteriorating structures considering probabilities of violating safety, condition and cost thresholds, Elsevier Journal: Probabilistic Engineering Mechanics, 2006

[42] Neszveda, J. Safety Lifecycle of Intermittently Operated Device, Academic and Applied Research in Military Science, Volume 8, Issue 2, 2009, p. 203-2011 ISSN 1588-8789

[43] Neszveda, J. Az aperiodikusan alkalmazott katonai berendezések ellenőrző tesztjeinek hatása a megbízhatóság állapotvektorra, ZMNE, Hadmérnök, 2010 V. évf. 2. szám, p. 322-329. ISSN 1788-1919

[44] MSz IEC 50 (191) Nemzetközi elektrotechnikai szótár. 191. kötet: Megbízhatóság és a szolgáltatások minősége, 1992.

[45] Fenyő, I - Frey, T. Matematika Villamosmérnököknek I. Műszaki Könyvkiadó, Budapest, 1964

[46] Karlin, S. - Taylor, H. M. Sztochasztikus folyamatok, Gondolat, Budapest, 1985

[47] Ramanathan, R. Introductory Econometrics with Application, 5th Edition, Thomson Learning, South-Western division, 2002. ISBN 963-545-374 4

[48] Montgomery D. C. Runger G. C. Montgomery D. Applied Statistics and Probability for Engineers, John Wiley and Sons, January 1994.

[49] Neumann, P. G. Computer Related Risk, Addison-Wesley, 1995.

[50] Winston, W. L. Operation Research. Application and Algorithms, International Thomson Publishing, Duxbury, 1997. ISBN 963 9478 60 1.

[51] Kletz, T. A. Computer Control and Human Error, Gulf-Publishing, 1995

[52] IEC 60812 Analysis Techniques for System Reliability – Procedure for Failure Mode and Effects Analysis, IEC, 1985

[53] Ohring, M. Reliability and Failure of Electric Materials and Device, Elsevier Inc., 1998, ISBN: 978-0-12-524985-0

[54] Evans, M. Hastings, N. Peacock, B. Statistical Distributions, 2nd edition, John Wiley & Sons, NY, 1993.

[55] Marszal, E. M. Tolerable risk guidelines, ISA Transaction Vol. 40, 2001, Available online at www.elsevier.com/locate/isatrans

[56] Neszveda, J. Időszakosan használt harctéri eszközök megbízhatóság szintjének elemzése diszkrét-diszkrét Markov-modellel, Robothadviselés 7. Tudományos konferencia 2007, ZMNE, Hadmérnök, 2008, különszám, p. 1-8, ISSN 1788-1919

[57] Chiang, J. H. Juan, J. Optimal maintenance policy for a Markovian system under periodic inspection, Reliable Engineering and System Safety Vol. 71, 2001, Available online at www.sciencedirect.com

[58] Human Reliability Assessors Guide, (SRDA R-11) UKAEA, Chesire, 1995 ISBN 085.3562.205

[59] Marszal, E. M. Derivation of an equitation for quantitative SIL assignment, ISA Transaction Vol. 42, 2003, Available online at www.elsevier.com/locate/isatrans

[60] Curtois, Pierre-J. Delsarte, P. On the optimal scheduling of periodic test and maintenance for reliable redundant components, Reliable Engineering and System Safety Vol. 91, 2006, Available online at www.sciencedirect.com

[61] Bukowski, J. V. Goble, W. M. Using Markov models for safety analysis of programmable electronic system, ISA Transaction Vol. 34, 1995.

[62] Bedford, T. Cooke, R. Probabilistic risk analysis foundations and methods, Cambridge University Publishing Ltd; 2001. Cambridge

[63] Nilsen, T. Aven, T. Models and model uncertainty in the context of risk analysis. Reliability, Engineering System Safety Volume: 79, 2003.

[64] Nolan, P. D. Safety and Security Review for the Process Industries, 2nd edition, William Andrew Inc., 2008. ISBN: 978-0-8155-1546-3

[65] Bolton, W. Programmable Logic Controllers, 4th edition, Elsevier Inc. 2006. ISBN: 978-0-7506-8112-4

[66] Lendvay, M Zsigmond, Gy. Komplex villamos rendszerek megbízhatóság-elemzési módszerei, 2004, http://www.zmne.hu/kulso/mhtt/hadtudomany/2004/2/2004-2-11.html

[67] Békési, B. A megbízhatósági elmélet és annak gyakorlati alkalmazása a meghibásodások valószínűségére, Repüléstudományi Közlemények, Szolnok, 2001/1.

[68] Békési, B. A megbízhatóság főbb mennyiségi mutatói, ZMNE Tudományos, Közlemények, Budapest, 2006/3.

[69] Békési, B. A megbízhatóság leggyakrabban használt mérőszámai, Konferencia kiadvány, Szolnok, 20076. április 20. http://www.szrfk.hu/konf2007

[70] Makkay, I. Robotics in the 21th century, AARMS volume 2, No..2, 2004 Budapest, Hungary

[71] Molnár, A. A polgári és katonai robotjárművek fejlesztésében alkalmazott új eljárások és technikai megoldások, Doktori (PhD) értekezés, ZMNE Kutató Könyvtár, 2005.

[72] Szabolcsi, R. Modern szabályzástechnika, ZMNE, Budapest 2004.

[73] Kun, L. Szász, G. Zsigmond, Gy. Megbízhatóságelmélet, LSI. 2004

[74] Ványa, L. Excepts from the history of unmanned ground vehicles development in the USA, AARMS 2003/2, ZMNE, 2003

Az Interneten letölthető források az Értekezés zárásakor elérhetőek voltak.

RÖVIDÍTÉSEK JEGYZÉKE

	Angol szöveg	Magyar jelentés
AC/DC	Alternating current/Direct current	Váltakozó áram/Egyenáram
ALARP	As low as reasonable practicable	Olyan kicsi, ami ésszerűen kivitelezhető
ANSI	American National Standards Institute	Amerikai Nemzeti Szabvány Hivatal
BPCS	Basic process control system	Alapfolyamat irányítórendszer
DC	Diagnostic Coverage	Tesztlefedettség
E/E/PE	Electrical/electric/ programmable electric	Villamos, elektronikus, programozható elektronikus
E/E/PES	Electrical/electric/ programmable electric system	Villamos, elektronikus, programozható elektronikus rendszer
FAT	Factory acceptance testing	Gyári átvételi teszt
FTA	Fault tree analysis	Hibafa analízis
HMI	Human Machine Interface	Ember-gép interfész
H&RA	Hazard and risk analysis	Hazárd és kockázat analízis
HW	Hardware	Hardver
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Bizottság
ISA	Instrumentation System and Automation Society	Műszerezési és Automatizálási Társaság
LVL	Limited variability language	Korlátozott változatosságú nyelv
NP	Non-programmable	Nem programozható
PFM_{Davg}	Average probability of dangerous failure of intermittently operated equipment	Az aperiodikusan alkalmazott berendezések átlagos veszélyes hiba valószínűsége
PFD	Probability of failure on Demand	Hibavalószínűség működtetési igénykor
PFD_{avg}	Average probability of failure on Demand	Átlagos hibavalószínűség működtetési igénykor
PLC	Programmable Logic Controller	Programozható Logikai Vezérlő
TC_A	Diagnostic Coverage of intermittently operated equipment	Az aperiodikusan alkalmazott berendezések tesztlefedettsége

SFF	Safe failure fraction	Kezelhető hiba rész
SIF	Safety Instrumented function	Biztonságra műszerezett funkció
SIL	Safety Integrity Level	Biztonság-sérthetetlenség szint
SIS	Safety Instrumented system	Biztonságra műszerezett rendszer
SRS	Safety requirement specification	Biztonsági előírások
SW	Software	Szoftver

ÁBRAJEGYZÉK

TÁBLÁZATOK JEGYZÉKE