Dr. Forgon Miklós mk. ezredes
ZMNE Bolyai János Katonai Műszaki Kar Katonai Elektronikai Tanszék
forgon.miklos@zmne.hu
Neszveda József főiskolai docens, irányítástechnikai szakmérnök
BMF Kandó Villamosmérnöki Kar Műszeripari és Automatizálási Intézet
neszveda.jozsef@bmf.kvk.hu

1002D STRUKTÚRÁJÚ, KRITIKUS ÜZEMBIZTONSÁGÚ RENDSZER (SCS[1]) ELEMZÉSE DISZKRÉT-DISZKRÉT MARKOV MODELLEL

Absztrakt

Összehasonlítva az alap és a vész, védelmi irányítás jellemzőit, a cikk az integrált vész, védelmi rendszerek tervezési eljárását javasolja a légvédelmi rakéták ráemelési technológiájának alap irányítására is, mivel a légvédelmi rakéták ráemelési technológiája a kritikus üzembiztonságú irányításokhoz sorolható. Hogyan módosítja a rendszeres ellenőrzés (meleg teszt és javítás) a biztonság sérthetetlenség szintet (SIL[2]), feltételezve, hogy a légvédelmi rakéták ráemelési technológiájának irányítási rendszere 1002D struktúrájú.

Comparing the performance of the basic process and the safety process this article suggest the SIS design method for the basic process of blastoff technologies of air protection missile too, because the blastoff technologies of air protection missile can be classifiable the Safety Critical Control. How the periodic inspection (warm test and repair) can modify the Safety Integrity Level, assuming that control system of the blastoff technologies of air protection missile uses a 1002D structure.

***Kulcsszavak**: redundáns struktúra, Markov modell ~ redundant structure, Markov model*

BEVEZETÉS

A folytonos technológiai irányításokban, az alap technológiai műveletek (BPCS[3]), és a vész, védelmi rendszer (SIS[4]) hardveresen és szoftveresen elkülönített két irányítási rendszer. Az elkülönülés okát jól magyarázza a hibás üzemmódokat felsoroló az [1] szakirodalomból átvett 1. táblázat. Ugyancsak indokolja az elkülönítést, hogy amíg az alapirányításban a hibajelenséget a kezelőszemélyzet szinte azonnal észleli, addig a vész, védelmi rendszerek hónapokig, vagy jó esetben akár több évig nem hajtanak végre műveletet. Mekkora a valószínűsége annak, hogy amikor szükséges, akkor a végrehajtó eszköz (a légvédelmi rakéták ráemelési technológiájában a hidraulikus szelep és munkahenger) ténylegesen működni fog? Hogy erre a fontos kérdésre a szakhatóságok számára ellenőrizhető választ lehessen adni kidolgozták az IEC 61508 szabványt [2], ami definiálja az alapfogalmakat és bevezeti a biztonság sérthetetlenség szint (SIL) mérőszámot. A definíciók közül a téma szempontjából fontosakat, valamint

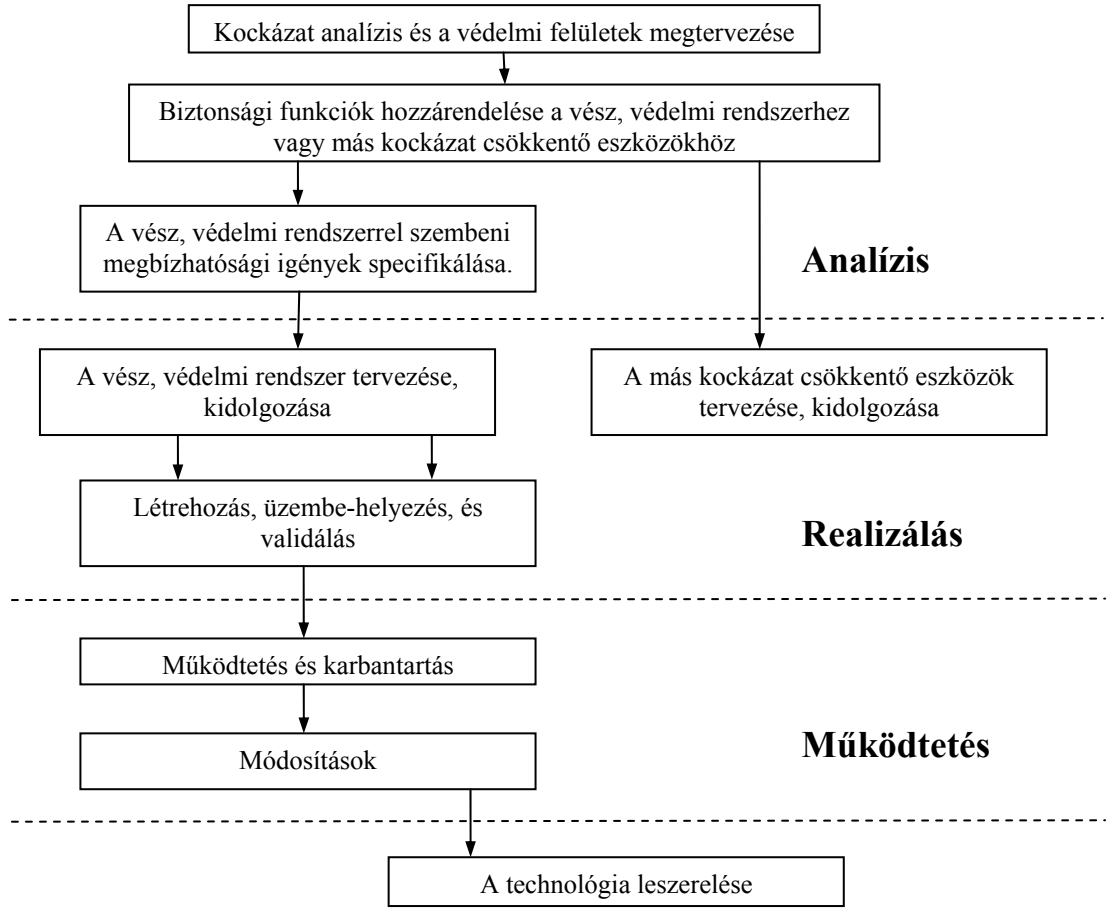
[1] Safety-Critical System
[2] Safety Integrity Level
[3] Basic Process Control System
[4] Safety Instrumented System

a SIL mérőszám értelmezését eszközökre, és ezen eszközökből épített redundáns rendszerekre az előző cikkemben [3] már tárgyaltam.

1. táblázat Hibás üzemmódok

Az alap irányítási rendszer	**Az vész, védelmi irányítási rendszer**
A beavatkozó eszköz alsó, felső véghelyzetben, vagy kifagyott	Hiba működtetéskor (Fail-Danger)
Az irányító kimenet túl alacsony, magas szintje (előjelzés)	Késleltetett működés (Fail-Danger)
Az irányító kimenet változása túl gyors	Hamis működtetés (Fail-Safe)
A beavatkozó eszköz reagálása lassú vagy akadozó	
A távadó jele alsó, felső véghelyzetben, vagy kifagyott	
A távadó jelének túl alacsony, magas szintje (előjelzés)	
A távadó jelének változása akadozó	

A veszély csökkentésére az IEC61511 szabvány az üzembiztonság életciklus[5] eljárástechnikáját javasolja, amelynek összefoglaló ábrája a [4] szabványból átvéve az 1. ábrán látható.



1. ábra:
Üzembiztonság életciklus diagram

Az IEC61511 szabvány az 1. ábra minden szövegdobozához az 1. ábrához hasonló alrendszert rendel. Például a módosításokat, a teljes rendszerhez hasonlóan, analízis előzi meg, vagy hogy a karbantartást tervezetten, a megbízhatóság sérthetetlenségi szint fenntarthatósága mellett kell végezni.

[5] Safety Lifecycle

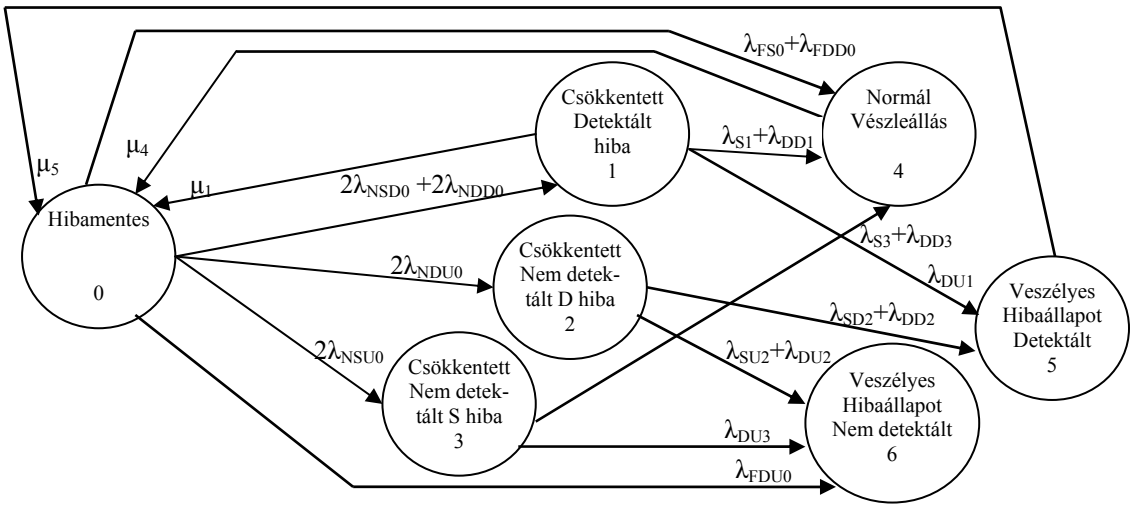
A folytonos technológiai irányításokban a vész, védelmi rendszer biztonságosan energia mentesíti a technológiát (shutdown), és az alap irányítási rendszer hibáját a kezelő személyzet számos esetben kiküszöbölheti, még mielőtt a vész, védelmi rendszer működésbe lépne. A vész, védelmi rendszer hamis működtetése, bár gazdaságilag káros, de nem veszélyes. Veszélyt a lassú működtetés, vagy a működtetéskor fellépő hiba jelent, amit leggyakrabban az okozhat, hogy a hosszú várakozási idő alatt rejtve marad valamely alkatrész, eszköz meghibásodása.

Vannak olyan rendszerek, amelyekben az alapirányításban fellépő legcsekélyebb hiba is veszélyhelyzetet jelent. A tízezer méteren repülő utasszállító repülőgép a legkedveltebb példa. Ezeket hívják kritikus üzembiztonságú (SCS) rendszereknek. A kritikus üzembiztonságú rendszerekben a vész, védelem hamis működése is veszélyes hiba. A légvédelmi rakéták ráemelési technológiáját a működtetés gyakorisága, és a működtetéskor megkövetelt igen nagy üzembiztonság okán célszerű a kritikus üzembiztonságú rendszerek közé sorolni. A kritikus üzembiztonságú rendszerekben az alap és a vész-, védelmi irányítást egybeintegrálva nagyonnagy üzembiztonságúra kell tervezni.

A Markov modell

A Markov modellben egy eszköz, vagy alrendszer, illetve a teljes rendszer működése egymást követő állapotok sorozatából áll, amelyek között az átmenetet valószínűségi változó írja le. Megbízhatóság vizsgálat csak néhány diszkrét állapotot (hibátlan, rejtett hibával, detektált hibával működés, illetve biztonságos vészleállás, baleset, stb.) tételez fel. Az átmenetek között valószínűségi változó teremt kapcsolatot. A veszélyesebb állapotba kerülés valószínűségét, más szavakkal a hibagyakoriságot, λ betűvel, a kevésbé veszélyesebb állapotba kerülés valószínűségét, más szavakkal a javíthatóságot μ betűvel szokás jelölni. A technológia működése lehet az időben folytonos vagy diszkrét. A λ értékét, a következmények miatt, célszerű megosztani kezelhető, detektált (λ_{SD}), veszélyes, detektált (λ_{DD}), kezelhető, nem detektált (λ_{SU}), és veszélyes, nem detektált (λ_{DU}) hibaarányra.

A légvédelmi rakéták ráemelési technológiájának irányítási struktúrájának az 1002D típust célszerű választani [3]. Az 1002D struktúra általános Markov gráfja a 2. ábrán látható.



2. ábra:
Általános 1002D Markov modell

A 2. ábrán diszkrét állapotok vannak, és a rendszer λ_i valószínűséggel kerül az i-edik állapotból egy másikba. Ebből az is következik, hogy az i-edik állapotban maradás valószínűsége

1- λ_i. Az 1002D struktúra a hibamentes állapotból kerülhet csökkentett (1001D struktúra) állapotba, amennyiben az egyik redundáns ág meghibásodik. Ennek valószínűsége λ_{N0}, és mert két párhuzamos ág van $2\lambda_{N0}$. Hibamentes állapotból hibás állapotba kerülésnek λ_{F0} a valószínűsége. Így $\lambda_0 = 2\lambda_{N0} + \lambda_{F0}$. Bármely λ_i tovább bontható kezelhető, detektált (λ_{SD}), veszélyes, detektált (λ_{DD}), kezelhető, nem detektált (λ_{SU}), és veszélyes, nem detektált (λ_{DU}) hibaarányra. Ha a hiba kijavításra kerül, akkor értelemszerűen a hibamentes állapotba kerül vissza a rendszer. Annak valószínűsége, hogy definiált időtartam alatt újra hibamentes legyen a rendszer μ_i A 2. ábra alapján definiálható a P valószínűségi mátrix. Az 1002D rendszerben a mátrix 7x7-es, mert a rendszert 7 állapot írja le.

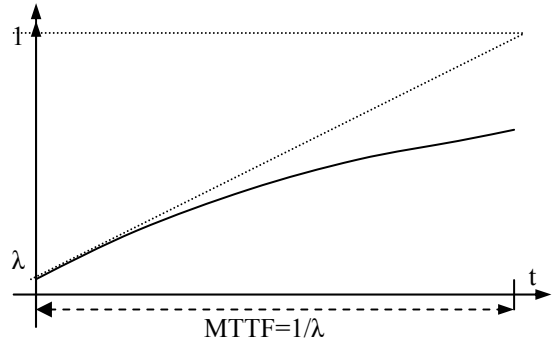
$$P = \begin{pmatrix} 1-\lambda_0 & 2\lambda_{SD0}+2\lambda_{NDD0} & 2\lambda_{NDU0} & 2\lambda_{NSU0} & \lambda_{FC0}+\lambda_{FDD0} & 0 & \lambda_{FDU0} \\ \mu_1 & 1-\lambda_1 & 0 & 0 & \lambda_{S1}+\lambda_{DD1} & \lambda_{DU1} & 0 \\ 0 & 0 & 1-\lambda_2 & 0 & 0 & \lambda_{SD2}+\lambda_{DD2} & \lambda_{SU2}+\lambda_{DU2} \\ 0 & 0 & 0 & 1-\lambda_3 & \lambda_{S3}+\lambda_{DD3} & 0 & \lambda_{DU3} \\ \mu_4 & 0 & 0 & 0 & 1-\lambda_4 & 0 & 0 \\ \mu_5 & 0 & 0 & 0 & 0 & 1-\lambda_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad <1>$$

A 2. ábra, és így az <1> összefüggés folytonos technológiák vész, védelmi rendszereire igaz, vagyis nem tartalmazza a légvédelmi rakéták ráemelési technológiájának sajátosságait. A légvédelmi rakéták ráemelési technológiája az időben diszkrét módon működtetett. A tényleges működtetés, beleértve a teszteket, rövid időtartamúak, és a működtetést hosszabb kikapcsolt állapotok szakítják meg. A λ és a μ diszkrét időpontokban értelmezett értéke önmagában nem probléma, hiszen a működtetés folyamata mintavételezetten is vizsgálható. Az eltérést az okozza, hogy valóságos éles gyakorlatot vagy harci helyzetet a 2. ábra gráfja jól írja le, de a hideg teszteket, és így az életciklus folyamatát, azonban nem.

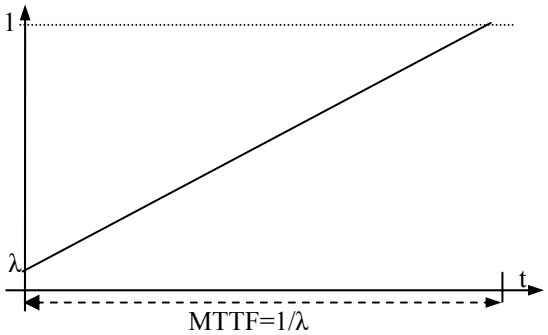
A különbség, hogy az időben diszkrét értékek nem pontjai semmilyen analitikus függvénynek, minthogy a tesztek lefolyása, erősen különbözik a valóságos éles gyakorlattól vagy harci helyzettől. A folytonos technológiákban a megbízhatóság (R) az üzemelési idő függvényében az 1-λ értékről folyamatosan csökken, ahol a λ hibaarány az MTTF (átlagos idő a meghibásodásig) reciprok értéke. Értelemszerű, hogy a meghibásodás valószínűsége (P(t)=1-R(t)) a működési idővel arányosan, nő. Az időbeli változást vagy a 3a. ábra szerint a < 2 > kifejezéssel, vagy a 3b. ábra szerint a < 3 > kifejezéssel szokás figyelembe venni.

$$P(t) = \lambda + (1-\lambda)(1-e^{-\lambda t}) = 1 - e^{-\lambda t} + \lambda e^{-\lambda t} \qquad <2>$$

$$P(t) = \lambda + (2\lambda - \lambda^2)t \qquad \text{feltéve, hogy } \lambda << 1 \qquad <3>$$



3a. ábra Az 1-R(t) függvény



3b. ábra Az 1-R(t) függvény

A légvédelmi rakéták ráemelési technológiája azért nem tekinthető folytonos technológia mintavételezett pontjainak, mert a hideg tesztek során, és a valódi helyzetekben az egyes állapotok értékelése eltérő. A hideg teszt alatt a 2. ábra gráfjához képest 1-es, 4-es, 5-ös állapotai-

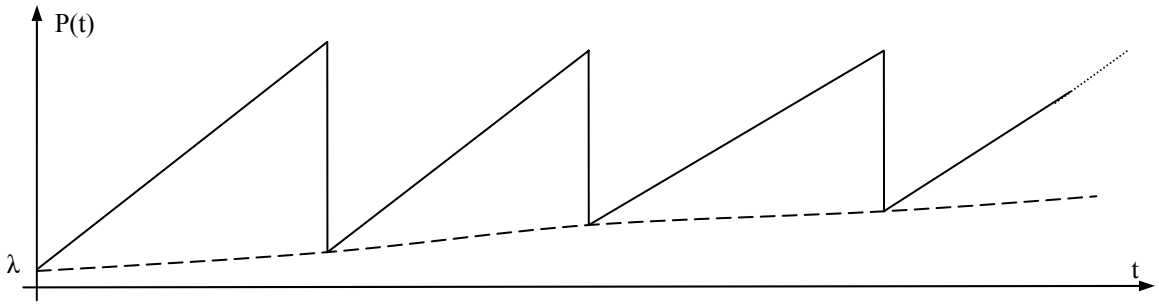
ban leállás következik, majd a detektált hiba kijavítása után újra indul a teszt, és ez mindaddig folytatódik, míg a teszt hibamentesen le nem fut. Ez azt jelenti, hogy teszt üzemmódban a $\mu_1 = \mu_4 = \mu_5 = 1$, vagyis a javításnak nincs éles időkorlátja.

Gond viszont, hogy a teszt befejeződhet a gráf 2-es, illetve 3-as állapotában. Ilyenkor a rendszer hibamentesnek van nyilvánítva, pedig van rejtett, nem detektált hibája.

A szabvány [4] a folytonos technológiákra kidolgozott, de feltételezhető, hogy az üzemközben történő diagnosztizálás eljárással (ellenőrző tesztekkel) analóg módon vizsgálható az időben diszkrét működtetés. Az eltérésekre egyrészt a folytonos technológiából a tesztelés idejére kivont résztechnológia hibaarány meghatározásának analógiájára kereshető megoldás, másrészt olyan algoritmust keresésével, amely megadja, hogy a hideg teszt mennyire fedi le (működtetésben, leterhelésben) a valódi helyzetet.

Az ellenőrző teszt hatása a hibaarányra

Folytonos technológiák esetén az P(t) meghibásodási valószínűség az üzemidővel arányosan nő (3. ábra). Ez akkor is igaz, ha az eszköz nincs működtetve, csak rendelkezésre áll. Az ellenőrző tesztek célja, hogy a hibaarány növekedését korlátozza (4. ábra).



4. ábra:
A meghibásodási valószínűség változása a rendszeres ellenőrző teszt hatására

A 4. ábrán látható, hogy a reális ellenőrző teszt modellek, nem számolnak az eredeti λ hibaarány érték visszaállításával. A 4. ábrán a szaggatott vonallal megrajzolt görbe emelkedése a nem detektált hibáktól, és így végső soron a teszt összeállításától függ, bár a nulla meredekség elméletileg sem érhető el.

A légvédelmi rakéták ráemelés technológiájának ellenőrző tesztje

A jelenlegi technológia közvetlen kézi irányítású, így a teszt célja a végrehajtó eszközök, érzékelők, és a kiegészítő berendezések működőképességének ellenőrzése. A teszteket, az alábbi protokollal, előírt időszakonként, és a tervezett éles gyakorlatok előtti héten végzik el.

- Szemrevételezés, hitelesítések ellenőrzése.
- A hidraulikus szivattyú nyomásellenőrzése. A szivattyú által továbbított folyadék, és a gázelvezető rendszer ellenőrzése.
- A hidraulikus munkahengerek végállásig történő mozgatása, a végálláskapcsolók ellenőrzése.
- Próbasúly emelés, és előírt ideig tartás.
- Működtetés utáni karbantartás

Az automatizált rendszer rendszeres karbantartásának protokollja alapvetően nem különbözik a manuális irányításúétól. A fő különbség, hogy az irányító berendezés alkalmas az érzékelőtől érkező jelek folyamatos „online” megfigyelésére, naplózásra. Az irányító berendezés rendszeres végez öndiagnosztikát, és a tesztelési protokollba egyszerűen (a bemeneti kapcsok időleges lekötésével) megoldható a csökkentett üzemmód (kezelhető hiba), és így a diagnosztikai kártya ellenőrzése. Az ellenőrztesztek gyakoriságát a teljes automatizált rendszer SIL méretezése fogja megszabni.

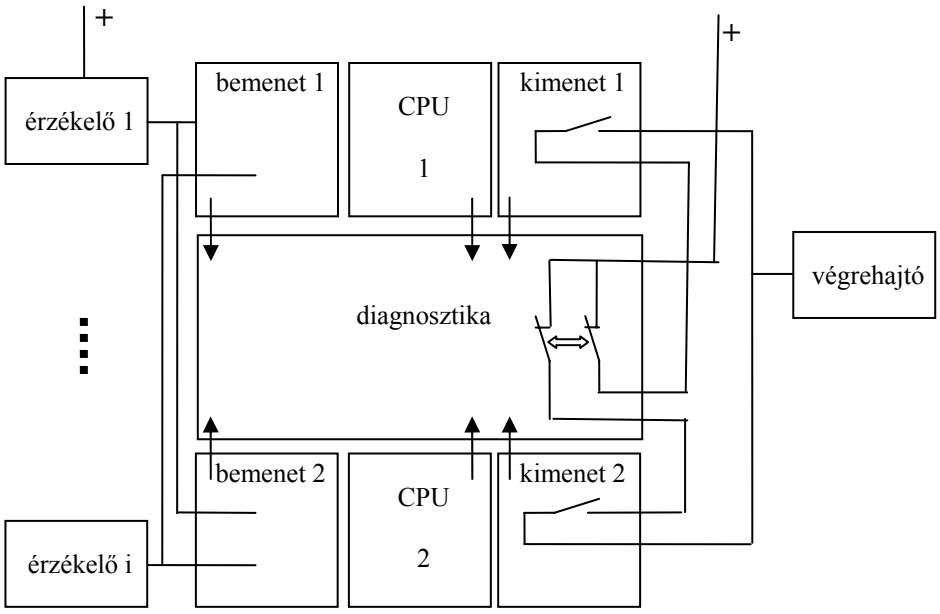
A rendszer biztonság sérthetetlenség szintjének (SIL) megállapítása

Az <1> összefüggés megoldás menete [1] szolgáltatja a teljes rendszerre vonatkoztatott MTTF[6] értékeket. Az MTTF reciprok értéke a teljes rendszerre vonatkoztatott λ hibaarány. A biztonság sérthetetlenségi szintje a teljes rendszernek ettől a λ értéktől függ (2. táblázat).

2. táblázat A biztonság sérthetetlenségi szintekhez tartozó hibavalószínűségek

SIL	Alacsony működés igényű üzemmód Az átlagos hibavalószínűség tervezett működtetés végrehajtásakor.
4	$10^{-5} \geq \lambda \geq 10^{-4}$
3	$10^{-4} \geq \lambda \geq 10^{-3}$
2	$10^{-3} \geq \lambda \geq 10^{-2}$
1	$10^{-2} \geq \lambda \geq 10^{-1}$

A rendszer viselkedése a kezelhető és a veszélyes hibákra függ a választott irányítási struktúrától. Az 1002D struktúra fizikai megvalósítása az 5. ábrán látható.



5. ábra:
Az 1002D struktúra

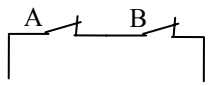
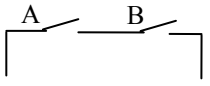
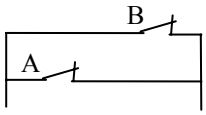
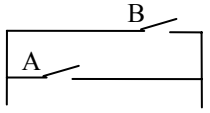
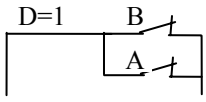
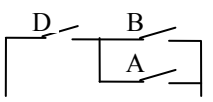
Ebben a struktúrában két processzor, saját be-, és kimeneti kártyákkal, dolgozik párhuzamosan. A két azonos funkciót megvalósító kimenet párhuzamosan van kötve. A diagnosztikai

[6] Mean Time To Failure

kártya sorba köt egy-egy kontaktus a két azonos funkciót megvalósító kimenettel, és veszélyes hiba detektálása esetén bontja a diagnosztikai kontaktusokat, ami 1002 struktúrának megfelelő. Hibátlan működés esetén, a diagnosztikai kontaktusok zárt állapotban vannak, és így a rendszer, mint 2002 struktúra viselkedik. Kezelhető hiba esetén a hibás ág diagnosztikai kontaktusát nyitja, a működő ág kontaktusa zárva marad, vagyis ez esetben a hibavalószínűséget a redundáns ágak párhuzamos, és a diagnosztikai kártya meghibásodásának soros eredője adja.

A 3. táblázatban a kontaktusok a redundáns ágak, illetve a diagnosztikai kártya hibavalószínűségének logikai kapcsolatát ábrázolja.

3. táblázat A redundancia hatása a hiba gyakoriságra

	Kezelhető hiba		Veszélyes hiba	
1002 kettő láncból egy jelez		$\lambda_E=\lambda_A+\lambda_B$		$\lambda_E=\lambda_A*\lambda_B$
2002 kettő láncból kettő jelez		$\lambda_E=\lambda_A*\lambda_B$		$\lambda_E=\lambda_A+\lambda_B$
1002D kettő láncból egy jelez diagnosztika		$\lambda_E=\lambda_A*\lambda_B$		$\lambda_E=$ $\lambda_D*(\lambda_A+\lambda_B)$

Mint ismert [3] a 2002 struktúra a kezelhető hibákra javítja, de a veszélyes hibákra rontja a megbízhatóságot, viszont az 1002 struktúra a kezelhető hibákra rontja, de a veszélyes hibákra javítja a megbízhatóságot. A diagnosztikai kártya önálló elektronika, melyeknek meghibásodási valószínűségét szintén figyelembe kell venni. Ez tulajdonképpen, mint minden plusz eszköz növeli λ_0 értékét. Az 1002D struktúra egyesíti az 1002 és a 2002 struktúrák előnyeit, mint azt a 3. táblázat mutatja.

A 2. és a 3. táblázatot összevetve látható, hogyha a redundáns ágakra külön-külön, és a diagnosztikai kártyára biztosítható a SIL2 közeli, de még csak SIL1-es érték (pl.: $\lambda = 0{,}02$), akkor az1002D struktúra kezelhető és a veszélyes hibatípusra egyaránt SIL3-as minősítésű rendszert eredményez. Ez a számítás nem tartalmazza a 4. ábrán mutatott hibaarány növekményből származó plusz veszélyt.

Az <1> összefüggés megoldásához a Markov gráf állapotaihoz tartozó λ_i értékeinek számszerű ismeretére van szükség. A λ_0, λ_1, stb. értékeinek meghatározásához a teljes vezérlő berendezést, az érzékelőktől a végrehajtókig, konkrét típusra bontva ismerni kell. A sorba kötött eszközök hibavalószínűsége az eszközök hiba valószínűségének uniója, a párhuzamosan kötött eszközök hibavalószínűsége az eszközök hiba valószínűségének metszete. Ezen egyszerű szabályok alapján, a szabványban [2] definiált módon, felépíthető a megbízhatósági blokk diagram, és így λ_0 meghatározható. Majd az egyes hibák kockázat elemzésével bontható a λ_0 a 2. ábrán szereplő részekre, és így tovább.

Irodalomjegyzék

1. Goble, William M. Cheddie, Harry L. Safety Instrumented System Verification. Practical Probabilistic Calculation, ISA, 2006
2. IEC 61508. Functional safety of Electrical/Electronic/Programmable electronic Safety-Related Systems, 1998
3. Neszveda, József. Redundáns struktúrák és a biztonság sérthetetlenség szint kapcsolata ZMNE, Hadmérnök, 2007 II. évf. 1. szám
4. IEC 61511-1, Functional safety – Safety integrated systems for the process industry sector – Part1: Framework, definitions, system, hardware and software requirements, 2002