HADMÉRNÖK

III. Évfolyam 4. szám - 2008. december

Neszveda József
Budapesti Műszaki Főiskola
neszveda.jozsef@kvk.bmf.hu

NUMERIKUS MODELL AZ IMET ESZKÖZÖK MEGBÍZHATÓSÁGI SZINTJÉNEK VIZSGÁLATÁRA

Absztrakt

Az időszakosan működtetett, energiamentesen tárolt technológia definiálása. Az IEC 61508 szabvány fogalmainak illesztése az periodikusan működtetett, energiamentesen tárolt (IMET) technológiákra. Az időszakosan változó hibaarány beillesztése a Markov modellbe. A MATLAB program folyamatábrája.

Definition of the periodically operated and durative stored without power technologies. Application of the terms of the IEC 61508 standard on the periodically operated and durative stored without power (PODS) technologies. Insert the seasonally varying failure rate in the Markov model. The flowchart of the MATLAB program.

Kulcsszavak: *változó hibaarány, periodikusan működtetett, Markov modell ~ varying failure rate, periodically operated, Markov model*

Bevezetés

Vannak olyan berendezések, melyeket időszakosan működtetnek és két működtetés között energiamentes állapotban vannak. Az energiamentes állapot jóval hosszabb, mint az aktív az üzemelés. Az elektronikus hadviselés számos ilyen technológiát használ. A tapasztalatok azt mutatják, hogy az elektronikus és mechanikus részegységeket tartalmazó berendezések meghibásodási valószínűsége energiamentesen tárolt állapotban is nő. A berendezéseknek üzemeléskor folytonos üzemmódban, rendkívül megbízhatóan kell működniük. A megbízhatóság növelése érdekében kézenfekvő az energiamentesen tárolt állapot megszakítása karbantartással és/vagy próbaüzemeléssel. A kérdés: Hogyan határozható meg egy konkrét eszköz esetén a karbantartás és/vagy próbaüzemelés optimális gyakorisága?

Az időszakosan működtetett, energiamentesen tárolt eszközök, technológiák három jellegzetesen eltérő üzemállapottal rendelkeznek. Ezek a:

- Az aktív üzemállapot. Az aktív üzemállapot sajátossága, hogy viszonylag rövid (3 – 10 nap), és folytonos üzemmódban működik a berendezés vagy technológia.

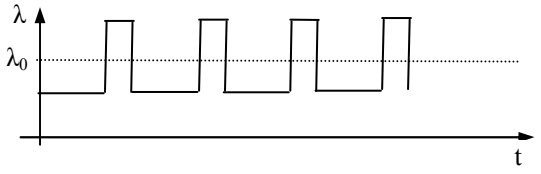
- Az időszakos teszt üzemállapot. Az időszakos teszt üzemállapot. sajátossága, hogy viszonylag rövid (kevesebb, mint 1 nap), és a folytonoshoz hasonló üzemmódban működik a berendezés vagy technológia.
- Az energiamentesen tárolt üzemállapot. Az energiamentesen tárolt állapotban az eszköz nem működik. Ezen sajátosság alapján az ilyen berendezések a vész, védelmi berendezésekhez, technológiákhoz hasonló [1]. Minthogy nem működik, biztosan nem detektálható hiba, de a tapasztalatok szerint az első működtetéskor éppúgy meghibásodhat, mint amikor az eszköz tápellátása biztosított, de fizikailag nem működtetett.

Az IEC 61508-1 szabvány [2], ami definiálja az alapfogalmakat és bevezeti a biztonság sérthetetlenség szint (SIL) mérőszámot, az eszközök megbízhatóságára ad a szakhatóságok számára ellenőrizhető választ. Az IEC 61511 szabvány [3] definiálja a folytonos alaptechnológiák és a vész, védelmi rendszereik biztonság sérthetetlenség szintjének fogalmait, és így a szakhatóságok számára ellenőrizhetővé teszi a technológiák megbízhatóságát.

Az IEC 61511 szabvány szigorún szétválasztja, és két különböző időléptékben tárgyalja a folytonos alaptechnológiák és a vész, védelmi rendszereik biztonság sérthetetlenség szintjének fogalmait. Az időszakosan működtetett, energiamentesen tárolt eszközök, technológiák üzemállapotai átlapolják ezen üzemmódokat. További probléma, hogy az alábbi józan megfontolások alapján nem lehet azonosnak tekinteni az energiamentesen tárolt üzemállapot, valamint az aktív és az időszakos teszt üzemállapotok meghibásodási valószínűségét.

- Az aktív és az időszakos teszt üzemállapotokban az emberi tényező növeli a (λ) hibaarányt.
- Az energiamentesen tárolt üzemállapotban a mechanikai és hőhatások hiánya csökkenti a (λ) hibaarányt, feltételezve, hogy a tárolás szakszerű, és egy évnél rövidebb az energiamentes állapot. Ezekre a jelenségekre nehéz számszerű becslést adni.

A jelenleg a folyamatosan működő, illetve a vész, védelmi berendezésekre, technológiákra vannak nemzetközileg elfogadott, szabványokban rögzített megbízhatósági számítási módszerek. Ezeknek az alapfeltevése a hibaarány (λ) állandó értékűnek tekintése.



1. ábra. A hibaarány váltakozása

A kiindulási feltételek

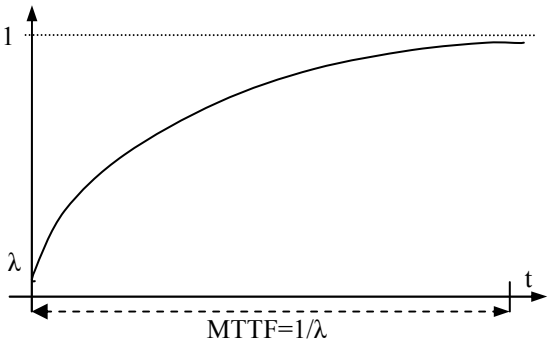
Az IEC szabványok [2] alapján:

- Üzembeállításkor egy berendezés vagy technológia meghibásodásának (F) kezdeti valószínűsége λ értékről indul.
- Ha adott időszakokra a hibamentes működés valószínűsége $P = (1-\lambda)$, akkor a kétszer olyan hosszú időszakra a hibamentes működés valószínűsége $P = (1-\lambda)(1-\lambda)$, és háromszor olyan hosszú időszakra a hibamentes működés valószínűsége $P = (1-\lambda)^3$.
- A λ hibaarány értéke a berendezést vagy technológiát alkotó eszközök elrendezéséből és megbízhatósági szintjéből számos eljárással [4] meghatározható.
- A meghibásodás valószínűség időbeli változása (F(t)) exponenciális (2. ábra)

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

A modell feltételezései:

- Az aktív és az időszakos teszt üzemállapotokban hibaarány (λ) értékéhez hozzáadódik az emberi tényező (λ_e) hibaaránya.
- Energiamentes üzemállapotban a hibaarány $\alpha \cdot \lambda$, ahol az $0 < \alpha \leq 1$
- Az energiamentesen tárolt üzemállapot időtartama hosszabb, mint az aktív vagy az időszakos teszt üzemállapotok időtartama. Két aktív üzemállapot között legalább egy időszakos teszt üzemállapot van.



2. ábra. Az F(t) meghibásodás valószínűség

- Az aktív és az időszakos teszt üzemállapotok periodikusan ismétlődnek. Az aktív és az időszakos teszt üzemállapotok időtartama azonos.
- A numerikus modellben diagnosztikával ellátott 1002D irányító berendezés struktúrát feltételezzünk.
- Ha egy adott időszakra a hibamentes működés valószínűsége $P = (1 - \lambda)$, és a következő ugyanolyan hosszú időszakra $P = (1 - \lambda - \lambda_e)$, akkor a hibamentes működés valószínűsége a két időszakra együttesen $P = (1 - \lambda)(1 - \lambda - \lambda_e)$.
- A vizsgálat alapegysége T_0 = 4 [nap]. A folyamatos (magas) működtetés igényű üzemmód 1 óra, és az alacsony működtetés igényű üzemmód 10000 óra (~1év) mértani átlaga a 4 nap (100 óra). A működtetés igényű üzemmód 1-2 időintervallummal lefedhető, és az időszakos teszt időigénye kisebb, mint egy 4 napos időintervallum.

Az Imet rendszer üzemmódjainak az IEC61511 szabványhoz illesztése

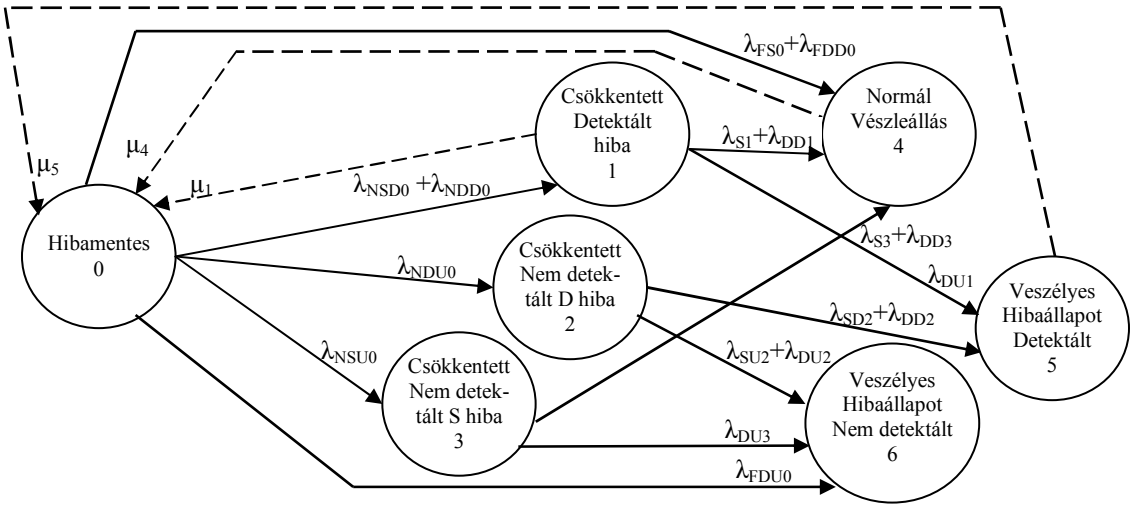
Az IEC61511-es szabvány a folytonos technológiákra lett kidolgozva. A folytonos technológiák a működtetés gyakorisága szerint magas működtetés igényű alapirányításra, és alacsony működtetés igényű vész, védelmi irányításra bonthatók. A λ hibagyakoriság, és a μ javíthatóság dimenziója ennek megfelelően [1/óra], illetve [1/év].

Az időszakosa működtetett, energiamentesen tárolt berendezések, technológiák az aktív és az időszakos teszt üzemmódokban magas működtetés igényű rendszerként, energiamentesen tárolt üzemmódban az alacsony működtetés igényű vész, védelmi irányításhoz hasonlóan viselkednek. Ha a λ hibaarány értékét folytonos üzemelést feltételezve állapítjuk meg, akkor a 4 napos időintervallum λ_0 hibaarány értéke $\lambda_0 = 100 \cdot \lambda$, mert 94 [óra.] kerekítve 100 [óra].

Az 1002D rendszer Markov modellje

Az 1002D struktúra hibamentes állapotból (0) kerülhet csökkentett biztonságú, de még működő állapotokba (1, 2, 3), vagy leállhat (4, 5, 6). 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 folytonos, illetve a vészvédelmi üzemmódokra kidolgozott javíthatóság fogalom itt nem alkalmazható., ezért a javasolt számítási módra a későbbiekben még kitérünk.



3. ábra. Általános 1002D Markov modell

Egy konkrét alkalmazásban az egyes hibák kockázatának elemzésével bontható a λ_0 a <2.> kifejezésben megadott részekre.

$$\lambda_0 = \lambda_{N0} + \lambda_{F0} = \lambda_{NSD0} + \lambda_{NSU0} + \lambda_{NDD0} + \lambda_{NDU0} + \lambda_{FS0} + \lambda_{FDD0} + \lambda_{FDU0} \qquad <2.>$$

Csökkentett biztonságú állapotok meghibásodásának együttes valószínűsége λ_{N0}. A leállásnak λ_{F0} a valószínűsége. A következmények miatt, hibaarányokat célszerű megosztani kezelhető, detektált (λ_{SD}), veszélyes, detektált (λ_{DD}), kezelhető, nem detektált (λ_{SU}), és veszélyes, nem detektált (λ_{DU}) hibaarányra.

A valószínűség mátrix, és számítása

Az 1002D rendszert 7x7-es a mátrix írja le. Az 2. ábra alapján definiálható a $\bar{\bar{P}}_C$ valószínűségi mátrix (<3.> kifejezés).

$$\bar{\bar{P}}_c = \begin{vmatrix} 1-\lambda_0 & \lambda_{NSD0}+\lambda_{NDD0} & \lambda_{NDU0} & \lambda_{Nsu0} & \lambda_{FS00}+\lambda_{FDD0} & 0 & \lambda_{FDU0} \\ \mu_1 & 1-\lambda_1 & 0 & 0 & \lambda_{S1}+\lambda_{DD1} & \lambda_{DU1} & 0 \\ 0 & 0 & 1-\lambda_2 & & & \lambda_{SD2}+\lambda_{DD2} & \lambda_{SU2}+\lambda_{DU2} \\ 0 & 0 & 0 & 1-\lambda_3 & \lambda_{S3}+\lambda_{DD3} & 0 & \lambda_{DU3} \\ \mu_4 & 0 & 0 & 0 & 1-\lambda_4 & 0 & 0 \\ \mu_5 & 0 & 0 & 0 & 0 & 1-\lambda_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix} \qquad <3.>$$

Az időszakosa működtetett, energiamentesen tárolt berendezésekre, technológiákra csak az időszakos teszt üzemmódban érvényes a 3. kifejezés, mivel az aktív, és az energiamentesen tárolt üzemmódban a javítások valószínűségi változói (μ_1, μ_4, μ_5) nullák, mert:

- Az energiamentesen tárolt üzemmódban a meghibásodásra nem derül fény, és így nem is javítható.
- Éles helyzetben, a folytonos üzemmódban a javításra csak korlátozottan van mód vagy idő, ezért legrosszabb esetet feltételezve a μ értékek nullák.

Éles helyzetben, szükség esetén, az $S_0(k)+ S_1(k)+ S_2(k)+ S_3(k)$ együttes valószínűsége a mérvadó, mert ekkor a feladat még végrehajtható.

Ez alapján az időszakosa működtetett, energiamentesen tárolt berendezések, technológiák valószínűség mátrixa energiamentesen tárolt és aktív üzemmódban a 4. kifejezés szerinti $\bar{\bar{P}}_0$.

$$\bar{\bar{P}}_0 = \begin{vmatrix} 1-\lambda_0 & \lambda_{NSD0}+\lambda_{NDD0} & \lambda_{NDU0} & \lambda_{Nsu0} & \lambda_{FS00}+\lambda_{FDD0} & 0 & \lambda_{FDU0} \\ 0 & 1-\lambda_1 & 0 & 0 & \lambda_{S1}+\lambda_{DD1} & \lambda_{DU1} & 0 \\ 0 & 0 & 1-\lambda_2 & & & \lambda_{SD2}+\lambda_{DD2} & \lambda_{SU2}+\lambda_{DU2} \\ 0 & 0 & 0 & 1-\lambda_3 & \lambda_{S3}+\lambda_{DD3} & 0 & \lambda_{DU3} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix} \quad <4.>$$

Az állapotvalószínűség vektor, és számítása

Az $\bar{S}(k) = (S_0(k) \quad S_1(k) \quad S_2(k) \quad S_3(k) \quad S_4(k) \quad S_5(k) \quad S_6(k))$ állapotvalószínűség vektor adja meg, hogy az 2. ábra 7 állapotából az eszköz vagy technológia a k-adik T_0 hosszú időintervallumban, a berendezés vagy technológia melyik állapotban, milyen valószínűséggel tartózkodik.

Az állapotvalószínűség vektor kezdeti értéke ($\bar{S}(0)$) megegyezik a $\bar{\bar{P}}_C$, illetve $\bar{\bar{P}}_0$ valószínűségi mátrix első sorával. Az $\bar{S}$ állapotvektor aktuális értéke a 4. kifejezés rekurzív formulájával [4] határozható meg.

$$\bar{S}(k+1) = \bar{S}(k)\,\bar{\bar{P}}_0 \quad <4.>$$

A μ javíthatóság valószínűség számítása az időszakos teszt üzemmódban

A μ_1, μ_4, μ_5 gráf élek csak az időszakos teszt idején aktívak. Az ilyenkor észlelt hibás üzemállapotok (1, 4, 5) kijavításának nincs erős időkorlátja, hiszen a vizsgálat szempontjából nem jelent erős kikötést, ha feltesszük, hogy az időszakos teszt, és az esetleges javítás egy időintervallum alatt (100 óra) befejeződik.

Az alábbi peremfeltételek fennállását természetesnek tekinthetjük:

- Annak valószínűsége, hogy az k-adik mintavételi időpontban végzett teszt alatt a rendszer az 1-es, vagy 4-es, vagy 5-ös állapotba kerül rendre $S_1(k)$, $S_4(k)$, $S_5(k)$.
- A javítás hatására a javított állapot legfeljebb a kezdeti $S_1(0)$, $S_4(0)$, $S_5(0)$ értékére áll vissza, és az $S_0(k)$ ennek megfelelően növekszik.
- A hibák, nem törvényszerűen, de a legrosszabb esetet feltételezve lehetnek függetlenek, ezért az egyik hibás állapot javítása nem csökkenti a másik hibaállapotba kerülés valószínűségét.

Értelemszerűen az k-adik időintervallumban végzett teszt alatt csak egy konkrét állapotba kerülhet az eszköz. Nem megjósolható, hogy melyik állapot következik be. A szerző javaslata, hogy az S_1, S_4, S_5 állapotok lehetséges változásainak számtani átlaga legyen a μ_0 átlagos javíthatóság valószínűségi érték.

$$\mu_0 = \delta\frac{1}{3}\{S_1(k) - S_1(0) + S_4(k) - S_4(0) + S_5(k) - S_5(0)\} \quad <5.>$$

- A $0 < \delta \le 1$ faktorral vehető figyelembe, hogy egyrészt az időszakos teszt terjedelme mennyire közelíti a valós működési körülményeket, másrészt a tényleges rendelkezésre állás időpontjáig milyen valószínűséggel fejezhető be a javítás.

A javítható $S_1(k)$, $S_4(k)$, $S_5(k)$ állapotoknak, az előfordulás valószínűségűkkel súlyozott korrekciója történjen, mert így hosszabb időtávon az előfordulásuk valószínűségének megfelelően vannak az állapotok figyelembe véve.

$$S_0(k+1) = S_0(k+1) + \mu_0 \qquad <6.>$$

$$S_1^*(k+1) = S_1(k+1) - \mu_0 \frac{S_1(k)}{S_1(k) + S_4(k) + S_5(k)} \qquad <7.>$$

$$S_4^*(k+1) = S_4(k+1) - \mu_0 \frac{S_4(k)}{S_1(k) + S_4(k) + S_5(k)} \qquad <8.>$$

$$S_5^*(k) = S_5(k+1) - \mu_0 \frac{S_5(k)}{S_1(k) + S_4(k) + S_5(k)} \qquad <9.>$$

A MATLAB modell paraméterei

Előkészítés:

A konkrét berendezés elemzéséből, folyamatosan aktív (folytonos) feltételezve, adódnak a 2. kifejezés hibaarány értékei. Javíthatóság nélküli esetet feltételezve a $\bar{\bar{P}}_0$ valószínűségi mátrix írható fel. Ebből a 10. kifejezés alapján számítható ki az időlépték váltást, illetve az α vagy β paramétereket tartalmazó $\bar{\bar{P}}_\alpha$ vagy $\bar{\bar{P}}_\beta$ valószínűségi mátrixok.

$$\bar{\bar{P}}_\alpha = \bar{\bar{I}} + 100 \cdot \alpha \cdot \left(\bar{\bar{P}}_0 - \bar{\bar{I}} \right), \qquad \bar{\bar{P}}_\beta = \bar{\bar{I}} + 100 \cdot \beta \cdot \left(\bar{\bar{P}}_0 - \bar{\bar{I}} \right) \qquad <10.>$$

- A $0 < \alpha \le 1$ faktorral vehető figyelembe, hogy az energiamentes üzemmódban menynyire csökken a hibaarány.
- A $1 < \beta = \frac{\lambda + \lambda_e}{\lambda} \le 2$ faktorral vehető figyelembe, hogy az emberi tényező mennyire növeli a hibaarányt.

A javíthatóság (μ) számításának elve

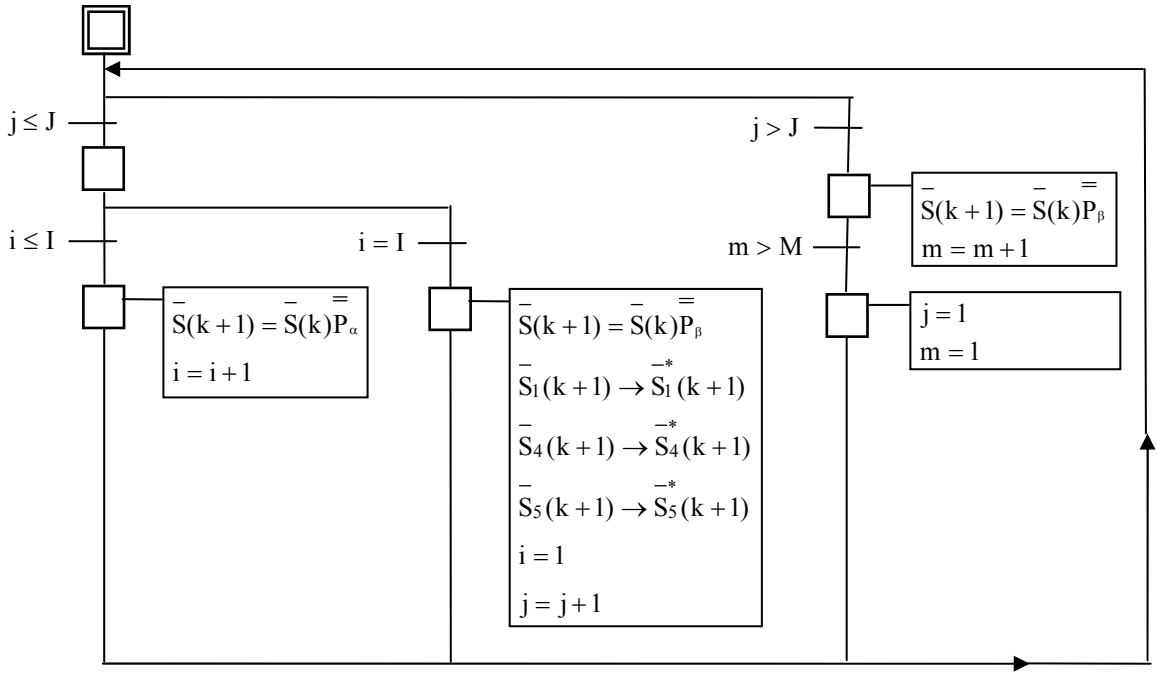
Az időszakos teszt üzemmódot bontsuk két részre, mert így biztosítható, hogy a μ_1, μ_4, μ_5 gráf éleknek megfelelő érték az éppen aktuális $\bar{S}(k)$ értékekből számítható legyen..

- Először határozzuk meg az $\bar{S}(k+1)$ állapot valószínűség vektort.

$$\bar{S}(k+1) = \bar{S}(k)\,\bar{\bar{P}}_0 \qquad <11.>$$

- Ezt követően az $\bar{S}(k+1)$ állapot valószínűség vektor $\bar{S}_1(k+1)$, $\bar{S}_4(k+1)$, $\bar{S}_5(k+1)$ elemeit korrigálni kell: (A fel nem sorolt állapotok értékei megmaradnak).

A MATLAB modell folyamat ábrája



4. ábra. A MATLAB program folyamatábrája

Paraméterek megválasztása:

Az „I” paraméter annak a mértéke, hogy hány energiamentes időintervallum után következik be az időszakos teszt.

A „J” paraméter annak a mértéke, hogy hány időszakos teszt időintervallum után következik be az aktív üzemmód.

Az „M” paraméter annak a mértéke, hogy hány időintervallumból áll az aktív üzemállapot.

Összefoglalás

A szerző a folyamatos (magas) működtetés igényű üzemmód 1 óra, és az alacsony működtetés igényű üzemmód 10000 óra (~1év) helyett bevezeti a 4 nap (100 óra) időintervallumot, mint az időszakosan működtetett, energiamentesen tárolt berendezések és technológiák hibaarány számításához jól illeszkedő mértékegységet, és definiálja a valószínűség mátrix konvertálásának egyenleteit.

A javíthatóság valószínűség változójának meghatározására a folyamatos, illetve vész, védelmi technológiák számára kidolgozott IEC 61511 szabványtól eltérő értelmezési, és ebből adódóan számítási eljárás javasol a szerző.

Irodalomjegyzék

1. Neszveda József, Redundáns irányítási struktúrák, és a biztonság sérthetetlenség szint kapcsolata, Hadmérnök II évf. 2. szám, 2007
2. IEC 61508. Functional safety of Electrical/Electronic/Programmable electronic Safety-Related Systems, 1998
3. IEC 61511-1, Functional safety – Safety integrated systems for the process industry sector – Part1: Framework, definitions, system, hardware and software requirements, 2002

4. Goble, William M., Cheddy, Harry. Safety Instrumented systems Verification, ISA 2006
5. IEC 61508-5. Examples of methods for the determination of safety integrity levels, 2001
6. Forgon Miklós, Neszveda József, 1002D strutúrájú, kritikus üzembiztonságú rendszer elemzése diszkrét-diszkrét Markov modellel, Hadmérnök II évf. 3. szám, 2007