**Neszveda József**[1]

# REDUNDÁNS IRÁNYÍTÁSI STRUKTÚRÁK ÉS A BIZTONSÁG SÉRTHETETLENSÉG SZINT (SIL[2]) KAPCSOLATA


## *Absztrakt*

*A biztonság sérthetetlenségi szint meghatározásához szükséges fogalmak rövid áttekintése. Az alapfolyamat irányítás és a vész-, védelmi rendszer egybe integrálásának előnyei és problémáinak tárgyalása. A légvédelmi rakéták rátöltési technológiájának besorolása. A hiba típusok osztályozása, és a redundancia hatása a kezelhető és a veszélyes hibára. A Markov modell és a közelítő egyenletek kapcsolata. A üzembiztosra tervezett integrált rendszer biztonság sérthetetlenség szint alapján történő redundáns struktúra választásának esettanulmánya.*

*The short overview the terms needed the determination of the safety integrity level. Discuss the advantages and the disadvantages of the integration of the basic process and the safety process. Classification of applying for blastoff technologies of air protection missile. Partition of type of the failure rate and how the redundancy work on the safe and the dangerous failures. Connection between the Markov model and the simplified equitation. Case study for choosing redundant structure of safety related system.*


***Kulcsszavak:*** *SIL, biztonság sérthetetlenség szint, közelítő egyenletek, redundáns struktúra.*

## *Bevezetés*

A vész-, védelmi rendszerek komplexitásának növekedése miatt vált szükségessé a biztonság sérthetetlenség szintjeinek a kialakítása és a szintek meghatározási módszereinek szabványba foglalása. A 80-as évek közepéig a vész-, védelmi rendszerek jellemzően egyszerű vezérlési láncokból álltak, és a vezérlési láncok egymástól és az alapfolyamat irányítását végző rendszertől fizikailag is elkülönülten működtek. A mikroprocesszor alapú eszközök látványos terjedése az automatizálásban új helyzetet teremtett. Az alapfolyamatok automatizált berendezései, amelyek jellemzően a kezelőszemélyzet által voltak összehangolva integrált irányítási rendszerré váltak. Az integrált rendszerek – megfelelően megtervezve – növelik az élőmunka, az anyag és energia hatékonyságot, valamint lehetővé teszik a folyamatos minőség ellenőrzés. A kedvező hatások éppen a teljes irányítási rendszer komplexitásának növekedéséből fakadnak. Mellékhatásként, már csak költséghatékony tervezési és telepítési megfontolásokból is, a vész-, védelmi rendszerekben is megjelentek a mikroprocesszor alapú eszközök, és ezáltal növekedett a komplexitásúk. A komplexitás növekedésnek pozitív vonzata, hogy megfelelő tervezéssel csökkenthető az irányított technológia teljes vagy részleges leállásának gyakorisága, azonban új hibaforrások (szoftver, nem várt kölcsönhatás, stb.) is keletkeznek.

[1] főiskolai docens, irányítástechnikai szakmérnök, BMF KVK Műszeripari és Automatizálási Intézet, Neszveda.jozsef@bmf.kvk.hu

[2] SIL: Safety Integrity Level

Az angol HSE[3], amely több magyar főhatóság (Országos Katasztrófavédelmi Főigazgatóság, Országos Munkaügyi és Munkabiztonsági Főfelügyelőség, Állami népegészségügyi és Tisztiorvosi Szolgálat) jogosítványával rendelkezik, 34 súlyos, különböző iparágakban bekövetkezett baleset okait elemezve tette közé [1] az 1. táblázatot.

1. táblázat: *Az ipari balesetek okai*

| | |
|---|---|
| Specifikáció (Mit és hogyan tegyen az irányítási rendszer) | 44% |
| Üzembe-helyezés utáni változtatás | 20% |
| Tervezés | 15% |
| Működtetés és karbantartás | 15% |
| Telepítés és üzembe-helyezés | 6% |

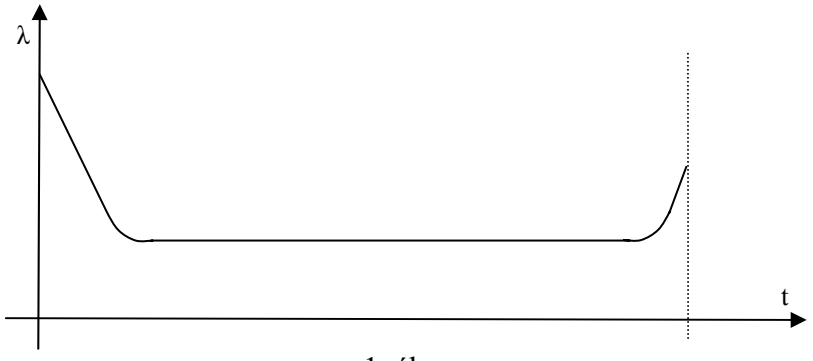
Az 1. táblázat jól szemlélteti, hogy a súlyos balesetek háromnegyede elkerülhető, ha a mérnökök rendelkezésére áll egy konzekvens a hibaforrásokat feltáró, kockázatot elemző és számszerűsítő eljárás. Elkerülendő az állami szabályozást, az angol mondás „Az előírás az ostobák, az ajánlás a bölcsek részére készül" tanácsát követve, a szabványosítással foglalkozó nemzetközi szervezet, az iparági és nemzeti szervezetekkel együttműködve a 90-es évek végétől folyamatosan teszi közé a mikroprocesszor alapú eszközök lehetőségeit figyelembe vevő a vész-, védelmi rendszerekre vonatkozó ajánlásait ajánlásait. A nemzetközi szabvány nem írja felül az iparági és a nemzeti szabványokat, de erős kölcsönhatás van közöttük. Minél kisebb egy ország, annál inkább csak a nemzetközi szabványokat honosítja.

## *A biztonság sérthetetlenség szint (SIL) meghatározásához szükséges fogalmak*

Az általános minden iparágra érvényes IEC 61508 szabványcsomag vezette be a megkülönböztetést az alacsony és a magas működtetés igényű[4] üzemmód között.

Alacsony működtetés igényű [2] 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"

Magas vagy folyamatos működtetés igényű [2] üzemmód: „Ahol a működtetési igény gyakorisága nagyobb, mint évente 1, illetve nagyobb, mint az ellenőrző tesztek közötti idő kétszerese években mérve per év"




1. ábra

*A hibaarány változása (átlagos hibavalószínűség) az életciklus alatt*

[3] HSE: Health and Safety Executive
[4] Low and High Demand Mode

Az üzembiztos működés szempontjából az a működtetési igény hibás végrehajtásának a valószínűsége a fontos. Ezt szokás hibaaránynak is nevezni, és általában a görög λ betűvel jelölik. Az 1. ábra mutatja a hibaarány változását az eszköz, a vezérlési lánc, vagy a vész-, védelmi rendszer életciklusa alatt.

Az 1. ábra baloldala a hibás alkatrészek és az első üzembe-helyezéskor előforduló túlterhelések, a jobb oldala az anyagfáradás miatt magasabb. Feltételezve a megfelelő próbaüzemet, illetve felújítást elegendő a közbenső értékkel számolni. A λ dimenziója hibavalószínűség per év, vagy per óra. A cikkben a továbbiakban csak az év dimenziót használjuk. A hétköznapi gondolkodásnak – különösen az alacsony működtetés igényű üzemmódú rendszerek esetén - jobban megfelel az 1/λ. Ennek MTBF[5] (hibák közötti átlagos idő) az elnevezése.

Az alacsony és a magas működtetés igényű üzemmódhoz rendelt átlagos hibavalószínűség eltérő dimenziójú és értékű. A [2] megadja az alsó határértékeket.

„Az alacsony működtetés igényű üzemmódban a megtervezett működés hibás végrehajtásának átlagos valószínűsége nem lehet kisebb, mint $10^{-5}$." Ez más szavakkal azt jelenti, hogy 100,000 működés közül legalább egy hibás. Figyelembe véve, hogy az alacsony működtetés igényű rendszerhez tartozik ez a limit, mondhatjuk azt is, hogy százezer évente legalább egy hiba előfordul.

„A magas vagy folyamatos működtetés igényű üzemmódban a veszélyes hiba átlagos valószínűsége nem lehet kisebb, mint $10^{-9}$/óra." Ami azt jelenti, hogy 1000,000,000 óra, vagyis nagyjából százezer év alatt legalább egy hiba előfordul. (Egy év 8760 óra.)

Minél komplexebb egy rendszer, annál jobban képes elkerülni a teljes leállást. Ennek megfelelően hibák feloszthatók kezelhető és veszélyes hibákra. A [2] definíciója: „A kezelhető hiba[6] nem teszi szükségessé a vész-, védelmi rendszer azonnali működtetését." A veszélyes hiba[7] szükségessé teszi a vész-, védelmi rendszer azonnali működtetését." Természetesen, hogy egy hiba kezelhető-e, vagy veszélyes az függ a hardver kialakítástól. A hibák egy másik csoportosítás szerint - mivel a hibák egy része felszínre kerül az ellenőrző tesztekkor, programozható eszközök esetén a diagnosztizáláskor, vagy karbantartáskor - lehetnek detektáltak és nem detektáltak. Az ellenőrző teszt és a diagnosztizálás működésközben is végezhető.

A biztonság sérthetetlenség (SIL) definíciója ugyancsak a [2] szerint: „Az E/E/PE[8] vész-, védelmi rendszerhez rendelt biztonsági műveletek sérthetetlenség igényének 4 diszkrét szintje van (egytől négyig). A 4 a legmagasabb, az 1 a legalacsonyabb biztonság sérthetetlenségi szint." A [2] két táblázatban adja meg az üzemmódokhoz tartozó SIL értékeket, amit a 2. táblázat egyben tartalmazz.

2. táblázat: *A biztonság sérthetetlenségi szintekhez tartozó hibavalószínűségek*

| SIL | Alacsony működés igényű üzemmód<br>Az átlagos hibavalószínűség tervezett működtetés végrehajtásakor. | Magas vagy folyamatos működés igényű üzemmód<br>Az óránként veszélyes hibák valószínűsége. |
|---|---|---|
| 4 | $10^{-5} \geq \lambda \geq 10^{-4}$ | $10^{-9} \geq \lambda \geq 10^{-8}$ |
| 3 | $10^{-4} \geq \lambda \geq 10^{-3}$ | $10^{-8} \geq \lambda \geq 10^{-7}$ |
| 2 | $10^{-3} \geq \lambda \geq 10^{-2}$ | $10^{-7} \geq \lambda \geq 10^{-6}$ |
| 1 | $10^{-2} \geq \lambda \geq 10^{-1}$ | $10^{-6} \geq \lambda \geq 10^{-5}$ |

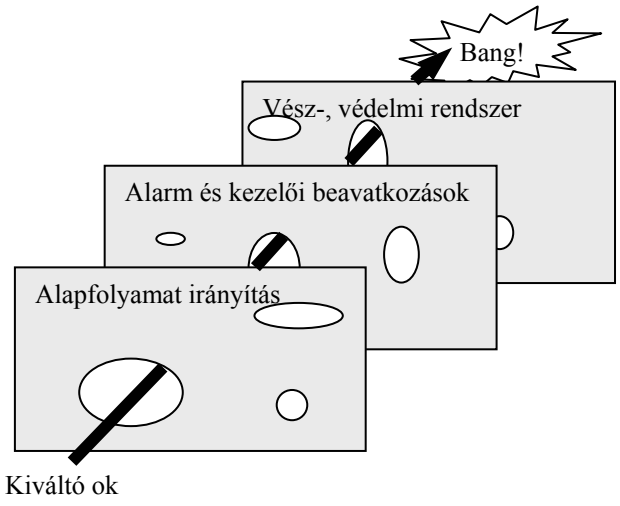
[5] Mean Time Between Failure
[6] Safe failure
[7] Dangerous failure
[8] Elektromos / Elektronikus / Programozható elektronikus

Vannak technológiák, amelyek évente csak egy-két napon át üzemelnek, ilyenkor azonban nagyon megbízhatóan kell működniük. A speciális katalizátor anyagot előállító vegyipari reaktort szokás példaképpen felhozni. Amikor egy ilyen rendszer működik, akkor az alapfolyamatainak az irányítása a folyamatos működtetés igényű üzemmódba tartoznak. Azonban egyrészt a 2. táblázat közvetve az 5. megjegyzésben feltételezi, hogy a magas vagy folyamatos működtetés igényű technológia berendezései szinte folyamatosan üzemkész állapotban vannak, és az ilyen technológiákban tipikusan nem ez a helyzet. Másrészt az 1. ábra mutatja, hogy üzembe-helyezéskor, és a hosszú üzemen kívüli állapot utáni újraindítás ennek felel meg, megnő a hibaarány. A 2. táblázat 5. megjegyzése [2]: „A magas vagy folyamatos működtetés igényű technológia hibavalószínűségét osztani kell az üzemkész állapot per év viszonyszámmal.” Ezekben a rendszerekben ez a viszonyszám jóval kisebb, mint 1, ami a λ értékét növeli és így a SIL besorolást csökkenti. Ezért számos szakértő azt javasolja, hogy az ilyen rendszerek alapfolyamatainak az irányítását is a költségesebb, de üzembiztos működést biztosító, a vész-, védelmi rendszerekre kidolgozott módszerekkel tervezzék meg.

*A szerző véleménye szerint ezen típusú technológiák közé tartozik számos katonai technológia, köztük a felkészített rakéták rátöltési folyamata is, és osztja azon szakértők álláspontját, akik az üzembiztos tervezési technikákat javasolják ezen esetekben.*

### *Integrálva vagy elkülönítve*

A 90-es évek közepéig a szabványok kategorikusan az alapfolyamat irányítás, és a vész-, védelmi rendszer fizikai szétválasztását írták elő. Manapság, amikor az alapfolyamat irányítása, és a vész-, védelmi rendszer kialakítása jórész programozható eszközökkel történik, és az eszközök egyre megbízhatóbbak, valamint képesek, akár többszörös redundáns működésre számos szakértő felveti a két rendszer integrálhatóságát. Az irányítási rendszerek független működésének hasznát a 2. ábra is jól szemlélteti.




2. ábra
*A baleset kialakulása*

Ha a baleset kialakulásának megelőzésére szolgáló felületek tömörek, és egymástól függetlenek, akkor nem alakulna ki baleset. Sajnos a felületen lyukak vannak, mert az alapfolyamat technológiai, és/vagy gépészeti és/vagy irányítástechnikai tervezésekor elkerülte a figyelmet néhány kölcsönhatás és/vagy határérték, vagy mert a kezelő téveszt és/vagy ignorálja az alarmjelzést, vagy mert a vész-, védelmi rendszer valamely eleme meghibásodott

és/vagy karbantartás állapotban van. A lyukak dinamikusan vándorolnak, mert mindig keletkezik új.

Az IEC 61508 előírása: „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." Ez engedékenyebb, mert többféleképp értelmezhető az elkülönülés. A szabvány más pontjai azonban előírják, hogy a vész-, védelmi rendszer érzékelői és a programozható irányító berendezése legyen fizikailag is független. De például információ szolgáltatás, ha az nem befolyásolja a vész-, védelmi rendszer működését, történhet az alapfolyamat irányítással közös hálózaton.

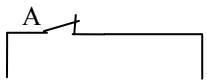
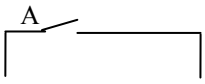
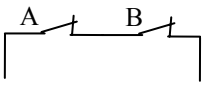
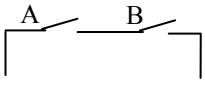
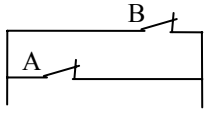
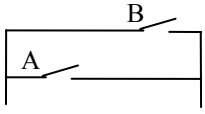
Az alapfolyamat irányítás aktív, ezért a rejtett hibák hamar kiderülnek. A kezelő személyzet hamar észleli, ha a berendezés nem megfelelően működik és gyorsan korrigál, elkerülve a nagyobb bajt. A vész-, védelmi rendszer passzív. Szerencsés esetben a kezelő személyzet sohasem látja működés közben, és így tapasztalatot sem szerez, nem veszi észre a baljós előjeleket. Csak az intenzív teszt és karbantartás biztosítja, hogy az eszközök, ha szükséges, akkor működni fognak. Sajnos ezek a műveletek is lehetnek hibaforrások. A másik lehetőség, hogy tervezéssel üzembiztos[10] rendszert alakítanak ki. Az olyan technológiákban – a repülőgép a szokásos példa - , ahol az alapfolyamat legkisebb hibája is végzetes lehet, az előzőektől eltérően egybe integrálva, és az alapfolyamatokra is az üzembiztos tervezési eljárásokat alkalmazva kel az irányító rendszert kialakítani.

*Az cikk szerzője az előkészített légvédelmi rakéták rátöltés technológiáját az ilyen speciális üzembiztos tervezésen alapuló automatikus rendszerrel javasolja megvalósítani.*

### *A redundancia és a hibavalószínűség kapcsolata.*

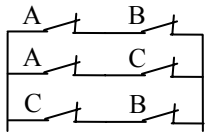
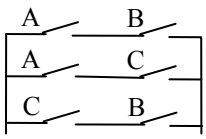
A [3] szerzőpárosa annak a tételnek a szemléltetésére, hogy „a kettő nem, mindig több, mint az egy, és a három nem mindig jobb, mint a kettő" azt javasolja, hogy reprezentálja a kezelhető hiba vezérlési láncát bontó és a hiba bekövetkezését az áramkör szakadása, a veszélyes hiba vezérlési láncát záró érintkező és hiba bekövetkezését az áramkör vezetése. Ha így vizsgáljuk a nem redundáns és a különböző redundáns rendszerekben hogyan változik a hibavalószínűség, hogy a különböző hibafajták eltérően viselkednek struktúraváltáskor.

**3. táblázat:** *A redundancia hatása a hiba gyakoriságra*

| | Kezelhető hiba | | Veszélyes hiba | |
|---|---|---|---|---|
| 1001 egy láncból egy jelez |  | $\lambda_E=\lambda_A$ =0,02 MTTF=1/ $\lambda_E$ = 50 év |  | $\lambda_E=\lambda_A$ =0,02 MTTF=1/ $\lambda_E$ = 50 év |
| 1002 kettő láncból egy jelez |  | $\lambda_E=\lambda_A+\lambda_B$ =0,04 MTTF=1/ $\lambda_E$ = 25 év |  | $\lambda_E=\lambda_A*\lambda_B$ =0,0004 MTTF=1/ $\lambda_E$ = 2500 év |
| 2002 kettő láncból kettő jelez |  | $\lambda_E=\lambda_A*\lambda_B$ =0,0004 MTTF=1/ $\lambda_E$ = 2500 év |  | $\lambda_E=\lambda_A+\lambda_B$ =0,04 MTTF=1/ $\lambda_E$ = 25 év |

[9] Equipment Under Control

[10] A szabvány által előírt eljárások végrehajtása összességében vezet ilyen rendszerhez.

| | | | | |
|---|---|---|---|---|
| 3002 három láncból kettő jelez |  | $\lambda_E = \lambda_A*\lambda_A+\lambda_A*\lambda_A+\lambda_A*\lambda_A$ =0,0012 MTTF=1/ $\lambda_E$ = 833 év |  | $\lambda_E = \lambda_A*\lambda_A+\lambda_A*\lambda_A+\lambda_A*\lambda_A$ =0,0012 MTTF=1/ $\lambda_E$ = 833 év |

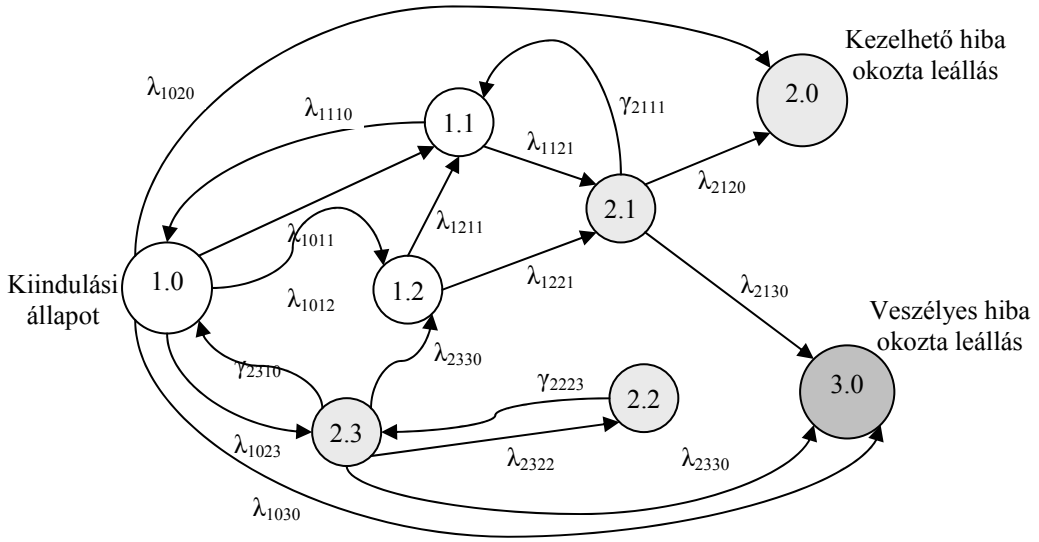
A cikk szerzője a 3. táblázatban, egy egyszerű számpélda segítségével, szemlélteti a fenti igazságot. A könnyű összehasonlíthatóság érdekében a kezelhető és a veszélyes hiba valószínűsége $\lambda = 0{,}02$ legyen. Az MTTF = $1/\lambda$= 50 év.

A 80-as évek negatív tapasztalatai hatására indított, főleg a Markov modellel végzett és a 90-es évek elején publikált kutatások eredménye, hogy a hibafajták eltérően viselkednek a különböző redundáns struktúrákban, és hogy a háromszoros redundancia nem minden szempontból jobb, mint a kétszeres. A 3. táblázat ezen kutatási eredményeknek csak egy szellemes prezentációja. A 1002 struktúra a legkedvezőbb a veszélyes hibák szempontjából, viszont kényelmetlen, hogy a különben kezelhető hibák rendkívül gyakran okozzák a technológia teljes vagy részleges kiesését. Ez huzalozott rendszerekben megkerülhetetlenül így volt. A programozható eszközök azonban képesek üzemközben diagnosztikára. Ha tudom, hogy a redundáns vezérlési lánc egyik ága azért jelez, mert valamelyik eleme hibás, akkor mint 1001 struktúra tovább működtethető. Ha elegendően gyorsan elhárítják a hibát, vagyis csekély a valószínűsége, hogy azért jelezzen, mert mindkét láncban van hibás elem, akkor a kezelhető hiba szempontjából a 2002 struktúrához közelít. Ezért hitelesítő intézetek kiadnak SIL tanúsítványt az úgynevezett 1002D (egy a kettőből diagnosztizálással) rendszerekre. Egyedi rendszerekre elvégezhető a SIL analízis az 1002D rendszerek esetén, azonban az elméleti kutatások ez idáig nem tudtak megalapozni olyan általánosítható szabályrendszer, aminek könnyen ellenőrizhető mechanikus végrehajtása megadná a kezelhető hiba valószínűségét. Ez egy támadási felület az ilyen rendszerekkel szemben.

*Az cikk szerzője az előkészített légvédelmi rakéták rátöltés technológiájának irányító rendszerének egyedi SIL elemzésen alapuló redundáns 1002D struktúrát javasolja.*

### *A Markov modell és az egyszerűsített egyenletek*

A Markov modell egy gráf, amellyel számszerűsítve elemezhető, hogy hogyan kerül egy rendszer hibás állapotba. A rendszer állapotai a gráf egy-egy csomópontja. A csomópontokat összekötő élek a hibagyakorisággal, vagy a karbantartás gyakoriságával vannak súlyozva. A gráf megkonstruálásához a rendszer állapotait, a hibagyakoriságot, a nem detektált hibák arányát ismerni kell. A gráf modell jól alkalmazható komplex több bemenetű, több kimenetű rendszerek esetén, és a gráf modell írja le a legjobban a redundáns rendszereket. A 3. ábra példaképp egy viszonylag egyszerű rendszer Markov modelljét ábrázolja.




3. ábra
*Minta Markov modell*

A gráf alapján felírhatók mátrix egyenletek. Összetett esetekben a mátrix egyenletek felírása és megoldása komoly szaktudást igényel.

Az összetett esetek egyszerű megoldására számos egyszerűsítést dolgoztak ki az elmúlt évtizedben. Az egyik legnépszerűbb a [4] által publikált egyszerűsített egyenleteknek nevezett formulák.

Az egyszerűsített egyenletek a kezelhető hibákra az $MTTF^{sp}$ (közelítő átlagos idő a hibáig) értéket adja meg. Ebben a képletben az $1/\lambda_{kezelhető}$ értékkel kell számolni.

A veszélyes hibákra a PFD[11] (hibavalószínűség működtetési igénykor) értéket adja meg, aminek két összetevője van $PFD = PFD_{avg} + PFD_{test}$. A nem detektált veszélyes hibák valószínűségét a $PFD_{avg}$ adja meg, aminek a képletében a $\lambda_{nem\_detektált\_veszélyes}$ értékkel kell számolni. Redundáns rendszerekben a javítás, vagy a kézi teszt alatt, a működő ágban a detektált hiba is veszélyes. Ezt az összetevő $PFD_{test}$, aminek a képletében a $\lambda_{veszélyes}$ értékkel kell számolni. A közelítő egyenletek a detektált, veszélyes hiba összetevő PFD érték kiszámítási képletét is megadják, ez azonban több nagyságrenddel kisebb értéket ad, mint a nem detektált összetevő, ezért elhanyagolható.

*A 4. táblázatban, a [4] egy vezérlési láncra érvényes alap formuláit és kiegészítő megjegyzéseit, a cikk szerzője, egybeszerkesztette és kiegészítette a kezelhető (s), és a veszélyes (d), valamint a nem detektált (u) hibaarány faktorokkal. Továbbá az eszközök számával (k).*

**4. táblázat:** *A kiegészített egyszerűsített egyenletek*

| | Kezelhető hiba | Nem detektált veszélyes hiba | Veszélyes hiba javítás/teszt közben |
|---|---|---|---|
| 1001 egy láncból egy jelez | $MTTF^{sp} = \frac{1}{\lambda \cdot s \cdot k}$ | $PFD_{avg} = \frac{\lambda \cdot d \cdot u \cdot k \cdot TI}{2}$ | $PFD_{test} = \frac{TD}{TI}$ |
| 1002 kettő láncból egy jelez | $MTTF^{sp} = \frac{1}{2 \cdot \lambda \cdot s \cdot k}$ | $PFD_{avg} = \frac{(\lambda duk)^2 \cdot TI^2}{3}$ | $PFD_{test} = \frac{2 \cdot TD \cdot \lambda \cdot d(TI + 2 \cdot MTTR)}{2 \cdot TI}$ |

[11] Probability of Failure on Demand

| | | | |
|---|---|---|---|
| 2002 kettő láncból kettő jelez | $MTTF^{sp} = \frac{1}{2 \cdot (\lambda sk)^2 \cdot MTTR}$ | $PFD_{avg} = \lambda \cdot d \cdot u \cdot k \cdot TI$ | $PFD_{test} = 2 \cdot \frac{TD}{TI}$ |
| 3002 három láncból kettő jelez | $MTTF^{sp} = \frac{1}{6 \cdot (\lambda sk)^2 \cdot MTTR}$ | $PFD_{avg} = (\lambda duk)^2 \cdot TI^2$ | $PFD_{test} = \frac{6 \cdot TD \cdot \lambda \cdot d(TI + 2 \cdot MTTR)}{2 \cdot TI}$ |
| | Igaz, ha: $\frac{1}{MTTR} >> \lambda$ | Igaz, ha: $MTBR >> TI$ | Igaz, ha üzemel a rendszer az egyik redundánság tesztje, vagy javítása közben. |

Az egyszerűsített egyenletekben szereplő további paraméterek:

Az MTTR[12] (a javítás átlagos ideje) egy évre vonatkoztatva. Ha az átlagos javítás 30 órányi időt igényel, akkor az MTTR = 30/8760 = 0,0034. A TI[13] (a manuális tesztek közötti idő) egy évre vonatkoztatva. Ha a tesztek között átlagosan hat hónap van, akkor TI = 6/12 = 0,5. A TD[14] (a teszt időtartama) egy évre vonatkoztatva. Ha a tesztek átlagosan 10 órát vesznek igénybe, akkor TD = 10/8760 = 0,0011.

A 4. táblázat eredményeinek értékelésekor, a hétköznapi gondolkodásmód számára jobban megfelel az RRF[15] (kockázat csökkentő tényező) használata, ami az 1/PDF és idő dimenziójú.

A 4. táblázat képleteinek használatakor a rendszer minden elemére (érzékelők, irányító berendezés, beavatkozók), és a rendszer kölcsönhatásaira el kell végezni a veszélyforrás és kockázat elemzést[16], és ez alapján lehet meghatározni a rendszer hibaállapotait, a hibaarány faktorokat. Ez természetesen iteratív művelet. Először a vész-, védelmi funkciók védelmi felületekhez (2. ábra) rendelését kell megtenni, amelyet a vezérlő berendezés struktúrájának megválasztása követ, amihez elegendő nagyságrendileg ismerni a vezérlő berendezés be és kimeneteinek számát, és nagyságrendileg megbecsülni a kezelhető, a veszélyes, és a nem detektált hibaarányokat.

## *Esettanulmány*

Az előkészített légvédelmi rakéták rátöltés technológiájának irányító rendszer struktúra választáshoz feltételezzük, hogy 24 bemenete és 6 kimenete van a vezérlő berendezésnek, és 5 bemenet jele közvetlen veszélyt jelez. Az irányítási algoritmus 25 vezérlési lánccal megvalósítható, amelyből 10 tartozik a veszélyes jelek kezeléséhez. A tápellátást, ami külön vizsgálatot igényel, az esttanulmány nem tárgyalja.

Huzalozott relés rendszer.

Feltételezzük, hogy a huzalozott rendszerben minden be-, és kimenet egy-egy ipari logikai relét igényel, és így k=30, a veszélyes jeleket kezelő bemenetek száma 5. Huzalozott rendszerben veszélyes a hiba, ha egy kimenet vagy egy közvetlen veszélyt jelző bemenet reléje nem húz meg, így mivel 6 kimenet és 5 közvetlen veszélyt jelző bemenet van így $k_d$=11. Az ipari relék átlagos meghibásodási ideje 100 év, azaz MTBF=100 és λ=0,01. A veszélyes hibaarány becsülhető. A 30 reléből 11 veszélyes hibához tartozik. A kezelhető hibák vezérlési láncai általában több kontaktust tartalmaznak. Vagyis 2*19+11=49 hibaforrást

[12] Mean Time To Repair
[13] Test Interval
[14] Test Duration
[15] Risk Reduction Factor
[16] Hazard and Risk analyses

feltételezve: d=11/49=0,22 és s=0,78. A rendszer nem redundáns, így 1001 struktúrájú, nincs működés közbeni diagnosztikája, vagyis u=1 (nem kell a képletben figyelembe venni) és $PFD_{test}$=0. Feltételezzük továbbá, hogy félévente ellenőrzik a rendszert manuális teszttel, és így TI=0,5.

A 4. táblázat alapján: (Az eredmény két értékes jegyre kerekítve.)

$$MTTF^{sp} = \frac{1}{\lambda \cdot s \cdot k} = \frac{1}{0{,}01 \cdot 0{,}78 \cdot 30} = 4{,}3[év]$$

$$PFD_{avg} = \frac{\lambda \cdot d \cdot k_d \cdot TI}{2} = \frac{0{,}01 \cdot 0{,}22 \cdot 11 \cdot 0{,}5}{2} = 0{,}00605$$

$$RRF = \frac{1}{PFD_{avg}} = \frac{1}{0{,}00605} = 166[év] \qquad (1)$$

Az (1) egyenlet azt mutatja, hogy a huzalozott rendszer veszélyes hibákra a 2. táblázat szerint SIL2. A kezelhető hibák bántóan gyakran okoznak felesleges, kellemetlen helyzetet, a 2. táblázat szerint SIL1.

Nem redundáns PLC.

Feltételezzük, hogy egy CPU, két bemeneti és egy kimeneti kártya szükséges, és így $k_{IO}$=3. A $k_{CPU}$=1, vagyis nem kell a képletben figyelembe venni. A CPU átlagos meghibásodási ideje 10 év, vagyis $MTBF_{CPU}$=10 és $\lambda_{CPU}$=0,1. Az I/O kártyák átlagos meghibásodási ideje 50 év, vagyis $MTBF_{IO}$=50 és $\lambda_{IO}$=0,02. Minthogy a logikát program valósítja meg a CPU veszélyes hibáinak aránya a veszélyes hibákat kezelő létraágak számából becsülhető (10/25), így $d_{CPU}$=0,4 és $s_{CPU}$=0,6. Az I/O veszélyes hibáinak aránya a veszélyes hibákat kezelő bemenetek, és az összes kimenet összegéből (11/30) becsülhető, vagyis $d_{IO}$=0,37 és $s_{IO}$=0,63. A rendszer nem redundáns, így 1001 struktúrájú, és így $PFD_{test}$=0. A PLC működés közbeni diagnosztikáját csak részben tudjuk kihasználni, vagyis $u_{CPU}$=0,1 (a diagnosztikai lefedettség[17] 90%) és $u_{IO}$=0,5. A rendszert évente ellenőrzik manuális teszttel, és így TI=1.

$$MTTF^{sp} = \frac{1}{\lambda_{CPU} \cdot s_{CPU} + \lambda_{IO} \cdot s_{IO} \cdot k_{IO}} = \frac{1}{0{,}1 \cdot 0{,}6 + 0{,}02 \cdot 0{,}63 \cdot 3} = 10[év]$$

$$PFD_{avg} = \frac{(\lambda_{CPU} \cdot d_{CPU} \cdot u_{CPU} + \lambda_{IO} \cdot d_{IO} \cdot u_{IO} \cdot k_{IO}) \cdot TI}{2} =$$

$$= \frac{0{,}1 \cdot 0{,}4 \cdot 0{,}1 + 0{,}02 \cdot 0{,}37 \cdot 0{,}5 \cdot 3}{2} = 0{,}0151$$

$$RRF = \frac{1}{PFD_{avg}} = \frac{1}{0{,}0151} = 66[év] \qquad (2)$$

Nem meglepő, hogy a kezelhető hibák okozta kellemetlenségek előfordulása csökken, azonban a veszélyes hibák előfordulása nő.

Redundáns PLC.

Minthogy a 2003 struktúra nagyon drága, próbálkozunk az 1002D struktúrával. A párhuzamos ágakban egy-egy CPU, két-két bemeneti és egy-egy kimeneti kártya szükséges. A 3. és a 4. táblázat képleteit összevetve, vegyük észre, hogy a negyedik táblázatban a λ, s, d, u, k tényezőket egy csatornára kell megadni, és így $k_{IO}$=3 és $k_{CPU}$=1. A CPU átlagos meghibásodási ideje 10 év, vagyis $MTBF_{CPU}$=10 és $\lambda_{CPU}$=0,1. Az I/O kártyák átlagos meghibásodási ideje 50 év, vagyis $MTBF_{IO}$=50 és $\lambda_{IO}$=0,02. Minthogy a logikát program valósítja meg a CPU veszélyes hibáinak aránya a veszélyes hibákat kezelő létraágak számából becsülhető (10/25), így $d_{CPU}$=0,4 és $s_{CPU}$=0,6. Az I/O veszélyes hibáinak aránya a veszélyes hibákat kezelő bemenetek, és az összes kimenet összegéből (11/30) becsülhető, vagyis $d_{IO}$=0,37 és $s_{IO}$=0,63. A rendszer redundáns, vagyis $PFD_{test}$ értékével is számolni kell.

[17] Diagnostic coverage

Tételezzük fel, hogy a hiba elhárításához 2 óra szükséges, az esetünkben azonban a tényleges működés 5 nap, így (2/120) TD=0,017. Manuális teszt évente van így TI=1. A PLC diagnosztikai lefedettsége 99,5%, az I/O kártyáké 90%, vagyis $u_{CPU}$=0,005 és $u_{IO}$=0,1.

A 4. táblázat kezelhető hiba képlete nem tartalmazza a diagnosztikai lefedettséget, pedig nyilvánvaló: ha a csatorna azért jelez, mert valamelyik eleme hibás, attól még a rendszer működhet, mint 1001 struktúrájú. Ez nyilván alsó határ, hisz a rendszer nagyobb részt nem 1001 struktúrájú. Azt, hogy egyszerre detektálunk hibát mindkét ágban, annak a valószínűsége $\lambda^2$, ennek használata azonban nem veszi figyelembe, hogy 1001 struktúrájúként is működik, és a diagnosztikai lefedettséget nem 1.

*A cikk keretében nem indokolva, a szerző az alábbi hibagyakoriság érték használatát javasolja a becsléshez:*

$$\lambda_k = \frac{\lambda^2}{1-TD} + \lambda \cdot TD \tag{3}$$

A (3) képlettel $\lambda_{kCPU}$=0,01187 és $\lambda_{kIO}$=0,00211

$$MTTF^{sp} = \frac{1}{2 \cdot (\lambda_{kCPU} \cdot s_{CPU} + \lambda_{kIO} \cdot s_{IO} \cdot k_{IO})} = \frac{1}{2 \cdot (0{,}01187 \cdot 0{,}6 + 0{,}00211 \cdot 0{,}63 \cdot 3)} = 90[\acute{e}v] \tag{4}$$

$$PFD_{avg} = \frac{(\lambda_{CPU} d_{CPU} u_{CPU} k + \lambda_{IO} d_{IO} u_{IO} k_{IO})^2 \cdot TI^2}{3} = \\ = \frac{(0{,}1 \cdot 0{,}4 \cdot 0{,}005 + 0{,}02 \cdot 0{,}37 \cdot 0{,}1 \cdot 3)^2 \cdot 1^2}{3} = 2 \cdot 10^{-6} \tag{5}$$

A karbantartó javítás legyen 2 nap, ebből MTTR = 2/365 = 0,00548 következne. Estünkben a karbantartó javítást célszerű üzemen kívüli időpontban elvégezni, ezért MTTR=0.

$$PFD_{test} = \frac{2 \cdot TD \cdot \lambda \cdot d(TI + 2 \cdot MTTR)}{2 \cdot TI} = TD \cdot \lambda \cdot d = TD \cdot (\lambda_{CPU} \cdot d_{CPU} + \lambda_{IO} \cdot d_{IO}) = \\ = 0{,}017(0{,}1 \cdot 0{,}4 + 0{,}02 \cdot 0{,}37) = 0{,}00081 \tag{6}$$

Az eredő PFD = $PFD_{avg}$+$PFD_{test}$ = 0,000002+0,00081=0,000812.
A RRF = 1/PFD = 1200 év.
Az eredmény kielégítő, a kezelhető hibára jó SIL2, a veszélyes hibára SIL3 értéket ad.

## *Irodalomjegyzék*


1. U.K. Health and Safety Executive. Out of Control: Why control systems go wrong and how prevent failure., 1995
2. IEC 61508. Functional safety of Electrical/Electronic/Programmable electronic Safety-Related Systems, 1998
3. Grun, Paul. Cheddie, Harry L. Safety Instrumented Systems: Design, Analysis and Justifications ISA, 2006
4. Smith, David J. Reliability, Maintainability, and Risk: Practical Methods for Engineers. 6th edition. Butterworth-Heinemann, 2001