BUDAPESTI MÛSZAKI EGYETEM
KÖZLEKEDÉSMÉRNÖKI KAR
KÖZLEKEDÉSAUTOMATIKAI TANSZÉK

Szabó Géza
egyetemi tanársegéd

Bevezetés a hibafaanalízisbe

Segédlet a "Nagybiztonságú számítógépes és hibrid rendszerek" c. tárgyhoz

BME Közlekedésautomatikai Tanszék

Budapest, 1996. november

TARTALOMJEGYZÉK

1. Bevezetés

Biztonsági rendszerek tervezésénél és minõsítésénél gyakran felmerülõ kérdés, hogy az adott rendszer valójában milyen biztonsági szintet képvisel. Fontos ez a tervezés alatt, elsõsorban azért, hogy a fejlesztõ megítélhesse, az általa tervezett rendszer megfelel-e az elvárásoknak, illetve melyek a gyenge pontjai, amelyeken javítani kell, vagy csekély ráfordítással javítani lehet, de fontos lehet azért is, nehogy többletköltség árán el nem várt, tehát indokolatlanul magas megbízhatóságú rendszert hozzon létre.

A biztonsági rendszereket az esetek nagy részében igen komoly ellenõrzési (validációs) eljárásoknak vetik alá, melynek során bizonyítani kell a rendszer megbízhatóságát, lehetõleg számszerû paraméterekkel.

A megbízhatóság jellemezhetõ valószínûségi paraméterekkel, melyek elõnye a számszerûség és az összehasonlíthatóság.

A valószínûségi adatokkal való számolás egyik segédeszköze a hibafa-analízis, amely alkalmazható egyedi alrendszerekre vagy egyes komponensekre, de az egész rendszerre is.

2. Rendszerek megbízhatósági paraméterei

Egy tetszõleges rendszer megbízhatósági jellemzésére több paraméter szolgálhat.

Rendelkezésre állás (nem javítható rendszereknél: **túlélési valószínûség**), **R(t)**: a rendszert egy adott idõpontban megfigyelve mekkora valószínûséggel lesz az mûködõképes.

Rendelkezésre nem állás (nem javítható rendszereknél: **meghibásodási valószínû-ség**), **Q(t)**: a rendszert egy adott idõpontban megfigyelve mekkora valószínûséggel nem lesz mûködõképes.

$$Q(t) = 1 - R(t)$$

Meghibásodássûrûség, f(t):

$$f(t) = \frac{dQ(t)}{dt}$$

Meghibásodási gyakoriság, λ(t): A rendszer egy adott idõtartam alatt hányszor hibásodik meg.

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\frac{dQ(t)}{dt}}{1 - Q(t)}$$

Ezen jellemzõk értékei lehetnek idõben konstansok és lehetnek idõfüggõek, ilyenkor a konkrét idõfüggvényen kívül az átlagérték és a maximális érték szolgálhat jellemzésül.

3. A hibafák felépítése

3.1 A hibafaanalízis módszertana

Bármilyen megbízhatósági számítás megkezdése elõtt definiálni kell azt az eseményt, amelynek szempontjából számoljuk a rendelkezésre állást (vagy rendelkezésre nem állást) és a meghibásodási gyakoriságot. Ez azért fontos, mert egy rendszer többféle funkciót valósíthat meg, és a különbözõ funkciók szempontjából más-más paraméterekkel rendelkezhet.

A hibafa-analízisnél a definiált esemény valamilyen hibás mûködés, vagy mûködés elmaradás. Ezt a definiált eseményt nevezik **csúcseseménynek**. Analízisünknél keressük azokat az un. **elemi eseményeket**, melyek bekövetkezésekor (esetleg más elemi események bekövetkezésétõl függõen) a csúcsesemény bekövetkezik. Elemi eseményen olyan eseményeket értünk, melyek bekövetkezési valószínûségérõl valamilyen információval rendelkezünk. Fontos az elemi események kapcsolatának helyes felírása, mert ez alapjaiban befolyásolja a számítások eredményét.

A hibafa könnyebb felépítése érdekében definiálhatunk **közbensõ eseményeket** is. A közbensõ esemény olyan esemény, amely bekövetkezési valószínûsége nem áll rendelkezésre, azt elemi eseményekbõl számoljuk ki, de ezen közbensõ esemény a csúcsesemény szempontjából az elemi eseményekkel azonos módon kezelendõ. Közbensõ események definiálásával hierarchikus hibafa-rendszert alakíthatunk ki.

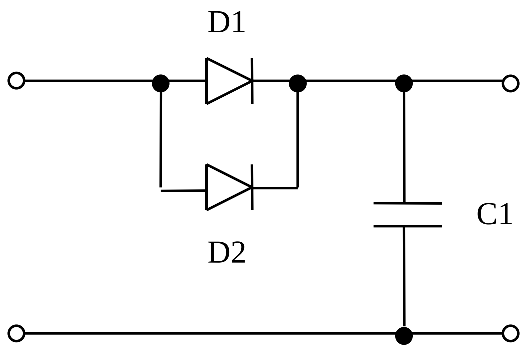
A hibafa felépítésekor az események okait az adott rendszer folyamatábráján visszafelé, az eseménytõl az ok irányába haladva nyomozzuk ki (deduktív analízis). Minden egyes lépésben veszünk egy okozatot, és keresünk hozzá egy vagy több eseményt (kiváltó okot), amely lehet elemi esemény, vagy közbensõ esemény, amelyet a késõbbiekben tovább bontunk. (Megjegyzendõ, hogy már a hibafa felépítése is igen hasznos segítséget nyújthat: rákényszeríti és rávezeti az analízist végzõt, hogy vegye számba az összes eseményt, amelyek a csúcseseményhez vezethetnek.)

Az események (elemi és közbensõ események) lehetséges logikai kapcsolatai:
1. ÉS; az események együttes bekövetkezése szükséges a következõ szint eseményének (esetleg a csúcseseménynek) a bekövetkezéséhez.
2. VAGY; az események közül bármelyik bekövetkezése elégséges a következõ szint eseményének (esetleg a csúcseseménynek) a bekövetkezéséhez.
3. NEM; az esemény be nem következése szükséges a következõ szint eseményének (esetleg a csúcseseménynek) a bekövetkezéséhez.
4. K/N; Az N esemény közül legalább K számú bekövetkezése szükséges a következõ szint eseményének (esetleg a csúcseseménynek) a bekövetkezéséhez. (Ez a logikai kapcsolat felépíthetõ ÉS és VAGY kapuk segítségével is, de a K/N logika alkalmazása a kapcsolatrendszert átláthatóbbá teszi.)

Természetesen további logikai kapcsolatok definiálhatóak az elõbb felsorolt 4 eset segítségével (pl. NAND).

Nem tartozik közvetlenül az események kapcsolatát leíró kapukhoz a **transzfer kapu** vagy **transzfer esemény**. A transzfer esemény a hibafa felosztását, lapokra tördelését segíti elõ. Egyes közbensõ eseményeket (amennyiben azokat transzfer eseményként deklaráljuk), kifejthetünk akár külön részhibafában is, elõsegítve egyrészt a hibafa érthetõségét, másrészt lehetõvé téve azt, hogy egyes közbensõ eseményeket több helyre is beillesszünk a hibafába.

Lássunk egy egyszerû példát a hibafa felépítésére. Példánkban egy soros diódás egyenirányító hibamodelljét alkotjuk meg. A kapcsolási rajzot az 1. ábra, míg a felépített hibafát a 2. ábra mutatja.



1. ábra: Diódás egyenirányító kapcsolási rajza

Elsõ lépésként definiálnunk kell a csúcseseményt, melynek bekövetkezési valószínûségét szeretnénk számítani. Ez a mi esetünkben a következõ esemény: “Az egyenirányító kimenetén nem jelenik meg az egyenirányított feszültség (vagy 0 V, vagy simítatlan egyenirányított feszültség jelenik meg) ”.

A modellünkben az alábbi meghibásodási típusokat vettük figyelembe (a figyelembe veendõ hibatípusok függhetnek a definiált csúcseseménytõl) :

- *Dx dióda szakadttá válik*
- *Dx dióda zárlatossá válik*
- *Cx kondenzátor üzemképtelen lesz (szakadt vagy zárlatos)*

A meghibásodási típusok ismeretében definiálhatjuk azokat az elemi eseményeket, amelyeket a csúcsesemény szempontjából figyelembe kell venni :

Az esemény sorszáma	*Megnevezés*	*Bekövetkezési valószínûség (fiktív érték)*
1.	*D1 dióda szakadttá válik*	$1.0*10^{-3}$
2.	*D1 dióda zárlatos lesz*	$1.5*10^{-6}$
3.	*D2 dióda szakadttá válik*	$1.0*10^{-3}$
4.	*D2 dióda zárlatos lesz*	$1.5*10^{-6}$
5.	*C1 kondenzátor üzemképtelen lesz*	$3.2*10^{-6}$

1. táblázat: Diódás egyenirányító meghibásodási elemi eseményei

A következõ lépésben felfedjük az egyes elemi eseményeknek a csúcsesemény bekövetkezésében játszott szerepét. A hibafa könnyebb felépítése és a könnyebb érthetõség miatt közbensõ eseményeket is definiálunk.
A definiált közbensõ események (ezek -eltérõen az elemi eseményektõl- tetszõlegesek lehetnek, illetve alkalmazásuktól el is lehet tekinteni) a következõk:

- *"A diódákon keresztül nem folyik áram", illetve*
- *"A diódák rövidzárként viselkednek"*

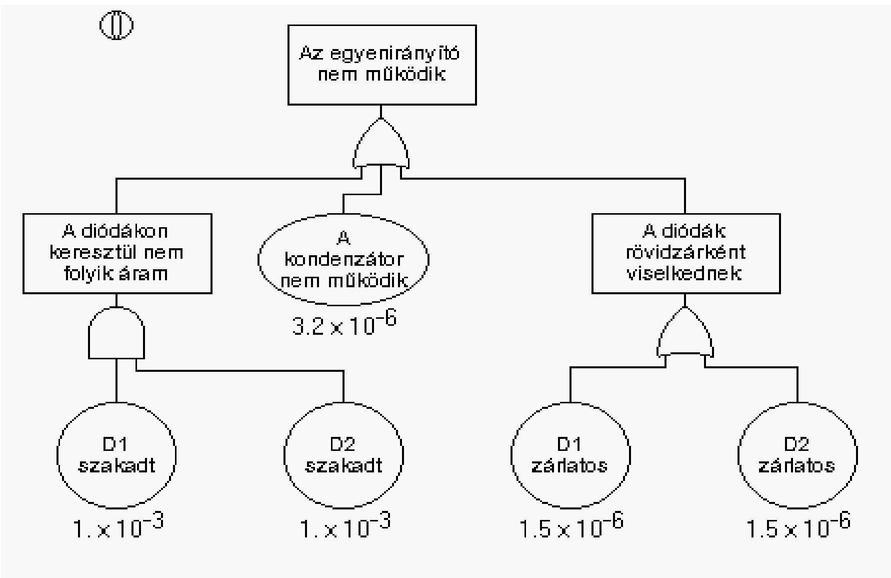
A csúcsesemény ("Az egyenirányító kimenetén nem jelenik meg az egyenirányított feszültség") az alábbi három esemény valamelyikének bekövetkezésekor következik be: "A diódák rövidzárként viselkednek", "A diódákon keresztül nem folyik áram", illetve "C1 kondenzátor üzemképtelen lesz". A csúcsesemény a három esemény VAGY kapcsolata.

Látható, hogy ezek közül csak egy az elemi esemény, míg a további kettõ közbensõ esemény, melyeket tovább tudunk bontani az alábbiak szerint:
"A diódák rövidzárként viselkednek" esemény akkor következik be, ha a két dióda közül legalább az egyik zárlatos, így ez az 1. táblázat 2-es és 4-es elemi eseményeinek VAGY kapcsolata.
"A diódákon keresztül nem folyik áram" esemény akkor következik be, ha mindkét dióda szakadttá válik, így ez az 1. táblázat 1-es és 3-as elemi eseményeinek ÉS kapcsolata.

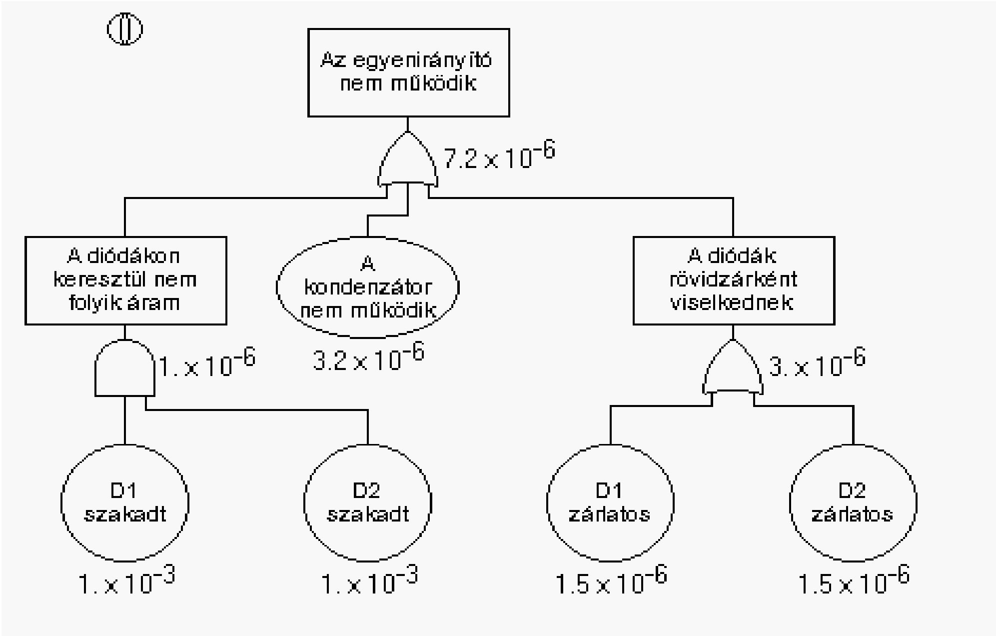
Ezek után lássuk a felépített hibafát:

A 2. ábra a hibafa struktúráját mutatja, az elemi események bekövetkezési valószínûségével.

A 3. ábra a hibafaanalízis befejezése után mutatja a hibafát. Ekkor már nem csak az elemi események valószínûsége olvasható le az ábráról, hanem a csúcsesemény és a közbensõ események bekövetkezési valószínûségei is. Az elemi események valószínûsége (vagy valószínûségi modellje) a számításhoz megkövetelt paraméter, míg az egyéb valószínûségek számítással határozhatóak meg. A számítás alapösszefüggéseit a 4. fejezet (Alapszámítások a hibafákon, 7. oldal) mutatja be.



2. ábra: Diódás egyenirányító hibafa-struktúrája



3. ábra: Diódás egyenirányító hibafája a kiszámolt értékekkel

3.2 Néhány javaslat a hibafa felépítéséhez

1. A fa legyen olyan egyszerû, amennyire a rendszer bonyolultsága ezt egyáltalán lehetõvé teszi.
2. Maradjon a fa mindig logikus.
3. Világos, tömör és egyszerû eseményleírásokat válasszunk.
4. A nagy terjedelmû hibafákat bontsuk részhibafákra transzferek (átviteli események) segítségével.

4. Alapszámítások a hibafákon

Az alapszámítások feladata, hogy az események alapvetõ logikai kapcsolatainak megfelelõen megadják az események kapcsolatához tartozó, számolt valószínûségeket. Az alapkapcsolatok, mint ahogy az a 3. fejezetben bemutatásra került, az alábbiak:

1. ÉS kapcsolat
2. VAGY kapcsolat
3. NEM kapcsolat
4. K/N kapcsolat

Az alábbi példákban rendre Q_n jelöli a bemeneti események hibavalószínûségeit, R_n a bemeneti események túlélési valószínûségeit, míg a kimeneti esemény hibavalószínûsége Q_{ki} , túlélési valószínûsége R_{ki} lesz.

4.1 Kétbemenetû ÉS kapu kimeneti valószínûsége

Az ÉS kapcsolat miatt a kimeneti esemény a bemeneti események együttes bekövetkezésekor következik be, így:

$$Q_{ki} = Q_1 \cdot Q_2$$

4.2 Általános, "n" bemenetû ÉS kapu

$$Q_{ki} = \prod_{i=1}^{n} Q_i$$

4.3 Kétbemenetû VAGY kapu kimeneti valószínûsége

A VAGY kapcsolat miatt a kimeneti esemény a bemeneti események bármelyikének bekövetkezésekor bekövetkezik, így:

$$Q_{ki} = Q_1 + Q_2 - Q_1 \cdot Q_2$$

A fenti összefüggéshez úgy jutunk, hogy a rendszer túlélési valószínûségeit vizsgáljuk. A rendszer helyesem mûködik, ha mindkét bemenet helyesen mûködik, vagyis:

$$R_{ki} = R_1 \cdot R_2 = (1 - Q_1) \cdot (1 - Q_2)$$

és így

$$Q_{ki} = 1 - R_{ki} = 1 - [(1 - Q_1) \cdot (1 - Q_2)] = 1 - (1 - Q_1 - Q_2 + Q_1 \cdot Q_2) = Q_1 + Q_2 - Q_1 \cdot Q_2$$

Ha a két bemeneti esemény együttes bekövetkezési valószínûsége 0 (egymást kizáró események), akkor az alábbi összefüggést kapjuk:

$$Q_{ki} = Q_1 + Q_2$$

4.4 Általános, "n" bemenetû VAGY kapu

$$Q_{ki} = 1 - \prod_{i=1}^{n} (1 - Q_i)$$

Ha az n eseménybõl mindig csak egy következhet be (egymást kizáró események), akkor az alábbi összefüggést kapjuk:

$$Q_{ki} = \sum_{i=1}^{n} Q_i$$

4.5 Egybemenetû NEM kapu kimeneti valószínûsége

A kimeneti esemény akkor következik be, ha a bemeneti esemény nem, így:

$$Q_{ki} = 1 - Q_1$$

4.6 3-ból 2 (2/3) kapu kimeneti valószínûsége

A kapu felbontható 3 ÉS kapura, melyek kimenetei egy VAGY kapuba csatlakoznak, így:

$$R_{ki} = \left(1 - Q_1 \cdot Q_2\right) \cdot \left(1 - Q_1 \cdot Q_3\right) \cdot \left(1 - Q_2 \cdot Q_3\right)$$

és

$$Q_{ki} = 1 - R_{ki} = 1 - \left[\left(1 - Q_1 \cdot Q_2\right) \cdot \left(1 - Q_1 \cdot Q_3\right) \cdot \left(1 - Q_2 \cdot Q_3\right) \right]$$

4.7 Általános, "n"-bõl "m" (m/n) kapu

$$Q_{ki} = 1 - \prod_{\substack{i_1 \\ i_2 \\ \vdots \\ i_m}} \left(1 - Q_{i_1} Q_{i_2} \cdot \ldots \cdot Q_{i_m}\right)$$

$$i_1 = 1 \ldots (n - m + 1),\ i_2 = i_1 + 1 \ldots (n - m + 2),\ \cdots\ i_m = i_{m-1} + 1 \ldots (n - m + m)$$

Lássunk egy példát a fenti képlet használatára. Írjuk fel a 4-bõl 3 logika kimeneti valószínûségét. Itt m=3, n=4. Így a $Q_{i_1} \cdot Q_{i_2} \cdot \ldots \cdot Q_{i_m}$ tag rendre 3 darab Q valószínûséget fog tartalmazni. Az i_1 index 1-tõl (n-m+1)-ig, azaz 2-ig fut. Ha i_1 =1, i_2 2 és 3 lehet, ha i_1 =2, i_2 csak 3 lehet. A fenti gondolatmenetet követve számítható i_3 értéke is.
Így:

$$Q_{ki} = 1 - R_{ki} =$$
$$= 1 - \left[\left(1 - Q_1 \cdot Q_2 \cdot Q_3\right) \cdot \left(1 - Q_1 \cdot Q_2 \cdot Q_4\right) \cdot \left(1 - Q_1 \cdot Q_3 \cdot Q_4\right) \cdot \left(1 - Q_2 \cdot Q_3 \cdot Q_4\right) \right]$$

5. Meghibásodási valószínûségi modellek

A meghibásodási valószínûségi modellek feladata, hogy az alkatrész rendelkezésre nem állásának idõbeli változását definiálják. Egyszerûbb számításoknál a bonyolultabb modellek helyett az idõbeli átlagértéket is szokás használni.

5.1 Konstans rendelkezésre nem állású komponens

A legegyszerûbb modell esetén az alkatrész rendelkezésre állását konstansnak feltételezzük:

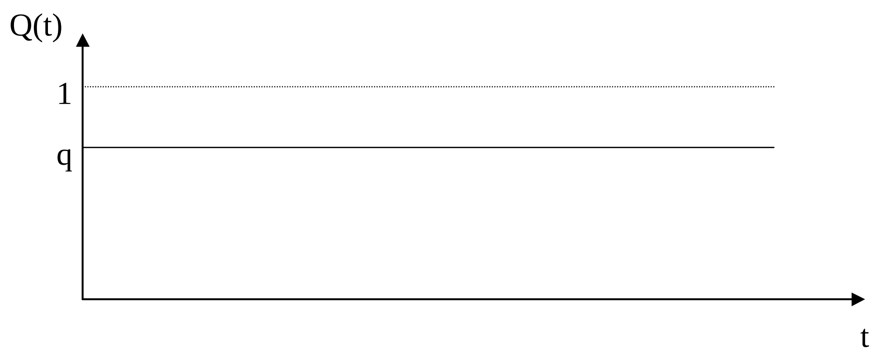
$$Q(t) = q$$

és így az átlagértékre az alábbi egyenlõséget kapjuk:

$$Q_{mean} = q$$

A fenti modellel jellemzett alkatrész csak bekapcsoláskor hibásodhat meg, és a bekapcsoláskori meghibásodás valószínûsége q . Ha az elem bekapcsoláskor meghibásodott, javítására lehetõség nincs, így bármely idõpontban vizsgálva a rendelkezésre nem állását, a bekapcsoláskori q valószínûséget kapjuk.

Ilyen típusú valószínûségi modellel rendelkeznek pl. az olyan szelepek, melyek két állapottal rendelkeznek és bekapcsoláskor váltanak állapotot. Amennyiben az állapotváltás már bekövetkezett, a szelep mûködésében nem léphet fel hiba, így csak a váltáskori (bekapcsolási) meghibásodást vesszük figyelembe.



4. ábra: Konstans rendelkezésre nem állású komponens Q(t) függvénye

5.2 Konstans gyakoriság

Ezt a modellt olyan esetekben célszerû használni, amikor az esemény legjobban Poisson folyamatként írható le.

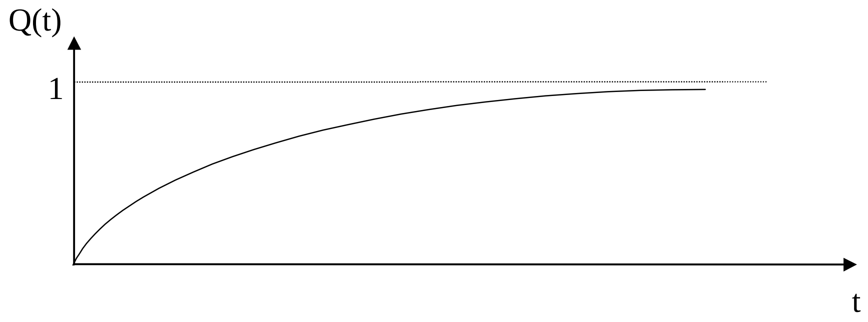
$$\lambda(t) = \lambda$$

5.3 Nem javítható komponens

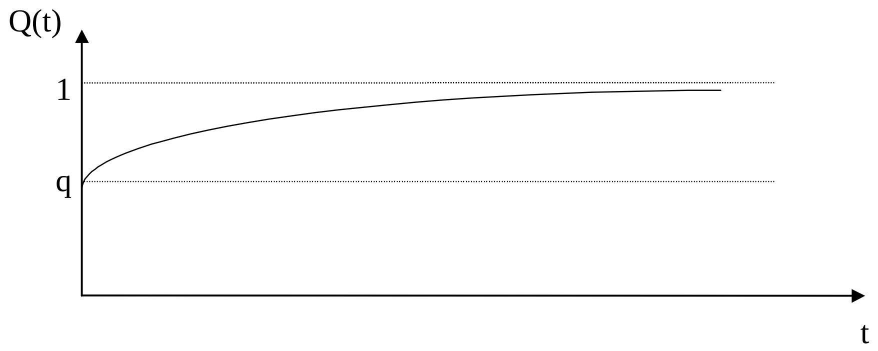
A leggyakoribb, nem javítható (vagy nem javított) komponens, konstans meghibásodási rátával. (A komponens meghibásodási rátája λ.)

$$Q(t) = q + 1 - e^{-\lambda \cdot t}$$

A képletben *q* a bekapcsoláskori meghibásodás valószínûségét jelenti.



5. ábra: Nem javítható komponens Q(t) függvénye kezdeti meghibásodási valószínûség nélkül



6. ábra: Nem javítható komponens Q(t) függvénye kezdeti meghibásodási valószínûséggel

A rendelkezésre nem állás hosszú idõre vett átlagát ennél a típusnál nincs értelme definiálni (és azzal számításokat végezni), mert az 1 lenne.

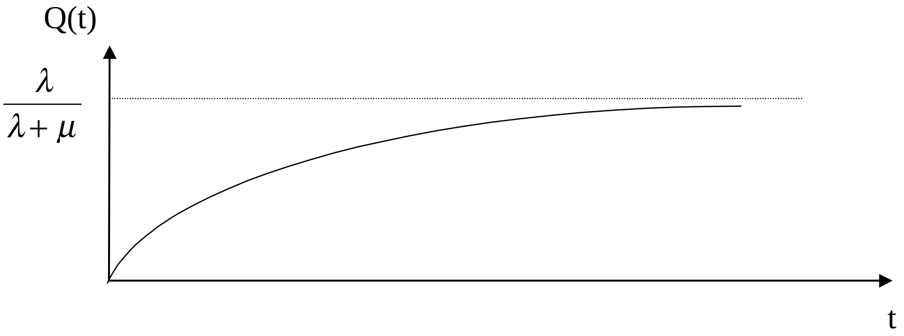
5.4 Folyamatosan figyelt, javítható komponens

Az alkatrész bármilyen meghibásodása azonnal felfedésre kerül, és megindul a javítás. (A javítás jelentheti a komponens azonos típusú, hibátlan elemre történõ lecserélését is.) A definiált javítási idõ elteltével a komponens ismét hibátlanul mûködik, egészen a következõ meghibásodásig.

A rendelkezésre nem állás idõfüggvénye:

$$Q(t) = \left(\frac{\lambda}{\lambda + \mu} \right) \cdot \left(1 - e^{-(\lambda + \mu) \cdot t} \right)$$

ahol λ a komponens meghibásodási rátája és μ a javítási idõ reciproka.



7. ábra: Folyamatosan figyelt, javítható komponens Q(t) függvénye

A rendelkezésre nem állás átlagos értéke:

$$Q_{mean} = \frac{\lambda}{\lambda + \mu}$$

Az igen hosszú idõre számolt átlagérték megegyezik az állandósult állapot értékével.

Amennyiben bekapcsoláskori meghibásodási valószínûséggel is számolunk, az alábbi összefüggést kapjuk a rendelkezésre nem állásra:

$$Q(t) = q \cdot e^{-\mu \cdot t} + \left(\frac{\lambda}{\lambda + \mu} \right) \cdot \left(1 - e^{-(\lambda + \mu) \cdot t} \right)$$

Az összefüggés elsõ tagja, $q \cdot e^{-\mu t}$ jelenti a bekapcsolási meghibásodásból származó részt. Látható, hogy a q bekapcsolási meghibásodási valószínûség hatása most nem marad meg tetszõleges ideig, mint az elõzõ típusoknál, hanem a javítási idõtõl függõen, exponenciálisan tart nullához, hiszen ennél a típusnál a bekapcsolási hibát is azonnal detektáljuk.

A rendelkezésre nem állás átlagos értéke ilyenkor is:

$$Q_{mean} = \frac{\lambda}{\lambda + \mu}$$

5.5 Periodikusan tesztelt komponens

Periodikusan tesztelt alkatrész hibái nem a hiba bekövetkezésekor, hanem egy elõre definiált idõpontban (elõre definiált idõintervallumonként periodikusan) lefutó tesztelés alkalmával fedõdnek fel. A hiba felfedésekor azonnal megkezdõdik a javítás, mely után az alkatrész ismét üzemképes lesz.

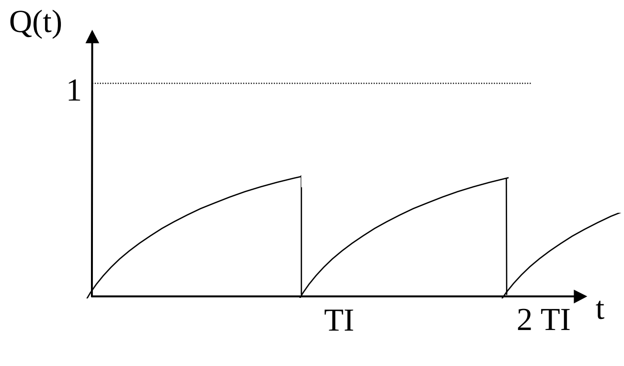
A periodikusan tesztelt komponens meghibásodási modellje talán a legkomplexebb modell, ezért több, a megadott paraméterek számának megfelelõen különbözõ alesetekre bontottuk a vizsgálatát.

5.5.1 Csak a minimálisan megkövetelt paraméterek adottak (λ, TI)

A legegyszerûbb esetben összesen két paraméter megadása szükséges: a komponens meghibásodási rátája (λ) és a tesztelési idõintervallum (TI). Ilyenkor a javítási idõ közel nulla hosszúságú (elhanyagolhatóan rövid), ami azt eredményezi, hogy a tesztelés után közvetlenül az alkatrész ismét hibátlan lesz. Ez a modell extrém rövid javítási idõk esetén jól használható.

A rendelkezésre nem állás idõfüggvénye:

$$Q(t) = 1 - e^{-\lambda(t - T_i)} \qquad T_i = 0, TI, 2TI, \ldots$$



8. ábra: Periodikusan tesztelt komponens Q(t) függvénye

Mivel Q(t) TI szerint periodikus, az átlagértéke:

$$Q_{mean} = \frac{1}{TI}\int_0^{TI} Q(t)dt = 1 - \frac{1}{\lambda \cdot TI}\left(1 - e^{-\lambda TI}\right)$$

5.5.2 A javítási idõ nem elhanyagolhatóan rövid, és az elsõ teszt lefutásának idõpontja különbözik a további tesztciklusoktól

Periodikusan tesztelt elemeknél gyakran alkalmazott az az eljárás, amikor a bekapcsolás utáni elsõ teszt nem a megadott tesztciklusidõ elteltével hajtódik végre, hanem annál jóval rövidebb idõ után.
Ha elsõ teszteléssel is számolunk, és a javítási idõt már nem lehet elhanyagolni, az alábbi képletekhez jutunk (a képletekben TR a javítási idõt, míg TF az elsõ teszt lefutásáig eltelõ idõt jelenti):

$$
\begin{aligned}
&Q(t) = 1 - e^{-\lambda \cdot t} && ha\ \ t < TF\ \ (T_i = 0)\\
&Q(t) = Q(TF) = 1 - e^{-\lambda \cdot FI} && ha\ \ t = TF\\
&Q(t) = Q(TI) = 1 - e^{-\lambda \cdot TI} && ha\ \ t = TF + nTI\\
&Q(t) = Q(TI) + \left(1 - Q(TI)\right) \cdot \left(1 - e^{\lambda \cdot (t - TI)}\right) && ha\ \ TI < t < TI + TR\\
&Q(t) = 1 - e^{-\lambda \cdot (t - n \cdot TI)} && ha\ \ n \cdot TI + TR < t < (n+1) \cdot TI
\end{aligned}
$$

A rendelkezésre nem állás átlagos értéke:

$$Q_{mean} = 1 - \frac{1}{\lambda \cdot TI}\left(1 - e^{-\lambda \cdot TI}\right) + \left(1 - e^{-\lambda \cdot TI}\right) \times \frac{TR}{TI}$$

5.5.3 Az alkatrész bekapcsoláskor konstans meghibásodási valószínûséggel rendelkezik

Konstans bekapcsolási (tesztelés utáni újbóli üzembeállítási) meghibásodási valószínûséggel rendelkezik, az alábbi képletek adódnak a rendelkezésre nem állásra:

$$
\begin{aligned}
&Q(t) = q + 1 - e^{-\lambda \cdot t} && ha\ \ t < TF\\
&Q(t) = Q(TI) = q + 1 - e^{-\lambda \cdot TI} && ha\ \ t = TF + nTI\\
&Q(t) = Q(TI) + \left(1 - Q(TI)\right) \cdot \left(q + 1 - e^{\lambda \cdot (t - TI)}\right) && ha\ \ TI < t < TI + TR\\
&Q(t) = q + 1 - e^{-\lambda \cdot (t - TI)} && ha\ \ TI + TR < t < 2TI
\end{aligned}
$$

A rendelkezésre nem állás átlagos értéke:

$$Q_{mean} = q + 1 - \frac{1}{\lambda \cdot TI}\left(1 - e^{-\lambda \cdot TI}\right) + \left(q + 1 - e^{-\lambda \cdot TI}\right) \times \frac{TR}{TI}$$

6. A hibafaanalízis eredményei

A hibafaanalízis a tervezõ vagy ellenõrzést végzõ számára számos, különbözõ típusú eredményt szolgáltat. Ezek közül egyesek elsõsorban a tervezést, a rendszer gyenge pontjainak feltárását segítik elõ, míg mások számszerû eredményt adnak a rendszer paramétereirõl.

6.1 A csúcsesemény bekövetkezési valószínûsége

Az egyik legfontosabb vizsgálat a definiált csúcsesemény bekövetkezési valószínûségének számítására irányul. Az analízis során a valószínûségszámítás alapszabályai szerint az egyes elemi események valószínûségébõl a definiált kapcsolatokon keresztül képezzük a csúcsesemény bekövetkezési valószínûségét.
A számszerû eredmény csak azt mutatja meg, hogy a rendszerünk megfelel-e az elvárásoknak, azt azonban nem, hogy melyek a rendszer gyenge pontjai.

6.2 Minimális vágatok halmaza

A rendszer gyenge pontjairól a minimális vágatok halmazán keresztül szerezhetünk értékes információkat. **Minimális vágatnak** az elemi események azon halmazát nevezzük, mely elemi események együttes bekövetkezésekor a csúcsesemény bekövetkezik, de amelyek közül bármelyik esemény be nem következésekor a csúcsesemény sem következik be.

A minimális vágatokhoz hozzárendelhetjük a bennük szereplõ elemi események bekövetkezési valószínûségének szorzatát. Ekkor a minimális vágatokat érték szerint sorba rendezve megállapíthatjuk, hogy elsõsorban melyik elemi események felelõsek a csúcsesemény bekövetkezéséért.

A minimális vágatok további elemzésével megállapítható, hogy minimálisan hány hiba szükséges a csúcsesemény bekövetkezéséhez. Ez azért fontos jellemzõ, mert sok esetben a rendszerekkel szembeni meghibásodási valószínûségi követelményeket kiegészítik azzal, hogy a rendszer legyen legalább egyszeresen hibatûrõ, vagyis egy hiba, bármilyen kis valószínûséggel is következne be, ne okozhassa a rendszer hibás reakcióját.

A 6. oldalon található hibafához tartozó minimális vágatok a hozzájuk rendelt valószínûségekkel:

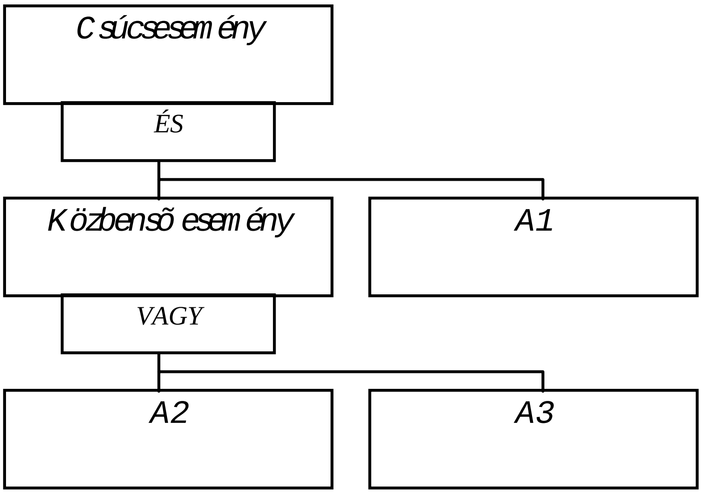
Sorszám	*Valószínûség*	*1. elemi esemény*	*2. elemi esemény*
1.	*3.2 e-6*	*A kondenzátor nem mûködik*	-----
2.	*1.5 e-6*	*D1 zárlatos*	-----
3.	*1.5 e-6*	*D2 zárlatos*	-----
4.	*1 e-6*	*D1 szakadt*	*D2 szakadt*

2. táblázat: Diódás egyenirányító minimális vágatai

Amint látható, a példabeli egyenirányító nem tesz eleget az egyszeres hibatûrés feltételének, hiszen 3 elemi esemény (3 hiba) közül bármelyik bekövetkezése önmagában elég a csúcsesemény bekövetkezéséhez, vagyis a mûködés elmaradáshoz.

Figyelmeztetés: Az egyes minimális vágatokhoz hozzárendelt számszerû eredmények összege nem a helyes végeredményt adja a csúcsesemény bekövetkezése szempontjából. Ennek oka, hogy a minimális vágatokban többször is szerepelhetnek (természetesen különbözõ kombinációkban) olyan elemi események, melyek a hibafában csak egyszer szerepelnek (az egyes minimális vágatokhoz tartozó értékek a többi minimális vágattal való kapcsolat értékeit is tartalmazzák). Így a minimális vágatokhoz tartozó számszerû valószínûségeket csak összehasonlításra szabad használni!

Következõ példánkban azt mutatjuk meg, hogy a minimális vágatokhoz rendelt valószínûségek összege nem a csúcsesemény bekövetkezési valószínûségét adja.
A példabeli hibafa 3 elemi eseményt tartalmaz: A1, A2, A3, melyek bekövetkezési valószínûsége rendre P_1 , P_2 , P_3 , *értékük egységesen* 10^{-3}.



9. ábra: Példahibafa minimális vágatok számításához

A példánkban a csúcsesemény bekövetkezési valószínûsége:

$$P_{csúcs}=(P_2+P_3-P_2P_3)*P_1 \quad = P_1P_2 + P_1P_3- P_1P_2P_3 \quad =2*10^{-6}-10^{-9}$$

A minimális vágatok:

Sorszám	*Valószínûség*	*1. elemi esemény*	*2. elemi esemény*
1.	$P_1 P_2= 10^{-6}$	*A1*	*A2*
2.	$P_1P_3= 10^{-6}$	*A1*	*A3*

3. táblázat: Példahibafa minimális vágatai

A minimális vágatok valószínûségeinek összege: $P_1P_2 + P_1P_3 =2*10^{-6}$. Ha minimális vágatoknak nem az összegét képezzük, hanem úgy tekintjük õket, mint VAGY kapcsolatban lévõ eseményeket (ez a megfontolás közelebb jár a valósághoz) és úgy is számolunk velük, ahogy a VAGY kapukra vonatkozó szabályok elõírják, akkor az alábbi eredményt kapjuk:

$$P_1P_2 + P_1P_3 - (P_1P_2)*(P_1P_3) = 10^{-6}+10^{-6}-10^{-6}*10^{-6}=2*10^{-6}-10^{-12} .$$

Látható, hogy egyik eredmény sem korrekt, tehát a minimális vágatokhoz rendelt valószínûségeket valóban csak összehasonlításra, illetve tájékoztató eredményként szabad használni.

6.3 Érzékenységvizsgálatok (fontosságvizsgálatok)

Az érzékenységvizsgálatok arra adnak választ, hogy mennyire érzékeny a csúcsesemény rendelkezésre nem állási értéke az egyes paraméterek értékeinek megváltoztatására. Az egyes paraméterek alatt az egyedi alkatrész-meghibásodásokhoz tartozó valószínûségi modellek paramétereit (λ, μ vagy TR, TI, TF) értjük. Ezt a tervezõnek azért kell ismernie, mert így választ lehet kapni arra a kérdésre, hogy milyen paraméterek változtatásával (javításával) lehet a csúcseseményre vonatkoztatott jellemzõket befolyásolni.

A vizsgálat elvégzéséhez a vizsgálni kívánt paraméter értékét elõbb n-szeresére, majd az eredeti paraméter n-ed részére változtatják, és kiszámolják a csúcsesemény rendelkezésre nem állásának értékeit (Q_{max} és Q_{min}) úgy, hogy közben a többi paramétert állandó értéken tartják. A Q_{max} / Q_{min} hányados értéke mutatja azt, hogy a paraméter megváltoztatásával mennyire változnak a globális jellemzõk. Az összes paraméterre elvégezve a vizsgálatot a paraméterek fontossági rangsorát állíthatjuk fel.

Az érzékenységvizsgálatokkal nem csak az egyes meghibásodási ráták változásának hatása térképezhetõ fel, de választ kapunk az egyes definiált idõintervallumok (tesztelési idõk, javítási idõk) változtatásának hatásaira is. Ez igen fontos lehet a tervezõmérnök számára, hiszen a rendszer jellemzõinek egyik javítási módja (amennyiben nem akarunk, vagy nem tudunk jobb, megbízhatóbb komponenseket használni) a tesztelések gyakoribb lefolytatása (ami a hibák hamarabbi felfedését eredményezi), illetve a javítási idõ csökkentése.

Az érzékenységvizsgálatok másik típusánál nem az elemi eseményekhez tartozó paramétereket változtatják, hanem az elemi esemény rendelkezésre nem állásának értékét befolyásolják közvetlenül. Ha az értéket konstans 1-nek feltételezzük, azt az esetet kapjuk, amikor az egyedi komponens meghibásodása mellett üzemel a rendszer, és erre az esetre számíthatjuk ki a csúcsesemény rendelkezésre nem állását. (Ha az ilyenkor kiszámolt rendelkezésre nem állás értéke 1, az azt jelenti, hogy a komponens meghibásodása a teljes rendszer hibájához vezet, vagyis a rendszer nem tesz eleget az egyszeres hibatûrés feltételének.)

Amennyiben az elemi esemény túlélési valószínûségét választjuk 1-nek, azt az elméleti esetet kapjuk, amelynél az alkatrész soha nem hibásodik meg, tehát ideális. Az ilyenkor kiszámolt csúcsesemény paraméterek azokat a határokat mutatják meg, amelyek az elemi esemény (alkatrész) paramétereinek változtatásával maximálisan elérhetõek.

7. Irodalomjegyzék

1. Risk Spectrum User's Manual - Relcon Teknik AB., Sweden
2. David B. Brown - System analysis and design for safety
3. Eugen Schaeffer - Megbízhatóság az elektronikában