A szolgáltatásbiztonság kvantitatív analízise: Kombinatorikus (Boole) megbízhatósági modellek

Majzik István
BME Méréstechnika és Információs Rendszerek Tanszék
majzik@mit.bme.hu

Célkitűzés

- Kvalitatív analízis:
  - Megbízhatósági analízis: Mik azok a komponens szintű hibák (hibamódok), amik rendszerszintű hibajelenséget okoznak?
    - Egyszeres hibapontok meghatározása
    - Kritikus hibák meghatározása
  - Veszély analízis: Milyen alacsonyabb szintű események vezetnek rendszerszintű veszélyhez?
    - Kockázati mátrix felvétele és kockázatcsökkentés a cél
- Kvantitatív analízis: Hogyan számszerűsíthető a komponens hibamódok jellemzői alapján a rendszer megbízhatósága illetve biztonsága?
  - Rendszerszintű hibákra:
    - Megbízhatósági jellemzők
  - Rendszerszintű veszélyekre:
    - Biztonsági jellemzők

Rendszerszintű jellemzők (ismétlés)

- Állapotparticonálás:
  Hibás (D) - Hibamentes (U) állapotpartíció
  - Várható értékek: MTFF, MUT, MDT, MTBF
  - Időfüggvények: r(t), a(t)
  - Aszimptotikus értékek: K

- Analógia:
  Biztonságos (S) illetve veszélyes (H) rendszerállapot
  - Időfüggvények: biztonságosság: s(t) (safety)
  - Gyakoriság: HR (hazard rate)

Komponens jellemzők (ismétlés)

- Meghibásodási tényező: $\lambda(t)$ gyakoriság (ráta)

  Milyen valószínűséggel hibásodik meg t környezetében?

  $\lambda(t)\Delta t = P\{ s(t+\Delta t) \in D \mid s(t) \in U \}$, miközben $\Delta t \to 0$

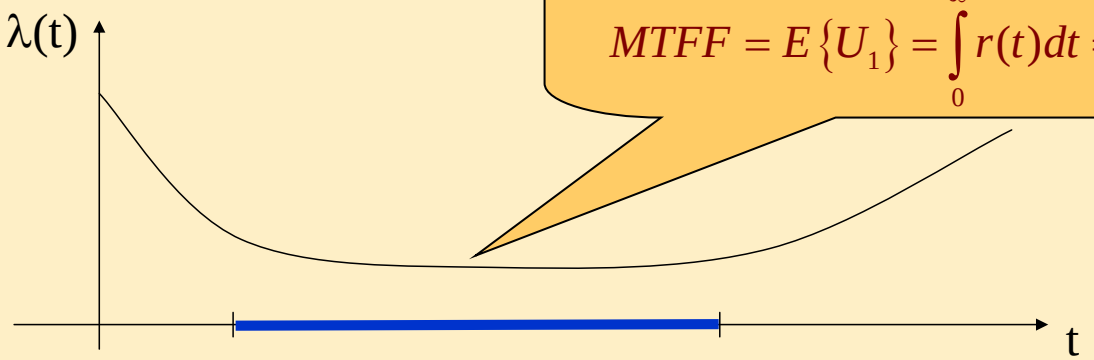
  a megbízhatóság definíciója alapján

$$\lambda(t) = -\frac{1}{r(t)}\frac{dr(t)}{dt}, \quad \text{így} \quad r(t) = e^{-\int_0^t \lambda(t)dt}$$

  Elektronikai alkatrészek:

$$r(t) = e^{-\lambda t}$$

$$MTFF = E\{U_1\} = \int_0^\infty r(t)dt = \frac{1}{\lambda}$$



Célkitűzés

- Komponens jellemzők
  - meghibásodási tényező (folyamatos üzem), FIT: 10^{-9} hiba/óra
  - hibázási valószínűség (igény szerinti végrehajtás)
  - megbízhatósági időfüggvény

  alapján

  rendszerszintű jellemzők
  - megbízhatósági időfüggvény
  - rendelkezésre állás időfüggvény
  - készenlét
  - MTFF
  - biztonságosság

  számítása

A számítás az architektúra és a hibamódok alapján történik

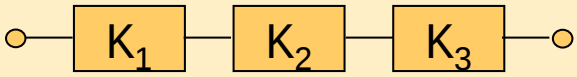
Boole-modellek

- Komponensek kétféle állapota:
  - Hibamentes (jó) vagy hibás (rossz)
- Nincsenek függőségek a komponensek között
  - sem meghibásodás,
  - sem javítás szempontjából
- Egyszerű összekapcsolási (redundancia) sémák
  - Soros: komponensek egyaránt szükségesek a rendszer működéséhez
  - Párhuzamos: komponensek egymást kiválthatják hiba esetén

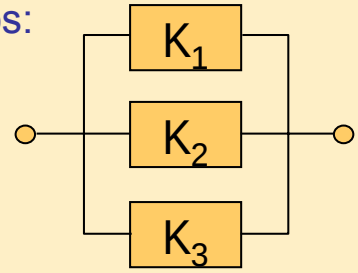
Megbízhatósági blokkdiagram (reliability block diagram)

- „Blokkok”: Komponensek (hibamódjai)
- „Kapcsolás”: Soros vagy párhuzamos kapcsolat
- „Utak”: Működőképes rendszerkonfigurációk
  - Működőképes a rendszer, ha van út a kezdőponttól a végpontig; komponens hibák ezt „megszakíthatják”

Soros:

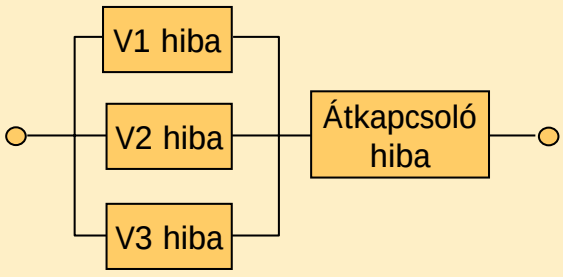


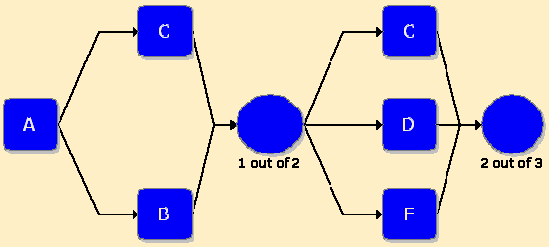
Párhuzamos:

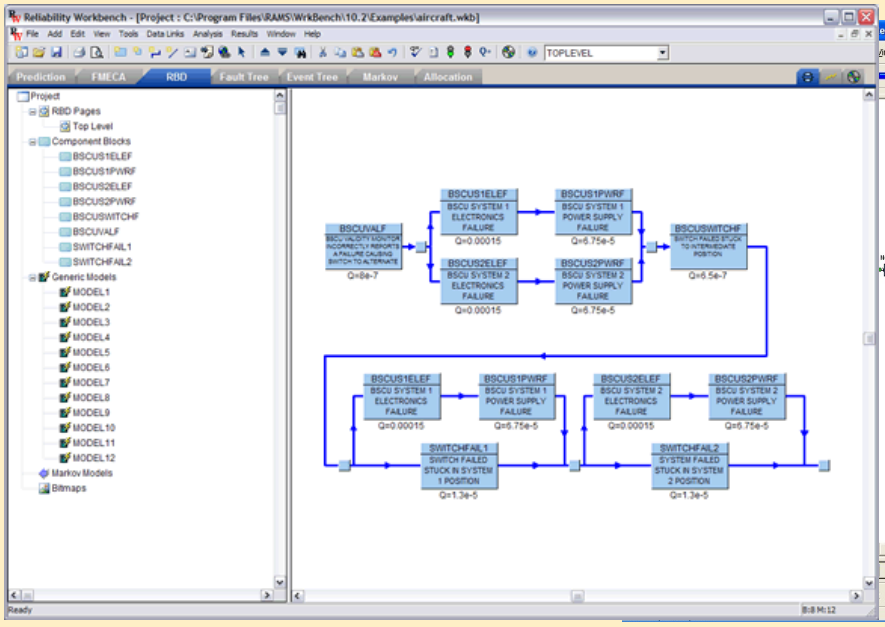


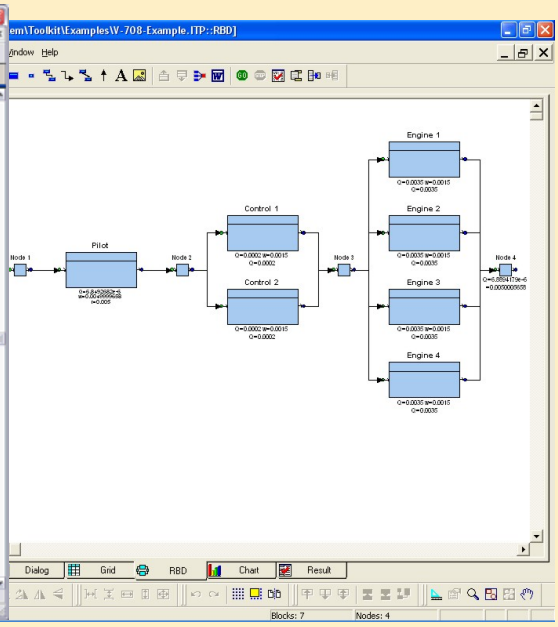
A „kapcsolás” (redundancia séma) a hibamódoktól függ!

Megbízhatósági blokkdiagram példák





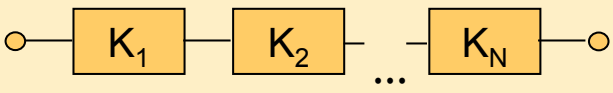


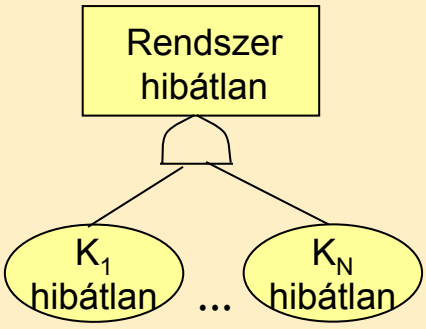


Leggyakoribb rendszerek (áttekintés)

- Soros rendszer
- Párhuzamos rendszer
- Összetett kanonikus rendszer
- „N-ből M” rendszer
- Ideális többségi szavazás (TMR)
- TMR/simplex rendszer
- Hidegtartalékolás

Soros rendszer





P(A∧B)=P(A)P(B)
ha függetlenek

- Megbízhatóság:

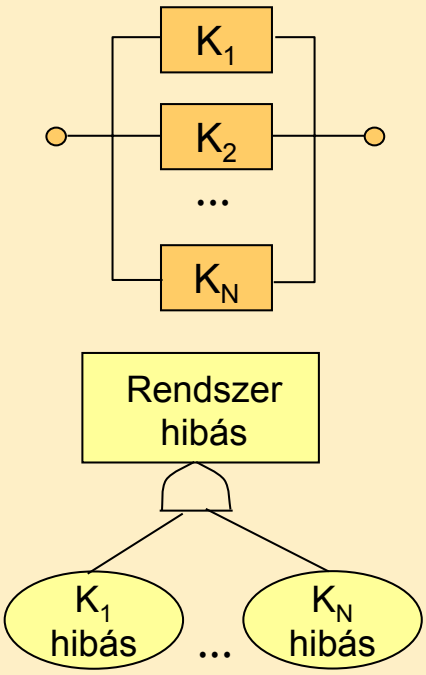
$$r_R(t) = \prod_{i=1}^{N} r_i(t)$$

- MTFF:

$$MTFF = \frac{1}{\sum_{i=1}^{N} \lambda_i}$$

Exp. eloszlású valsz. változók minimumaként

Párhuzamos rendszer



P(A∧B)=P(A)P(B)
ha függetlenek

- Megbízhatóság:

$$1-r_R(t)=\prod_{i=1}^{N}(1-r_i(t))$$

- Egyforma N komponens:

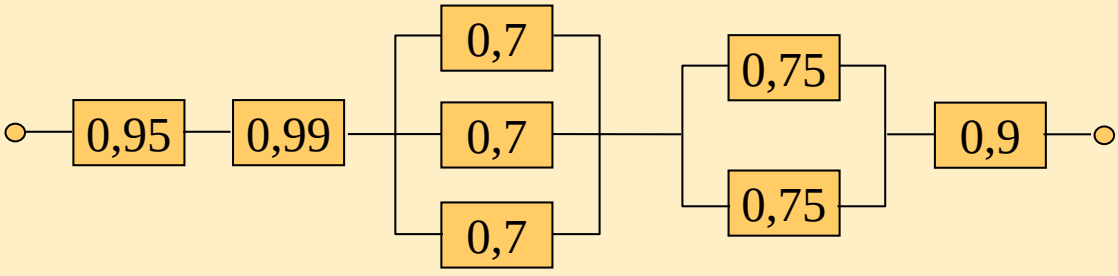
$$r_R(t)=1-(1-r_K(t))^N$$

- MTFF (levezetés nélkül):

$$MTFF=\frac{1}{\lambda}\sum_{i=1}^{N}\frac{1}{i}$$

Összetett kanonikus rendszer

- Részenként számolható (pl. készenlét):



$$K_R=0,95\cdot 0,99\cdot\left[1-(1-0,7)^3\right]\cdot\left[1-(1-0,75)^2\right]\cdot 0,9$$

TMR (NMR)

- N egyforma komponens;
  M vagy több komponens hiba esetén a rendszer is hibás

$$r_R = \sum_{i=0}^{M-1} P\{\text{"éppen i hiba van"}\}$$

$$r_R = \sum_{i=0}^{M-1} \binom{N}{i} (1-r)^i \cdot r^{N-i}$$

- Ideális többségi szavazás (TMR): N=3, M=2

$$r_R = \sum_{i=0}^{1} \binom{3}{i} (1-r)^i \cdot r^{3-i} = \binom{3}{0} (1-r)^0 \cdot r^3 + \binom{3}{1} (1-r)^1 \cdot r^2 = 3r^2 - 2r^3$$

$$MTFF = \int_0^\infty r_R(t)dt = \int_0^\infty (3r^2 - 2r^3)dt = \frac{5}{6} \cdot \frac{1}{\lambda}$$

Kisebb, mintha csak 1 komponens lenne!

TMR/simplex rendszer

- Ha egy komponens meghibásodik, akkor az egyik megmaradó hibátlan komponens működik tovább egyedül

$$r_R = \frac{3}{2} r - \frac{1}{2} r^3$$

$$MTFF = \frac{4}{3} \cdot \frac{1}{\lambda}$$

Hidegtartalékolás

- Meghibásodó komponens helyébe új komponens lép (ami nem volt üzemben)

$$MTFF = \sum_{i=1}^{N} MTFF_i$$

- Megbízhatóság általános felírása zárt alakban nehézkes (valószínűségi változók összegének sűrűségfüggvénye)
  - Azonos komponensek, exp. eloszlású komponens megbízhatóság:

$$r_R(t) = \sum_{i=0}^{N-1} \frac{(\lambda t)^i}{i!} e^{-\lambda t}$$

Architektúra változatok összevetése

Diagramok:

- Referencia: Simplex rendszer (egy komponens)
- Soros illetve párhuzamos rendszer
- Párhuzamos rendszer nem tökéletes átkapcsolóval
- Többségi szavazás ideális szavazóval
- Többségi szavazás nem ideális szavazóval

Összefoglalás

- Megbízhatósági blokkdiagram
- Kanonikus rendszerek
  - Soros
  - Párhuzamos
  - N-ből M
  - TMR
- Architektúra változatok összevetése