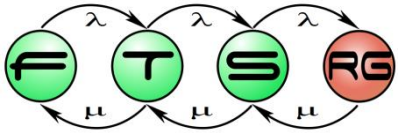
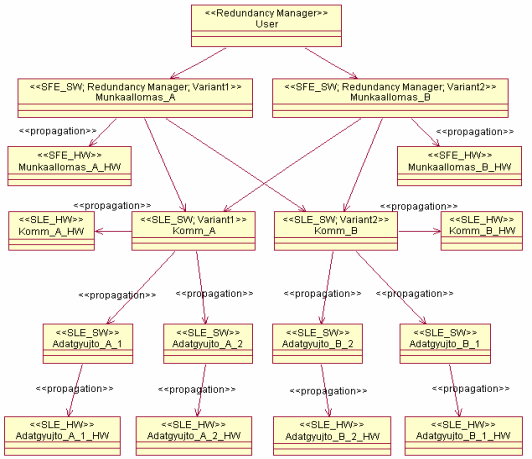
Szolgáltatásbiztonság verifikációja: Megbízhatósági analízis

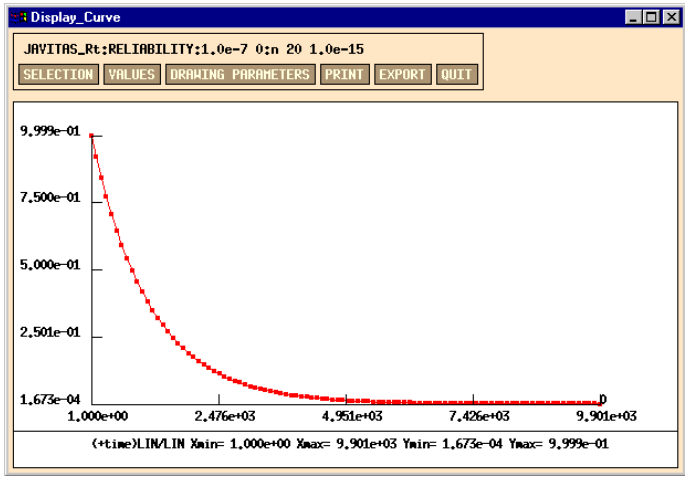
Rendszer- és szoftverellenőrzés előadás

dr. Majzik István



A szolgáltatásbiztonság jellemzői





A szolgáltatás használhatóságának jellemzése

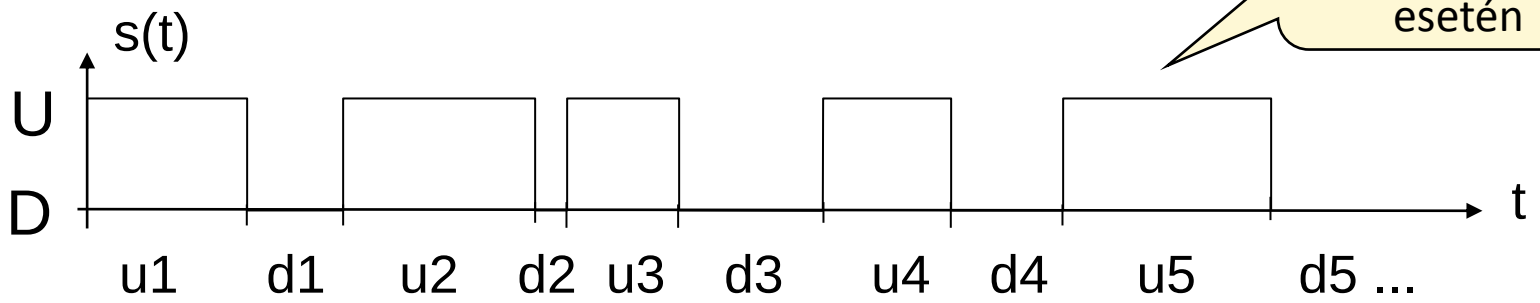
- Jellegzetes szolgáltatásminőségi követelmények:
  - Megbízhatóság, rendelkezésre állás, adatintegritás, ...
  - Ezek a használat közben előforduló hibáktól is függenek (nem elég az előállítási folyamat jó minősége)
- Összetett jellemző: Szolgáltatásbiztonság
  - Angol terminológia: Dependability
  - Definíció: Képesség olyan szolgáltatás nyújtására, amiben igazoltan bízni lehet
    - Igazoltan: elemzésen, méréseken alapul
    - Bizalom: szolgáltatás az igényeket kielégíti
  - Mennyire kerülhetők el illetve kezelhetők a szolgáltatásokat érintő hibahatások?

Szolgáltatásbiztonság alapjellemzői

- Rendelkezésre állás (availability):
  - Helyes szolgáltatás valószínűsége (közben hiba esetén javítás végezhető)
- Megbízhatóság (reliability):
  - Folyamatosan helyes szolgáltatás valószínűsége (az első hibáig tekinthető megbízhatónak)
- Biztonságosság (safety):
  - Elfogadhatatlan kockázattól való mentesség
- Integritás (integrity):
  - Hibás változás, változtatás elkerülésének lehetősége
- Karbantarthatóság (maintainability):
  - Javítás és fejlesztés lehetősége

Definíciók: Várható értékek

- Állapot particionálás s(t) rendszerállapot esetén
  - Hibamentes (Up) illetve Hibás (Down) állapotpartíció



- Várható értékek:
  - Első hiba bekövetkezése: MTFF = E{u1}
    (Mean Time to First Failure)
  - Hibamentes működési idő: MUT = MTTF = E{ui}
    (Mean Up Time, Mean Time To Failure)
  - Hibás működési idő: MDT = MTTR = E{di}
    (Mean Down Time, Mean Time To Repair)
  - Hibák közötti idő: MTBF = MUT + MDT
    (Mean Time Between Failures)

Definíciók: Valószínűség időfüggvények

- Rendelkezésre állás:

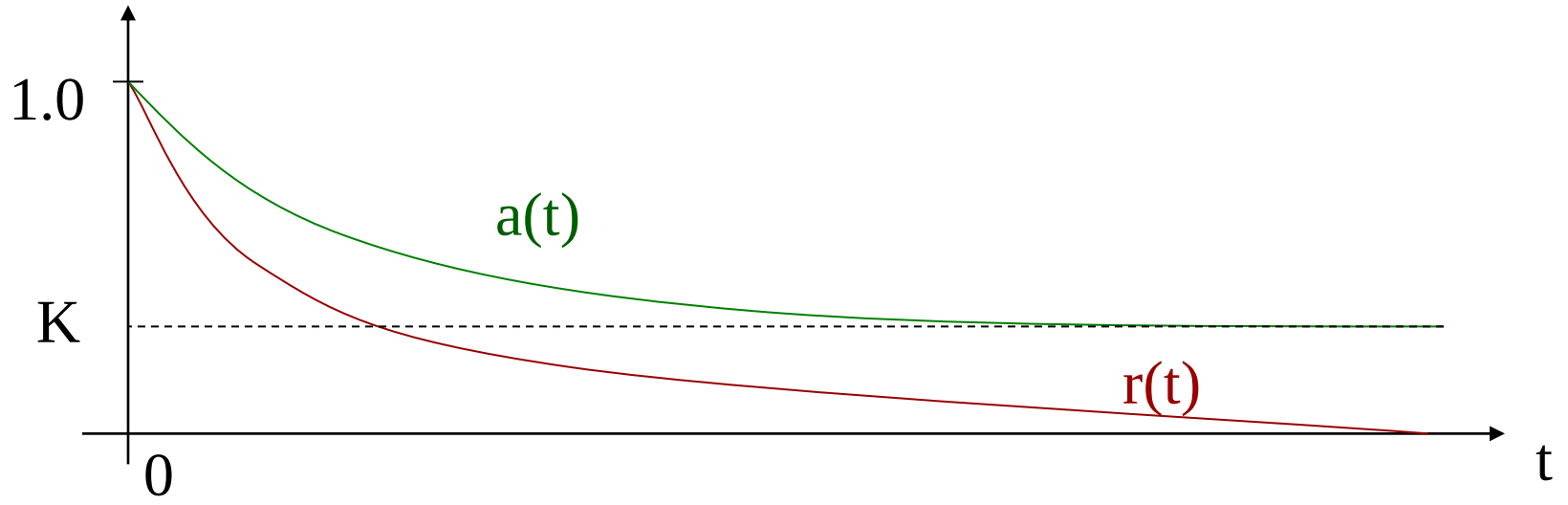
  $a(t) = P\{ s(t) \in U \}$ (közben meghibásodhat)

- Megbízhatóság:

  $r(t) = P\{ s(t') \in U, \ \forall t'<t \}$ (t-ig nem hibásodhat meg)

- Készenlét: $K=\lim_{t\to\infty} a(t)$ (rendszeresen javított)

  Jelölhető A-val is: $K = A = MTTF / (MTTF + MTTR)$



Készenlét tipikus értékei

Készenlét	Max. kiesés egy év alatt
99%	~ 3,5 nap
99,9%	~ 9 óra
99,99% („4 kilences”)	~ 1 óra
99,999% („5 kilences”)	~ 5 perc
99,9999% („6 kilences”)	~ 32 másodperc
99,99999%	~ 3 másodperc

Komponensekből felépített rendszer készenléte, ahol egy komponens készenléte 95%:

- 2 komponensből álló rendszer: 90%
- 5 komponensből álló rendszer: 77%
- 10 komponensből álló rendszer: 60%

Komponens jellemző

- Meghibásodási tényező (gyakoriság): $\lambda(t)$
  - A komponens mekkora valószínűséggel fog éppen t időpont környezetében elromlani, feltéve, hogy t-ig jól működött

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

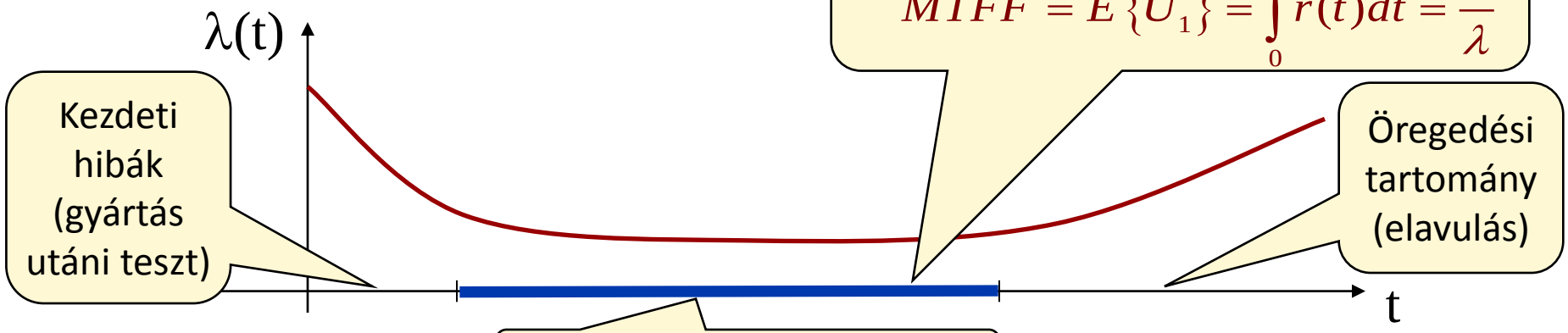
  - Másképp is felírható, a megbízhatóság definíciója alapján:

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

  - Elektronikai alkatrészekre:

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

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



Analízis módszerek

- Kvalitatív analízis:
  - Mik azok a komponens szintű hibák (hibamódok), amik rendszerszintű hibajelenséget okoznak?
    - Egyszeres hibapontok meghatározása
    - Kritikus hibák meghatározása
  - Technikák: Szisztematikus hatásanalízis
    - Hibafa, eseményfa, ok-következmény analízis, FMEA, …
- Kvantitatív analízis:
  - Megbízhatósági analízis: Hogyan számszerűsíthető a komponens meghibásodások jellemzői alapján a rendszer megbízhatósága?
    - Rendszerszintű megbízhatóság, rendelkezésre állás, …
  - Technikák: Megbízhatósági modell készítése és megoldása
    - Kombinatorikus modellek
    - Markov láncok
    - Sztochasztikus Petri hálók

A kvantitatív analízis célkitűzése

- Komponens jellemzők
  - meghibásodási tényező (folyamatos üzemben)
  - hibázási valószínűség (igény szerinti végrehajtás esetén)
  - megbízhatósági időfüggvény

  alapján

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

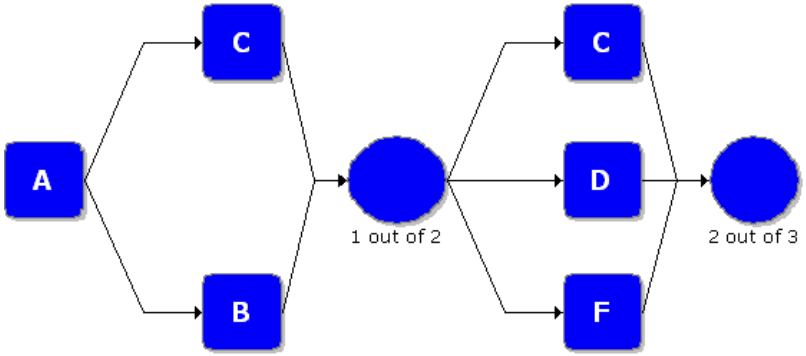
  számítása

A számítás az architektúra és a hibamódok alapján történik

A kvantitatív analízis felhasználása

- Átadás: Szolgáltatásbiztonsági jellemzők igazolása
  - Service Level Agreement
  - Tolerable Hazard Rate (biztonságkritikus rendszerek)
- Tervezés: Architektúra változatok összevetése
  - Ugyanolyan komponensekből építkezve melyik architektúra változat rendelkezik jobb jellemzőkkel?
- Tervezés, módosítás: Érzékenységvizsgálat
  - Komponens lecserélése mennyit ront vagy javít?
  - Hol érdemes módosítani, ha nem megfelelőek a jellemzők?
  - Mennyire fontos ismerni a pontos jellemzőket komponens szinten? $\rightarrow$ Kísérleti vizsgálat igénye (pl. hibainjektálás)

Kombinatorikus modellek a megbízhatósági analízisben



Boole-modellek

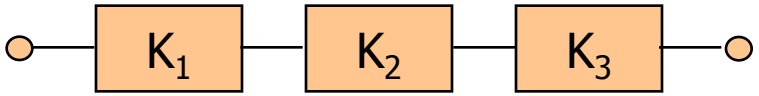
- Komponensek kétféle állapota:
  - Hibamentes (jó) vagy hibás (rossz)
- Nincsenek függőségek a komponensek között
  - sem meghibásodás,
  - sem javítás szempontjából
- Komponensek kapcsolata a megbízhatóság szempontjából:
  Leírja, hogy milyen az alkalmazott redundancia
  - Soros kapcsolat:
    - A komponensek egyaránt szükségesek a rendszer működéséhez,
    - azaz a komponensek nem redundánsak
  - Párhuzamos kapcsolat:
    - A komponensek egymást kiválthatják hiba esetén
    - azaz a komponensek redundánsak

  A kapcsolat (redundancia séma) a hibamódoktól függhet

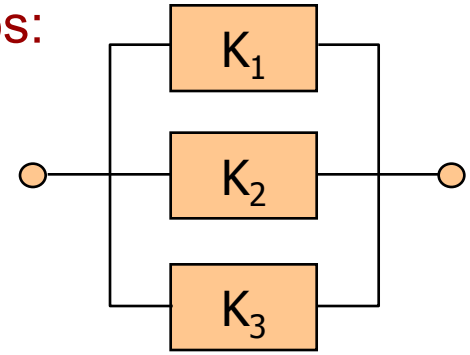
Megbízhatósági blokkdiagram

- „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”

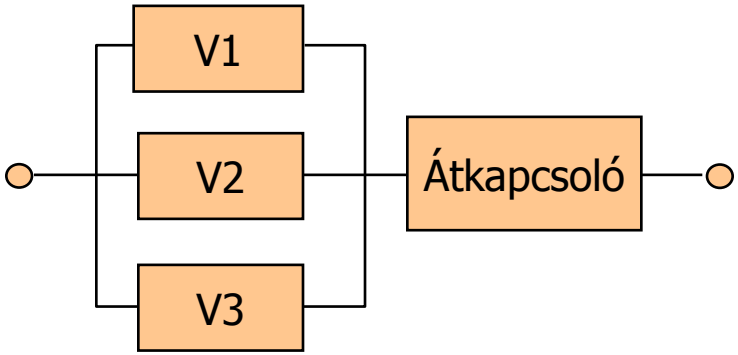
Soros:

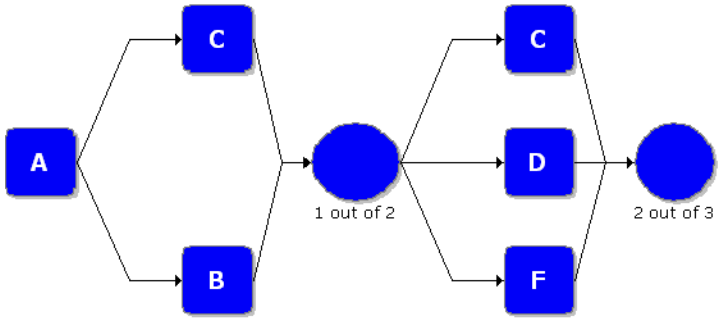


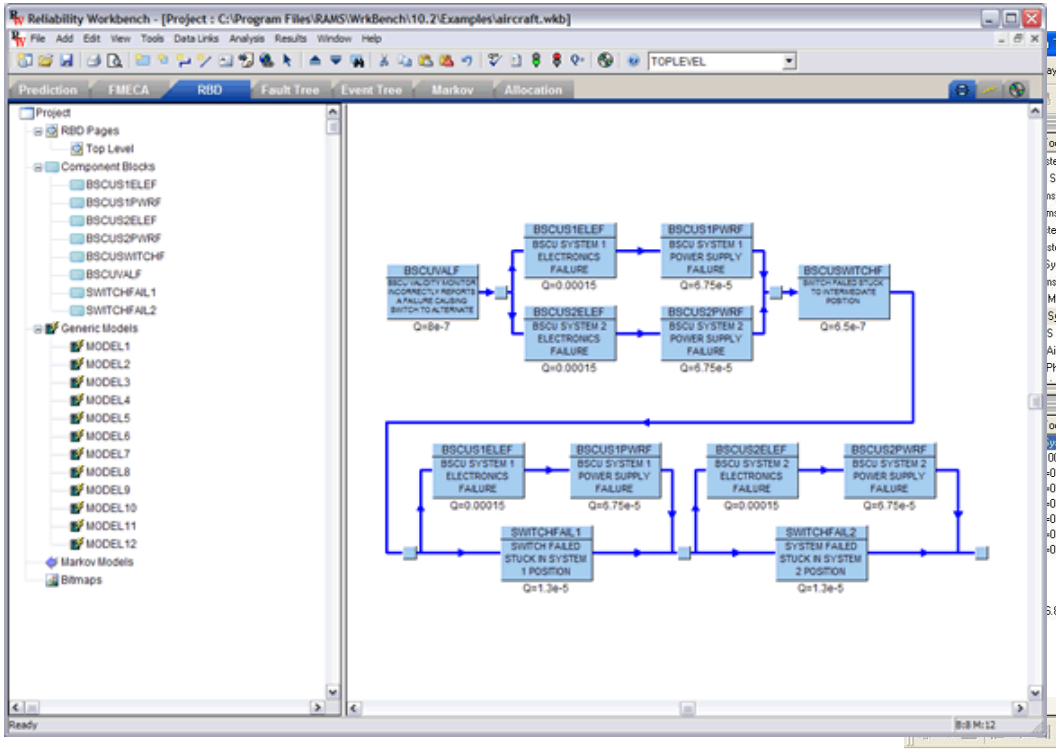
Párhuzamos:

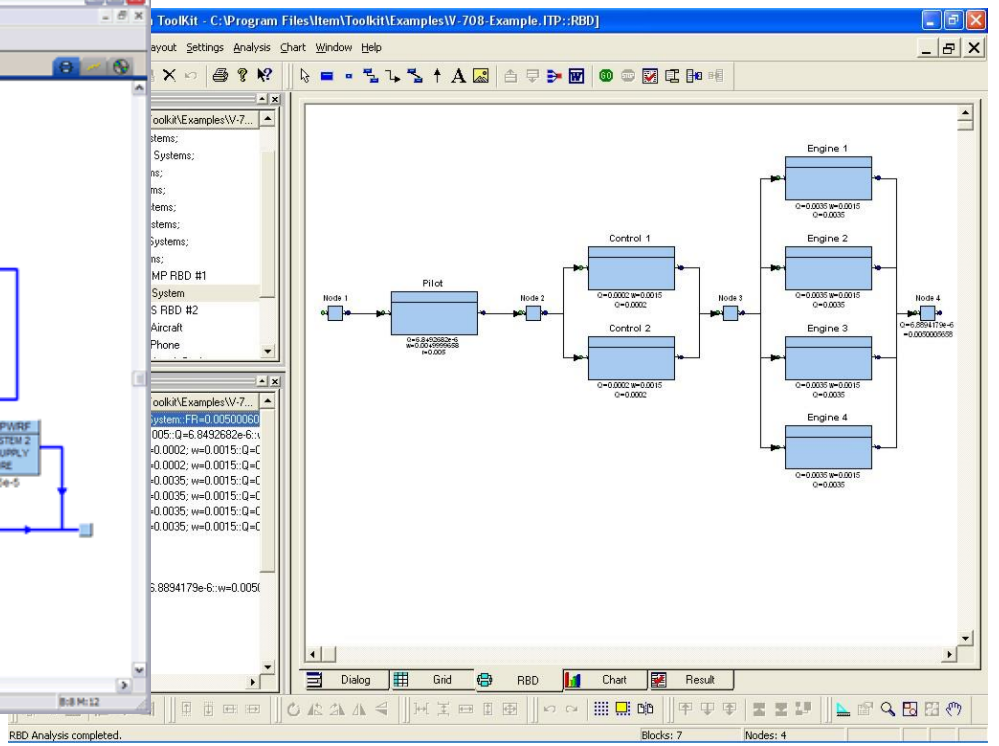


Megbízhatósági blokkdiagram példák





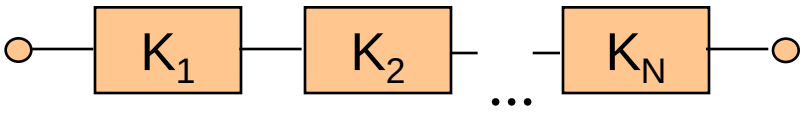


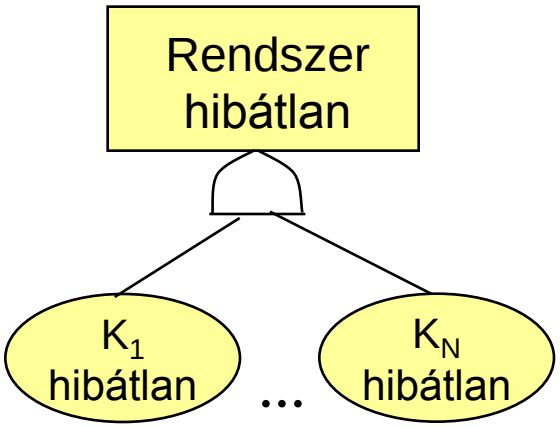


Leggyakoribb rendszerek (áttekintés)

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

Soros rendszer





$P(A \wedge B)=P(A)\cdot P(B)$
ha függetlenek

- Megbízhatóság:

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

A rendszer megbízhatósága

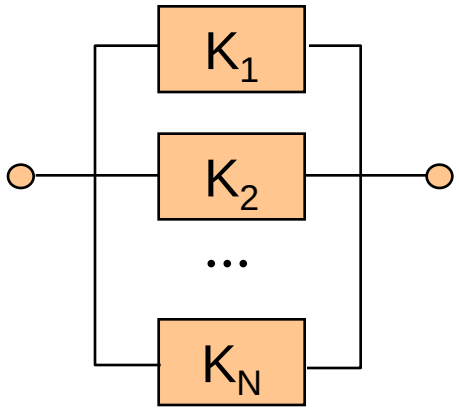
A komponensek megbízhatósága

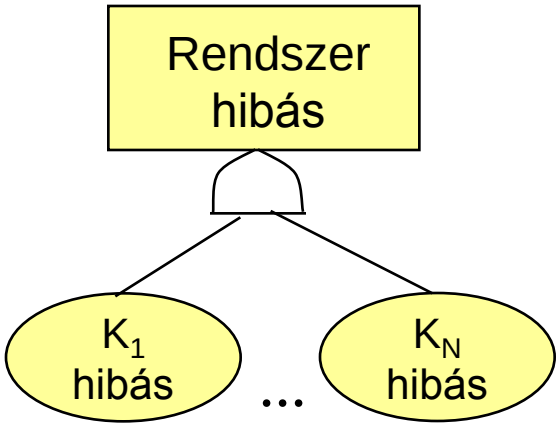
- MTFF:

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

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:

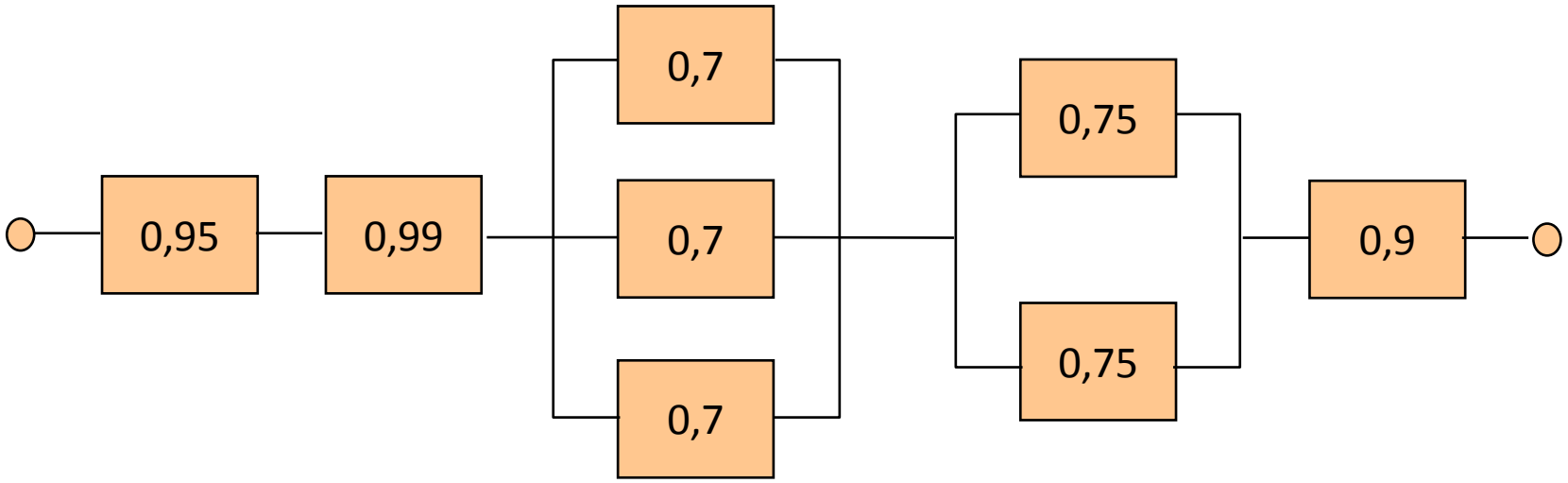
$$r_R(t) = 1 - (1 - r_K(t))^N$$

- Itt MTFF (levezetés később):

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

Összetett kanonikus rendszer

- A rendszerstruktúra és a komponensek készenlétei ismertek:



- A rendszer készenlét számítható:

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

N-ből M hibás komponens

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

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

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

Itt egyszerűen r jelöli a komponens r(t) megbízhatóságot

N-ből M hibás komponens és TMR

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

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

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

- Alkalmazás: 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!
Miért használják mégis?

TMR/simplex rendszer

- Ha a TMR egy komponense meghibásodik
  (ezt a szavazó logika azonosítja),
  akkor az egyik megmaradó hibátlan komponens működik tovább egyedül (de már hibadetektálás nélkül)

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

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

Hidegtartalékolás

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

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

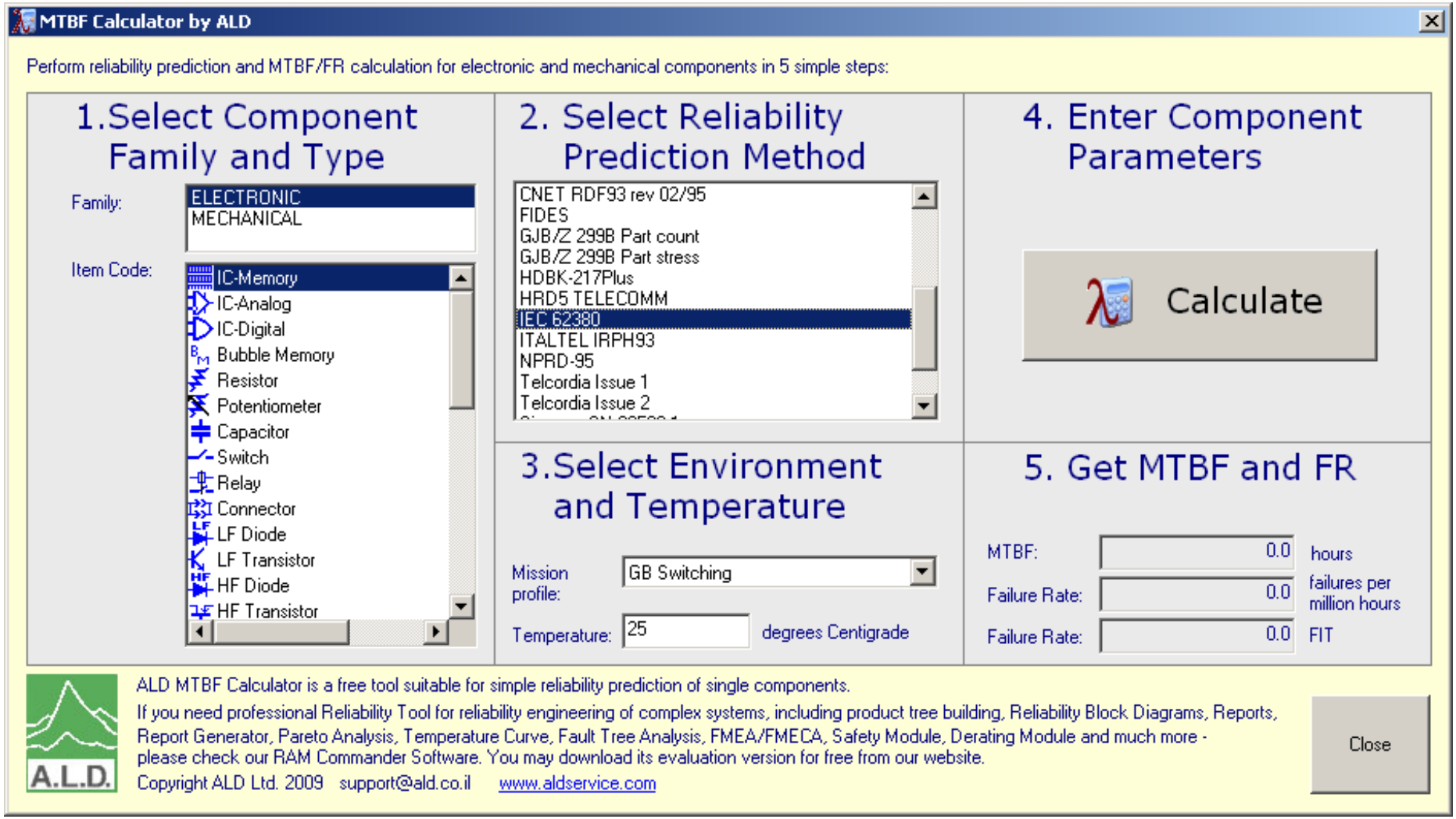
- Megbízhatóság általános felírása zárt alakban bonyolult (valószínűségi változók összegének sűrűségfüggvénye)
  - Azonos komponensek, exponenciális eloszlású komponens megbízhatósági függvény esetén:

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

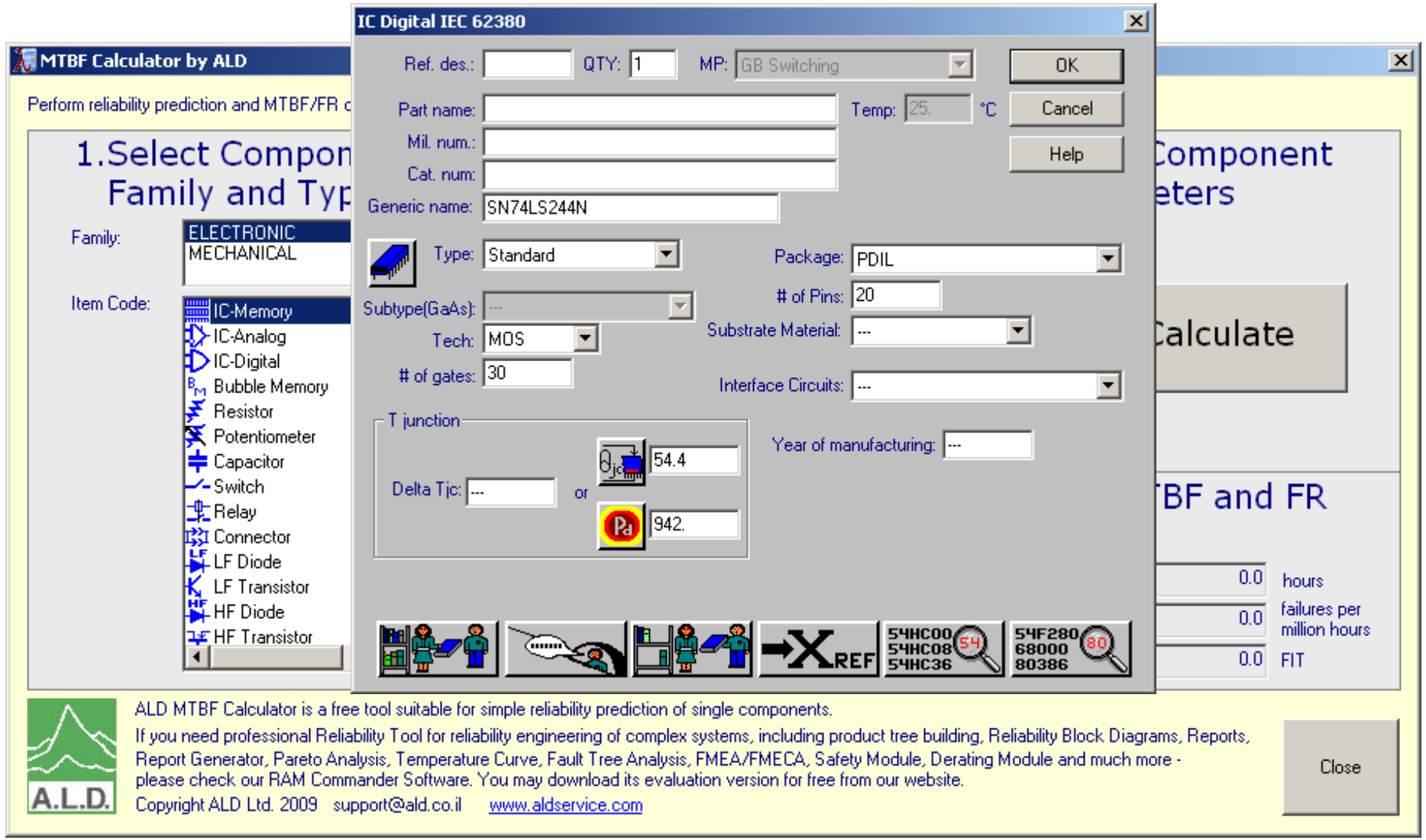
Konkrét megbízhatósági számítások

- Hierarchikus megközelítés (redundancia sémák alkalmazása)
  - Alkatrész –> modul –> részrendszer –> rendszer
- Alkatrész szintű meghibásodási gyakoriság becslési módszerek
  - MIL-HDBK-217: The Military Handbook Reliability Prediction of Electronic Equipment (katonai alkalmazásokhoz, pesszimista)
  - Telcordia SR-332: Reliability Prediction Procedure for Electronic Equipment (telco alkalmazásokhoz)
  - IEC TR 62380: Reliability Data Handbook - Universal Model for Reliability Prediction of Electronic Components, PCBs, and Equipment (kevésbé pesszimista, korszerűbb alkatrészekhez is)
- Alkatrész szintű meghibásodási gyakoriság függőségei:
  - Hőmérséklet, időjárási kitettség, rázkódás (pl. jármű fedélzet), magasság, …
  - Jellegzetes felhasználási profilok
    - Ground; stationary; weather protected (pl. klimatizált teremben lévő)
    - Ground; non stationary; moderate (pl. jármű fedélzeti rendszer)

Példa: Az ALD MTBF Calculator

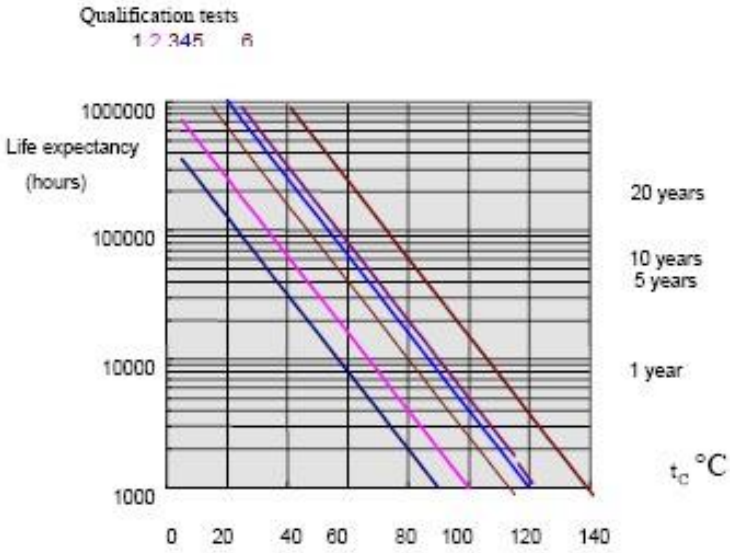


Példa: Az ALD MTBF Calculator

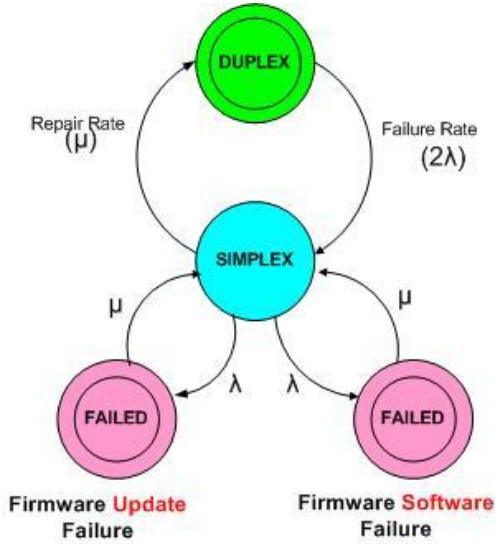


Élettartam becslése

- Milyen élettartam figyelembe vételével használhatók az elektronikai komponensek?
  - Mikortól kezd nőni a meghibásodási tényező?
  - Ekkorra ütemezett karbantartás (csere) előírható
- IEC 62380: „Life expectancy”
- Elsősorban korlátoz: Elektrolit kondenzátorok (kiszáradás)
  - Hőmérsékletfüggő
  - Kezdeti bevizsgálástól is függ
  - Példa: ~ 100 000 óra (~ 11 év)



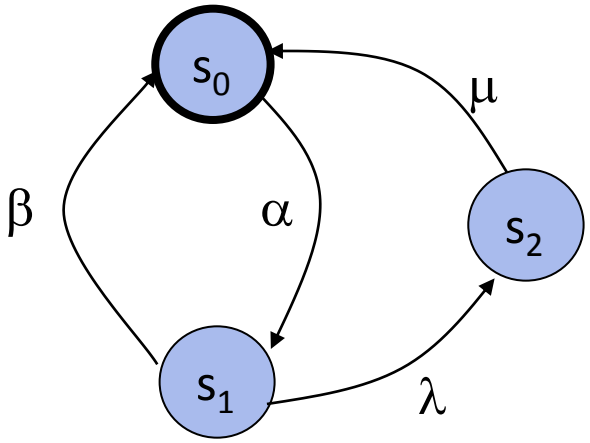
Markov láncok használata a megbízhatósági analízisben



A modell: Folytonos idejű Markov lánc

- Definíció: CTMC = (S, **R**)
  - S diszkrét állapotok halmaza:

    $s_0, s_1, \ldots, s_n$
  - **R**: $S \times S \rightarrow R_{\geq 0}$ állapotátmeneti gyakoriságok



- Jelölések:
  - Állapot elhagyás összesített gyakorisága: $E(s) = \sum_{s' \in S, s \neq s'} R_{s,s'}$
  - **Q** = **R**–diag(E) „infinitezimális generátormátrix”
  - $\sigma = s_0, t_0, s_1, t_1, \ldots$ (t_i időpontban lép ki s_i-ből)
  - $\sigma@t$ az állapot a t időpillanatban
  - Path(s) az s-ből induló útvonalak halmaza

A modell megoldása

- Tranziens állapotvalószínűségek:
  - $\pi(s_0, s, t) = P\{\sigma \in Path(s_0) \mid \sigma@t=s\}$ annak valószínűsége, hogy s_0-ből indulva a t időpillanatban s-ben tartózkodik
  - $\underline{\pi}(s_0, t)$ az állapotok valószínűségei s-ből indulva t időpillanatban
  - CTMC tranziens megoldása:

$$\frac{d\,\underline{\pi}(s_0,t)}{dt} = \underline{\pi}(s_0,t)\underline{\underline{Q}}$$

Állapot tartása:

$$P\{\text{s-ben marad t ideig}\} = e^{-E(s)t}$$

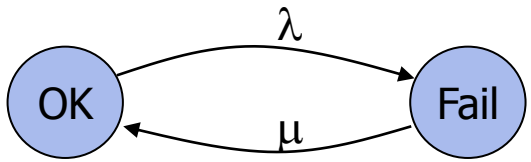
$$E\{\text{s-ben maradás ideje}\} = \frac{1}{E(s)}$$

- Állandósult állapotbeli állapotvalószínűségek:
  - $\pi(s_0, s) = \lim_{t\to\infty} \pi(s_0,s,t)$ az állapotok valószínűsége s_0-ból indulva
  - $\underline{\pi}(s_0)$ az állapotok valószínűsége (sorvektorként)
  - CTMC állandósult állapotbeli megoldása:

$$\underline{\pi}(s_0)\underline{\underline{Q}} = 0 \quad \text{ahol} \quad \sum_s \pi(s_0, s) = 1$$

A CTMC megbízhatósági modell

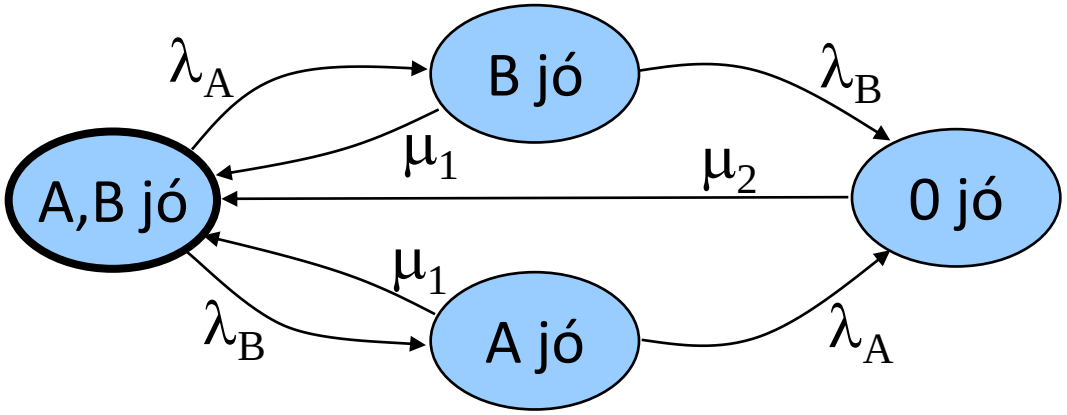
- CTMC állapotok
  - Rendszerszintű állapotok: A komponens állapotok (hibamentes, hibás adott hibamód szerint) kombinációi
- CTMC átmenetek
  - Komponens szintű meghibásodás:
    Az állapotátmeneti gyakoriság a meghibásodási tényező (λ)
  - Komponens szintű javítás:
    Az állapotátmeneti gyakoriság a komponens javítási tényezője (μ, a javítási idő reciproka)



  - Rendszer szintű javítás:
    Az állapotátmeneti gyakoriság a rendszerállapot javítási tényezője (javítási idő reciproka)

Példa: CTMC megbízhatósági modell

- Két szerverből (A, B) álló rendszer:
  - Bármelyik szerver meghibásodhat
  - A szerverek külön-külön vagy együtt is javíthatók
- Rendszerszintű állapotok: Szerverek állapotai (jó / hibás) alapján
- Állapotátmenetek és gyakoriságok:
  - Az A szerver meghibásodása: λ_A meghibásodási tényező
  - A B szerver meghibásodása: λ_B meghibásodási tényező
  - Egy szerver javítása: μ_1 javítási tényező
  - Teljes rendszer javítása: μ_2 javítási tényező

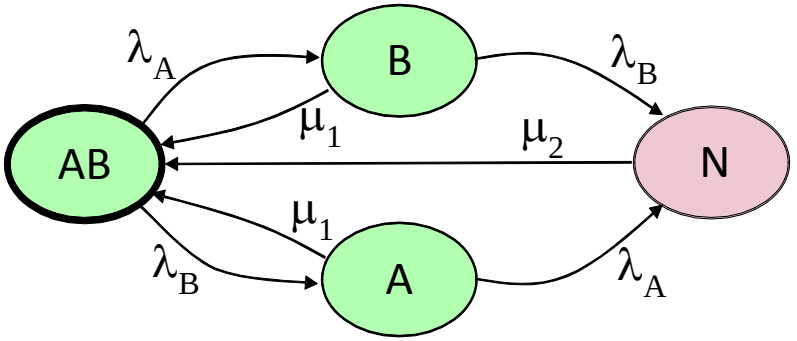


A rendszerszintű jellemzők számítása

- Állapotpartíciók kijelölése
  - Rendszerszintű hibamentes U illetve hibás D
- A modell megoldása:
  - Tranziens analízis: $\pi(s_0, s, t)$ időfüggvények
  - Állandósult állapotbeli analízis: $\pi(s_0, s)$ valószínűségek
- Rendelkezésre állás: $a(t) = \sum_{s_i \in U} \pi(s_0, s_i, t)$
- Készenlét: $K = A = \sum_{s_i \in U} \pi(s_0, s_i)$
- Megbízhatóság: $r(t) = \sum_{s_i \in U} \pi(s_0, s_i, t)$
  - Itt: A modell megoldása előtt a modell módosítása: D-ből U-ba vezető állapotátmenetek törlése

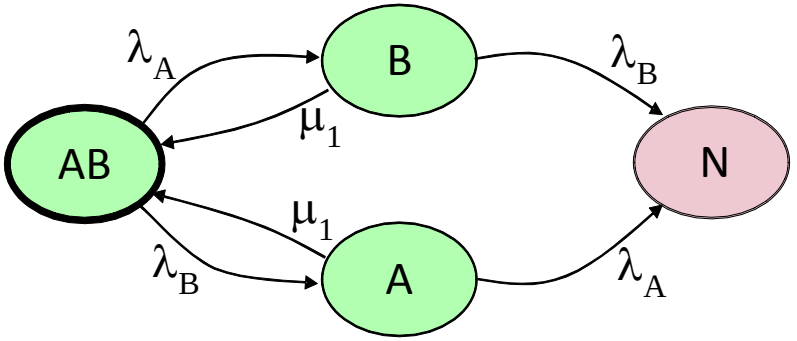
Példa: CTMC megbízhatósági modell

- Két szerverből (A, B) álló rendszer:
  - Bármelyik szerver meghibásodhat
  - A szerverek külön-külön vagy együtt is javíthatók



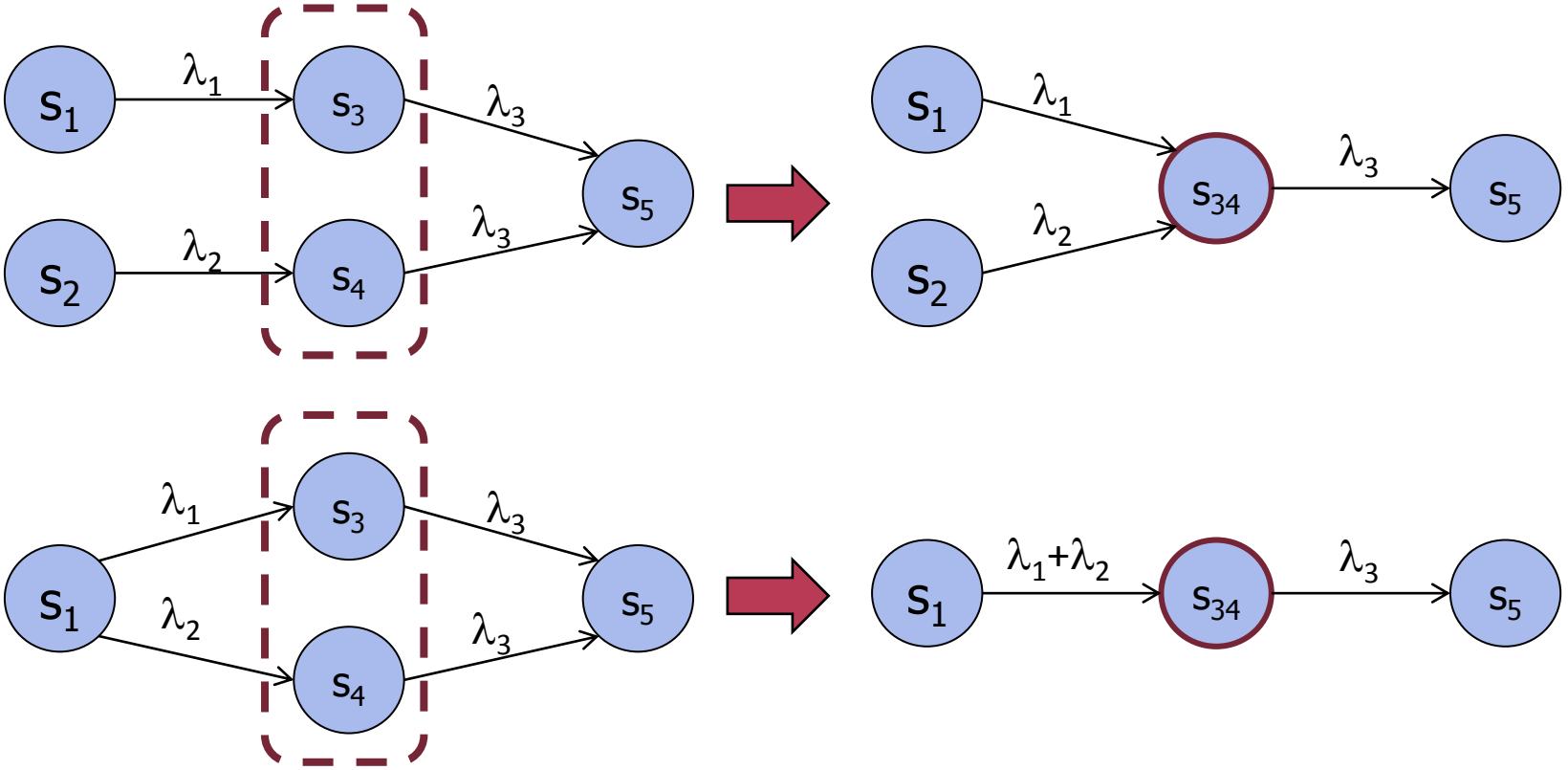
- Állapotpartíciók:
  - $U = \{s_{AB}, s_A, s_B\}, \quad s_0 = s_{AB}$
  - $D = \{s_N\}$
- Rendelkezésre állás: $a(t) = \pi(s_0, s_{AB}, t) + \pi(s_0, s_A, t) + \pi(s_0, s_B, t)$
- Készenlét: $K = A = \pi(s_0, s_{AB}) + \pi(s_0, s_A) + \pi(s_0, s_B)$
- Megbízhatóság:
  - Modell módosítása: $D = \{s_N\}$ partícióból U partícióba vezető élek törlése
  - Módosított modell megoldása:

$r(t) = \pi(s_0, s_{AB}, t) + \pi(s_0, s_A, t) + \pi(s_0, s_B, t)$



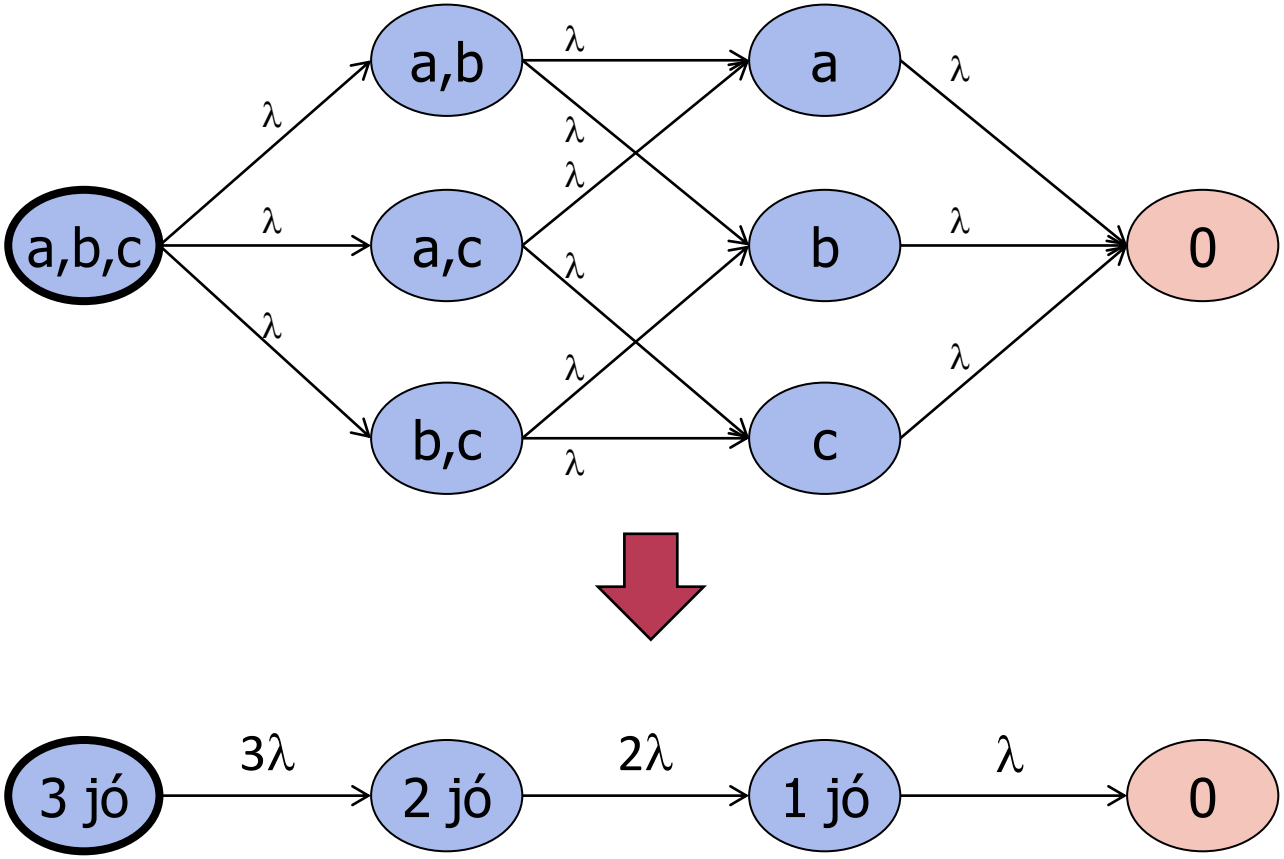
CTMC modellek redukálása

- Állapotok összevonhatók
  - Feltétel: Átmenetek azonos állapot(ok)ba, azonos gyakoriságokkal (kimenő átmenetek és gyakoriságok nem különböztetik meg az állapotokat)
  - Bejövő gyakoriságok megmaradnak (azonos állapotból: összegződnek)
  - Kimenő gyakoriság nem összegződik!



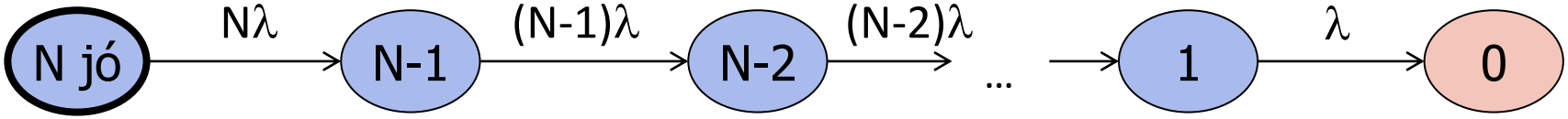
Példa: Állapotok összevonása

- Modell: 3 redundáns komponensből álló rendszer
- A komponensek (a, b, c) azonos λ tényezőjűek

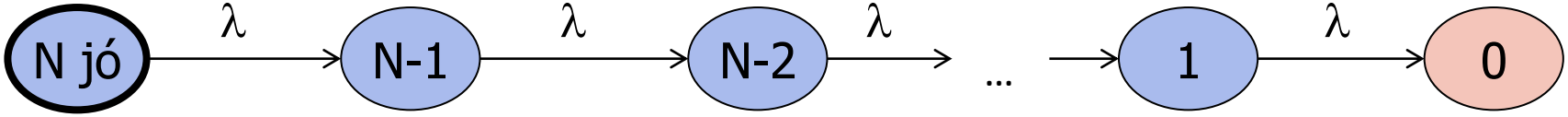


CTMC megbízhatósági modell példák (1)

- Aktív redundancia (melegtartalék), N komponens

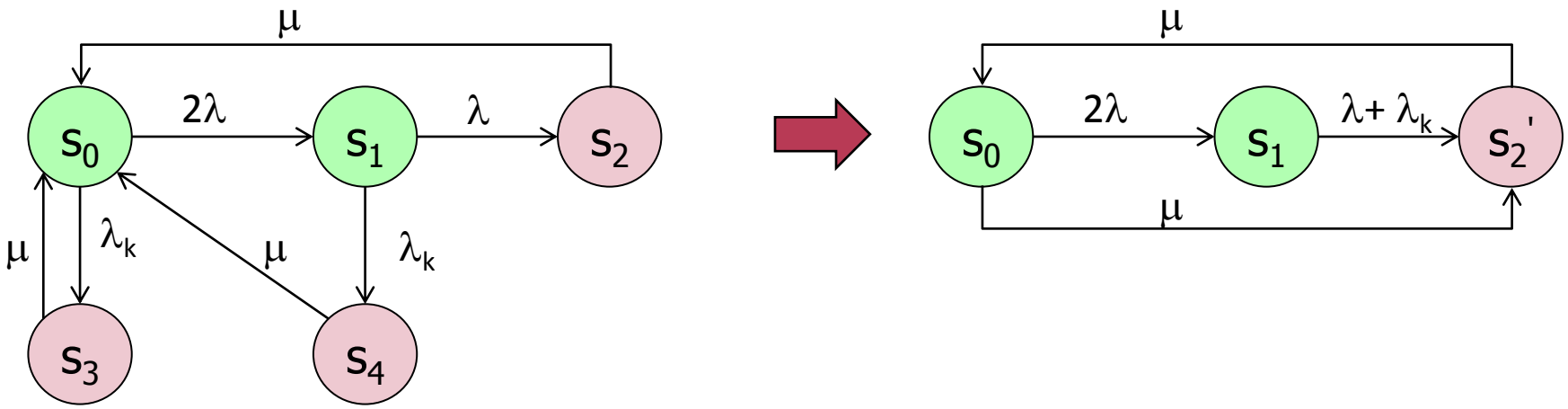


- Az MTTF levezetése aktív redundancia esetén
  - Állapot tartási ideje, ha k komponens jó: $\frac{1}{k\lambda}$
- Passzív redundancia (hidegtartalék)



CTMC megbízhatósági modell példák (2)

- Aktív redundancia
  - 2 komponens, λ meghibásodási gyakorisággal
  - Nem ideális átkapcsoló, λ_k meghibásodási gyakorisággal
  - Hiba esetén teljes javítás μ javítási tényezővel



Eszközök

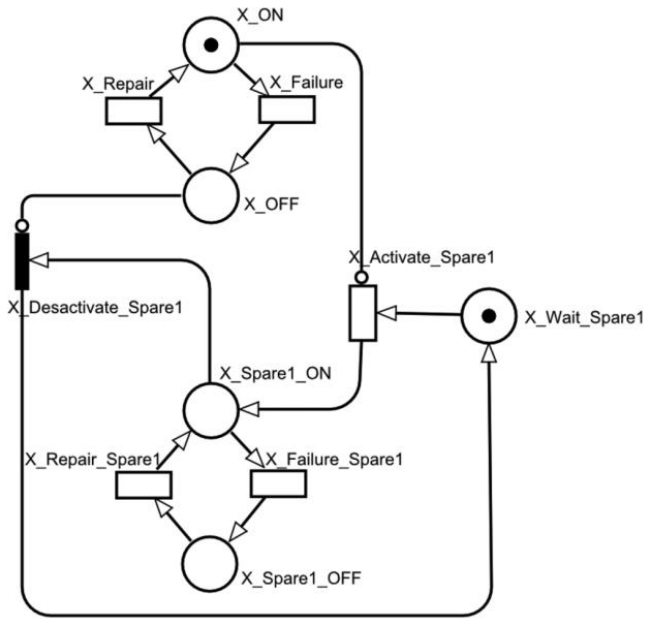
Kombinatorikus megbízhatósági modellekhez

- hibafa,
- eseményfa,
- megbízhatósági blokk diagram,
- FME(C)A, …

és Markov láncokhoz is:

- Relex 2009 (www.relex.com)
- Item Toolkit (www.itemuk.com)
- RAM Commander, … (www.aldservice.com)
- Functional Safety Suite

Sztochasztikus Petri-hálók a megbízhatósági analízisben



Modell: Sztochasztikus Petri-hálók (SPN)

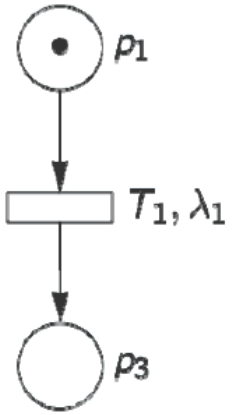
- SPN: Stochastic Petri Net
- Az egyszerű Petri-hálók kiterjesztése
  - A tranzíciókhoz véletlen tüzelési késleltetést rendelünk
  - A késleltetés negatív exponenciális valószínűségi eloszlásfüggvénnyel jellemezhető
- A tüzelés szemantikájának módosulása
  - Engedélyezettség feltétele: Nem változik
  - Tüzelési szabály: Egy tranzíció tüzelhet t+d időpontban, ha
    - t időpontban engedélyezetté vált
    - d késleltetési időt sorsolt a hozzá tartozó eloszlásfüggvény szerint
    - a [t, t+d) időtartományban folyamatosan engedélyezett volt

Jelölések

- Tranzíciók paramétere (tüzelési gyakorisága):
  - λ_i egy T_i tranzíció d_i késleltetési idejéhez tartozó negatív exponenciális eloszlás paramétere (pozitív valós szám)
- Grafikus jelölés
  - Tranzíciók mint üres téglalapok
- Egy λ paraméterű tranzíció esetén:
  - A sorsolt d_i késleltetési időre:

$$P\{d_i \le t\} = 1 - e^{-\lambda_i t}$$

$$P\{d_i > t\} = e^{-\lambda_i t}$$



Jellemzők összefoglalása az SPN-re

- Az új jelölés kialakulásához szükséges idő exponenciális eloszlású
  - Konfliktusban lévő vagy konkurens tranzíciók esetén is
- Az időzítéssel ellátott elérhetőségi gráf egy CTMC
  - Struktúrája független a tranzíciók paramétereinek értékétől
  - A CTMC megoldási módszerei használhatók az SPN analíziséhez
- Az analízis eredményei
  - Állandósult állapotbeli megoldás (létezik, ha az SPN korlátos és megfordítható):
    - Jelölések valószínűsége (időfüggvény illetve aszimptotikus)
    - Tranzíciók tüzelési gyakorisága
  - Tranziens megoldás:
    - Jelölések valószínűségi időfüggvényei

Általánosított sztochasztikus Petri-hálók

- GSPN: Generalized Stochastic Petri Net
- Kiterjesztések SPN-hez képest
  - Azonnal tranzíciók: Logikai függőségek modellezésére
    - Prioritás: > 0
    - Súlytényező: az azonos prioritású tranzíciók közötti konfliktusfeloldáshoz
  - Időzített tranzíciók: Időzített események modellezésére
    - Prioritás: 0
    - Paraméter: a késleltetési idő sorsolásához a negatív exp. valószínűségi eloszlásfüggvény paramétere (jelölésfüggő paraméter is lehet)
  - Tiltó élek
  - Őrfeltételek: Predikátumok tranzíciók engedélyezettségéhez
- Az elérhetőségi gráf továbbra is CTMC
  - Eltűnő (vanishing) jelölések
  - Adott ideig fennálló (tangible) jelölések

További kiterjesztések és használatuk

- DSPN: Deterministic and Stochastic Petri Net
  - Determinisztikus késleltetéssel (konstans tüzelési idővel) ellátott tranzíciók is lehetségesek
  - Javítási idő modellezésére alkalmas
  - Az analízis hatékonyságának feltétele: Egy jelölésben csak egy determinisztikus időzítésű tranzíció engedélyezett
- Általános időzített Petri-hálók (TPN)
  - Általános eloszlásfüggvény adható a tranzíciók tüzelési idejének (késleltetésének) sorsolásához
  - A késleltetések újrasorsolásának többféle szemantikája egy-egy új jelölésben
  - Tevékenység folytatása, újrakezdése modellezhető
  - Általános esetben az elérhetőségi gráf nem CTMC:
    - Szimulációval történő analízis lehetséges
    - Közelítő analízis lehetséges

Reward hozzárendelések

- SRN: Stochastic Reward Net
  - Reward: Haszon (vagy költség, ha negatív) függvények megadása
- Ráta jellegű reward (rate reward):
  - Jelöléseken értelmezett, haszon/időegység értéket ad meg
  - Példa: Ha jó a szerver, 300 Ft/óra a haszon, egyébként 200 Ft/óra a kötbér:

    ```
    if (m(Healthy)>0) then ra=300
    ```

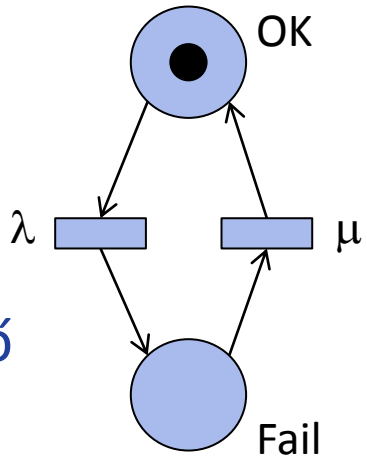
  - Számítható: Időintervallumra megállapítható haszon a reward ráta idő szerinti integrálásával
- Impulzus jellegű reward (impulse reward):
  - Egy-egy tranzíció tüzeléséhez rendelhető hasznot ad meg
  - Példa: Egy-egy javítás költsége 500 Ft:

    ```
    if (fire(Repair)) then ri=500
    ```

  - Számítható: Időintervallumra összegezhető a tüzelésekre összeadva

Az SPN (GSPN) megbízhatósági modell

- Előnyök a CTMC-hez képest
  - Konkurens események modellezése lehetséges
  - Nem „kiterített” rendszerszintű állapotokat kell felvenni
- SPN helyek
  - Komponens állapotok: Hibamentes, hibás adott hibamód(ok) szerint; egymástól függetlenül felvehetők
- SPN tranzíciók
  - Komponens szintű meghibásodás: A tranzíció paramétere a λ meghibásodási tényező
  - Komponens szintű javítás: A tranzíció paramétere a komponens μ javítási tényezője (javítási idő reciproka)



  - Rendszerszintű javítás (tranzíció több forrás és cél hely között): a tranzíció paramétere a rendszerállapot javítási tényezője

Rendszerszintű jellemzők számítása

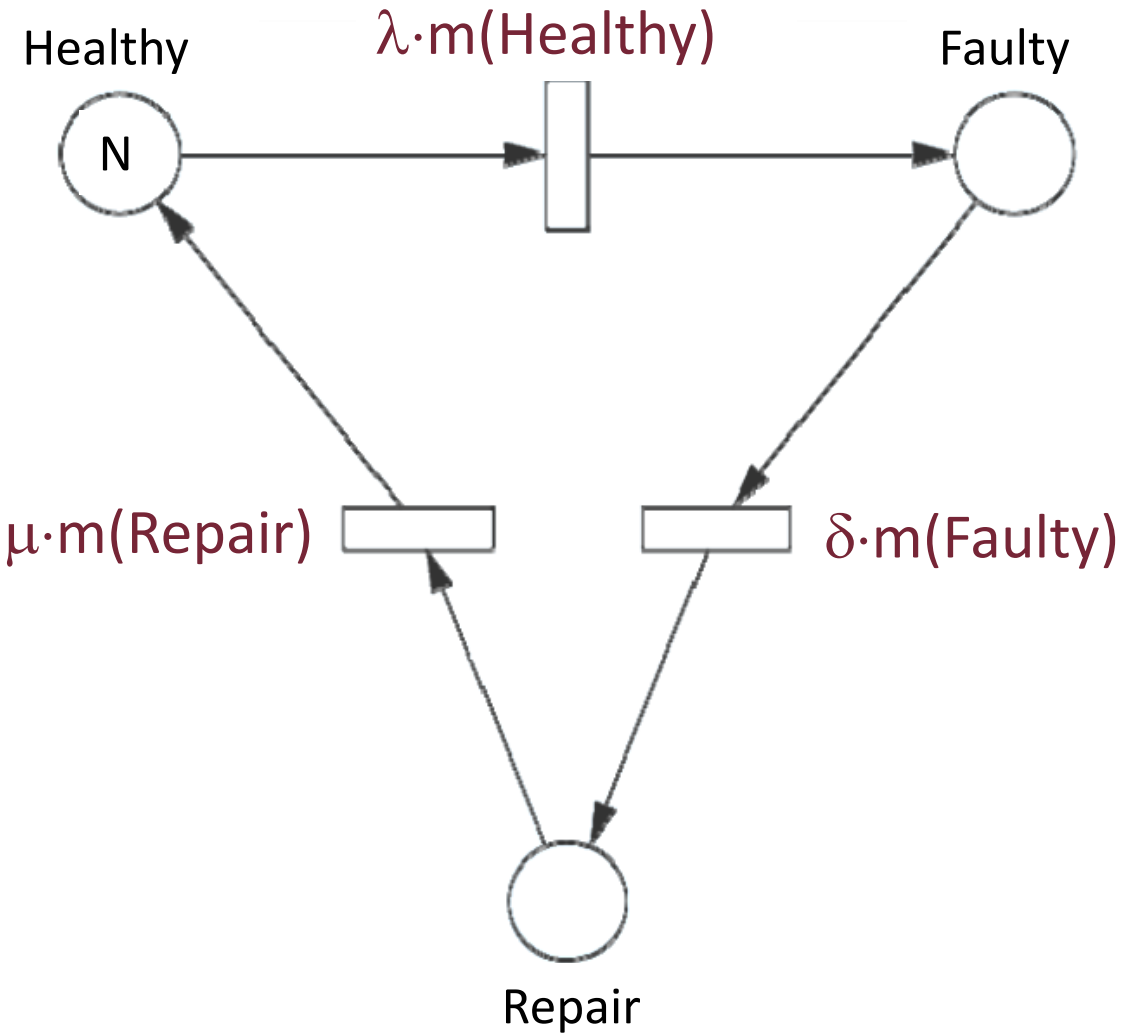
- Állapotpartíciók definiálása: Jelölések alapján
  - Hibamentes U illetve hibás D partíció
- Rendelkezésre állás számítása
  - Közvetlen: U állapotpartíció valószínűsége
  - Reward alapján:
    - if ($m \in U$) then ra=1 else ra=0
    - ra várható értéke: készenlét K=E{ra}

Példa: Redundáns szerverek

- N azonos típusú szerverből álló fürt
  - A rendszer jó, ha legalább egy szerver jó
- Meghibásodás:
  - Egy-egy szerver meghibásodási tényezője λ
  - A szerverek függetlenül hibásodhatnak meg
- Javítás:
  - A detektált hiba javítási ideje μ paraméterű exp. eloszlásfüggvénnyel jellemezhető, egyszerre több szerver is javítható
  - A hiba detektálási ideje δ paraméterű exp. eloszlásfüggvénnyel jellemezhető, egyszerre több szerver hibája is detektálható
- Modell:
  - Helyek: Healthy, Faulty, Repair (jelölés: szerverek száma)
  - Tranzíciók: Meghibásodás, detektálás, javítás (jelölésfüggő tényezők)
  - U állapotpartíció: m(Healthy)>0
  - Rendelkezésre állás: U állapotpartíció valószínűsége

Példa: Redundáns szerverek

- Redukált modell jelölésfüggő paraméterekkel:



Összefoglalás

- Szolgáltatásbiztonság alapjellemzői
  - Megbízhatóság, rendelkezésre állás: Valószínűségi időfüggvények
- Kombinatorikus modellezés: Megbízhatósági blokkdiagramok
  - Soros, párhuzamos komponensek alapképletei
- Állapotfüggő modellezés: Markov láncok
  - Számítás: Állapotpartíciók valószínűsége
- Konkurens modellezés: Sztochasztikus Petri hálók
  - Számítás: Jelölések valószínűsége