

8. gyakorlat – Szolgáltatásbiztonság – Megoldások

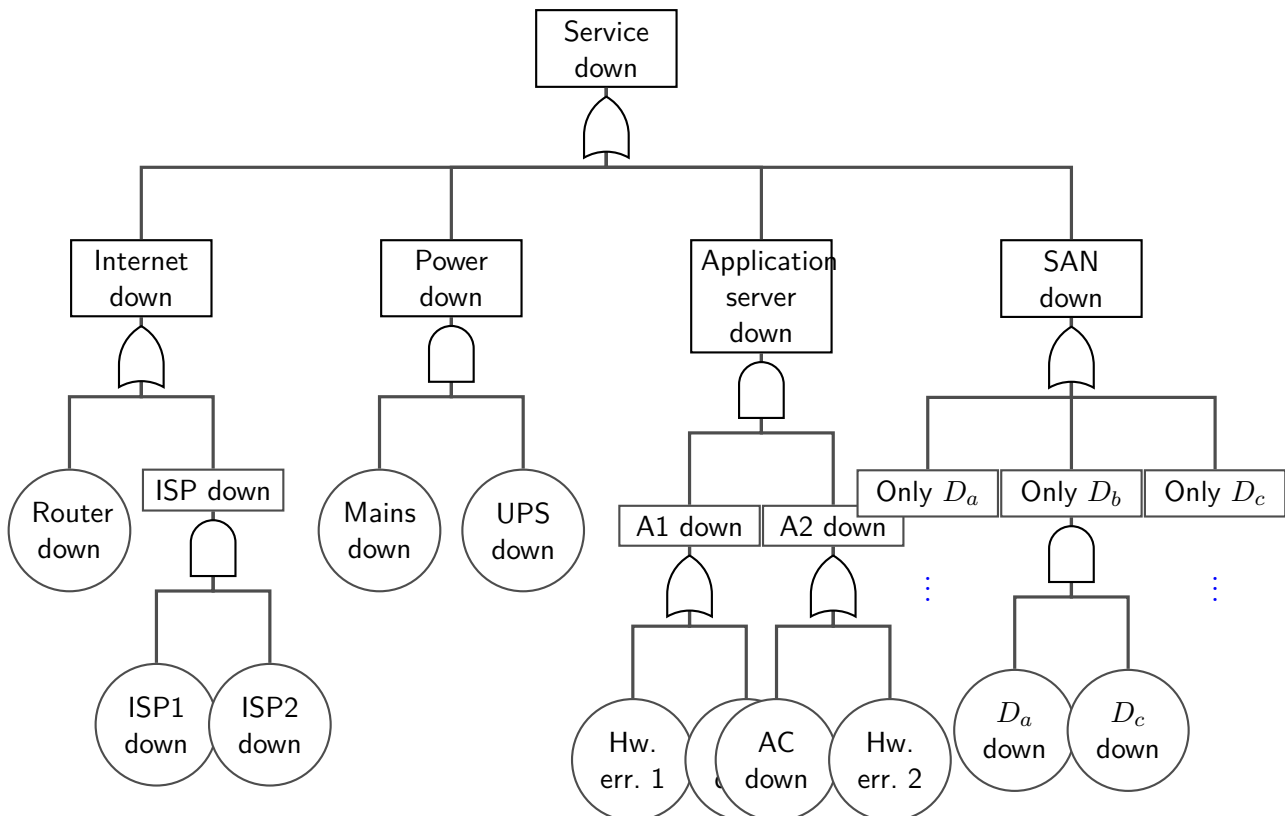
1. Hibafa

Internetes reklámcégünk szolgáltatása ügyfélre szabott hirdetések ajánl fel weboldalak részére. Szolgáltatásunk működéséhez szükséges, hogy a szerverteremből elérhető legyen az internet, rendben legyen a tápellátás, a melegtartalék rendszerben üzemeltetett két alkalmazáserver közül legalább az egyik fusson, és az általuk közösen használt külső SAN háttértár kifogástalan állapotban legyen. Mindkét alkalmazáserver kiesését belső hardware meghibásodás vagy a szerverterem hűtésének leállása okozhatja. A netsatlakozás működése a router üzemképességén múlik, és persze a két ISP legalább egyikének szolgáltatnia kell. A hibatűrő SAN tárolórendszer RAID-5 elven három merevlemezt tartalmaz (D_a, D_b, D_c), és egyetlen (tetszőleges) lemez kiesését még tolerálja. A szerverterem tápellátása mindaddig biztosított, amíg a hálózati tápellátással és a szünetmentes tápegységgel nincs egyszerre gond.

- Rajzolja le a „nem érhető el a szolgáltatás” rendszerszintű hibajelenség hibafáját!
- A hibafa redukció módszerrel azonosítsa a rendszer egyszeres hibapontjait és kritikus eseményeit!
- Az összes elemi hibaállapot tetszőleges időpillanatban $p = 10^{-5}$ valószínűséggel áll fent. Mi következik a rendszerszintű hibajelenségre?
- A kiszámított érték a szolgáltatás melyik szolgáltatásbiztonsági jellemzőjéhez kapcsolódik? Milyen feltételezéseket és közelítéseket kellett tenni az elvégzett számításhoz?

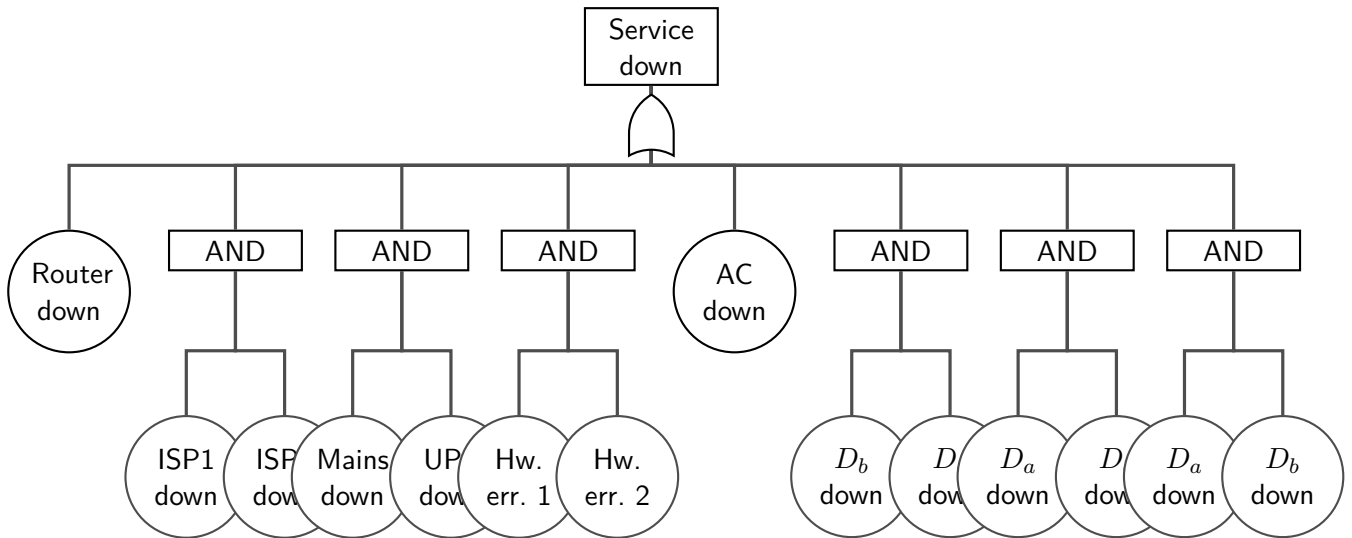
Megoldás

- A „nem érhető el a szolgáltatás” rendszerszintű hibafája:



Jól látható, hogy például a router komponens egyszeres hibapont (SPOF).

- Redukcióval diszjunktív normálformára hozzuk a kifejezést. A redukált hibafában a gyökérellem alatt egy “vagy” kapu van. Ezt leszámítva csak “és” kapuk és elemi események szerepelhetnek.



Az *AC down* rejtett SPOF, ami levezethető az alábbi módon:

$$\begin{aligned}
 (E_1 \vee AC) \wedge (E_2 \vee AC) &= \\
 [(E_1 \vee AC) \wedge E_2] \vee [(E_1 \vee AC) \wedge AC] &= \\
 [(E_1 \wedge E_2) \vee (AC \wedge E_2)] \vee [(E_1 \wedge AC) \vee AC] &= \\
 (E_1 \wedge E_2) \vee (AC \wedge E_2) \vee (AC \wedge E_1) \vee AC &= \\
 (E_1 \wedge E_2) \vee AC &
 \end{aligned} \tag{1}$$

Látható, hogy ha *AC down* fennáll, a kifejezés igaz lesz, vagyis a szolgáltatás elérhetetlenné válik. Tehát az *AC* komponens SPOF a rendszerben.

Kritikus események a *D_a down*, *D_b down*, *D_c down* események.

c. A **rendszer szintű hibajelenség** valószínűsége:

- Az eredeti hibafán:
 - *Internet down*: $p^2 + p$
 - *Power down*: p^2
 - *Application server down*: $4p^2$
 - *SAN down*: $3p^2$

Összesen $9p^2 + p \approx p$ a *Service down* valószínűsége.

- A redukált hibafán: $p + p^2 + p^2 + p^2 + p + p^2 + p^2 + p^2 = 6p^2 + 2p$
 Összesen $6p^2 + 2p \approx 2p$ a *Service down* valószínűsége.

d. A kiszámított érték a **rendelkezésreállítás komplementere**.

Az alábbi feltételezéseket tettük:

- A “vagy” kapcsolatok esetén összeadást használtunk: ez felülről becsül.
- Az “és” kapcsolatok esetén szorzást használtunk: ehhez feltételnünk kell, hogy a kiváltó események függetlenek.

2. Kvantitatív hibamodellezés

A szervereinkhez két évvel ezelőtt 800 darab új, egyforma merevlemezt szereztünk be egyazon gyártó egyazon sorozatából. Egy évvel ezelőtt már csak 600 működött az eredeti készletből (a többit újakkal pótoltuk, de ezt most nem vizsgáljuk), mostanra pedig újabb 150 eszköz mondta fel a szolgálatot.

A lemezek a vizsgált időszak alatt intenzíven, de egyenletesen és egyformán voltak terhelve. A gyártási hibás darabokat előzetes teszteléssel kiszűrtük, az eszközök elöregedése pedig két-három év alatt még nem következik be.

- Mit mondhatunk a merevlemez típus megbízhatósági függvényéről?
- A második bekezdés alapján mi következik a merevlemez erőforrástípus viselkedésére? Hogyan támasztják ezt alá a mért adatok?
- Milyen becslés adható arra, hogy a következő évben mennyi lemezt kell az eredeti készletből pótolni?
- Az adott típusból egyetlen merevlemez a használatbavételétől számítva várhatóan mennyi ideig működőképes? A számítás menete az érdekes, nem kell számszerű eredményt adni.
- Ha az egyik szerverben ezen lemezek közül 2 üzemel melegtartalékban, várhatóan mennyi idő alatt fog mindkettő meghibásodni?
- Ha a meghibásodás után két napot vesz igénybe a csere, mekkora egy merevlemez hely készletléti tényezője?

Megoldás

Kapcsolódó fogalmak: MTTF (vagy MTFF), MTBF, MUT, MDT, MTTR

Érdekes lehet belenézni a Szolgáltatásbiztonságra tervezés tárgy „A szolgáltatásbiztonság alapfogalmai” és a „A szolgáltatásbiztonság analízise” anyagrészeibe (<https://inf.mit.bme.hu/edu/courses/szbt/materials>).

- A megbízhatóság definíciója:

$$r(t) = P(s(t') \in U, \forall t' < t) \quad (2)$$

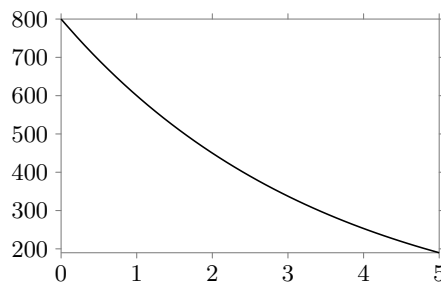
Itt a $t_0 = 1$ év időpontban tudjuk, hogy az eszközök $\frac{600}{800} = \frac{3}{4}$ valószínűséggel működnek, tehát $r(t_0) = \frac{3}{4}$. Elektronikai eszközökre $\lambda(t)$ konstansnak tekinthető, a megbízhatósági függvény pedig $r(t) = e^{-\lambda t}$ alakú.

$$e^{-\lambda \cdot 1 \text{ [év]}} = \frac{3}{4} \quad (3)$$

$$-\lambda \text{ [év]} = \ln \frac{3}{4} \quad (4)$$

$$\lambda = -\ln \frac{3}{4} \left[\frac{1}{\text{év}} \right] = 0,2877 \quad (5)$$

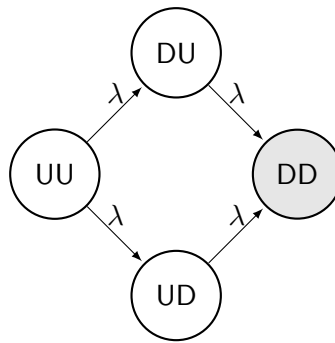
Az ábrán a $800 \cdot \left(\frac{3}{4}\right)^t$ függvény látható, amely megadja az adott időpillanatban még működő merevlemezünk van:



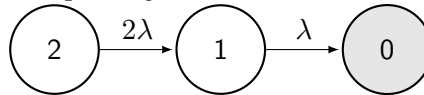
- A kádgörbe alján, a kvázi konstans részen helyezkedik el.
- $450 \cdot \frac{3}{4} = 337,5$ marad, tehát $\lceil 112,5 \rceil = 113$ -at kell majd potenciálisan pótolni.
- A keresett érték az MTTF, amit az alábbi módon számíthatunk ki:

$$\text{MTTF} = \frac{1}{\lambda} \approx 3,4761 \text{ [év]} \quad (6)$$

- Markov-lánc a lehetséges diszkállapotokról λ meghibásodási tényező mellett:



Az egyszerűsített Markov-lánc, az állapotok jelölik a működő diszkek számát:



$$\text{MTTF} = \frac{1}{2} \cdot \frac{1}{\lambda} + \frac{1}{\lambda} = \frac{3}{2} \cdot \frac{1}{\lambda}$$

Magyarázat: azt kell összegezni, mennyi ideig van a rendszer átlagosan a helyes működést jelentő állapotpartícióban. Ez az egyes állapotok esetén $\frac{1}{k \cdot \lambda_i}$, ahol λ_i megadja az egyes állapotokat elhagyó állapotátmeneti valószínűségek összegét.

Mivel $\lambda \approx 0,2877$, így $\text{MTTF} \approx 5,214$ [év]. (1 lemez esetén $\text{MTTF} = 1/\lambda \approx 3,4761$ [év] volt, így ezzel javult az érték)

f. Hibajavítás felvétele a modellbe:

$$\text{MDT} = \frac{2 \text{ [nap]}}{365 \text{ [nap/év]}} \approx 0,0054 \text{ [év]} \quad (7)$$

A készenléti tényező:

$$K = \frac{\text{MUT}}{\text{MUT} + \text{MDT}} \quad (8)$$

Mivel a diszkek javítása cserével történik, ezért $\text{MUT} = \text{MTTF}$ -fel számolhatunk. $\text{MTTF} \approx 3,4761$ [év] (ez nem változott a javítás lehetőségével)

$$K = \frac{\text{MTTF}}{\text{MTTF} + \text{MDT}} \approx 0,9959 \quad (9)$$