A szolgáltatásbiztonság alapfogalmai

Majzik István
majzik@mit.bme.hu

http://www.inf.mit.bme.hu/edu/courses/szbt

Tartalomjegyzék

Motiváció: Hibamentes működés

- Szolgáltatási szint szerződések (SLA):
  - Ügyfél által elvárt jellemzők (pl. rendelkezésre állás)
  - Telekom szolgáltatások szerver rendszerei („carrier grade”):
    „Öt kilences”: 99,999% (5 perc/év kiesés)
- Biztonságkritikus rendszerek:
  - Szabvány előírások a hibák gyakoriságára
  - Biztonságintegritási szintek (Safety Integrity Level)

SIL	Biztonságkritikus funkció hibája / óra
1	$10^{-6} \leq THR < 10^{-5}$
2	$10^{-7} \leq THR < 10^{-6}$
3	$10^{-8} \leq THR < 10^{-7}$
4	$10^{-9} \leq THR < 10^{-8}$

Ha 15 év az élettartam, akkor ez alatt kb. 750 berendezésből 1-ben lesz hiba

Hiba nélküli működés ~ 11.000 év??

Elkerülhetetlen: Hibahatások

Fejlesztési folyamat → **Működő termék**

- Tervezési hibák
- Implementációs hibák

- Hardver hibák
- Konfigurációs hibák
- Kezelői hibák

Fejlesztési folyamat jellemzői:

- Jobb minőségbiztosítás, jobb módszertanok
- De növekvő bonyolultság, nehezebb ellenőrzés

Szokásos becsült értékek 1000 kódsorra:

- Jó kézi fejlesztés és tesztelés: <10 hiba marad
- Automatizált fejlesztés: ~1-2 hiba marad
- Formális módszerek használata: <1 hiba marad

Elkerülhetetlen: Hibahatások

Fejlesztési folyamat → **Működő termék**

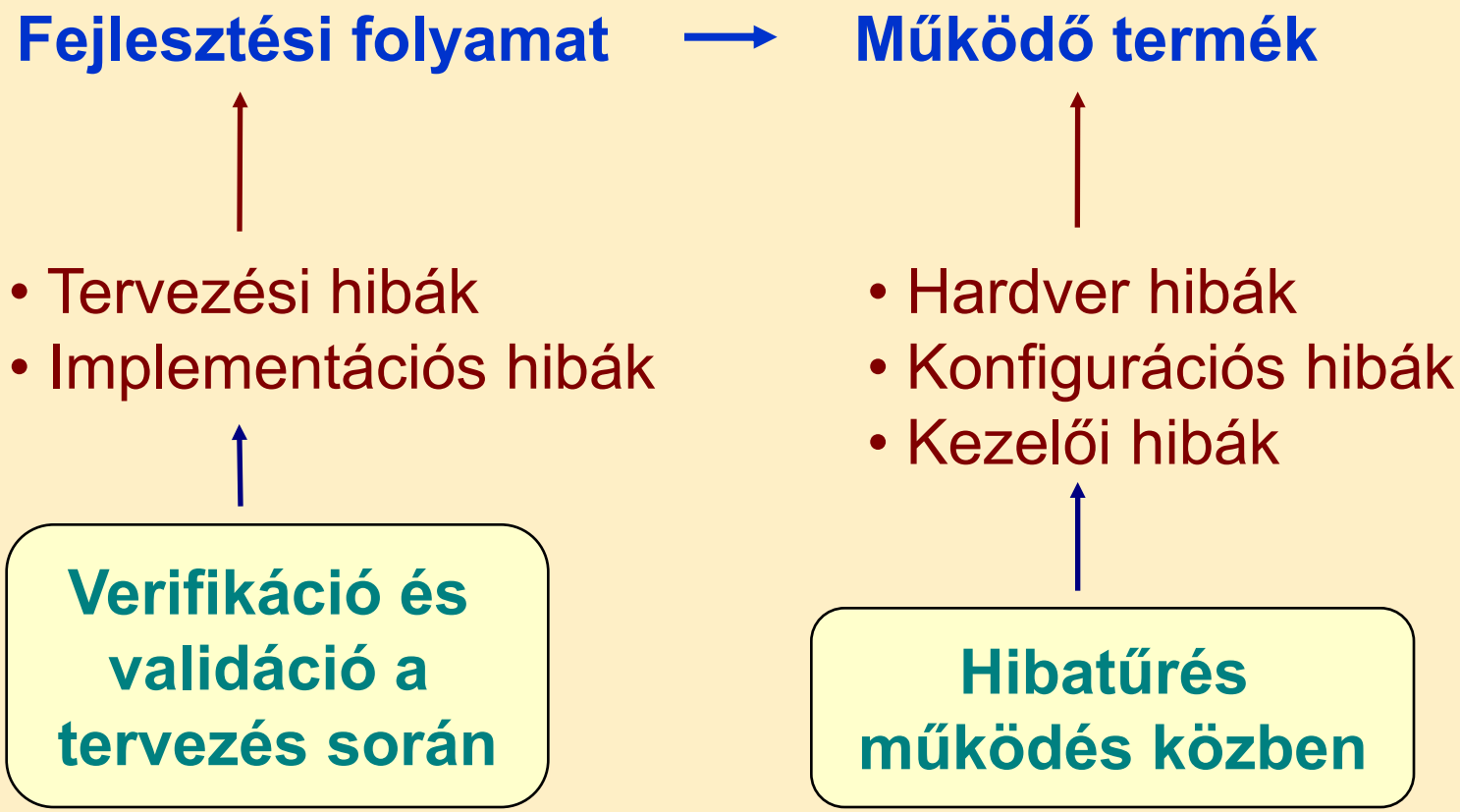
- Tervezési hibák
- Implementációs hibák

- Hardver hibák
- Konfigurációs hibák
- Kezelői hibák

Technológia korlátai:
- Jobb paraméterek, jobb anyagok
- De növekvő bonyolultság (érzékenység)

Szokásos becsült értékek:
- CPU: 10^{-5}…10^{-6} hiba/óra
- RAM: 10^{-4}…10^{-5} hiba/óra
- LCD: ~ 2…3 év élettartam

Elkerülhetetlen: Hibahatások



A hibamentesség jellemzése

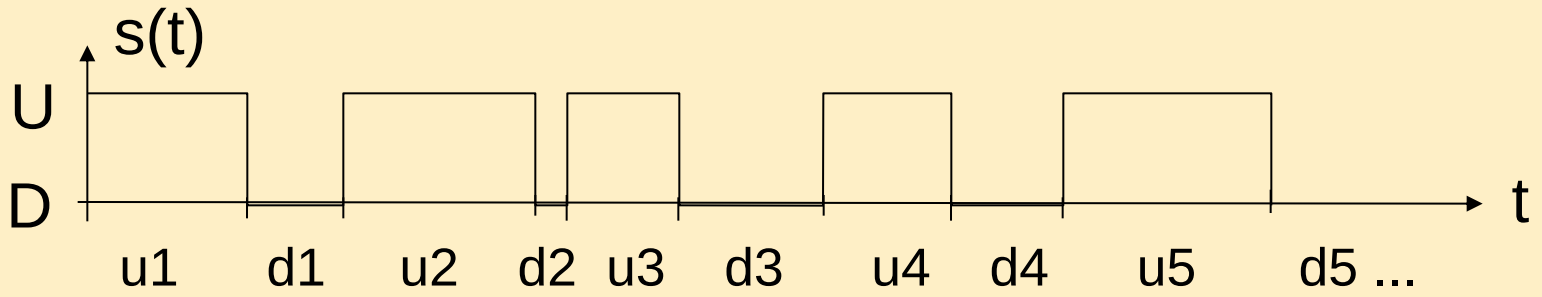
- Felhasználó: Szolgáltatás jellemzői érdeklik
  - Szolgáltatásminőség:
    - Használhatóság, rendelkezésre állás, javíthatóság,...
  - Termékminőség: ezt nyújtja a gyártó
    - Előállítási folyamat (ISO 9000)
- Szolgáltatásbiztonság (dependability):
  - Milyen biztonsággal képes ellátni feladatait a rendszer?
  - Képesség: igazoltan bízni lehet a szolgáltatásban
    - Igazoltan: elemzésen, méréseken alapul
    - Bizalom: szolgáltatás az igényeket kielégíti
  - Összetett fogalom

A szolgáltatásbiztonság jellemzői

- A szolgáltatásbiztonság (dependability) alapjellemzői:
  - Rendelkezésre állás:
    - Helyes szolgáltatás valószínűsége (javítást is figyelembe véve)
  - Megbízhatóság:
    - Folyamatosan helyes szolgáltatás valószínűsége (az első hibáig)
  - Biztonság(osság):
    - Elfogadhatatlan kockázattól való mentesség valószínűsége
  - Integritás:
    - Hibás változás, változtatás elkerülésének lehetősége
  - Karbantarthatóság:
    - Javítás és fejlesztés lehetősége
- Az adatbiztonság (security) alapjellemzői:
  - Rendelkezésre állás
  - Integritás
  - Bizalmasság:
    - Jogosulatlan információközlés elkerülésének lehetősége

Megbízhatósági mértékek: Várható értékek

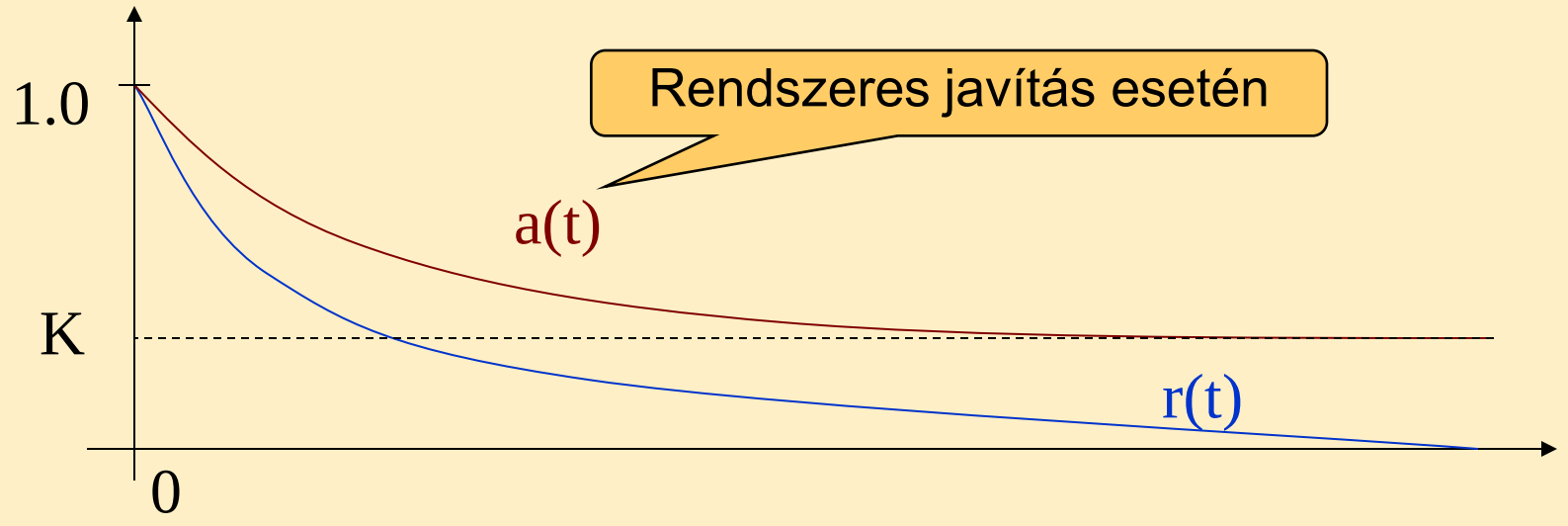
- Állapot particionálás: s(t) rendszerállapot
  - Hibás (Down) - Hibamentes (Up) állapotpartíció



- 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 állapot ideje: MDT = MTTR = E{di}
    (Mean Down Time, Mean Time To Repair)
  - Hibák közötti idő: MTBF = MUT + MDT
    (Mean Time Between Failures)

Megbízhatósági mértékek: Időfüggvények

- Valószínűség időfüggvények
  - Rendelkezésre állás (availability):
    $a(t) = P\{ s(t) \in U \}$ (közben meghibásodhat)
  - Készenlét (asymptotic availability):
    $K=\lim_{t\to\infty} a(t)$ (aszimptotikus)
  - Megbízhatóság (reliability):
    $r(t) = P\{ s(t')\in U, \forall t'<t \}$ (nem hibásodhat meg)



Megbízhatósági mértékek: Alkatrész szinten

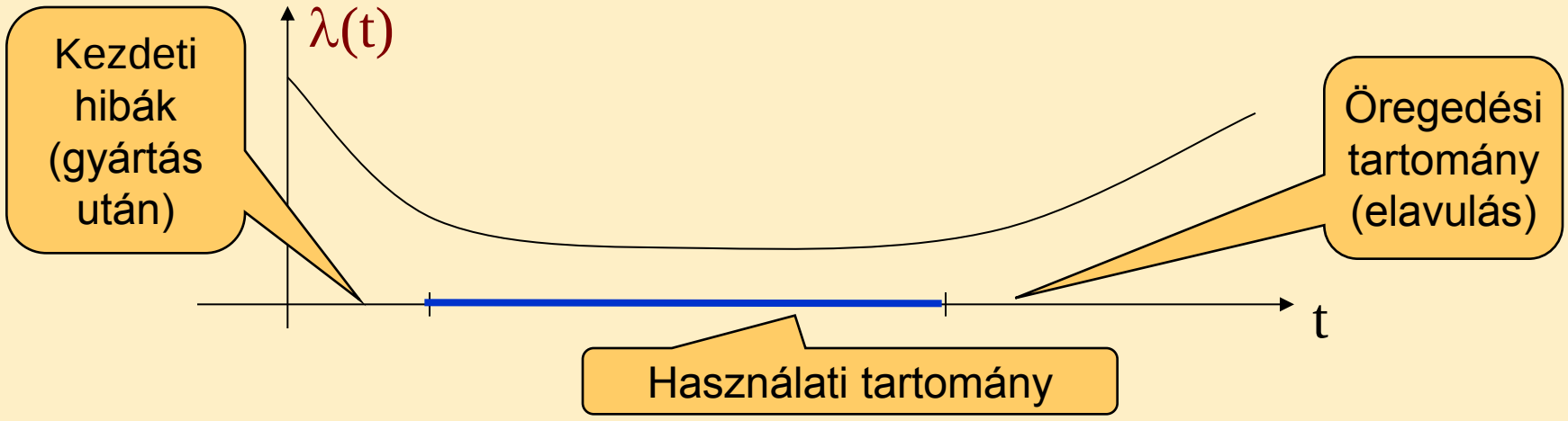
- Meghibásodási tényező (gyakoriság):
  - A rendszer mekkora valószínűséggel fog éppen t-ben elromlani, feltéve, hogy t-ig jól működött:

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

másként felírva:

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

  - Elektronikai alkatrészekre:



Alkatrészek használati tartománya

Elektronikai alkatrészek használati tartományában:

- Konstans a meghibásodási tényező:

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

- Megbízhatóság:

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

- Első hiba bekövetkezése:

$$\mathrm{MTFF} = \frac{1}{\lambda}$$

Rendelkezésre állás követelményei

Rendelkezésre állás	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

95%-os rendelkezésre állású számítógépekből épített elosztott rendszer rendelkezésre állása:

- 1 szgép: 95% a rendelkezésre állás
- 2 szgép: 90%
- 5 szgép: 77%
- 10 szgép: 60%

Példa: SAFEDMI mozdonyvezetői kezelőfelület

Mozdony-vezető

DMI

EVC
European Vital Computer

Maintenance Centre

- Safety Integrity Level 2
  - Információ megjelenítés
  - Parancs feldolgozás
  - EVC kommunikáció
- Biztonságos vezeték nélküli kommunikáció
  - Konfiguráció
  - Diagnosztika
  - Szoftver frissítés

Példa: SAFEDMI követelmények

- Biztonság:
  - Biztonságintegritási szint: SIL 2
  - Biztonsági funkció elviselhető hibája óránként (Tolerable Hazard Rate): $10^{-7} <= THR < 10^{-6}$ (10^6 óra: ~114 év)
- Megbízhatóság:
  - Mean Up Time: MUT > 5000 hours (5000 óra: ~ 7 hónap)
- Rendelkezésre állás (készenlét):
  - A = MUT / (MUT+MDT), A > 0.9952
    Hibás állapot: évenként kevesebb, mint 42 óra
    MDT < 24 óra, ha a fenti MUT biztosítható

Tartalomjegyzék

A „hiba” fogalom finomítása

- Hibajelenség (failure):
  A specifikációnak nem megfelelő szolgáltatás
  - Értékbeli / időzítésbeli, katasztrofális / „jóindulatú”
- Hiba (error):
  Hibajelenséghez vezető rendszerállapot
  - Lappangó → detektált
- Hibaok, meghibásodás (fault):
  A hiba feltételezett oka
  - Hatás: alvó → aktív
  - Fajta: véletlen vagy szándékos, időleges vagy állandósult
  - Eredet: fizikai/emberi, belső/külső, tervezési/működési

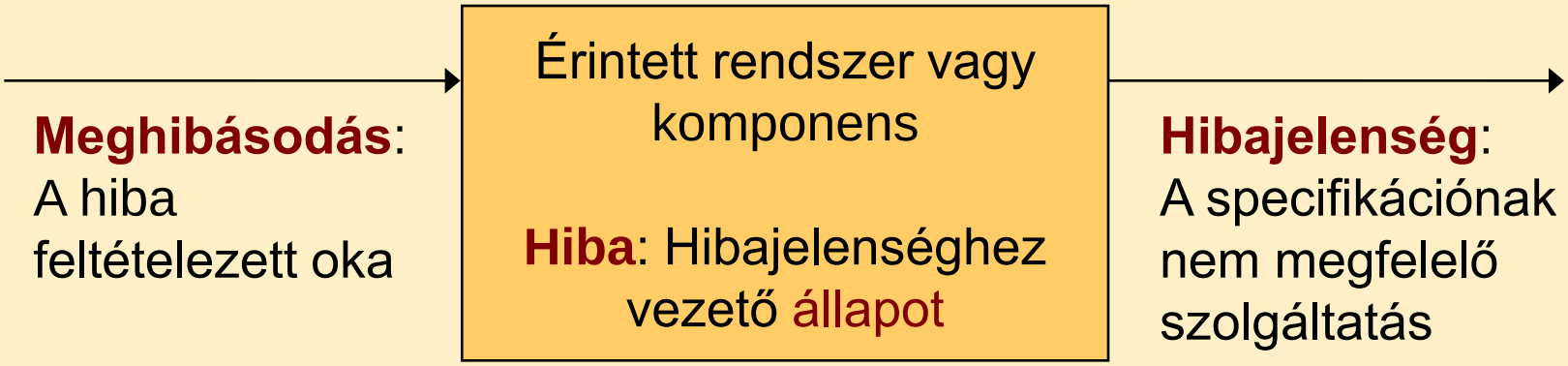
Tipikus meghibásodások

Fajta	Eredet	Hely	Fázis	Idő	Példa
Véletlen	Fizikai	Belső	Működés	Állandó-sult	Maradandó hiba
Véletlen	Fizikai	Külső	Működés	Időleges	Tranziens hiba
Véletlen	Emberi	Belső	Tervezés	Állandó-sult	Tervezési hiba
Véletlen	Emberi	Külső	Működés	Időleges	Kezelési hiba
Szándé-kos	Emberi	Külső	Működés	Állandó-sult	Rongálás
Szándé-kos	Emberi	Külső	Működés	Időleges	Behatolás

Szoftver hibák

- Szoftver hiba: Állandósult, tervezési hiba
- Aktiválás a működési profil függvénye
  - Adott bemeneti tartomány (program útvonal) aktivál
- Becslési módszerek:
  - Megbízhatóság arányos:
    Tesztelés után bennmaradó hibák számával
  - Bennmaradó hibák száma arányos:
    Időegység alatt detektált hibák számával a tesztelés végén
  - Statisztikai módszerekkel becsülhető,
    meddig kell a tesztelést folytatni
    adott megbízhatóság eléréséhez

Mi befolyásolja a szolgáltatásbiztonságot?



Meghibásodás → Hiba → Hibajelenség hatáslánc példák:

Meghibásodás	Hiba	Hibajelenség
Kozmikus sugárzás egy bitet átbillent a memóriában	→Hibás memóriacella olvasása	→Robotkar a falnak ütközik
Programozó csökkentés helyett növel egy változót	→Vezérlés ráfut, a változó értéke hibás lesz	→A számítás végeredménye rossz

A hatáslánc befolyásolása

- Meghibásodási tényező csökkentése
  - Jobb minőségű komponensek
  - Szigorúbb fejlesztési folyamat (ellenőrzés, tesztelés)
  - A meghibásodás-mentesség nem garantálható (csökkenő chipméretek, bonyolultabb programok)
- Hibajelenség kialakulásának megakadályozása
  - Rendszerstruktúra kialakítása: redundancia
- Hibatípusok:
  - Előre figyelembe vehető hibák: optimális kezelés a tervezési folyamat során
  - Előre figyelembe nem vehető hibák: megfelelő rendszerstruktúra kialakítása szükséges

Tartalomjegyzék

Eszközök

- Hiba megelőzés: Meghibásodás megakadályozása
  - Fizikai hibák: jó minőségű alkatrészek
  - Tervezési hibák: jól meghatározott folyamatok, jó eszközök
- Hiba megszüntetés:
  - Fejlesztés közben: verifikáció, tesztelés, javítás
  - Próbaüzem során: monitorozás, diagnosztika, javítás
- Hibatűrés: Szolgáltatást nyújtani hiba esetén is
  - Működés közben: hibakezelés, redundancia használat
- Hiba előrejelzés: Hibák és hatásuk becslése
  - Mérés és „jóslás”, megelőző karbantartás

A redundancia megjelenése

1. Hardver redundancia
   - Többlet hardver erőforrások
2. Szoftver redundancia
   - Többlet szoftver modulok
3. Információ redundancia
   - Többlet információ a hibajavítás érdekében
4. Idő redundancia
   - Ismételt végrehajtás, hibakezelés többlet ideje

Együttes megjelenés!

A redundancia típusainak összehasonlítása

Redundancia / tulajdonság	Hideg tartalék (passzív redundancia)	Langyos tartalék (másodlagos funkciók)	Meleg tartalék (aktív redundancia)
Alapelv	Csak hiba esetén aktiválva	Csökkentett terheléssel működik	Ugyanúgy működik, mint az elsődleges
Előnye	Nem hibásodik meg a passzív komponens	Kisebb meghibásodási tényező	Gyorsan átveheti az elsődleges helyét
Hátránya	Lassan veszi át az elsődleges helyét	Közepes sebességű feladat átvétel	Azonos meghibásodási tényező
Példa	Kikapcsolt tartalék számítógép	Naplózó számítógép belép elsődlegesként	Árnyék számítógép

1. Hardver redundancia

- Hardver állandósult hibák esetén
  - Tipikus cél az egyszeres hibapont (single point of failure, SPOF) elkerülése

- Megjelenése:
  - Eleve a rendszerben lévő redundáns komponensek
    - Elosztott rendszer, adaptív átkonfigurálás
  - Hibatűréshez betervezett redundancia (tartalékolás)
    - Kettőzés
    - TMR: Triple-modular redundancy
    - NMR: N-modular redundancy

2. Szoftver redundancia

Használat:

1. Szoftver tervezési hibák esetén:
   - Egyszerű többszörözés nem segít...
   - Eltérő tervezésű redundáns modulok szükségesek
     Variánsok: azonos specifikáció, de
     - eltérő algoritmus, adatstruktúrák
     - más fejlesztési környezet, programnyelv
     - elszigetelt fejlesztés
2. Időleges (hardver) hibák esetén:
   - Ismételt végrehajtás esetén a hiba nem jelentkezik
   - Hibahatások kiküszöbölése a fontos (helyreállítás)

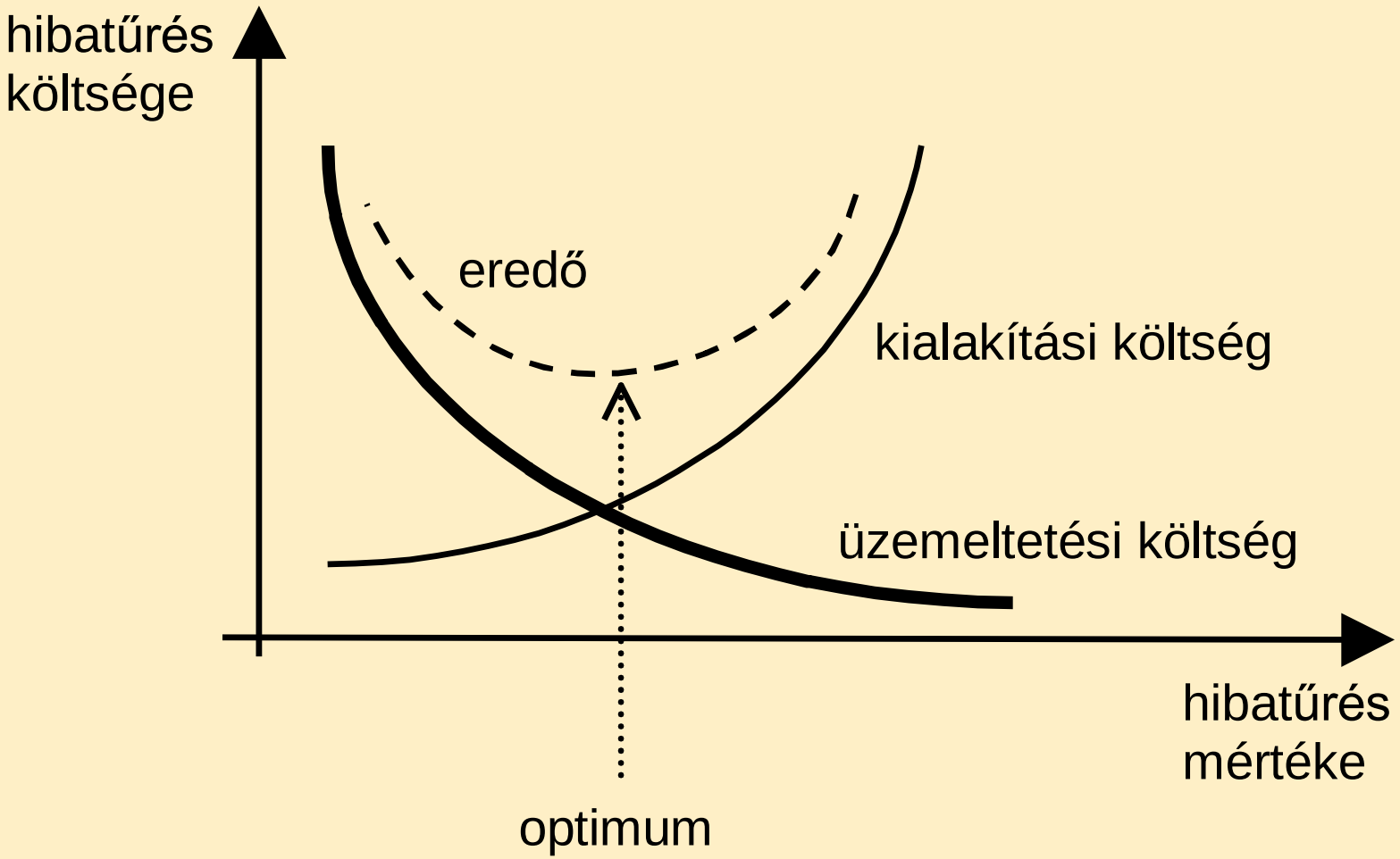
3. Információ redundancia

- Hibajavító kódolás
  - Memóriák, háttértárak, adatátvitel esetén
  - Pl. Hamming-kód, Reed-Solomon kódok
  - Korlátozott hibajavító képesség
    - Hosszú idejű adatstabilitás rossz lehet ("felgyűlnek" a hibák)
    - Háttértárak: "memory scrubbing" folyamatos olvasás és javítva visszaírás
- Többpéldányos (elosztott) adattárolás
  - Probléma: Hozzáférések konzisztenciájának biztosítása
    - Egypéldányos sorosíthatóság

4. Idő redundancia

- Tiszta eset: utasítás újrapróbálás (retry)
  - Alacsony hardver szinten: processzor utasítás
  - Időleges hibák esetén hatásos
- Idő redundancia “velejárója” a többi típusnak
  - Valósidejű rendszerek: tervezési szempont, hogy mennyire garantálható a hibakezelés ideje
    - Állandósult hardver hibák: melegtartalék, hiba maszkolása
    - Időleges hardver hibák: előrelépő helyreállítás
    - Szoftver tervezési hibák: aktív redundancia (aktív variánsok)

Költségoptimalizálás



Összefoglalás

- Szolgáltatásbiztonság
  - Jellemzők: Megbízhatóság, rendelkezésre állás, biztonság, integritás, karbantarthatóság
  - Hatáslánc: Meghibásodás $\rightarrow$ hiba $\rightarrow$ hibajelenség
  - Eszközök: Hiba megelőzés, hiba megszüntetés, hibatűrés, hiba előrejelzés
- Hibatűrés
  - Redundancia megjelenése: Szoftver, hardver, idő, információ redundancia
  - Redundancia típusa: Meleg, langyos, hideg tartalék