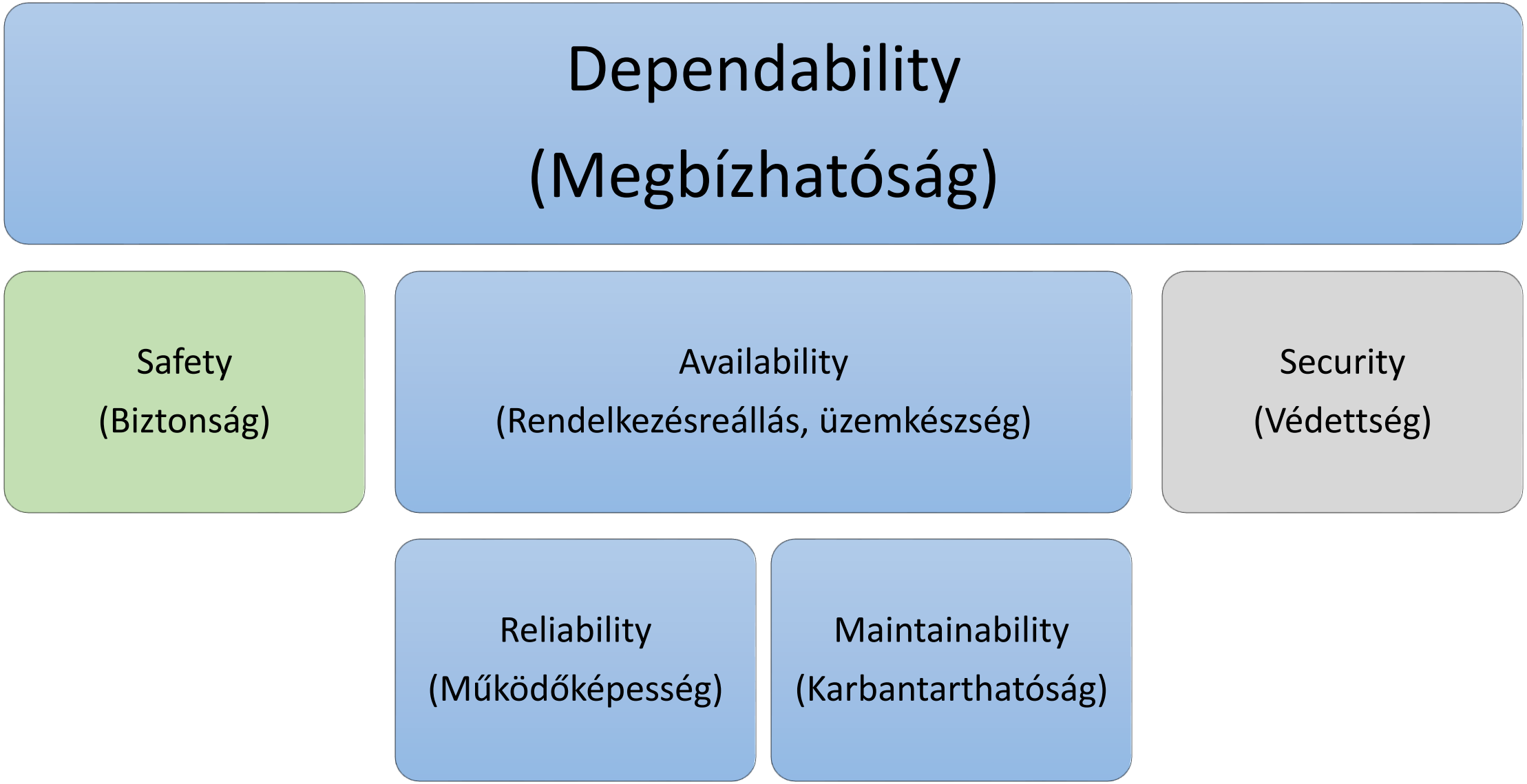
Közlekedési automatika MSc.

BMEKOKAM202

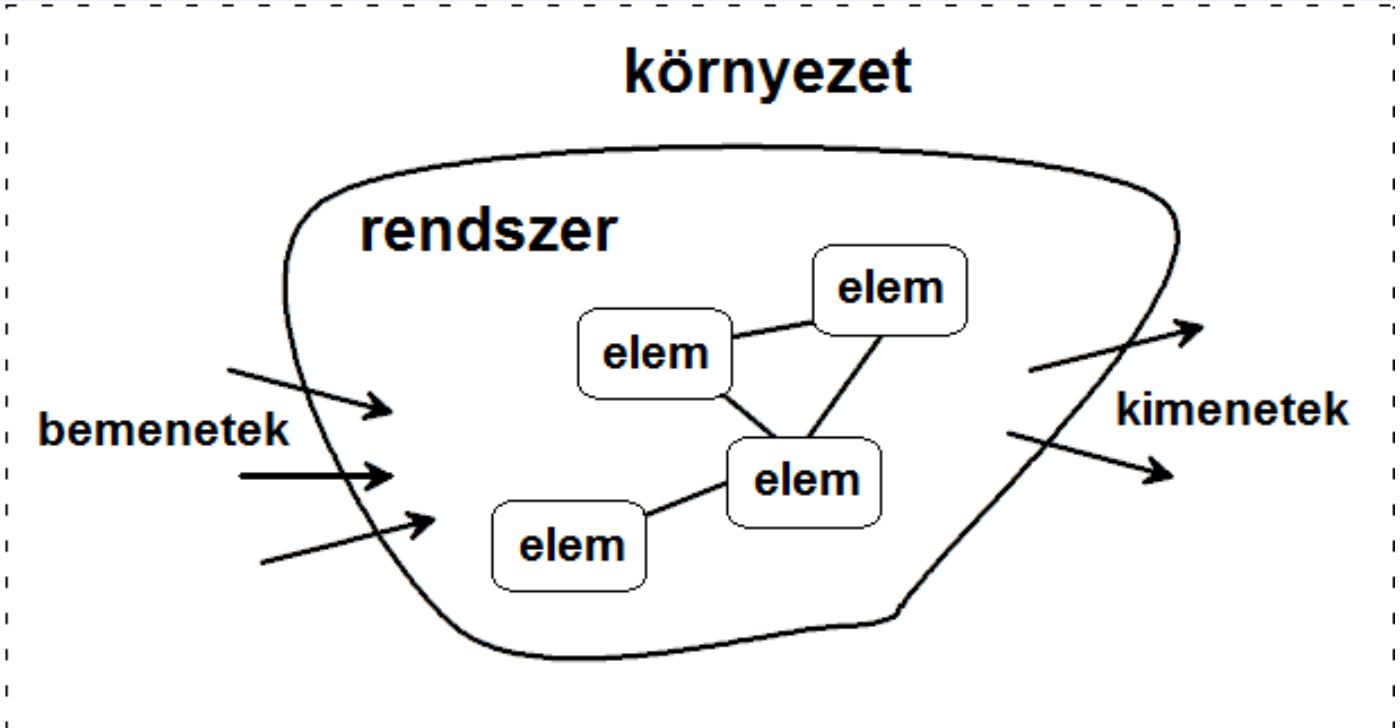
Fogalmak - biztonság

(Ismétlés)

RAMS-S


Dependability
(Megbízhatóság)
Safety
(Biztonság)
Availability
(Rendelkezésreállás, üzemkészség)
Security
(Védettség)
Reliability
(Működőképesség)
Maintainability
(Karbantarthatóság)

Rendszer	• egymással kölcsönhatásban álló elemek együttese • közös ismérvek alapján együvé tartozó, egymással kapcsolatban álló elemek, melyek egészet alkotnak • elemek és az elemek közötti kapcsolatok
Elem	a rendszer legkisebb önálló egysége
Részrendszer	a rendszer olyan része, amely egy önálló egészet alkot, és további részekre bontható
Alrendszer	olyan részrendszer, amely egy adott funkcióterületet fog át
Környezet	a rendszer működésére hatást gyakorló elemek (nem képezik a rendszer része)



Biztonságkritikus rendszerek

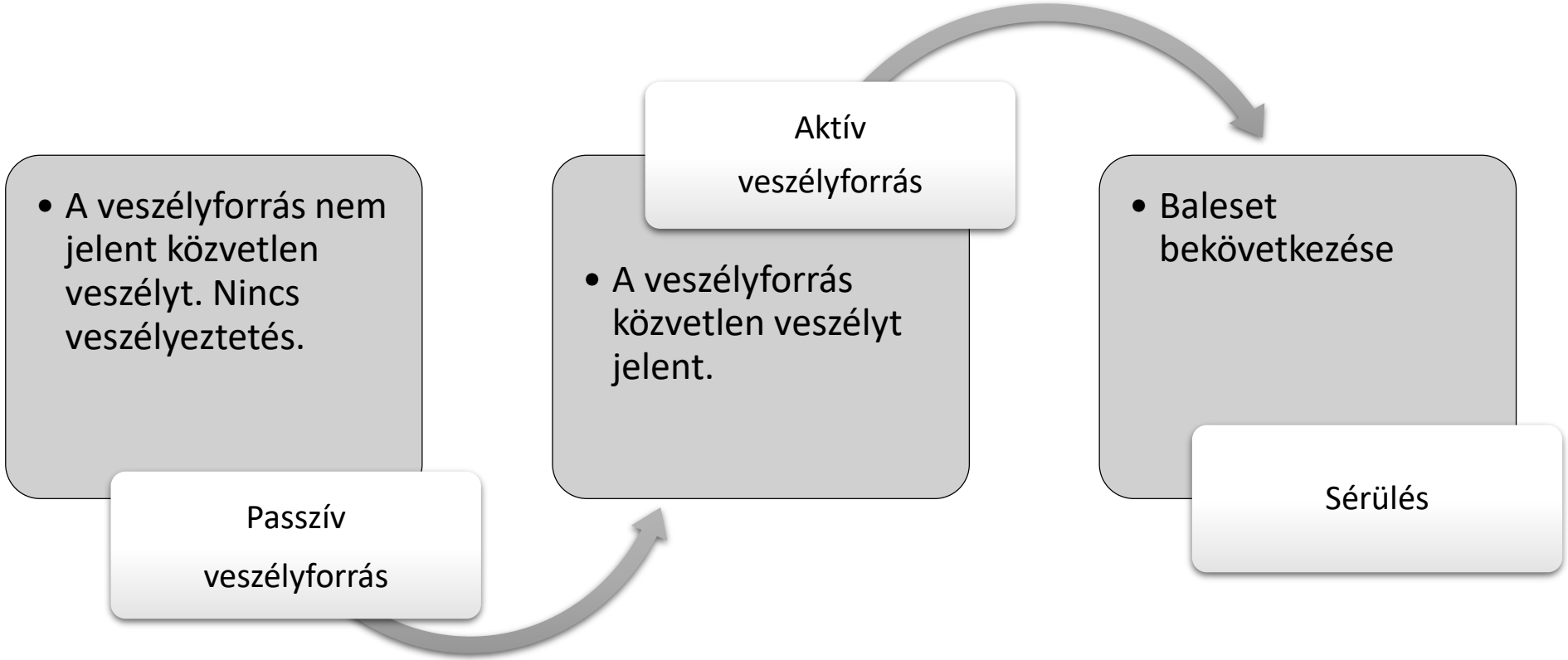
- Biztonságkritikus rendszer: a hibás működés emberéletet veszélyeztethet.
  - Pl. vasúti biztosítóberendezések, vonatbefolyásoló berendezések, gépjárművek beágyazott (pl. vezetéstámogató) rendszerei, atomerőművek, vegyi művek folyamatirányító berendezései
- Beágyazott rendszer: valamilyen speciális feladatot ellátó számítógép.
- Biztonság?

Biztonság

- egy rendszer azon tulajdonsága, hogy nem veszélyezteti az emberi életet és a környezetét (általánosan)
- az elfogadhatatlan kockázatoktól való mentesség (pl. MSZ EN 50126, IEC 61508)
- az ésszerűtlen kockázatok hiánya (ISO 26262)
- az elfogadhatatlan károk kockázatától való mentesség (EUROCONTROL)
- az az állapot, amikor a repüléssel összefüggő kockázatok amelyek közvetve vagy közvetlenül a repülőgépek üzemeltetéséhez kapcsolódnak, elfogadható szintre vannak csökkentve, és ott kontrollálva vannak (ICAO)

Baleseti eseménylánc

- Veszély: sérülés okozásának a lehetősége
- Kár: fizikai sérülés vagy az emberi egészség károsodása, direkt vagy indirekt módon, javak károsodásának vagy a környezet károsodásának az eredményeként



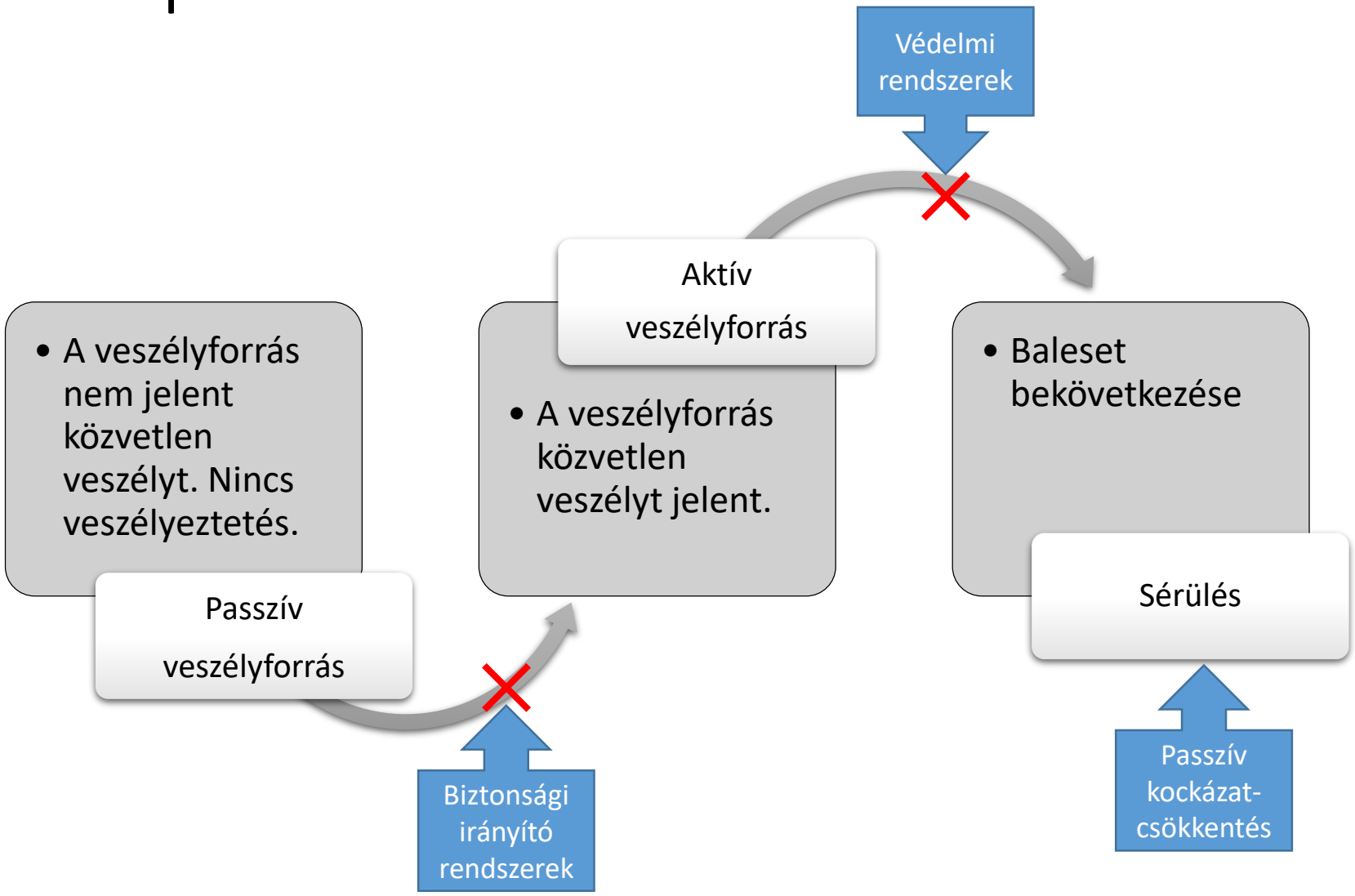
Kockázat

- Kockázat: (adott veszélyből származó) káresemény fellépési valószínűségének (gyakoriságának) és a kárkövetkezmény súlyosságának kombinációja (esetlegesen további paraméterekkel kombinálva).
- Szubjektív/objektív
- Meghatározható minőségileg/ mennyiségileg
- Egyéni/kollektív

→ Kockázatcsökkentés/ kockázatmentesség

Gyakoriság		Súlyosság			
		Katasztro-fális 4	Kritikus 3	Csekély 2	Elhanya-golható 1
gyakori	A				
valószínű	B				
néha	C				
alig	D				
valószínűtlen	E				
rendkívül valószínűtlen	F				

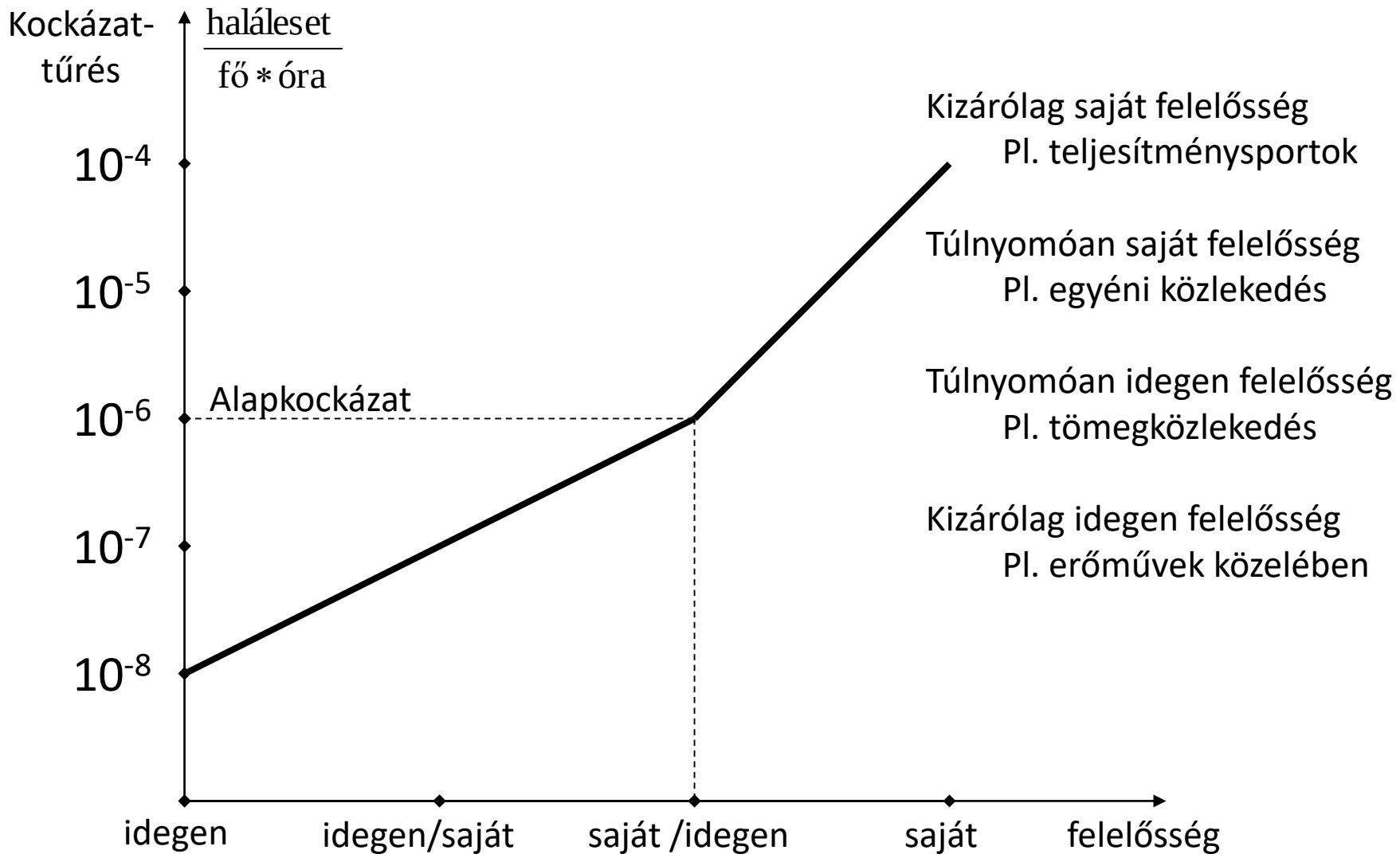
Aktív és passzív kockázatcsökkentés



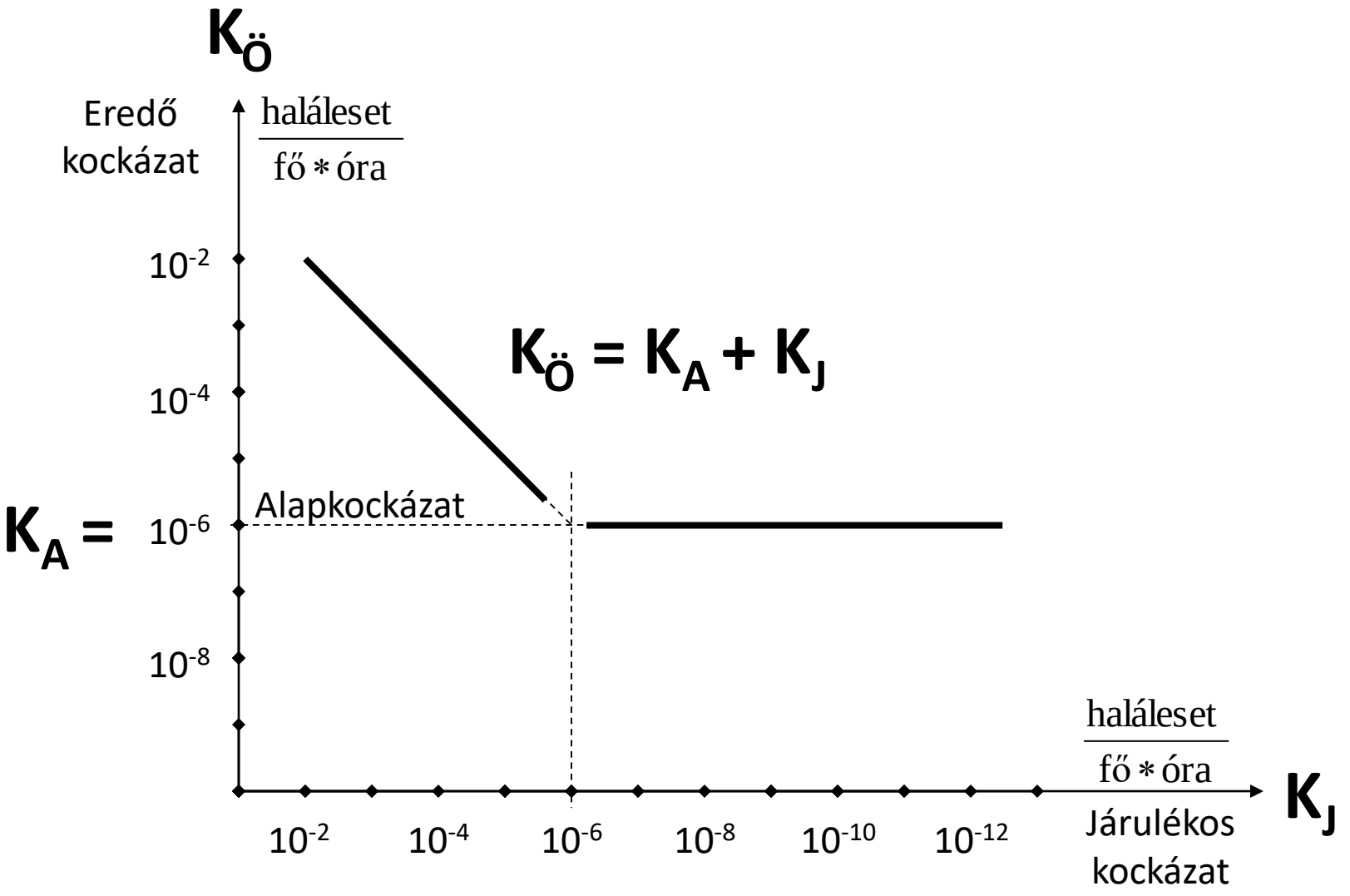
Kockázatcsökkentő/biztonsági intézkedések - példák

- aktív kockázatcsökkentés/biztonság
  - biztonsági irányítórendszer
    - Utolérés kizáró berendezés
    - Légi irányítás (humán+műszaki támogatás)
  - védelmi rendszer
    - Menetstabilizáló rendszerek
    - Éberségi, vonatmegállító rendszerek
    - TCAS (Traffic collision avoidance system)
- passzív kockázatcsökkentés/biztonság
    - Légzsák, gyűrődési zóna
    - Légiutas-kísérő felszállás előtti útmutatója

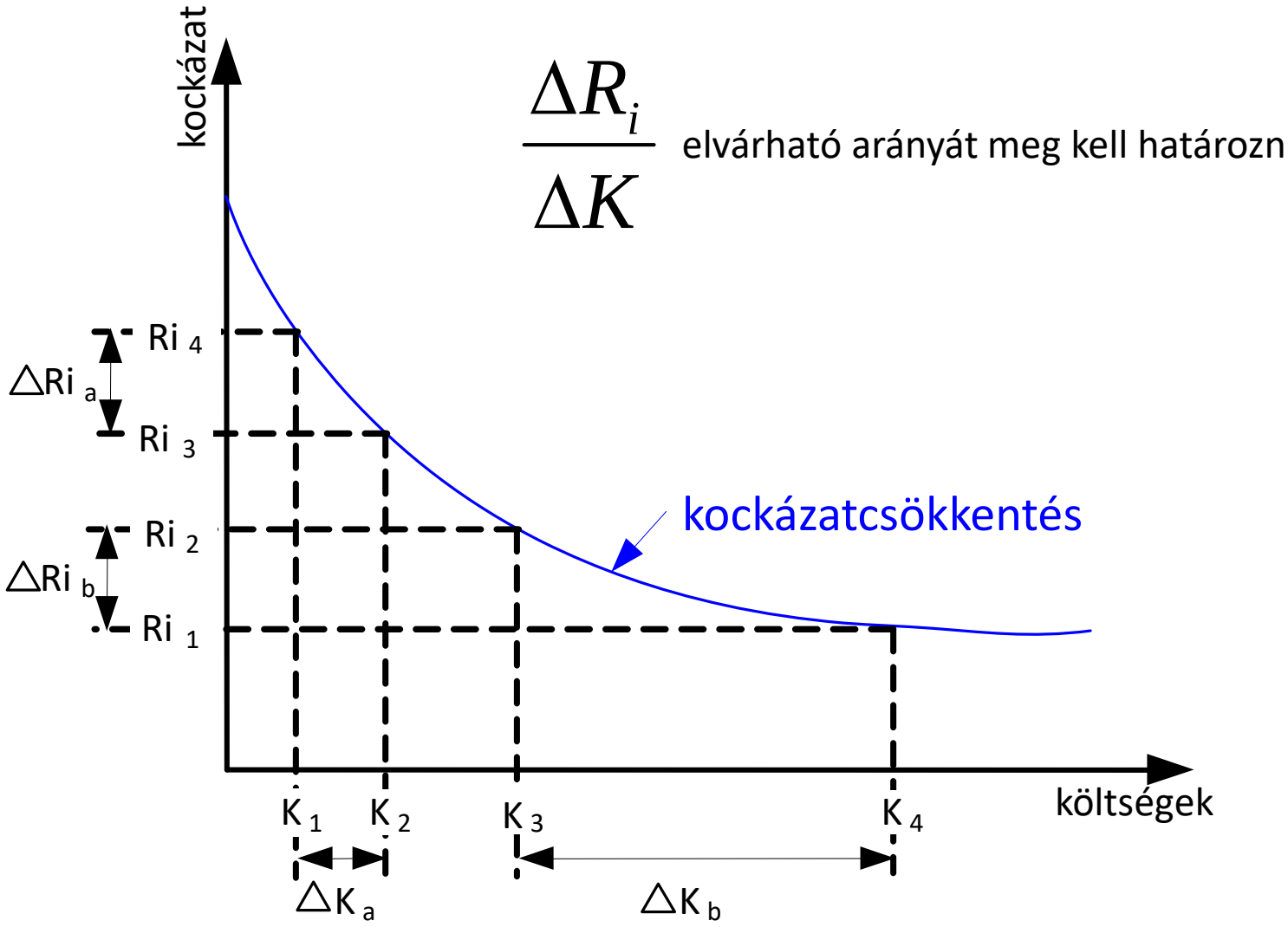
A kockázattűrés függése a felelősségtől



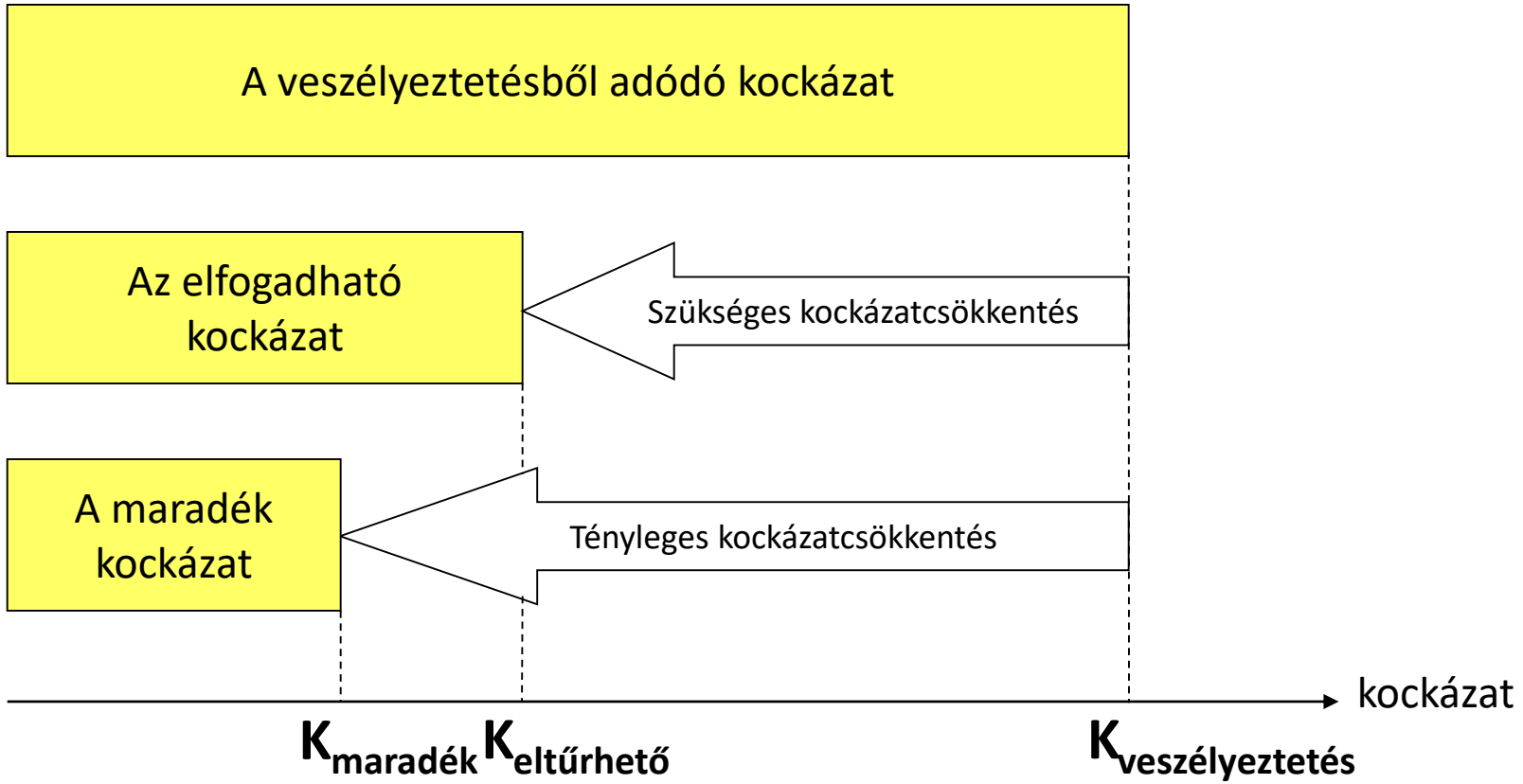
Alap- és járulékos kockázat



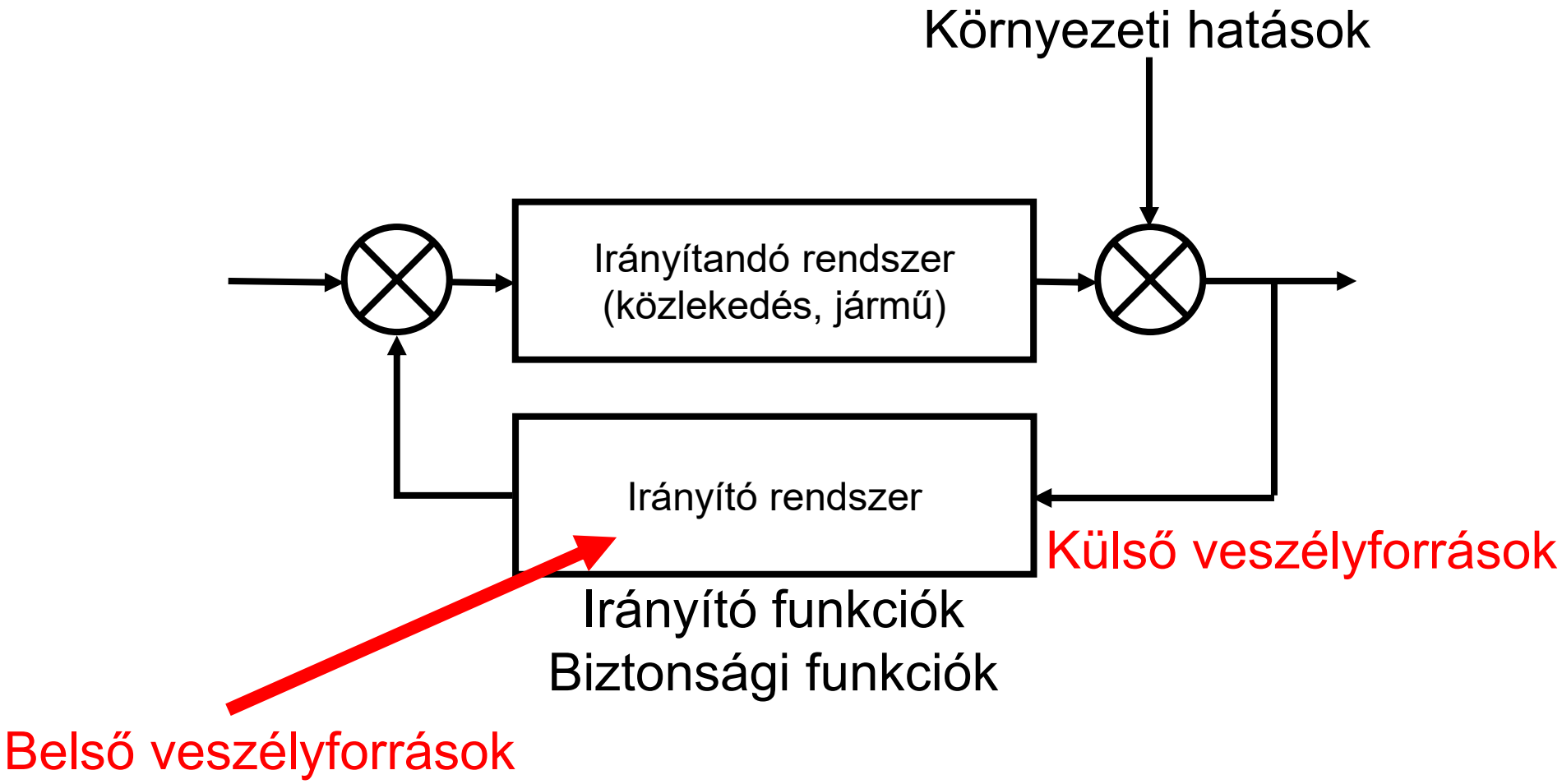
A kockázatcsökkentés hatékonysága



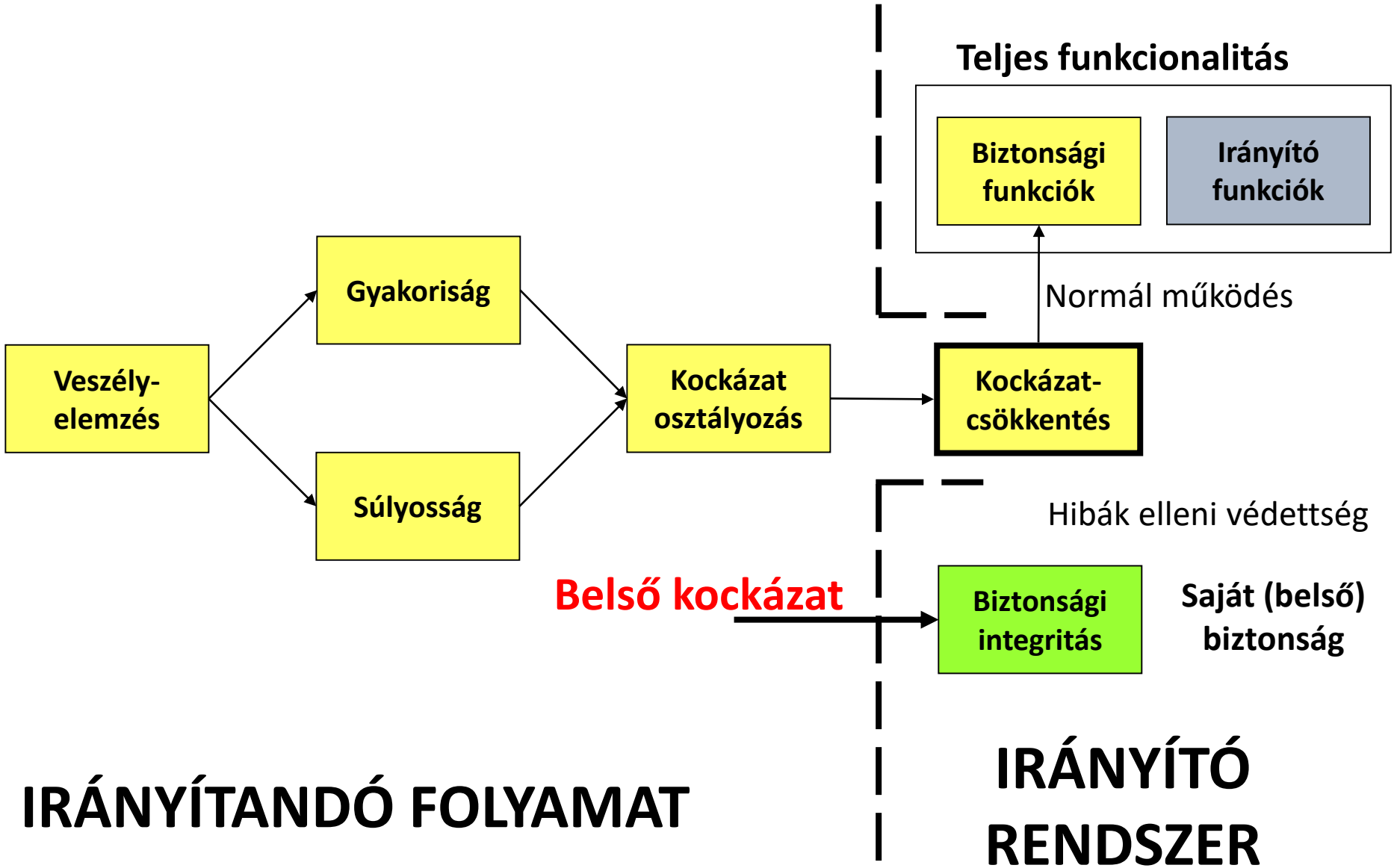
Kockázatcsökkentés – Kockázatmenedzselés



Az irányító rendszer szerepe



Biztonsági funkciók – Biztonsági integritás



A biztonsági rendszerek belső veszélyforrásai

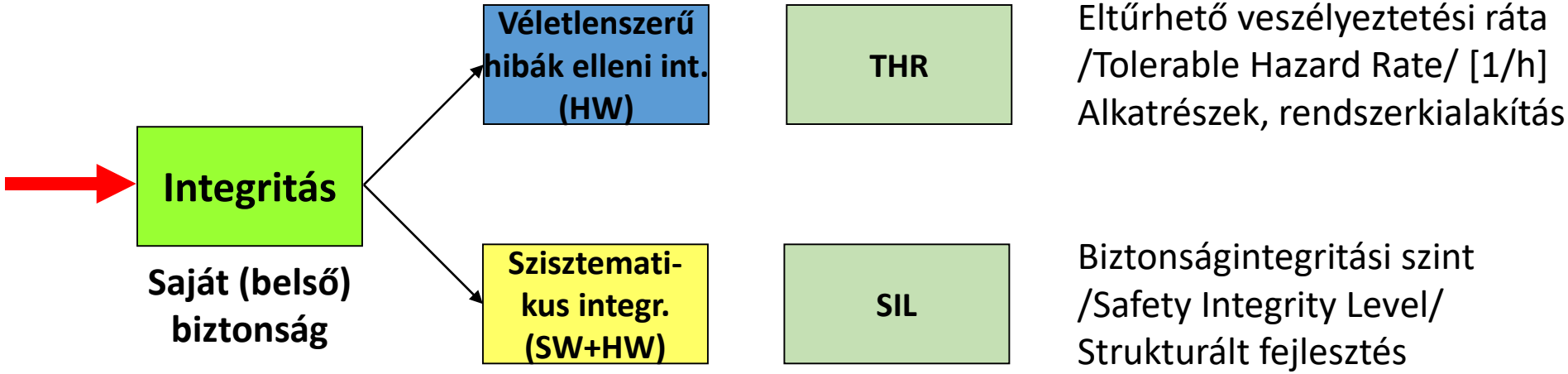
Szisztematikus hibák

- A rendszer **létrehozása során** elkövetett emberi hibák, amelyek a rendszer üzemelése során helytelen működést okoznak.
- Specifikációs hibák, tervezési hibák, gyártási hibák, szoftverhibák stb.
- Fellépési gyakoriság nem adható meg.

Véletlenszerű hibák

- A rendszer **üzemelése során** fellépő meghibásodások.
- Fellépési gyakoriságuk megadható.
- A fellépési gyakoriságot befolyásolja az üzemmód, környezeti hatások, túlterhelés stb.

Biztonsági integritási szintek és hibakezelés



Biztonsági stratégiák

MŰKÖDŐKÉPESSÉG FENNTARTÁSA Megbízhatóságnövelő módszerek	**SAFE-LIFE** Tökéletesség, hibakizárás (egy elem)
	FAULT-TOLERANT Hibatűrés, hibahatás maszkolása (redundancia)
BIZTONSÁGI ÁLLAPOT ELÉRÉSE	**FAIL-SAFE** Hibabiztos, akadályozó állapot Azonnali vagy szabályozott leállás

AZ IRÁNYÍTOTT FOLYAMAT JELLEGÉTŐL FÜGGŐ VÁLASZTÁS

- BIZTONSÁG = MŰKÖDŐKÉPESSÉG
  Pl. repülés → SAFE-LIFE FAULT-TOLERANT
- BIZTONSÁGOS HIBAÁLLAPOT
  Pl. energiaminimum (szárazföldi) → FAIL-SAFE

Diverz rendszerkialakítás

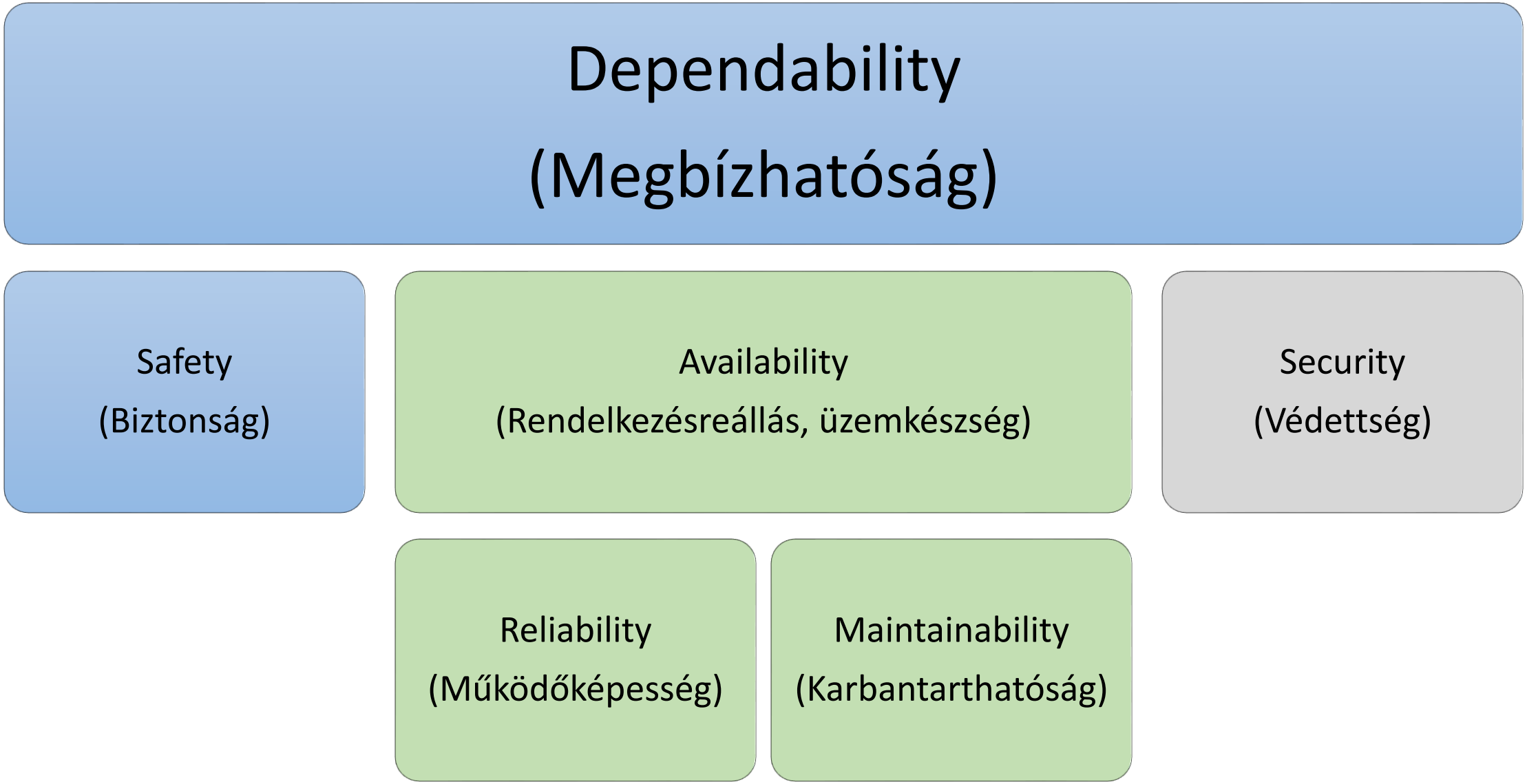
- Megvalósítható
  - hardveresen (különböző alkatrészek)
  - szoftveresen (különböző szoftverek ugyanarra a feladatra)
    - eltérő specifikáció
    - eltérő programozó csapatok
    - eltérő programnyelv stb.
- A szisztematikus hiba megjelenésekor (üzem közben) észlelhető
- Megfelelő hibareakciót kell kiváltani

- Előny
  - védelem a szisztematikus hibák veszélyes hatása ellen
  - „polcról levett” komponensek (COTS, Commercial Off-The-Shelf) alkalmazhatósága
- Hátrány
  - A hibadetektálás az üzem közbenre tolódik (kisebb rendelkezésreállás)
  - A különböző csatornák szinkronizálása nehéz
  - Drága (fejlesztés és üzemeltetés)

Fogalmak - megbízhatóság

(Ismétlés)

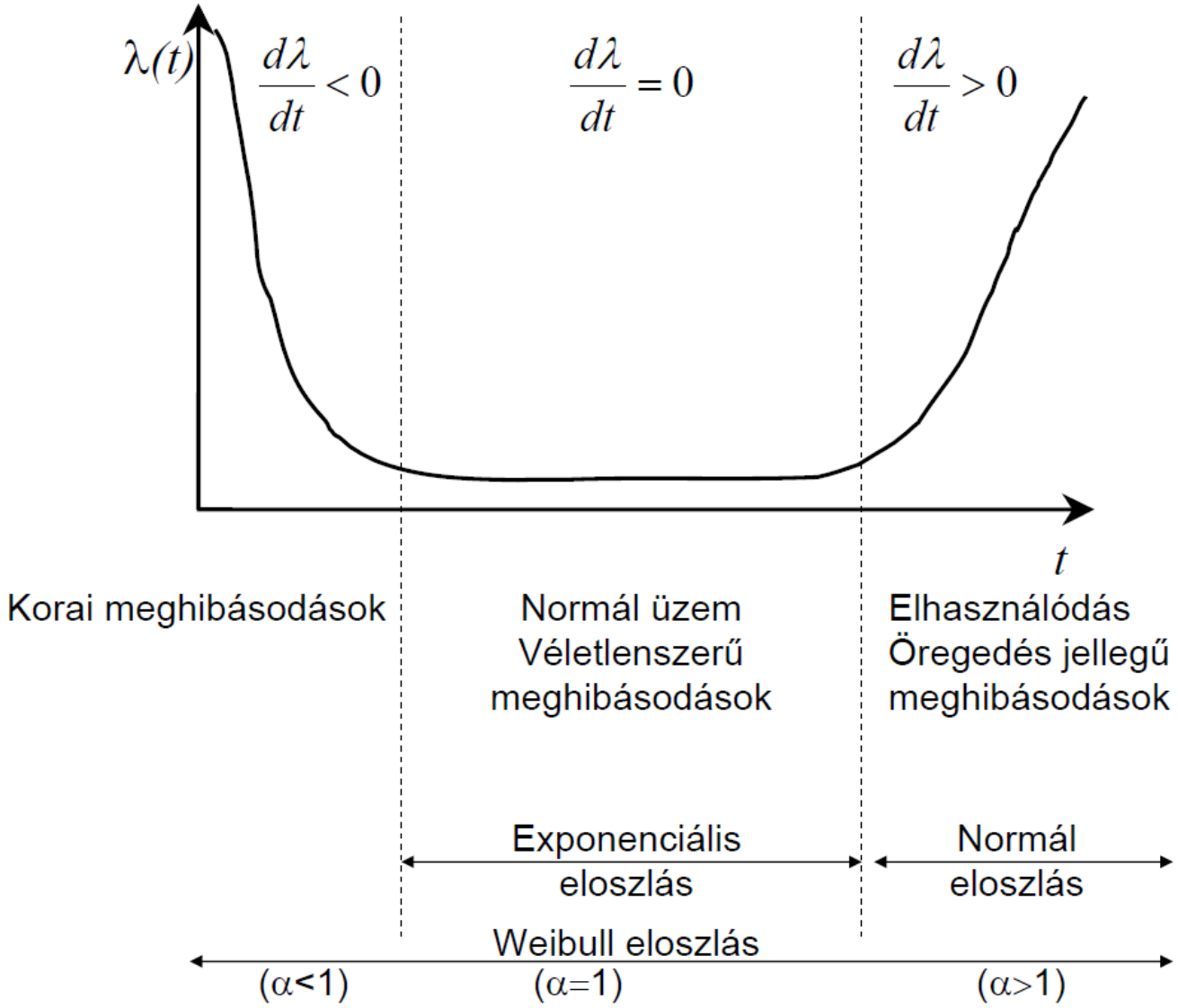
RAMS-S


Dependability
(Megbízhatóság)
Safety
(Biztonság)
Availability
(Rendelkezésreállás, üzemkészség)
Security
(Védettség)
Reliability
(Működőképesség)
Maintainability
(Karbantarthatóság)

Megbízhatósági paraméterek

Név	Jelölés	Dimenzió
Működőképesség valószínűsége	$R(t)$	[1]
Meghibásodás valószínűsége	$F(t)$	[1]
Meghibásodási sűrűség	$f(t)$	[1/h]
Meghibásodási ráta	$\lambda(t)$	[1/h]
Várható/közepes élettartam	T, m	[h]
Elemek száma	$N(t)$	[1]

Elemek megbízhatósága – fürdőkádgörbe



Korai meghibásodások	Véletlenszerű meghibásodások	Elhasználódás
• Gyártási hiányosságok • Szállítási sérülések • Tapasztalat hiánya → Próbaüzem, előöregítés	• Különböző független hatások statisztikai együtthatása → Lehetőleg ebben a szakaszban üzemeltetni	• Elhasználódás • Elöregedés • Kopás • Bizonyos igénybevételt követően → Lehetőleg itt nem üzemeltetni (felújítás, csere)

Weibull eloszlás

- Weibull szerint a túlélési valószínűség definíciója:

$$R(t) = e^{-\left(\frac{t-\gamma}{\beta}\right)^{\propto}}, \text{ ha } t > \gamma$$

- A Weibull függvény tartalmazza az „*e*” eloszlást is:

$$\propto = 1, \beta = T, \gamma = 0$$

$$R(t) = e^{-\left(\frac{t-\gamma}{\beta}\right)^{\propto}} = e^{-\left(\frac{t-0}{T}\right)^{1}} = e^{-\left(\frac{t}{T}\right)} = e^{-\lambda t}$$

- A meghibásodás valószínűsége:

$$F(t) = 1 - e^{-\left(\frac{t-\gamma}{\beta}\right)^{\propto}}, \text{ ha } t > \gamma$$

EXPONENCIÁLIS ELOSZLÁS

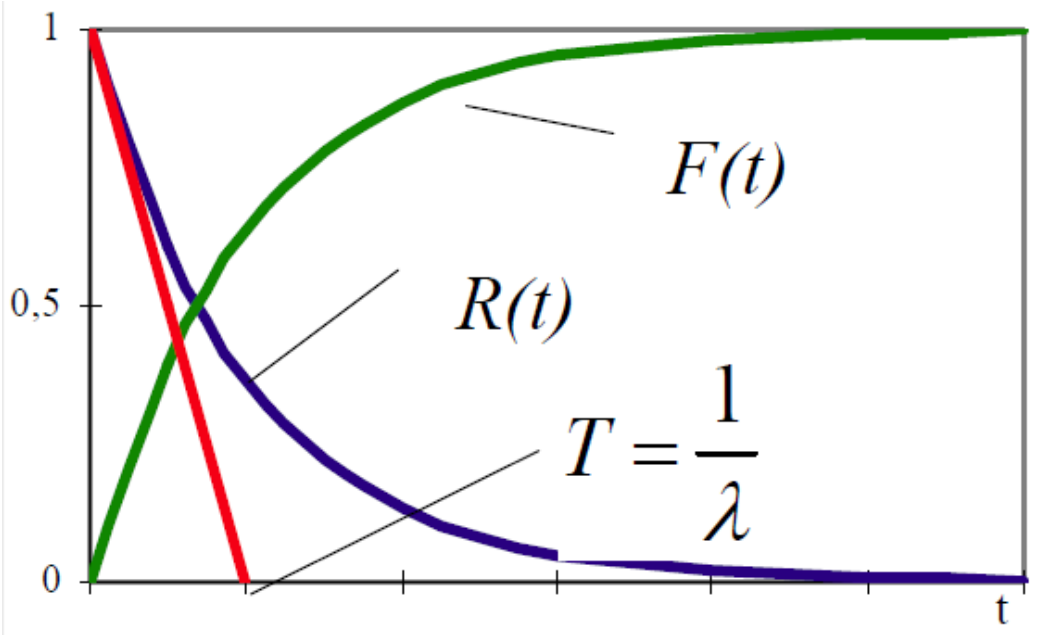
$$R(t) = e^{-\lambda t}$$

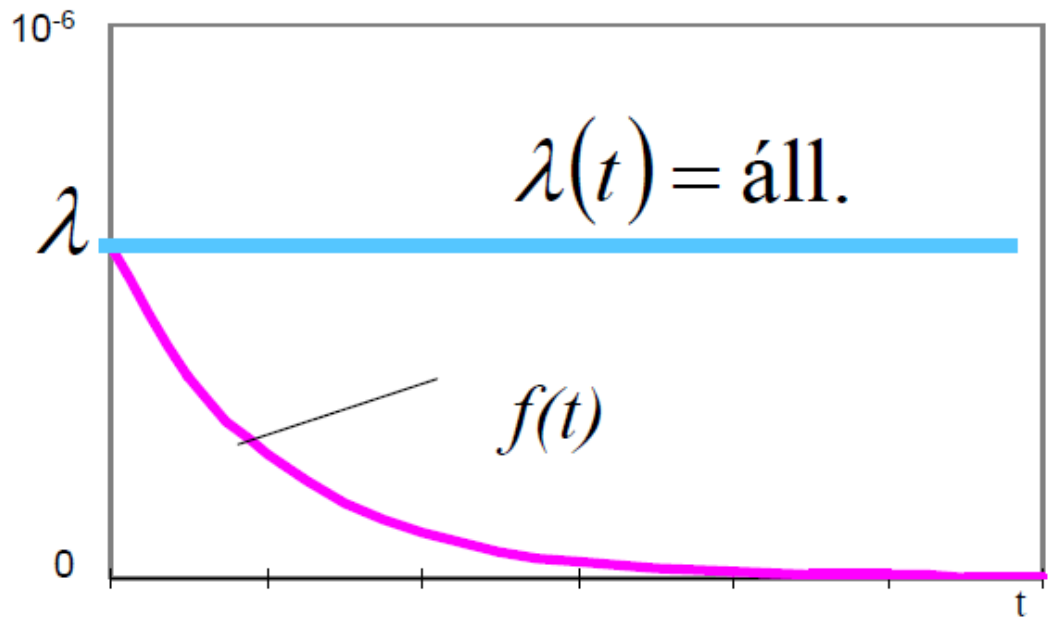
$$F(t) = 1 - e^{-\lambda t}$$

$$T = \int_0^{\infty} R(t) = \int_0^{\infty} e^{-\lambda t} = \left[-\frac{1}{\lambda} e^{-\lambda t}\right]_0^{\infty} = -\frac{1}{\lambda}(e^{-\infty} - e^{-0}) = -\frac{1}{\lambda}(0 - 1) = \frac{1}{\lambda}$$

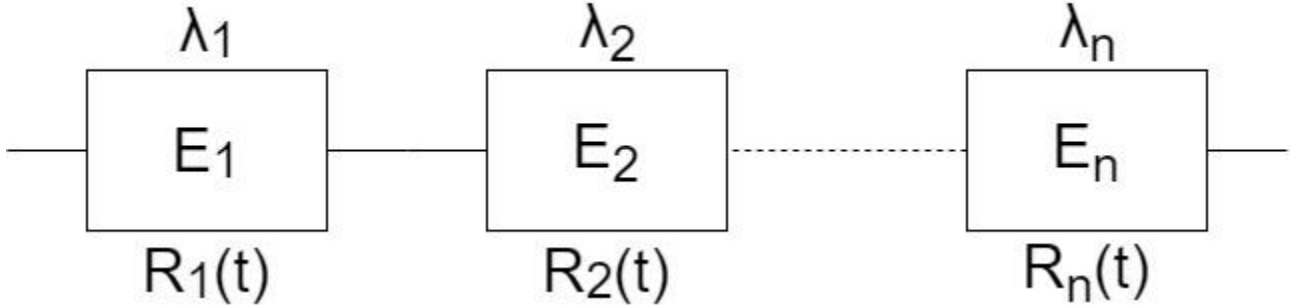
R(t) meredeksége a *t = 0* pontban:

$$\big(R(t)\big)' = \big(e^{-\lambda t}\big)' = -\lambda * e^{-\lambda t}\Big|_{t=0} = -\lambda$$





SOROS RENDSZEREK MEGBÍZHATÓSÁGA



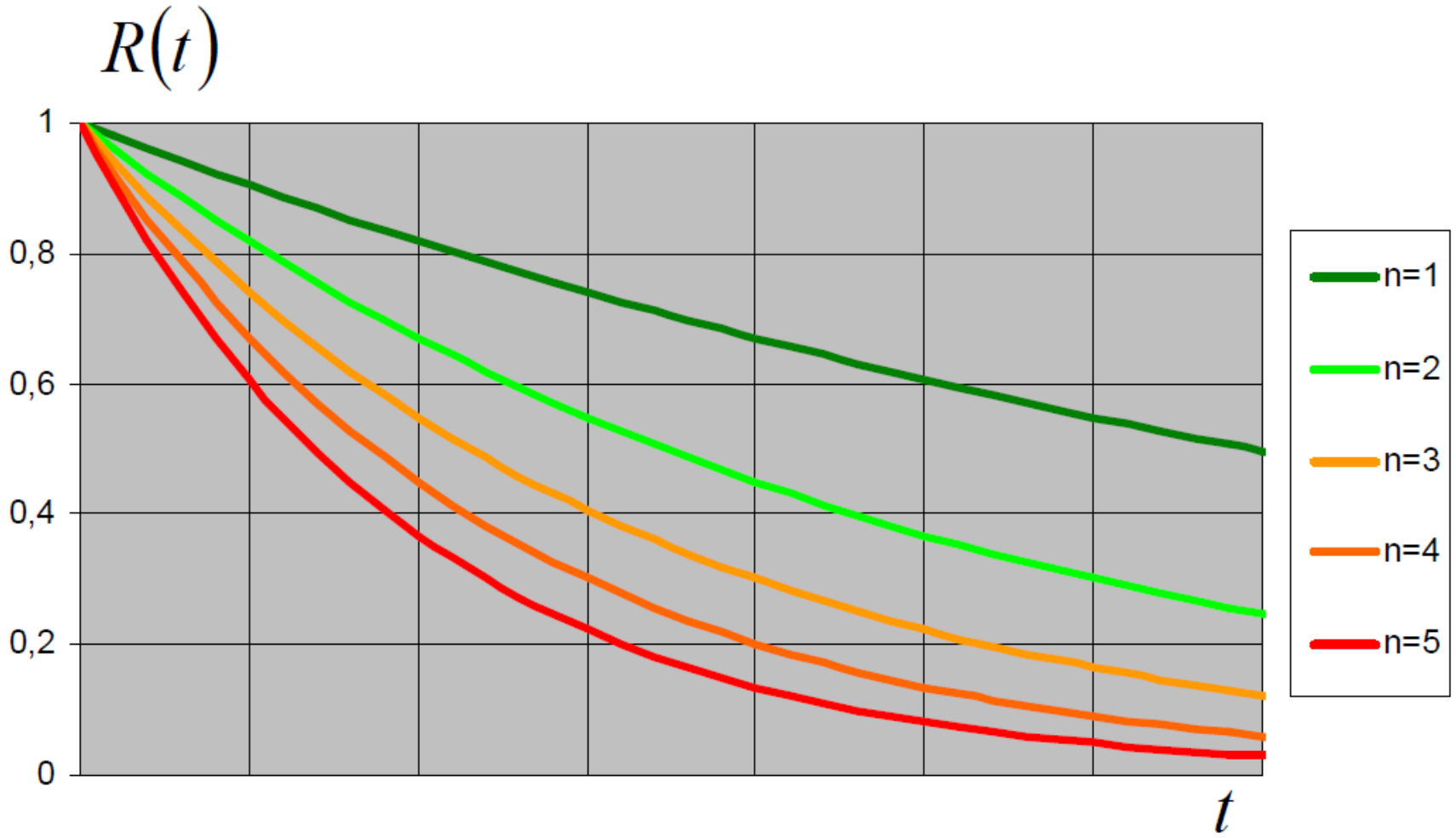
- Soros rendszer működőképességének valószínűsége (minden elem egyidejűleg működőképes):

$$R_S(t) = R_1(t) * R_2(t) * \cdots * R_n(t) = \prod_{i=1}^{n} R_i(t)$$

$$R_S(t) = e^{-\lambda_1 t} * e^{-\lambda_2 t} * \cdots * e^{-\lambda_n t} = e^{-\sum_{i=1}^{n} \lambda_i t}$$

$$\lambda_S = \lambda_1 + \lambda_2 + \cdots + \lambda_n = \sum_{i=1}^{n} \lambda_i$$

Soros rendszerek



A REDUNDANCIA FOGALMA

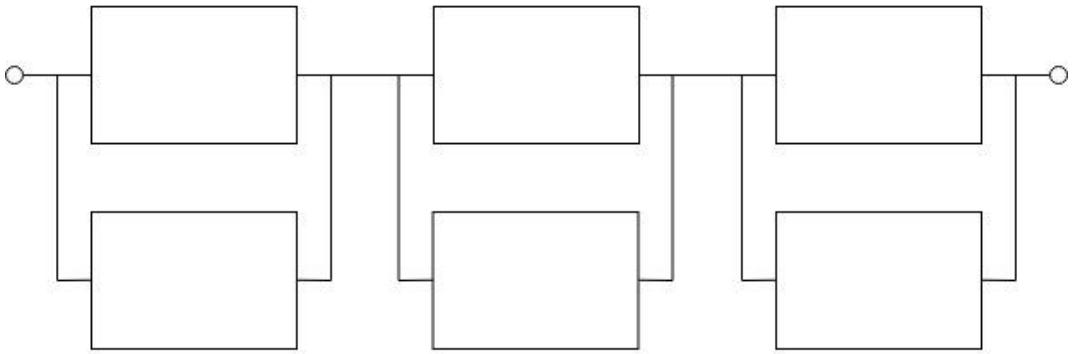
- A redundancia olyan, a rendszer funkcióinak teljesítéséhez minimálisan szükséges, ún. alapkiépítését meghaladó többlet, amelyre a megbízhatóság, azaz
  - a működőképesség és/vagy
  - a belső biztonság

kívánt értékének elérése érdekében van szükség.

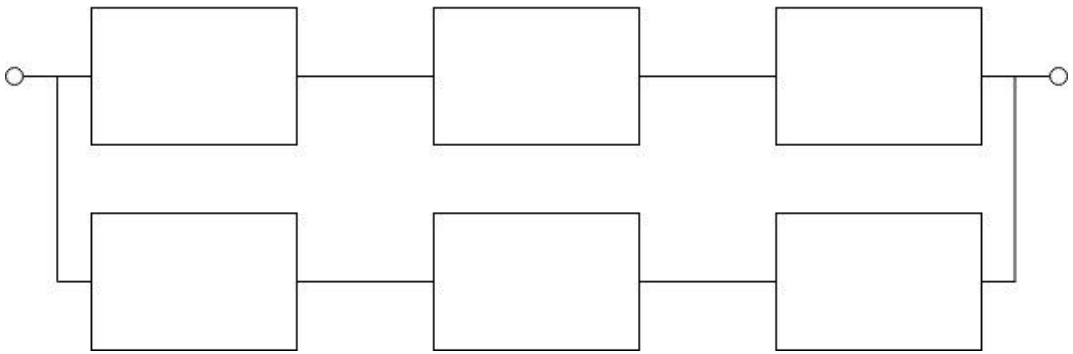
- A működőképesség növelése növeli a belső biztonságot is, azonban a belső biztonság növelése érdekében alkalmazott redundancia a működőképességet csökkenti.
- A redundanciát önmagában vagy más megbízhatóságnövelő módszerekkel kombinálva alkalmazzák.

HW TARTALÉKOLÁS SZINTJEI

- Alap rendszer
  (pl. egy autóbusz)



- Alkatrész, fokozat, készülék
  (pl. autóbusz fődarabok: motor, hajtómű, stb.)



- Teljes rendszer
  (pl. még egy autóbusz)

A HARDVER REDUNDANCIAFAJTÁI

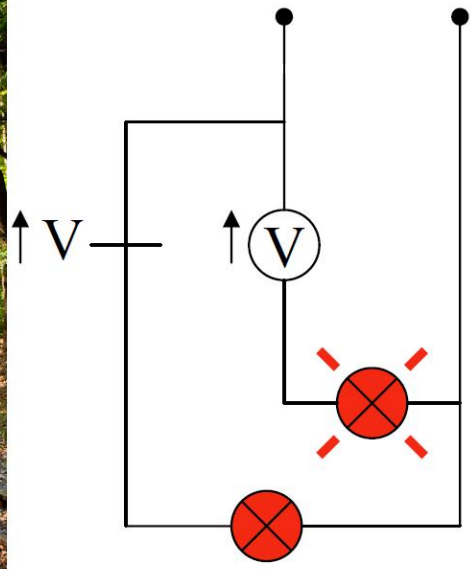
- Passzív redundancia (hideg tartalék)
  - Kapcsolt („1 az n-ből”),
  - Csúszó tartalék („k az n-ből”)

- Aktív redundancia (meleg tartalék)
  - Nem kapcsolt (párhuzamos, „1 az n-ből”)
  - Kapcsolt („1 az n-ből”)
  - Csúszó tartalék („k az n-ből”)
  - Többségi (szavazólogikával „k az n-ből”)

PASSZÍV REDUNDANCIA – ALKALMAZÁSI PÉLDÁK

Kapcsolt („1 az 2-ből”): pótvörös

forrás:
http://keptar.gyermekvasut.hu/var/albums/oktatas/jelzok/gyvasut_20111015-47206.jpg?m=1318959895



Csúszó(„4 az 5-ből”): Pótkerék

forrás:
ttps://www.donwhites.com/assets/stock/colormatched_02/white/640/cc_2018jes160001_02_640/cc_2018jes160001_02_640_pw7.jpg

PASSZÍV REDUNDANCIA SZÁMÍTÁSA

- Annak a valószínűsége, hogy a rendszer az i jelű állapotban tartózkodik:

$$P_i(t) = \frac{(\lambda t)^i}{i!} e^{-\lambda t}; i = 0 \dots n-1$$

- A rendszer működőképes a 0, 1, … n-1 állapotokban:

$$R_S(t) = \sum_{i=0}^{n-1} P_i(t) = \sum_{i=0}^{n-1} \frac{(\lambda t)^i}{i!} e^{-\lambda t}$$

- A rendszer várható élettartama:

$$T_S = \sum_{i=1}^{n} T_i = nT = n\frac{1}{\lambda}$$

AKTÍV REDUNDANCIA – ALKALMAZÁSI PÉLDÁK

Nem kapcsolt (párhuzamos): DB főjelző

forrás: https://upload.wikimedia.org/wikipedia/de/b/b0/Hp_0.jpg

Csúszó(„k az n-ből”): Központi tartalék

forrás: http://iho.hu/img/161021_ikarus/201607270.jpg

AKTÍV REDUNDANCIA SZÁMÍTÁSA

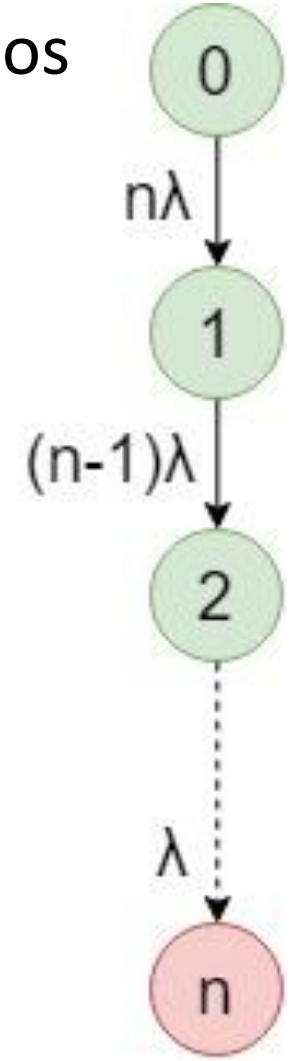
- A rendszer csak akkor hibásodik meg, ha valamennyi párhuzamos elem meghibásodott:

$$F_S(t) = \prod_{i=1}^{n} F_i(t) = F_i^n(t); ha\ \lambda_1 = \lambda_2 = \cdots \lambda_n$$

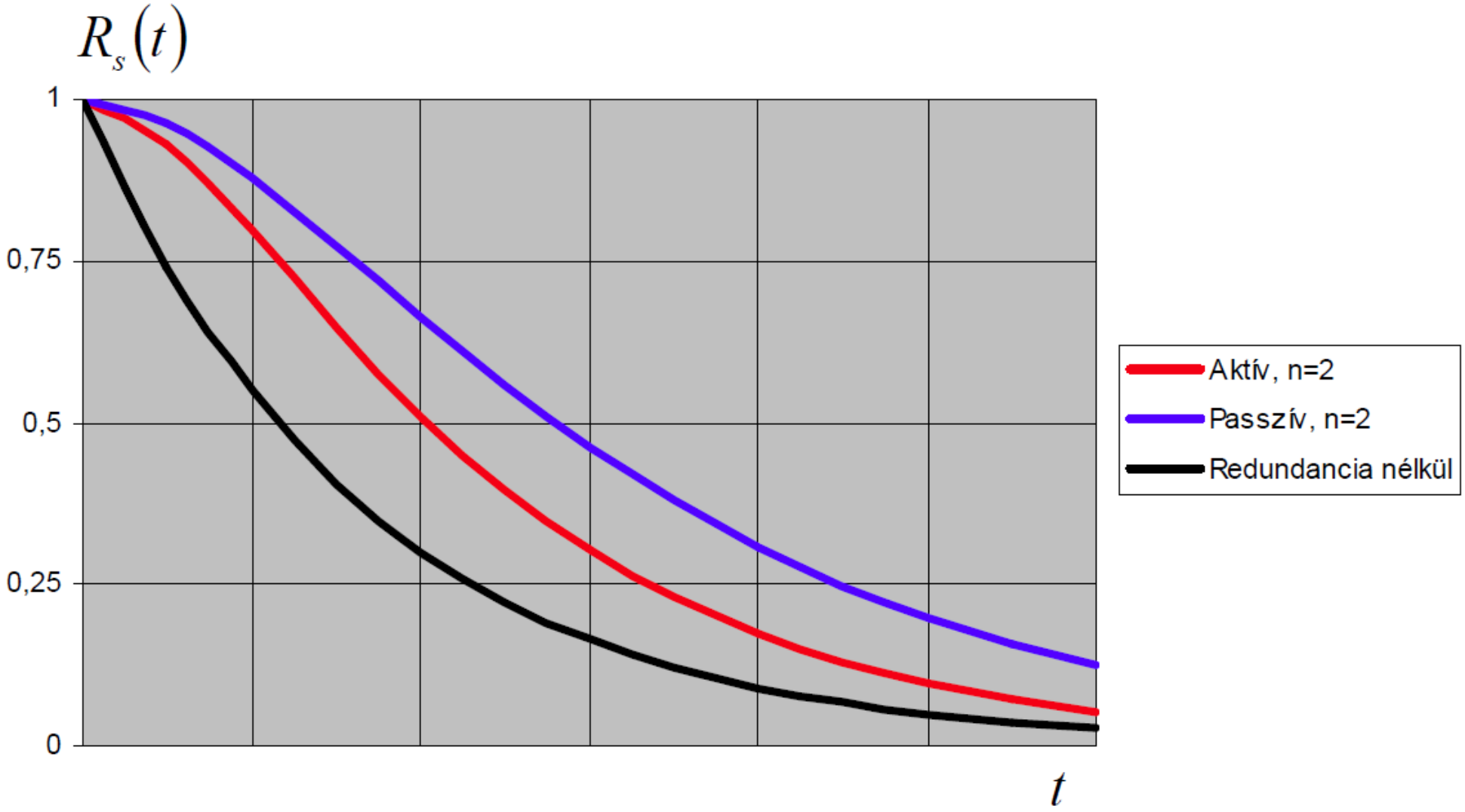
- A rendszer működőképessége:

$$R_S(t) = 1 - \big(1 - R(t)\big)^n$$

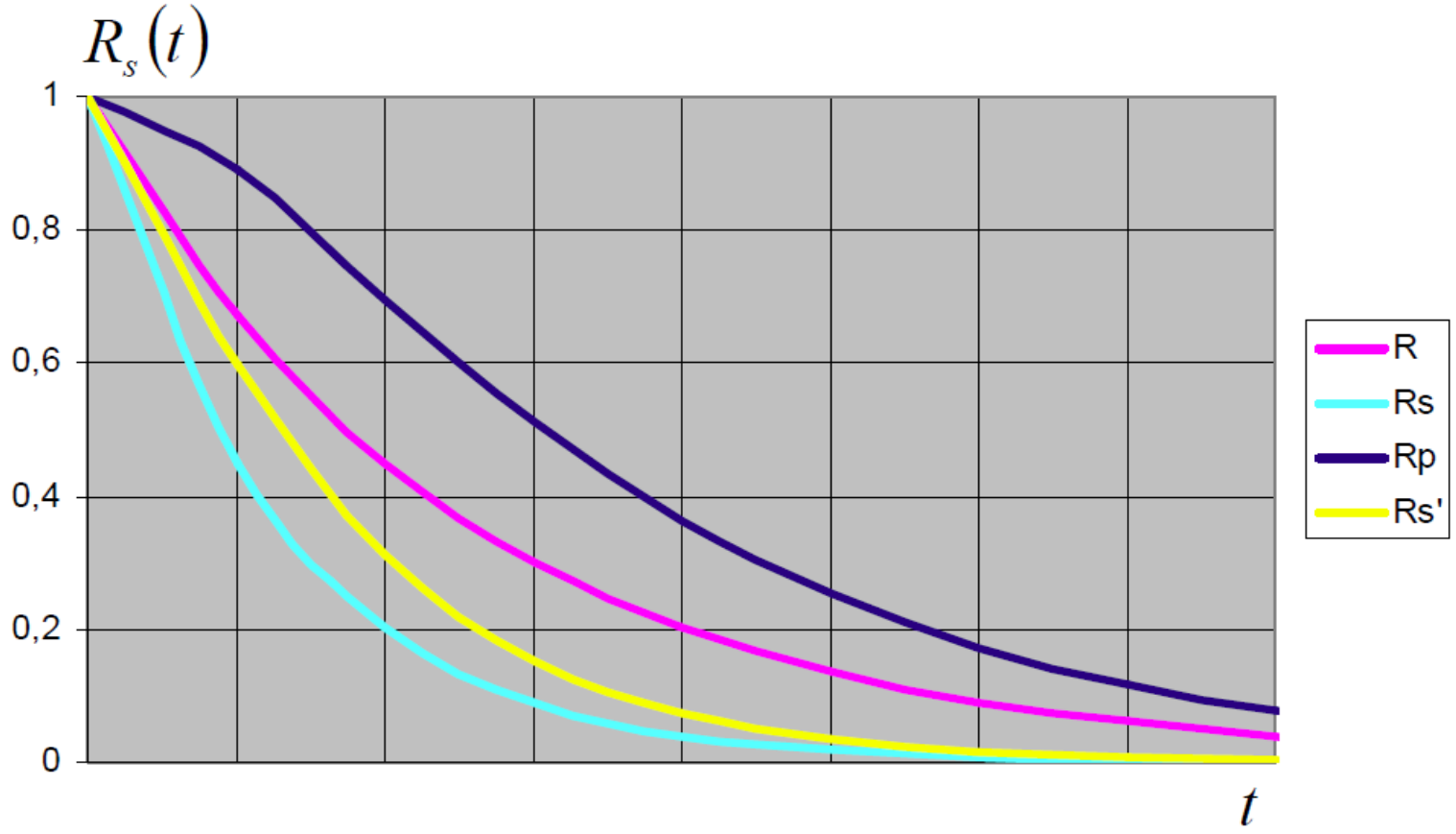
$$R_S(t) = -\sum_{i=0}^{n} \binom{n}{i} \big(-R(t)\big)^{n-i}$$

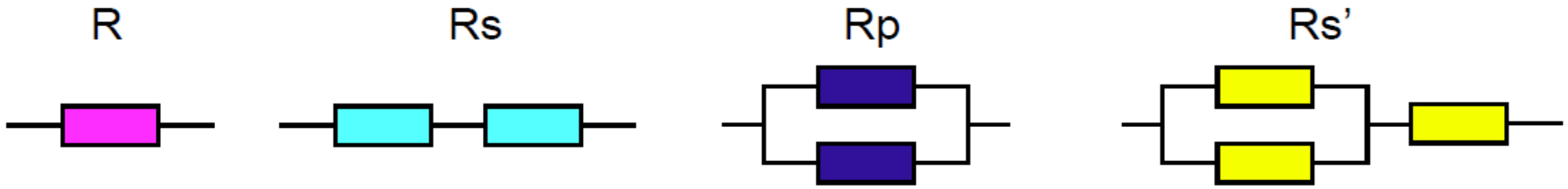


Passzív-aktív redundancia összehasonlítás

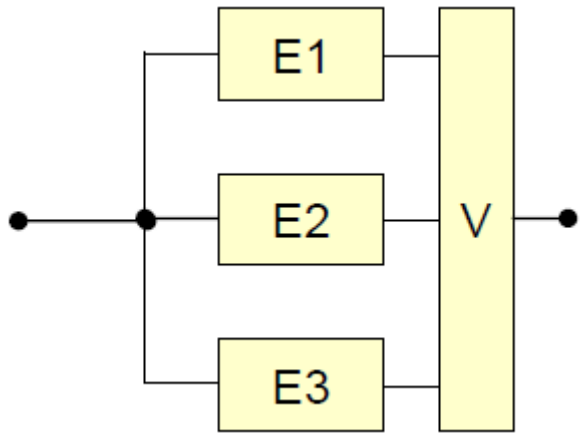


Vegyes rendszerek



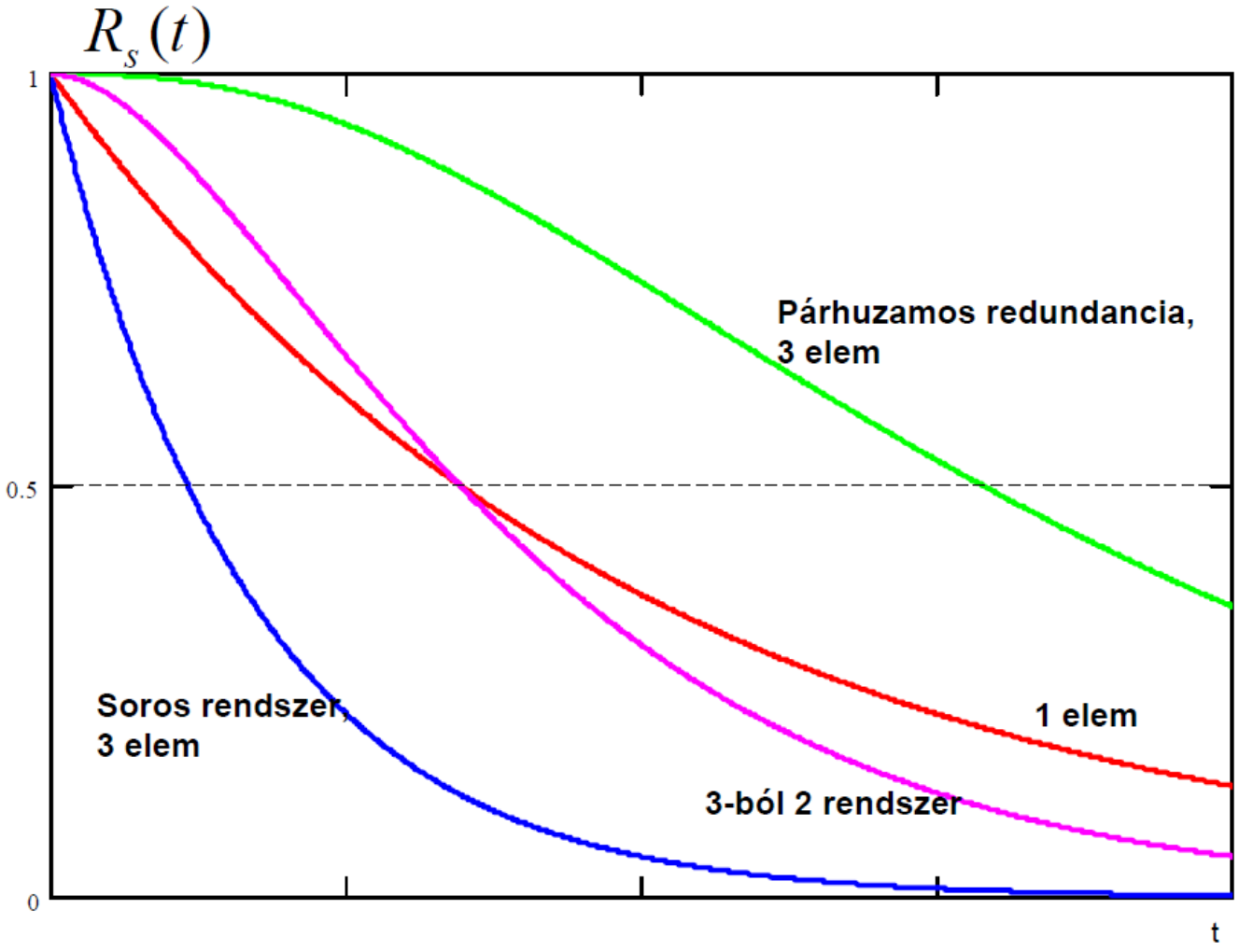


„k” az „n”-ből rendszerek



Szavazólogikás (többségi vagy majoritásos) rendszerek esetén a helyes döntéshez legalább az elemek fele működőképes kell hogy legyen.

$$k \geq \frac{n+1}{2}$$



Karbantarthatóság

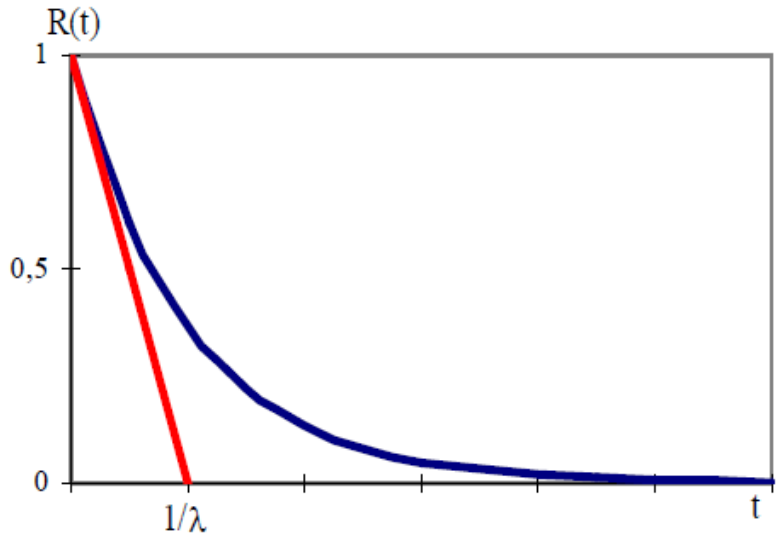
- A karbantartás (maintenance) azon intézkedések összessége, amelyek célja egy rendszer készenlétének, vagy más szóval rendelkezésreállásának (availability) a biztosítása.
- A karbantartás fajtái:
  - tervszerű(megelőző) karbantartás, a működőképesség megtartása érdekében,
  - terven kívüli (javító) karbantartás, a működőképesség helyreállítása érdekében.

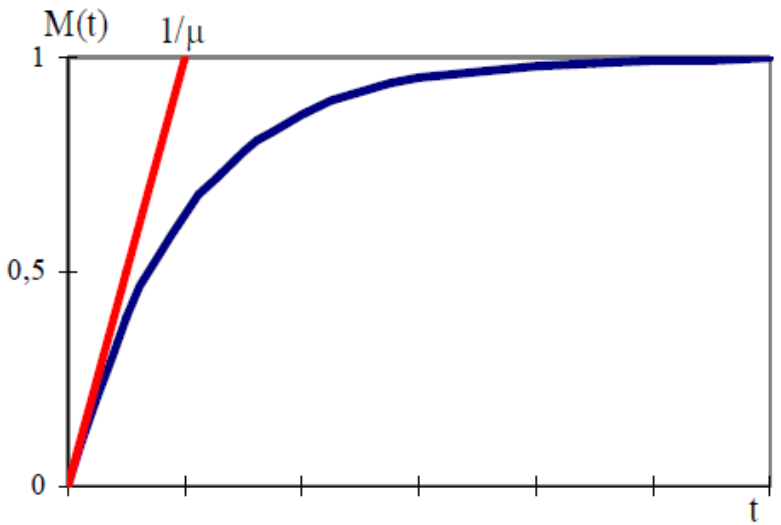
$$M(t) = 1 - e^{-\mu t}$$

MTBF és MTTR

$$MTBF = \int_0^\infty R(t)dt = \frac{1}{\lambda}$$

$$MTTR = \int_0^\infty [1 - M(t)]dt = \frac{1}{\mu}$$





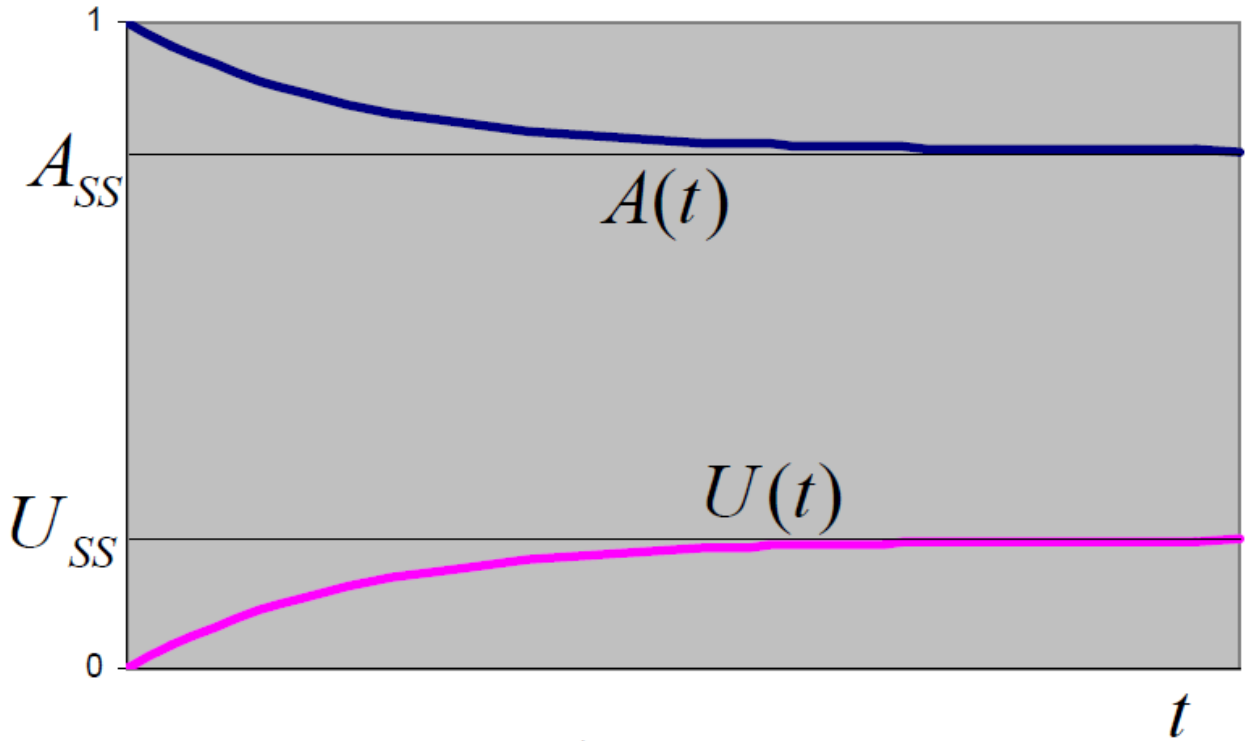
Rendelkezésreállás

Készenlét
Availability

$A(t)$

Nem-készenlét
Unavailability

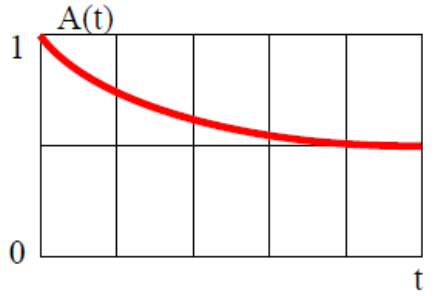
$U(t) = 1 - A(t)$



A készenlét fajtái

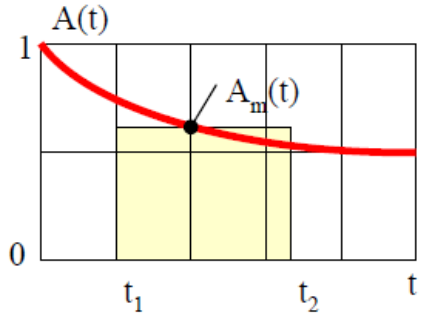
Pillanatnyi készenlét:
annak valószínűsége, hogy a rendszer az adott időpontban működőképes:

$$A(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda} e^{-(\mu+\lambda)t}$$



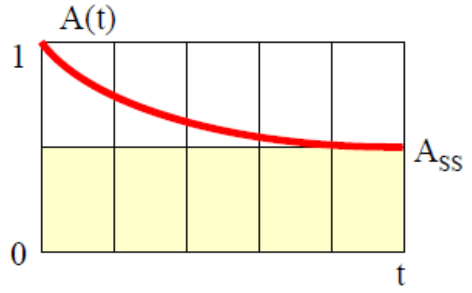
Adott feladatra készenlét:
annak valószínűsége, hogy a rendszer a $t_1 \le t \le t_2$ időintervallumban működőképes:

$$A_m(t) = \frac{1}{t_2 - t_1} \cdot \int_{t_1}^{t_2} A(t)dt$$



Tartós (Steady State) **készenlét**:
azt fejezi ki, hogy egy rendszer hosszabb idő elteltével az időalap hány százalékában működőképes:

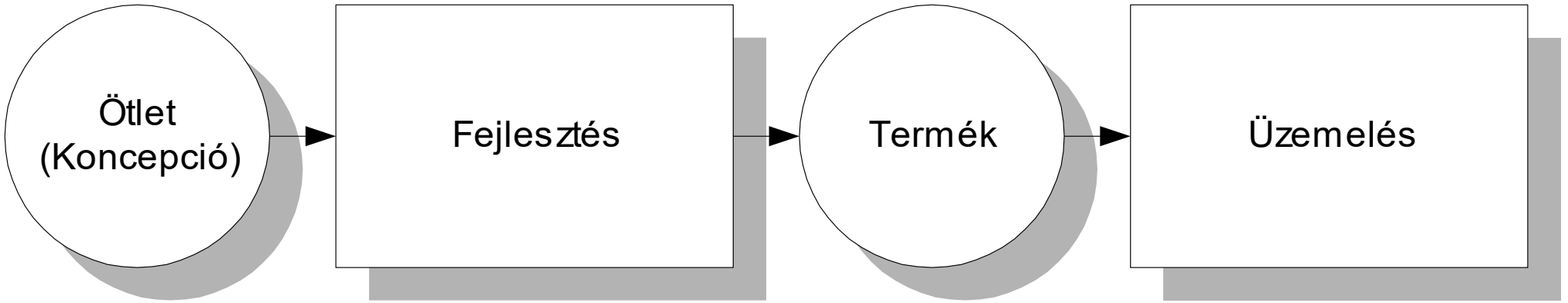
$$A_{ss} = \frac{\mu}{\mu+\lambda} = \frac{MTBF}{MTBF + MTTR}$$



Rendszerfejlesztés

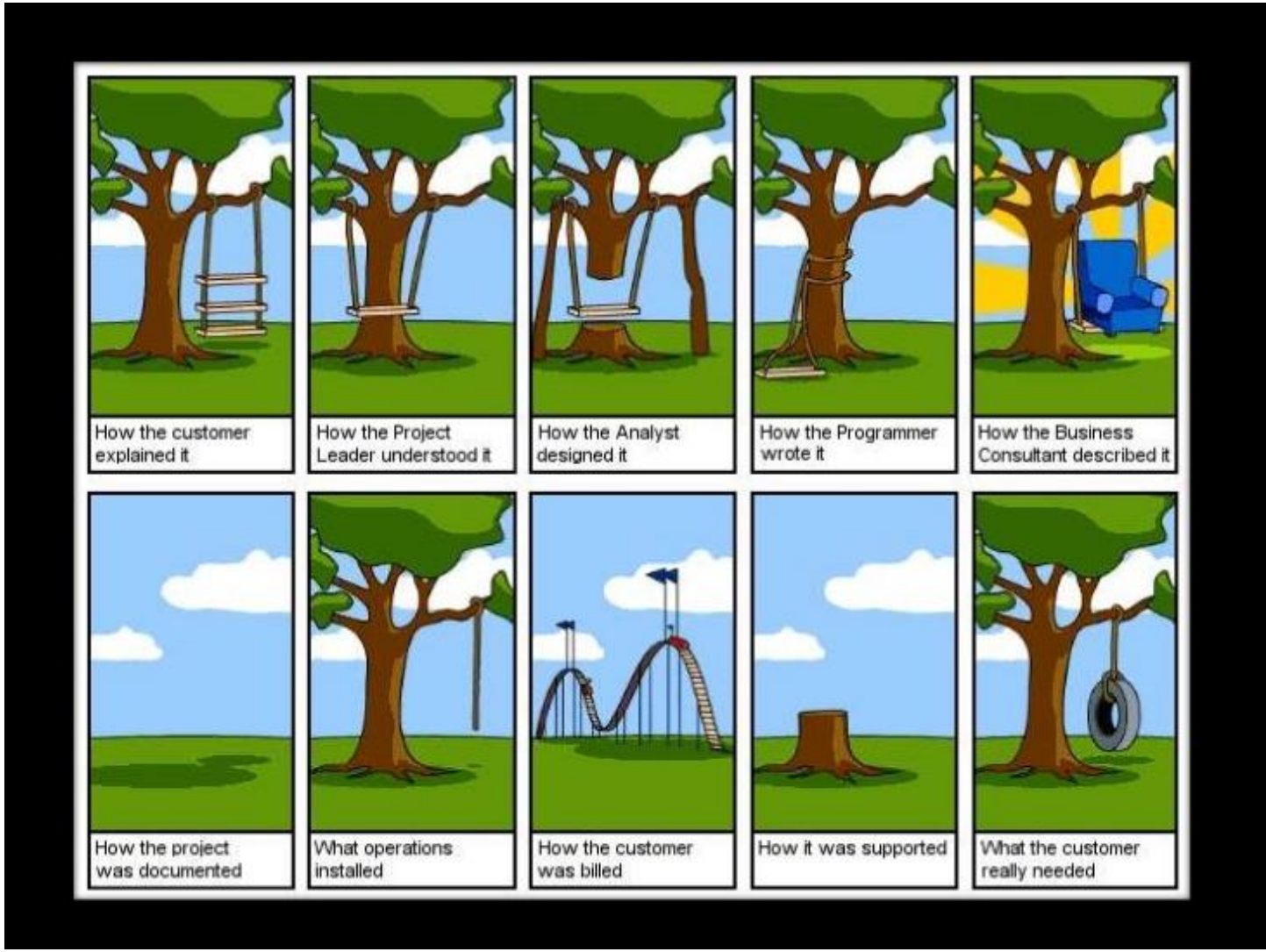
(Ismétlés)

Életciklus

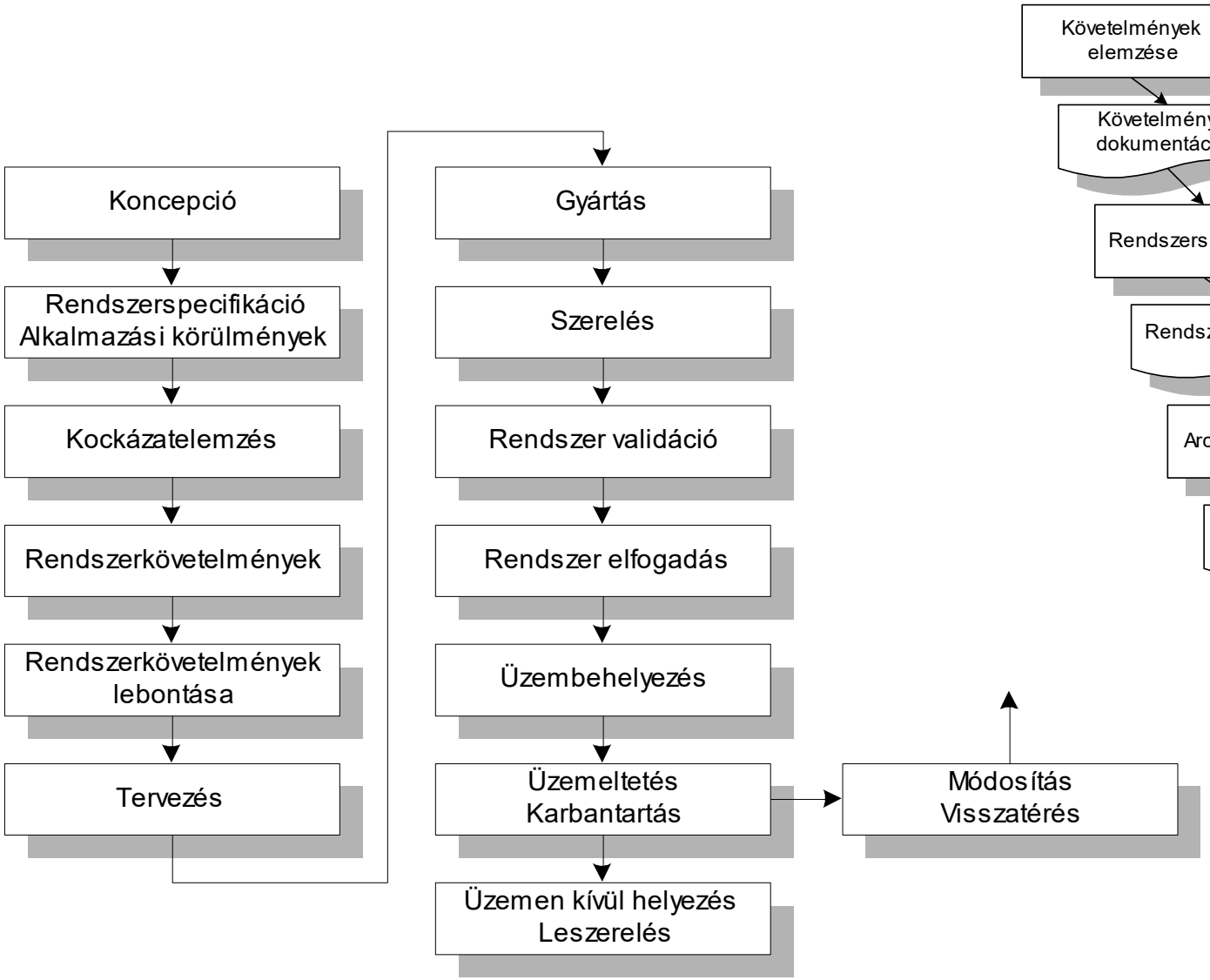


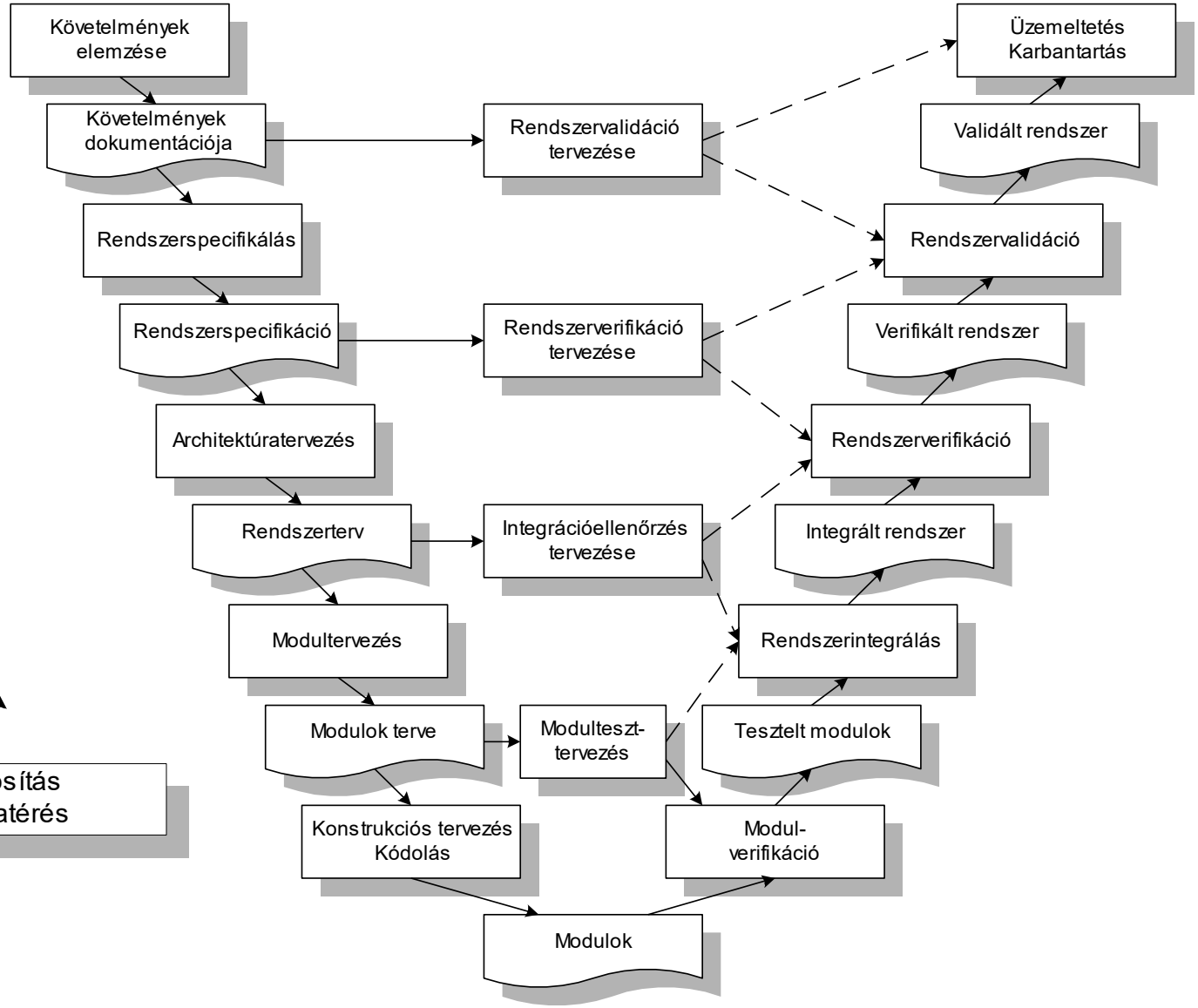
Fejlesztési módszerek, lépések

- Követelményelemzés
  - Funkcionális
  - Biztonsági
- Előzetes veszélyelemzés, kockázatelemzés
- Specifikáció
- Architektúra tervezés
- Részletes (modul) tervezés
- A modulok megvalósítása és tesztelése/verifikáció
- Rendszer-integráció és rendszerteszt/validáció
- Engedélyezés
- Üzemeltetés, karbantartás



Fázismodell és V-modell





Verifikáció és validáció

Verifikáció (igazolás)

- „Jól készítem a rendszert?”
- Összhang ellenőrzése a fejlesztési fázisokban és azok között
- Fejlesztési lépések során használt tervek (modellek) és specifikációjuk közötti megfelelés ellenőrzése

Validáció (érvényesítés)

- „A jó rendszert készítettem?”
- A fejlesztés eredményének ellenőrzése
- A kész rendszer és a felhasználói elvárások közötti megfelelés ellenőrzése

Formális módszerek

- Matematikai technikák (elsősorban diszkrét matematika és matematikai logika), melyek egyes (HW/SW) életciklus fázisok végrehajtásához, ellenőrzéséhez és dokumentálásához használhatók.