Nyíregyháza, 2016/2017. 2. fé.

KÖZLEKEDÉSAUTOMATIKA

Dr. Bede Zsuzsanna

adjunktus

(BME Közlekedés- és Járműirányítási Tanszék)

bede.zsuzsanna@mail.bme.hu

BIZTONSÁG VESZÉLYEZTETÉS SÉRÜLÉS

A BIZTONSÁG FOGALMA

- Egy lehetséges definíció:

  A **biztonság** egy rendszer azon tulajdonsága, hogy nem veszélyezteti az emberi életet, illetve a környezetet
- Az előbbi alapján:

  A **biztonsági rendszer** olyan rendszer, amelynek révén egy rendszer vagy berendezés biztonsága elérhető
- Terjedelem: mikrokapcsolótól az erőművi védelmi rendszerig
- Feladat lehet:
  - Kifejezetten biztonsági
  - Egyéb feladatok mellett biztonsági is
- Abszolút biztonság helyett az alkalmazásnak megfelelő biztonság elérése
- A megfelelőség megítélése gyakran szubjektív (pl. repüléstől való félelem - az autózás veszélyesebb)

ELVÁRÁSOK A KÖZLEKEDÉSSEL SZEMBEN

Elvárások

- költség
- gyakoriság
- sebesség
- eljutási idő
- biztonság
- megbízhatóság
- utazási komfort
- egyéb

Megfelelés az elvárásoknak: ráfordítás

attraktivitás

Az egyes tényezők fontossága viszonylatfüggő, de a **biztonság** mindig az első helyen áll.

AUTOMATIKUS FOLYAMATIRÁNYÍTÓ RENDSZEREK A KÖZLEKEDÉSBEN

- jármű fedélzeti rendszerek
- forgalomirányító rendszerek
- egyéb rendszerek (pl. energiaellátás irányítása)

BIZTONSÁGKRITIKUS FOLYAMATOK

A **közlekedés** veszélyes üzem:

- személyek
- tárgyak
- a környezet

biztonságát **sérülések okozásával** veszélyeztetheti.

Példák más **veszélyes folyamatokra**, rendszerekre:

- vegyipari és energiaipari folyamatok,
- gyártási folyamatok (gyártósorok, ipari robotok),
- anyagmozgatás, raktározás,
- orvosi technológiák (orvosi, radiológiai műszerek/készülékek).

A veszélyeztetést az adott folyamattal, berendezéssel vagy rendszerrel, illetve annak funkcióival összefüggő egy vagy több

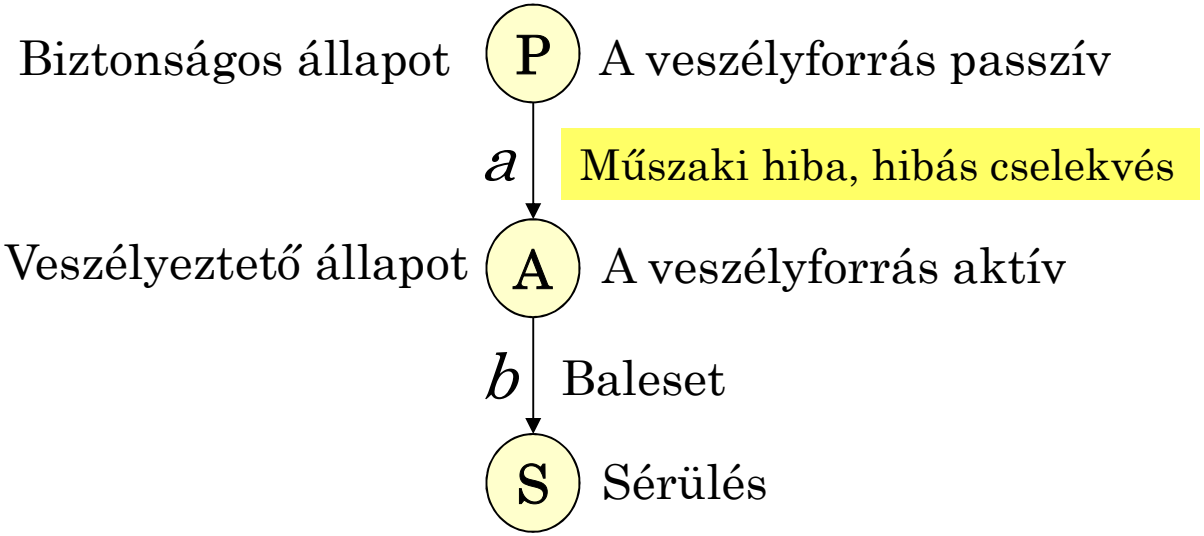
veszélyforrás

okozhatja.

BIZTONSÁG ÉS VESZÉLYEZTETÉS – BALESETI ESEMÉNYLÁNC

Biztonság:
a veszélyeztetettségtől mentes állapot valószínűsége

Balesetmentesség:
a sérüléstől mentes állapot valószínűsége



„Majdnem balesetek”

BIZTONSÁGI SZEMLÉLET

- Szabály alapú
  - Veszélymentesség
  - Balesetmentesség
  - Sérülésmentesség
- Kockázatmentesség?
  - Gyakoriság ?
  - Súlyosság ?

- Kockázati alapú
  - A kockázat nem haladja meg az elfogadható értéket
- Tényleges kockázat
  - Gyakoriság
  - Súlyosság

Veszélyforrások a közlekedésben

Egyetlen jármű esetén

- pályahiba
- személyek, tárgyak, idegen jármű a pályán, ill. a pálya veszélyes megközelítése
- rakomány nem megfelelő elhelyezése/rögzítése
- utasok nem megfelelő magatartása
- járműhiba
- jármű/pálya kapcsolat megváltozása
- járművezetési hiba

Műszaki vagy emberi hiba

Több jármű vonatkozásában

- a forgalmi helyzet téves megítélése
- veszélyes megközelítés
  - ❑ hátulról
  - ❑ szemből
  - ❑ oldalról

Emberi hiba (ritkán műszaki)

A belátható távolságnál hosszabb fékút

A jármű/vontató jármű energiaellátása

Adottság

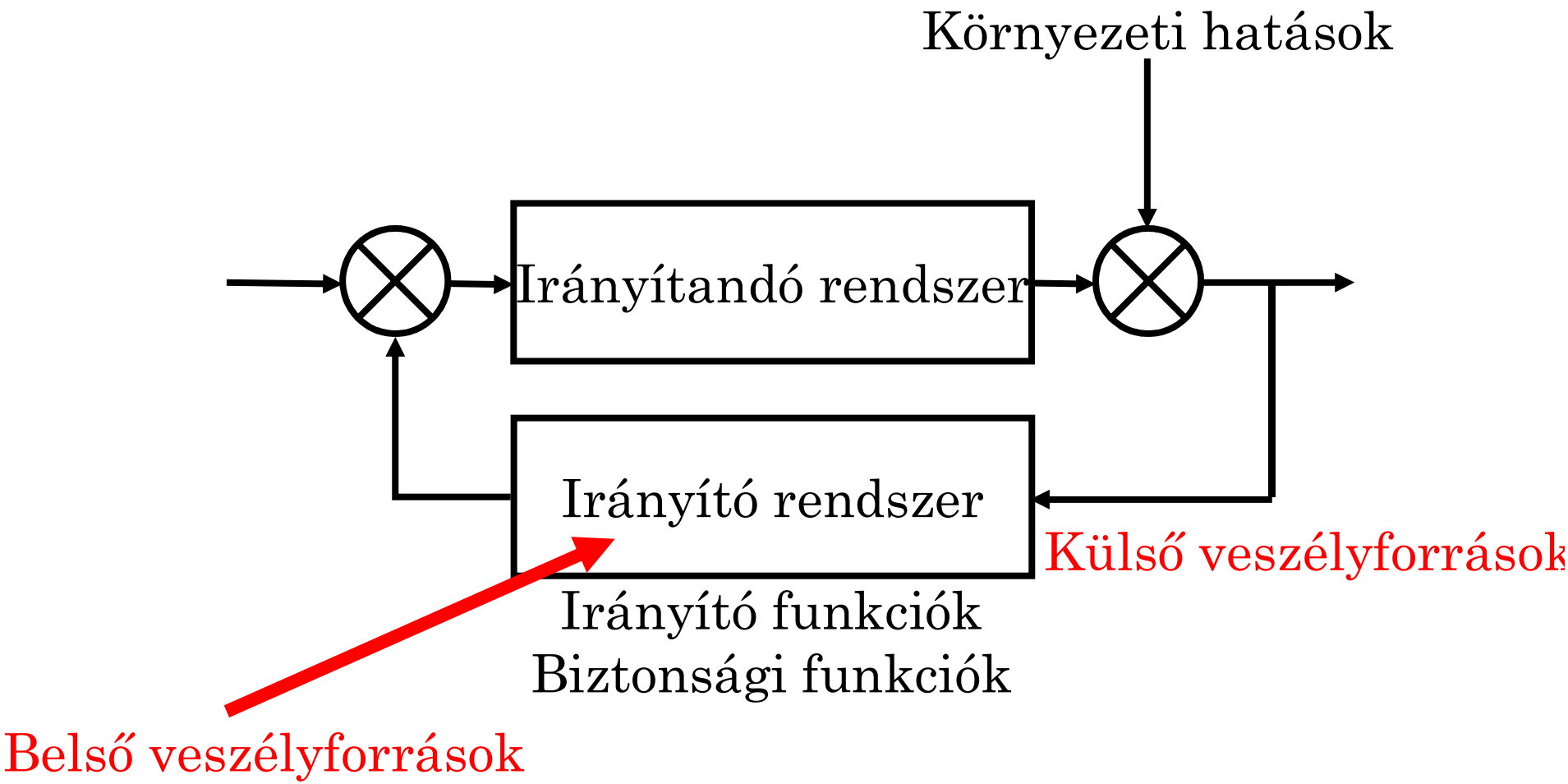
Veszélyforrások a közlekedésben

A forgalomirányítás szabály- és eszközrendszere a veszélyforrások egy részének hatását kizárja, illetve mérsékeli, és ezáltal lehetővé teszi a nagyobb sebességgel való közlekedést, illetve a pályakapacitás jobb kihasználását.

Ugyanakkor a forgalomirányítással kapcsolatos hibák is veszélyforrást jelentenek.

Forgalomirányítási szabályok • hiányosságai • helytelen értelmezése • figyelmen kívül hagyása	Emberi hiba
Forgalomirányító jelzések • hiánya, megrongálódása, észlelhetetlensége • helytelen értelmezése • figyelmen kívül hagyása	Emberi hiba
Helytelen forgalomirányító jelzések adása	Emberi hiba
Forgalomirányító berendezések hibája	Műszaki hiba

Az irányító rendszer szerepe



BIZTONSÁGI KOCKÁZAT

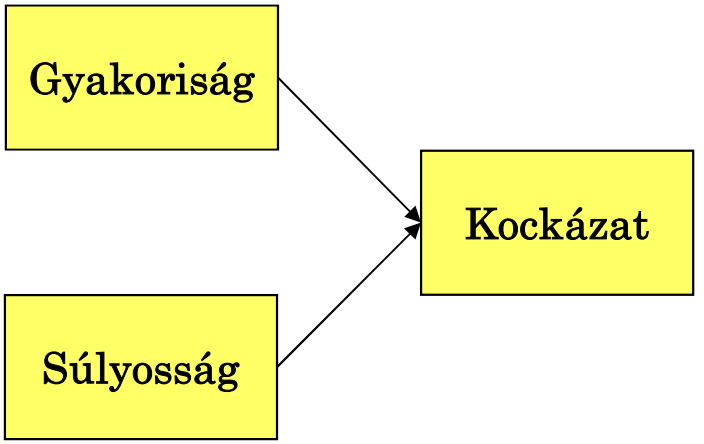
Biztonsági kockázat

Valamely veszélyeztető hatás jelentőségét egy alkalmazásban az ún. **biztonsági kockázat** fejezi ki.

Biztonsági kockázat:

- a veszélyeztetésből adódó baleset bekövetkezési valószínűségének vagy **gyakoriságának** és
- a keletkező sérülések **súlyosságának**

kombinációja.



A kockázat **meghatározható**

- mennyiségileg
- minőségileg (kockázatosztályozás)

Példa a kockázat számszerű kifejezésére

Valamely speciális alkatrész meghibásodása robbanást okozhat egy rendszerben, aminek következtében 100 ember halhat meg.
Az alkatrész átlagosan 10 000 évenként egyszer hibásodik meg.

Mekkora az alkatrészhibához kapcsolódó kockázat?

Kockázat = súlyosság x gyakoriság = 100 ember halála/hiba x 0,0001 hiba/év

Kockázat = 0,01 ember halála/év

Példa a kockázat számszerű kifejezésére

Egy 50 milliós lakosságú országban évente átlagosan 25 embert ér halálos villámcsapás.

Mekkora a villámcsapásból adódó halálozás kockázata?

Évente a lakosság $25/50\ 000\ 000 = 5 \times 10^{-7}$ részét éri villámcsapás.

Az **egyes emberek** számára ennyi annak a valószínűsége, hogy az adott évben villámcsapás éri őket.

A **lakosság egészére** vonatkozó kockázat: **5×10^{-7} halál/ember-év**

Kockázatosztályozás - Kárkihatási kategóriák (példa)

Kategó-ria	Leírás	Következmények
4	Katasztrofális	Több haláleset és súlyos sérült
3	Kritikus	Egy haláleset és/vagy több súlyos sérült
2	Csekély	Egy súlyos sérült; több kisebb sérülés
1	Elhanyagolható	Legfeljebb egy kisebb sérülés

Kockázatosztályozás - Veszélybekövetkezési gyakoriság (példa)

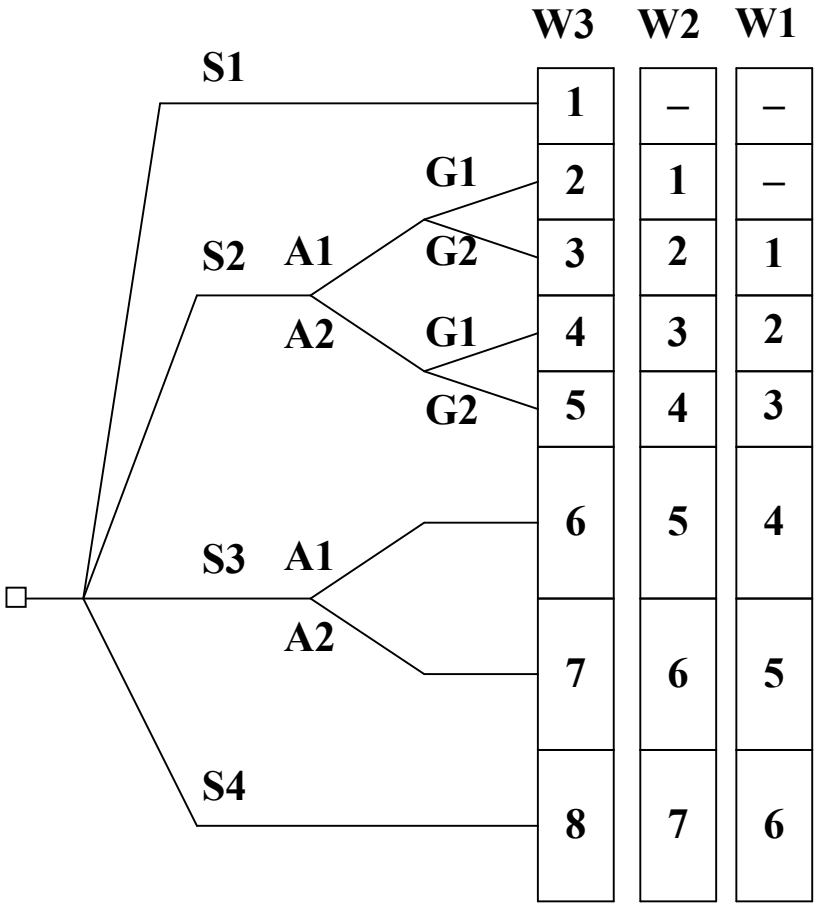
Szint	Leírás	Fogalom	Fellépési gyakoriság [h^{-1}]
A	gyakori	Feltételezhetően gyakran fellép; a veszélyeztetés állandóan jelen van	$> 10^{-3}$
B	valószínű	Többször fellép; várható, hogy a veszélyeztetés gyakran fellép	$10^{-3} \ldots 10^{-4}$
C	néha	Várható, hogy a veszélyeztetés többször bekövetkezik	$10^{-4} \ldots 10^{-5}$
D	alig	Várható hogy a veszélyeztetés a rendszer életében bekövetkezik	$10^{-5} \ldots 10^{-7}$
E	valószí-nűtlen	Valószínűtlen; azzal lehet számolni, hogy a veszély csak kivételesen lép fel	$10^{-7} \ldots 10^{-9}$
F	rendkí-vül való-színűtlen	Rendkívül valószínűtlen bekövetkezés; azzal lehet számolni, hogy a veszély nem lép fel	$<10^{-9}$

Kockázati **osztályok** (példa)

Valószínűségi szint		Kárkihatási kategóriák			
		Kataszt-rofális **4**	Kritikus **3**	Csekély **2**	Elhanya-golható **1**
gyakori	**A**	**K4**			
valószínű	**B**				**K2**
néha	**C**		**K3**		
alig	**D**				
valószínűtlen	**E**			**K1**	
rendkívül valószínűtlen	**F**				

Kockázati gráf - Követelményosztályok (DIN 19250)

S - kárkihatás súlyossága
A - a veszélyövezetben tartózkodás időtartama/gyakorisága
G - menekülési lehetőség
W - a veszélyeztetés valószínűsége



KOCKÁZATCSÖKKENTÉS
KOCKÁZATTŰRÉS

Kockázatmentesség, kockázatcsökkentés

Társadalmi igény:

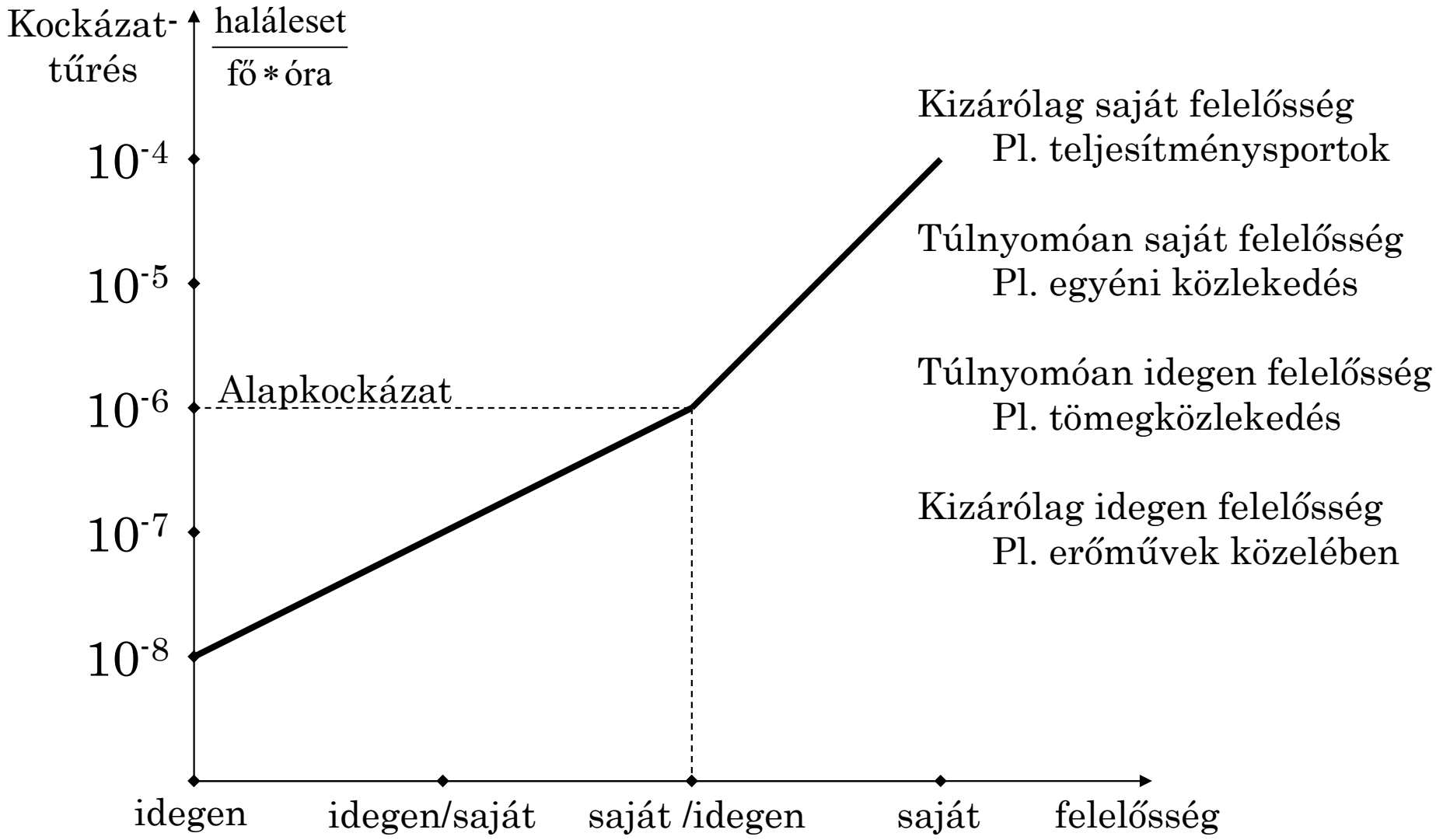
- kockázatmentesség (veszélyforrás-specifikus)
  - a potenciális veszélyeztető hatás megszüntetése
  - a veszélyforrás helyének/hatókörének elkerülése
- kockázatcsökkentés
- **elfogadott kockázati szint** (kockázattűrés)
  - érdekegyeztetés (a kockázat okozója, elszenvedője,hatóság)
  - költségek – elérhető eredmény
  - sok szubjektív szempont

A kockázatcsökkentés eszközei

A kockázatcsökkentés eszközei (műszaki/szervezési intézkedések)

- a rendszer és környezete megfelelő kialakítása, üzemeltetése, karbantartása
- a veszélyforrás és a környezet fizikai elkülönítése
- a veszélyeztető hatású rendszer használatának szabályozása
- **folyamatirányító rendszerek alkalmazása**

A kockázattűrés függése a felelősségtől



Kockázatosztályozás – kockázatcsökkentés

Valószínűségi szint		Kárkihatási kategóriák			
		Kataszt-rofális 4	Kritikus 3	Csekély 2	Elhanya-golható 1
gyakori	A	K4			
valószínű	B				K2
néha	C		K3		
alig	D				
valószínűtlen	E			K1	
rendkívül valószínűtlen	F				

K4 - **elfogadhatatlan kockázat;**

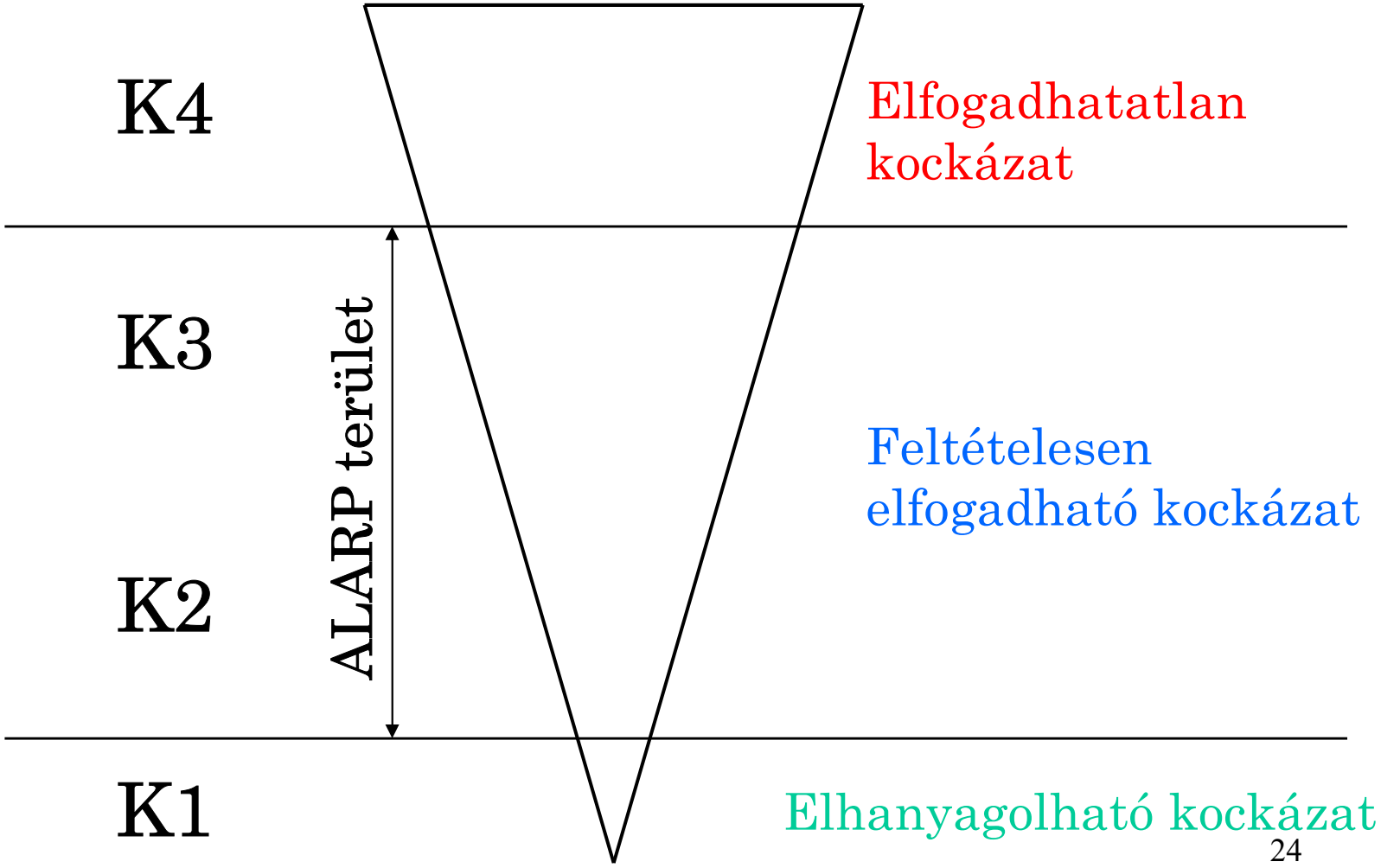
K3 - **nem kívánatos kockázat**; csak akkor fogadható el, ha a kockázatcsökkentés **kivihetetlen**, vagy költségei az eredményhez képest **rendkívül aránytalanok**

K2 – **elfogadható kockázat**, ha a kockázatcsökkentés költségei meghaladnák az eredményt (nem fogadható el, ha kis ráfordítással jó eredmény érhető el)

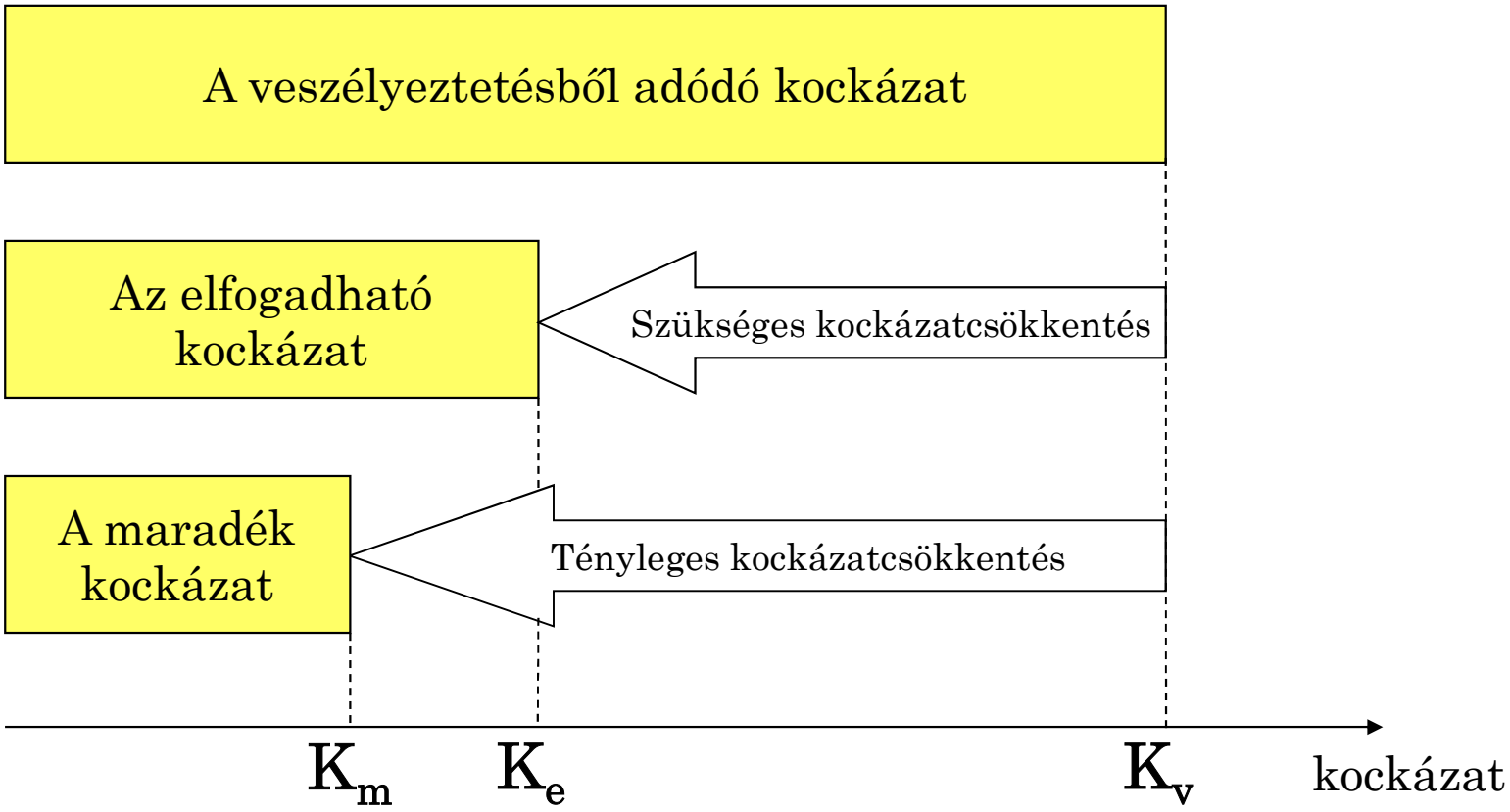
K1 – **elhanyagolható kockázat**

Kockázatcsökkentés – Az ALARP elv

As Low As Reasonably Practicable
Olyan alacsony, amennyire ésszerűen megvalósítható



Kockázatcsökkentés – Kockázatmenedzselés



A kockázatcsökkentés eszközei

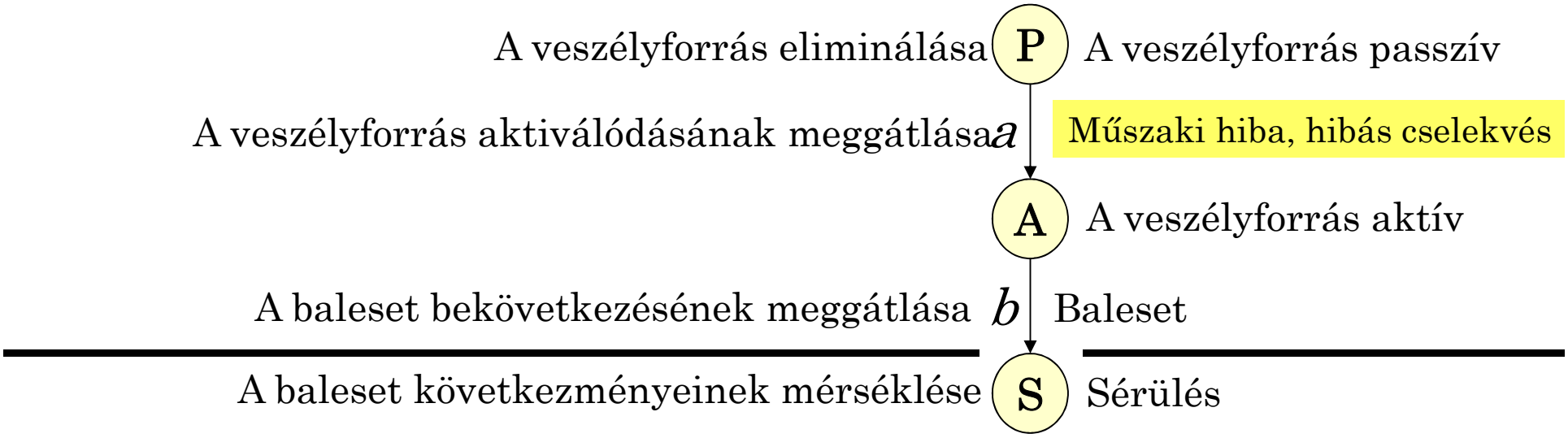
A kockázatcsökkentés eszközei (műszaki/szervezési intézkedések)

- a rendszer és környezete megfelelő kialakítása, üzemeltetése, karbantartása
- a veszélyforrás és a környezet fizikai elkülönítése
- a veszélyeztető hatású rendszer használatának szabályozása
- **folyamatirányító rendszerek alkalmazása**

A kockázatcsökkentés formái – Biztonsági szűrők

A kockázatcsökkentés formái

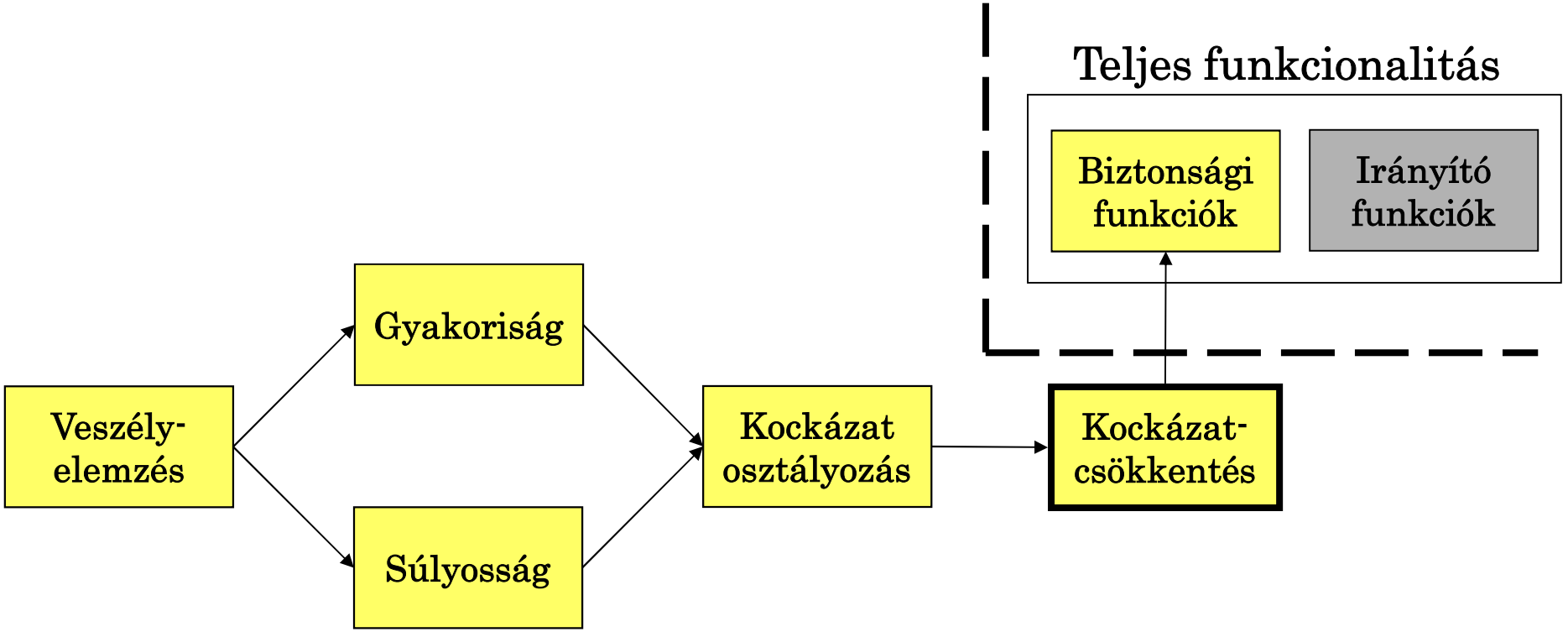
- aktív (a baleset bekövetkezési valószínűségének csökkentése)
- passzív (a kárkövetkezmények mérséklése)



Biztonsági funkciók
Biztonsági integritás

KÜLSŐ ÉS BELSŐ BIZTONSÁG

Biztonsági funkciók

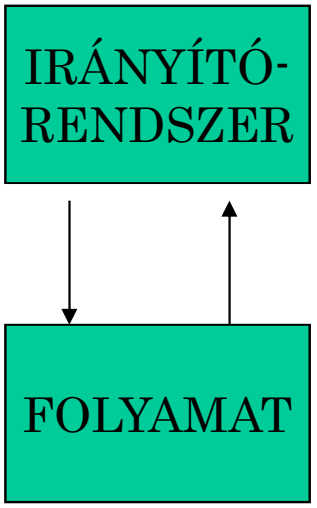


IRÁNYÍTANDÓ FOLYAMAT

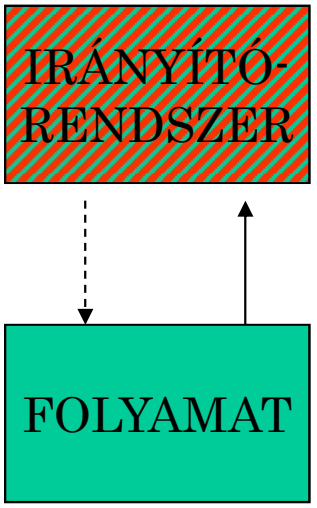
IRÁNYÍTÓ RENDSZER

A biztonsági funkció kiesése

Mi a valószínűsége annak, hogy az irányító rendszer hibátlanul ellátja feladat



Ha az irányítórendszer jól működik, akkor elvégzi a szükséges kockázat-csökkentést



Mi történik, ha az irányítórendszer meghibásodik és

nem látja el a feladatás vagy rosszul látja el?

Minél nagyobb az irányító rendszer szerepe a kockázatcsökkentésben, annál kevésbé engedhető meg, hogy ne lássa el feladatát.

Biztonsági integritás

A **biztonsági integritás** (safety integrity – a biztonság sértetlensége) annak valószínűsége, hogy egy biztonsági rendszer

- az előírt biztonsági funkciókat
- egy adott időszakban
- meghatározott körülmények között

megfelelően végrehajtja: nem lépett fel veszélyeztető meghibásodás.

Biztonsági integritási szintek
(Safety Integrity Levels)

Integritási szintek	Megnevezés
4	Igen magas
3	Magas
2	Közepes
1	Alacsony
0	Nem biztonsági

PÉLDA!

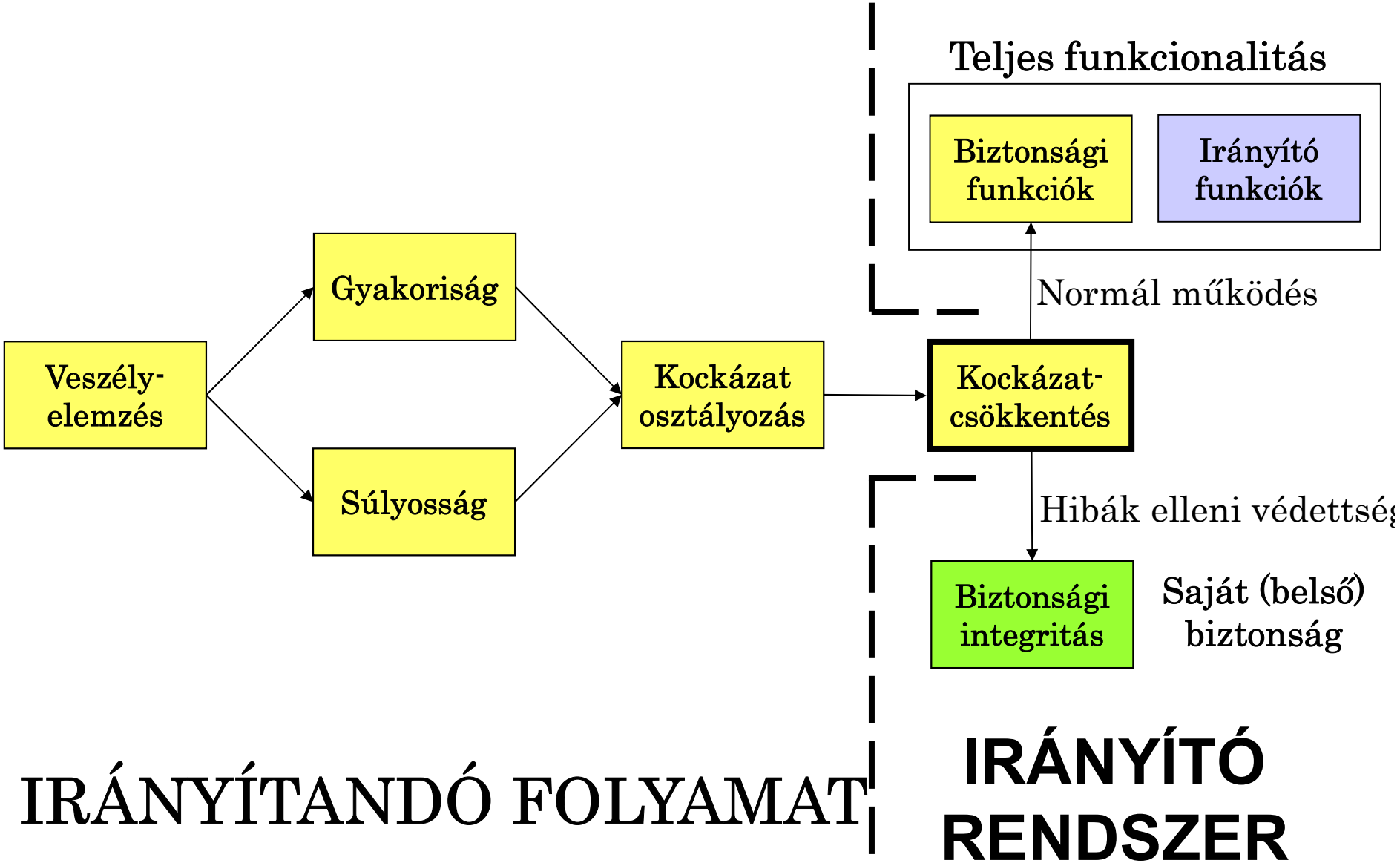
A biztonsági integritási szintek száma és értelmezése

A biztonsági integritási szintek száma a különböző alkalmazási területeken: 1 … 8

Biztonsági integritási szintek **SIL**	Az **irányító** rendszer veszélyes meghibásodásának valószínűsége [h^{-1}]	A **védelmi** rendszer elmaradt működéseinek aránya az összes kívánt működéshez képest
4	10^{-9} … 10^{-8}	10^{-5} … 10^{-4}
3	10^{-8} … 10^{-7}	10^{-4} … 10^{-3}
2	10^{-7} … 10^{-6}	10^{-3} … 10^{-2}
1	10^{-6} … 10^{-5}	10^{-2} … 10^{-1}
0	---	---

PÉLDA!

Biztonsági funkciók – Biztonsági integritás

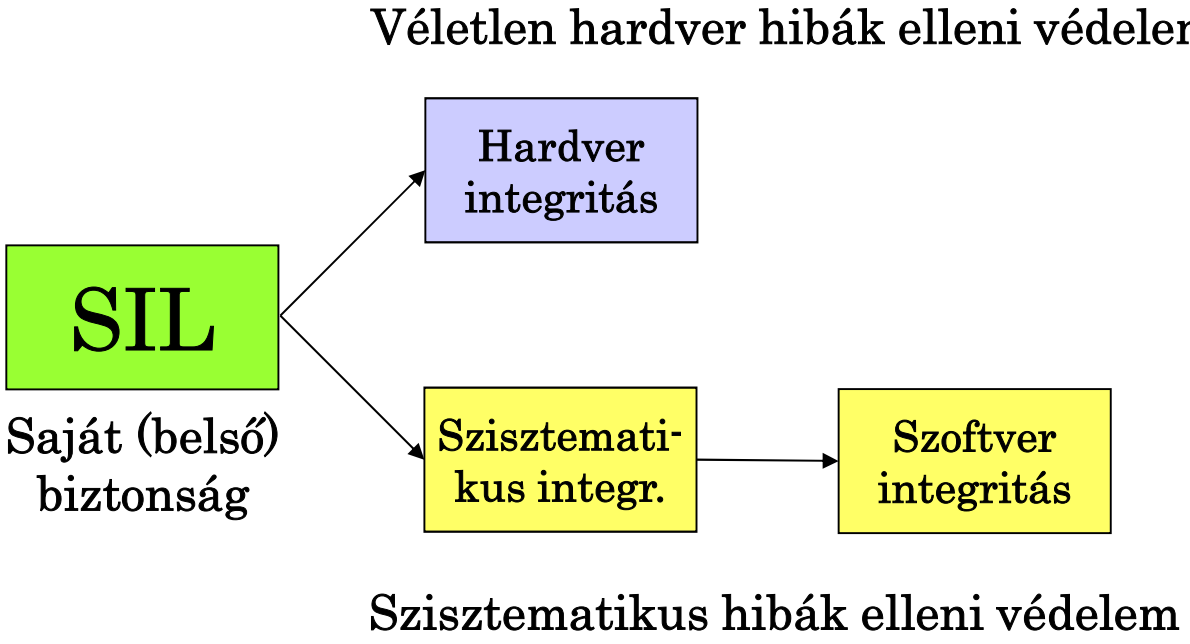


Biztonsági rendszerekben fellépő hibák

Szisztematikus hibák (emberi eredetűek)	Véletlenszerű hibák (hardver meghibásodások)
• Követelményspecifikációs hibák • Tervezési/megvalósítási meg nem felelőségek • Gyártási hibák • **Szoftver** fejlesztési, javítási hibák • Szerelési/üzembehelyezési meg nem felelőségek • Kezelési/karbantartási előírások hibái • Egyéb emberi eredetű hibák	• Üzemmód • Környezeti hatások • Alulterhelés • Túlterhelés • Elhasználódás • Egyebek **Fellépési gyakoriság megadható!**

A biztonsági integritás összetevői

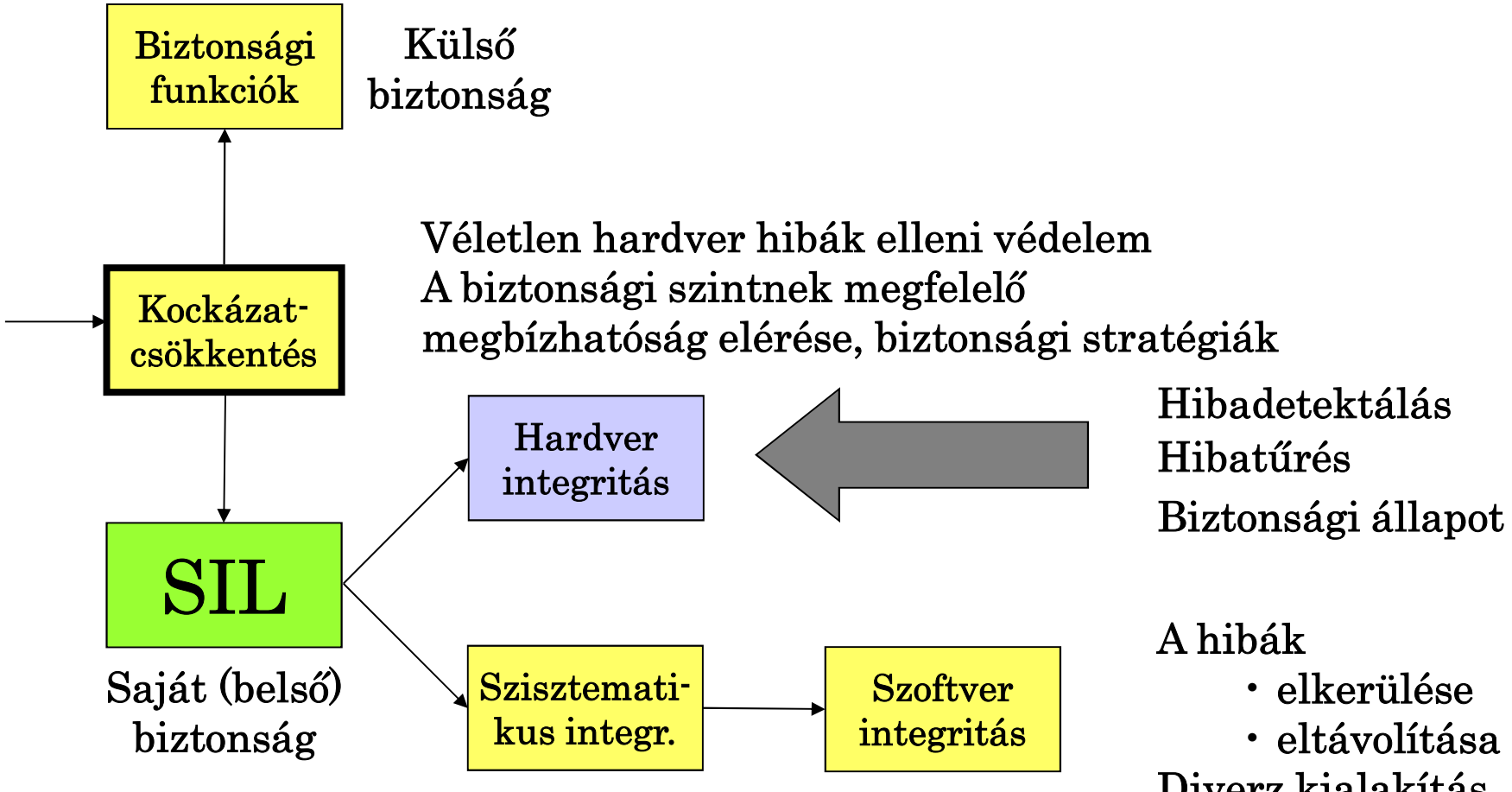
A **hardver integritás** a biztonsági integritásnak
a veszélyes véletlenszerű hardver meghibásodásokra vonatkozó része.



A **szisztematikus integritás** a biztonsági integritásnak
a veszélyes szisztematikus hibákra vonatkozó része.

A **szoftver integritás** a biztonsági integritásnak
a veszélyes szoftver hibákra vonatkozó része.

Biztonsági integritási szintek és hibakezelés

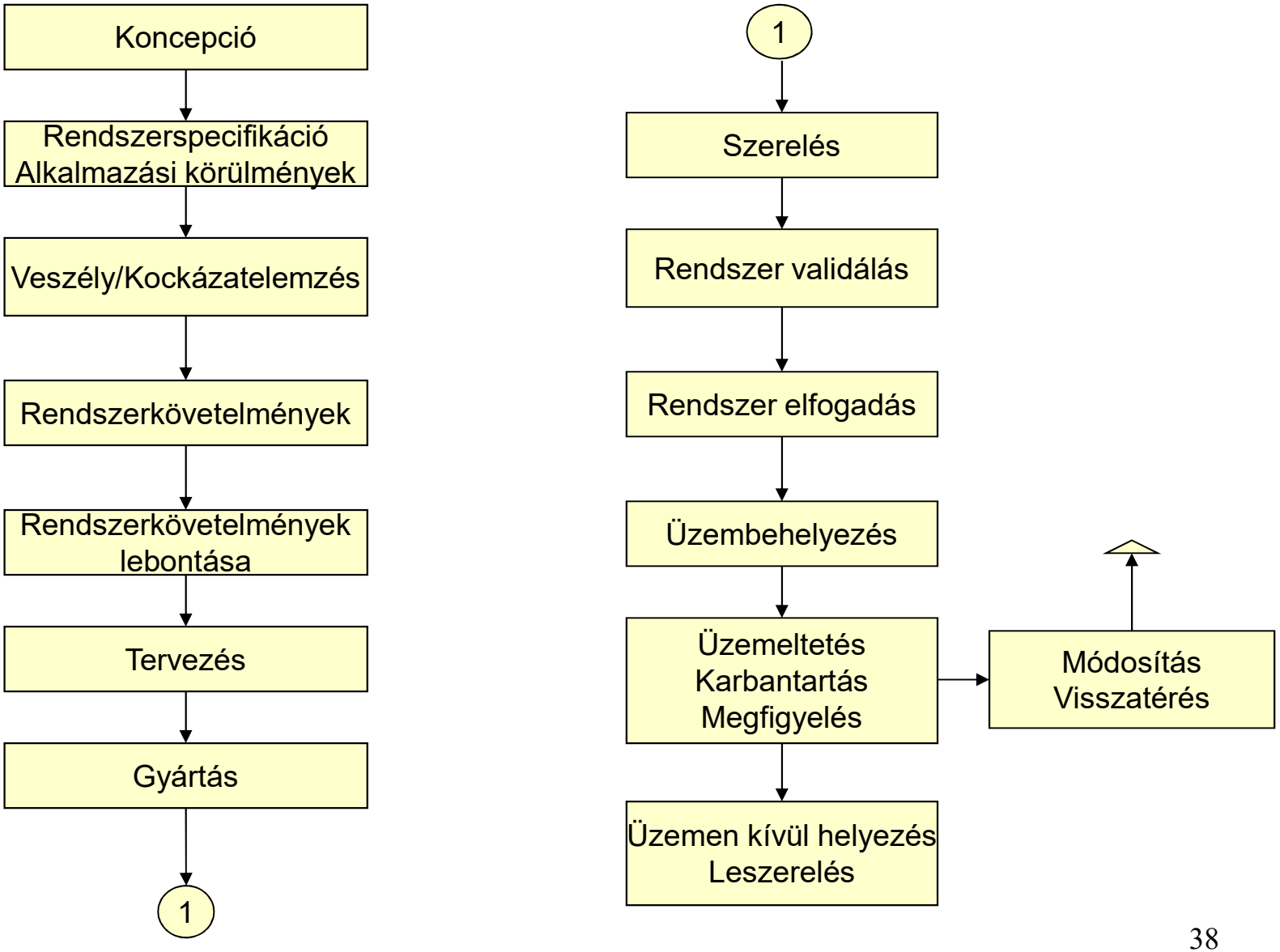


A SZISZTEMATIKUS HIBÁK ELLENI VÉDELEM

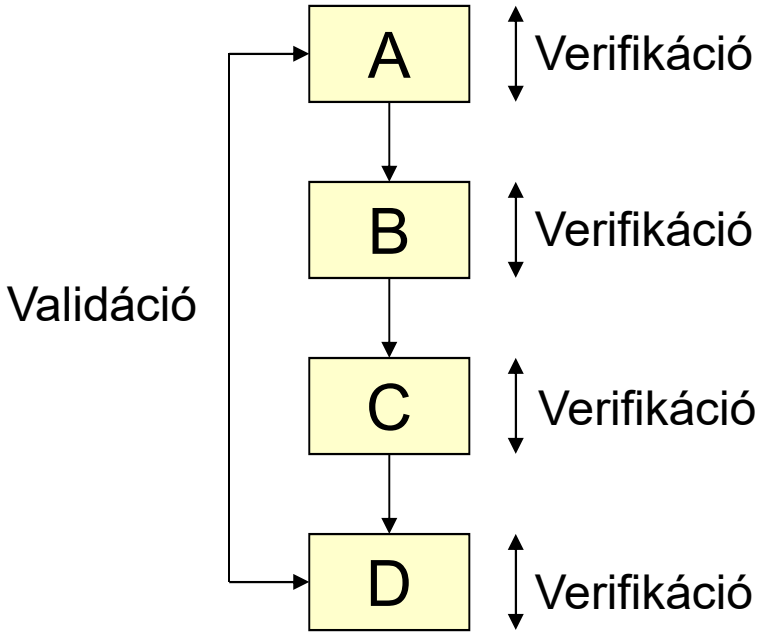
Biztonsági folyamatirányító rendszerek

- életciklusa
- szoftvere

RENDSZER ÉLETCIKLUS MODELL



VERIFIKÁCIÓ, VALIDÁCIÓ



Biztonsági folyamatirányító rendszerek szoftvere

Programozott irányítórendszerek

- Célgépek
  - Nincs operációs rendszer
  - Egyszerű szoftver
  - Pl. egy-chipes mikrokontrollerek
- Univerzális alkalmazású rendszerek
  - Moduláris hardver (általában kártya rendszerű)
  - Tagolt szoftverfelépítés

Követelmények a biztonsági szoftverekkel szemben

Cél: hibamentesség.

Szoftver-megbízhatóságot növelő módszerek

- Jól strukturáltság
- Moduláris felépítés
- Áttekinthetőség – szükséges az ellenőrzéshez is
  - Modulonként kevés be/kimenet (lehetőleg 1-1) → könnyű tesztelni
  - Jól definiált interfészek
  - Feltétel nélküli ugrások (GOTO) kerülése
  - Tesztelhetőség kialakítása – „tesztelés-barát tervezés”
- Jól dokumentáltság
  - Funkciók leírása
  - Interfészek leírása
- Nem-biztonsági részek: arra kell ügyelni, hogy a nem-biztonsági rész semmilyen módon ne legyen hatással a biztonsági részekre – visszahatásmentesség.

A szisztematikus hibák elleni védelem

- A fejlesztési/tervezési/gyártási folyamat szabályozása → életciklus modellek
  - követhetőség, ellenőrizhetőség, áttekinthetőség
- Személyi függetlenségek
  - ellenőrizhetőség
- Megfelelő módszerek alkalmazása
  - hibaelkerülés

A VÉLETLENSZERŰ HIBÁK ELLENI VÉDELEM

Megbízhatóság

Biztonsági stratégiák

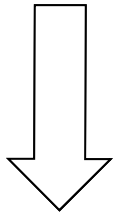
BIZTONSÁGI STRATÉGIÁK

AZ IRÁNYÍTÓ RENDSZER VÉLETLENSZERŰ MEGHIBÁSODÁSAI ELLENI VÉDELEM ESZKÖZEI

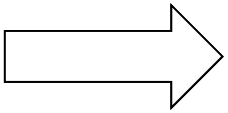
BIZTONSÁGI STRATÉGIÁK
- MÓDSZEREK
- ELJÁRÁSOK

VESZÉLYFORRÁSOK
- KIKÜSZÖBÖLÉSE
- HATÁS KIKÜSZÖBÖLÉSE
- HATÁS MÉRSÉKLÉSE

$P_B(t) \geq P_{Bmin} \leftrightarrow P_V(t) \leq P_{Vmax}$



IRÁNYELVEK, INTÉZKEDÉSEK
- MŰSZAKI
- SZERVEZÉSI



IRÁNYÍTÓ RENDSZER
- KIALAKÍTÁSA
- ÜZEMELTETÉSE

(Karbantartás, javítás)

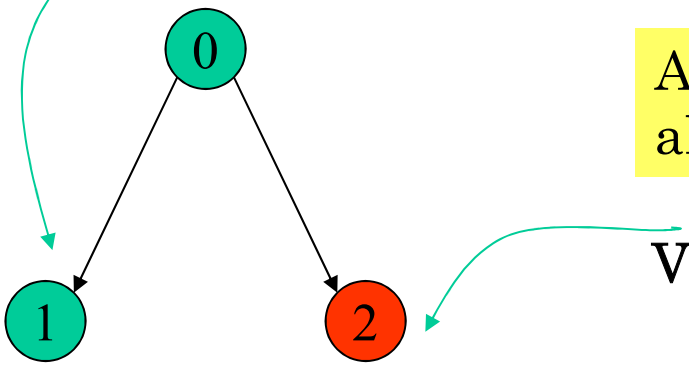
BIZTONSÁGI STRATÉGIÁK

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

AZ IRÁNYÍTOTT FOLYAMAT JELLEGÉTŐL FÜGGŐ VÁLASZTÁS

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

FAIL-SAFE STRATÉGIA



AKADÁLYOZÓ ÁLLAPOT

- hibafelismerés, lekapcsolás
- hibakatalógus ⇒ hibaszituációk

A hibafelismerő mechanizmus hibája is akadályozó állapotot kell, hogy kiváltson!

VESZÉLYEZTETŐ ÁLLAPOT

- tudatos kockázatvállalás - hibakizárás
  kockázat-tűrés!!!
- nem tudatos kockázatvállalás

Intézkedések
a nem tudatos kockázatvállalás mérséklésére

A rendszer az egyszer már elért akadályozó állapotot csak emberi beavatkozásra (javítás) hagyhatja el.

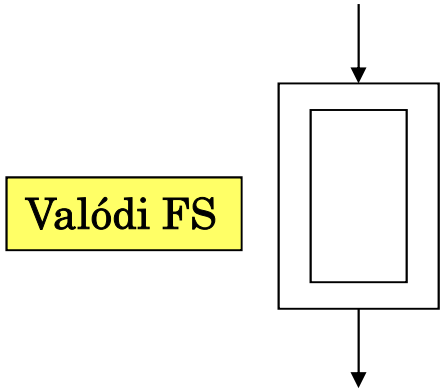
FAIL-SAFE STRATÉGIA

VALÓDI FAIL-SAFE RENDSZEREK

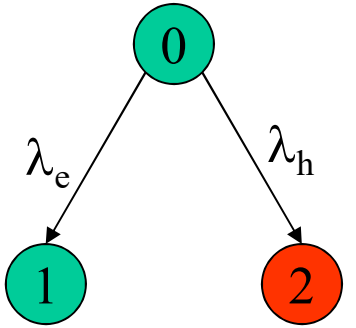
Önellenőrző tulajdonság:
kapcsolóelemek +
kapcsolástechnika
Egycsatornás kialakítás

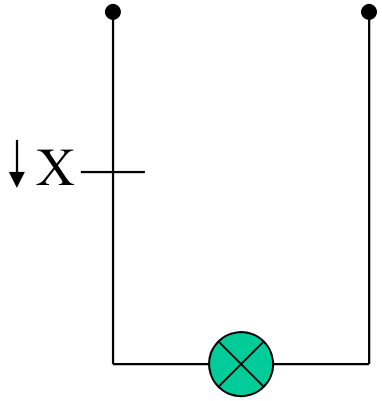
ASZIMMETRIKUS MEGHIBÁSODÁSI TULAJDONSÁG

különböző parciális meghibásodási ráták



Valódi FS





Kapcsolóelemek
- biztonsági jelfogók
- speciális elektronika

$\lambda = \lambda_e + \lambda_h$

$\lambda_h << \lambda_e$

$\lambda_v << \lambda_a$

FAIL-SAFE STRATÉGIA

EGY HIBA ELV

- a kapcsolásokat úgy kell kialakítani,egy hiba önmagában ne okozhasson veszélyeztető állapotot;

- a hibafelismerő mechanizmus kialakításánál elegendő egyidejűleg egy hibát feltételezni ha,

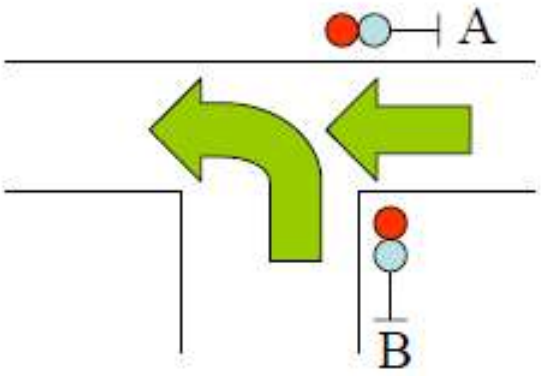
  - ez a hiba felismerhető, és
  - a hibafelismerő mechanizmusnak nem kell túl sok elemet ellenőriznie;

- a fellépő hibát még egy újabb hiba fellépése előtt fel kell ismerni, és a rendszert akadályozó állapotba kell vezérelni, hogy az esetleges további hibák hatástalanok legyenek:

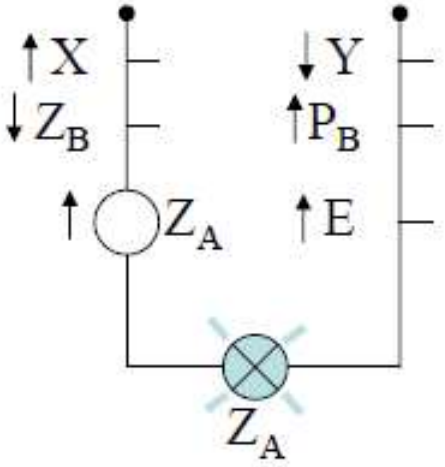
- amennyiben az első hiba nem ismerhető fel, úgy további egyidejű hibákat kell feltételezni mindaddig, amíg a hibakombináció felismerhetővé nem válik.

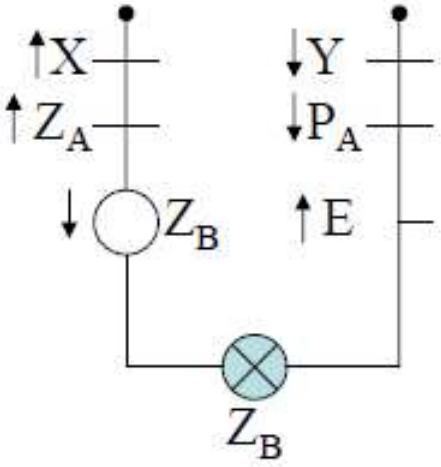
FAIL-SAFE STRATÉGIA

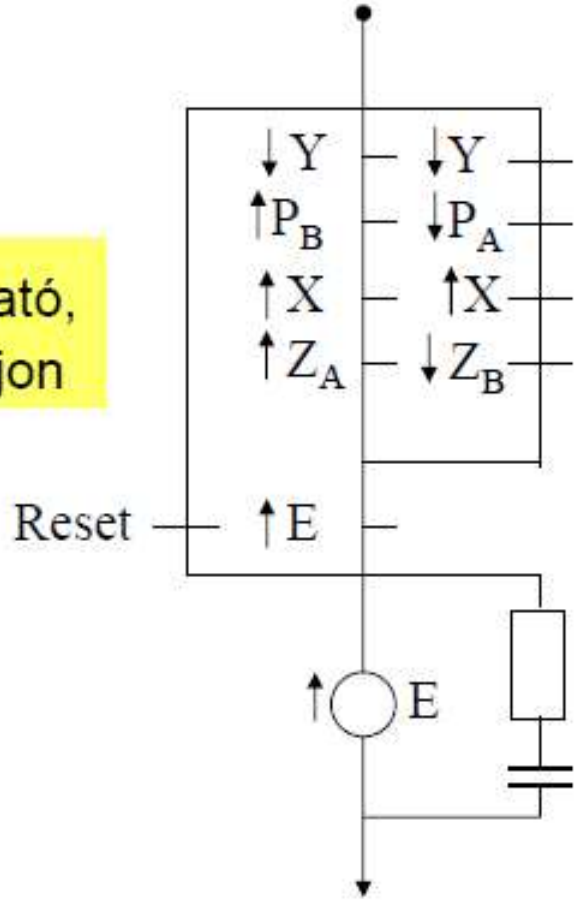
PÉLDA



Biztonsági jelfogóknál konstrukciós alapon kizárható, hogy a jelfogó állapotával ellentétes érintkező zárjon

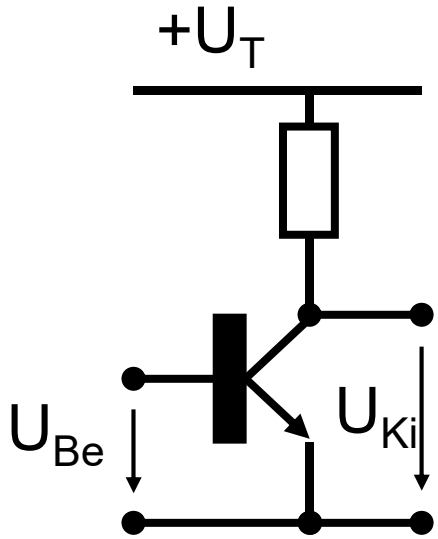


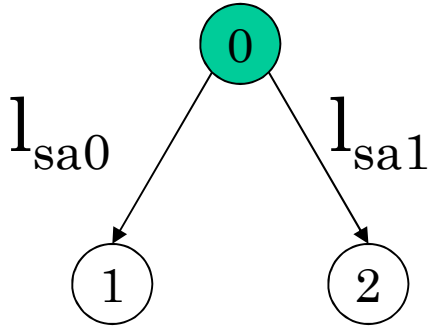




FAIL-SAFE STRATÉGIA

FÉLVEZETŐ ELEMEK PROBLÉMÁJA





$$l_{sa0} \approx l_{sa1}$$

Szimmetrikus meghibásodási tulajdonság
Nincs veszélytelen hibaállapot

Stuck at 1 – sa1

Stuck at 0 – sa0

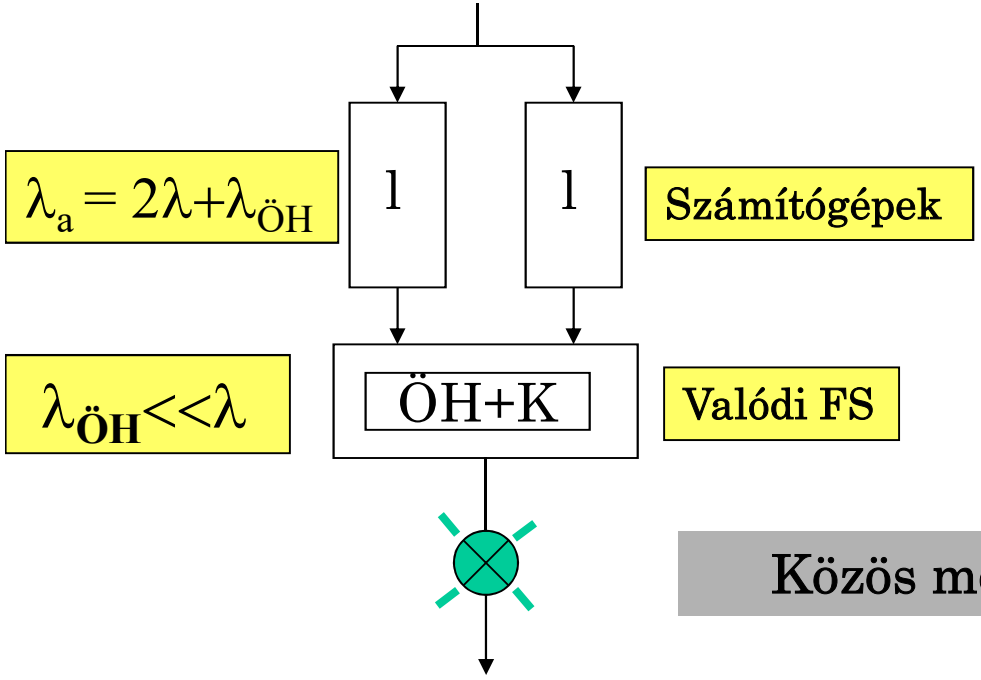
Megoldás:

- speciális,valódi FS elektronika
- többcsatornás kialakítás

FAIL-SAFE STRATÉGIA

KVÁZI FAIL-SAFE RENDSZEREK

Információfeldolgozás:
nem fail-safe
Többcsatornás kialakítás
Valódi FS összehasonlító



Közös módusú hibák ellen nem véd

Összetett (kompozit) hibabiztosság

KVÁZI FAIL-SAFE RENDSZEREK

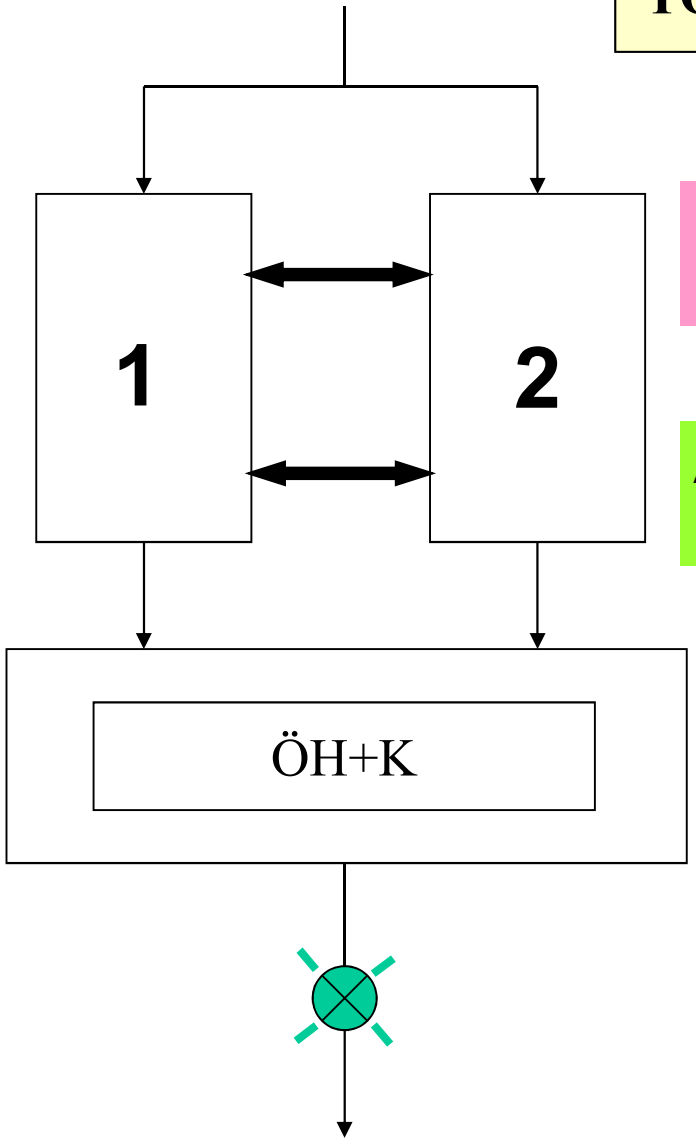
Minden egyes biztonságreleváns funkciót ***legalább két egység*** lát el.
Ezeknek az egységeknek függetlenek kell lenniük minden más egységtől
a ***közös eredetű hibák elkerülése*** végett.

A nem akadályozó (restrictive) jellegű működések csak akkor hajtódhatnak végre, ha a szükséges számú egység “egyetért”.

Egy egység veszélyes hibájának felismerése és hatástalanítása
adott időn belül meg kell, hogy történjen annak érdekében,
hogy a második egység azonos jellegű
hibája elkerülhető legyen.

FAIL-SAFE STRATÉGIA

TÖBBSZINTŰ ÖSSZEHASONLÍTÁS



A beolvasott adatok cseréje és összehasonlítása

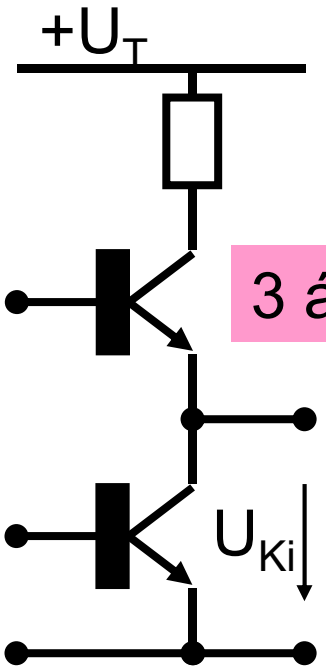
A feldolgozott adatok cseréje és összehasonlítása

FS összehasonlító és kapcsoló

FAIL-SAFE STRATÉGIA

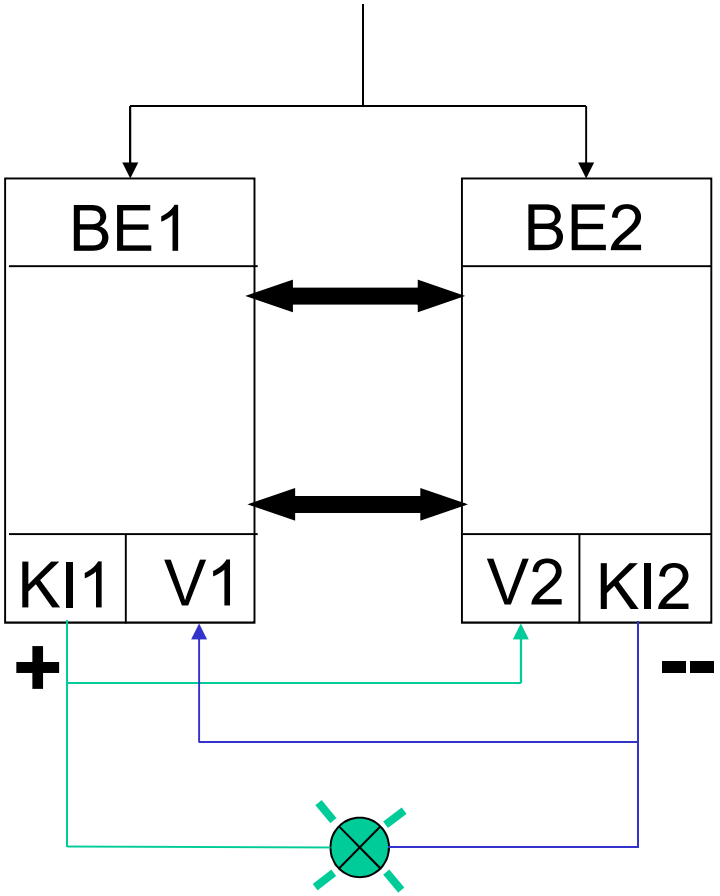
ÖSSZEHASONLÍTÁS
KÖZVETLEN VEZÉRLÉSSEL ÉS VISSZAOLVASÁSSAL

Totem-pole kapcsolás



3 állapotú kimenetek

Tristate



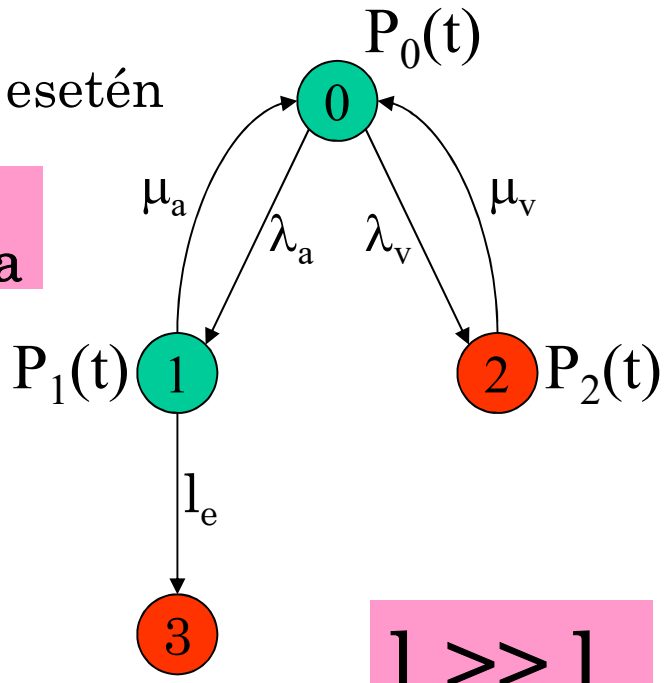
FAIL-SAFE STRATÉGIA

Ember-gép rendszer

Az irányító rendszer **akadályozó** állapota esetén
a forgalom fenntartása érdekében
az ember beavatkozik.

l_a

Ezzel részben vagy egészben átveszi
a meghibásodott műszaki rendszertől
a **biztonsági felelősséget** is.



Hibás emberi tevékenység
következtében
az ember-gép rendszer **veszélyeztető**
állapotba kerülhet („3”).

$l_e >> l_a$

A szükséges emberi beavatkozások száma függ attól is,
hogy az akadályozó állapot milyen hosszú ideig áll fenn

m_a

FAIL-SAFE STRATÉGIA

A humán hibagyakoriság mérséklése

A hibás emberi cselekvés gyakorisága $\lambda_e = 10^{-3} \ldots 10^{-4}$ / cselekvés.

Mérséklési lehetőségek (forgalomirányító személyzet, járművezetők, javító személyzet):

- a biztonsági feladatot ellátó irányító rendszer minél ritkábban kerüljön akadályozó állapotba, és minél rövidebb ideig tartózkodjon ebben az állapotban;
- a rutinműveletektől való mentesítés (kevesebb cselekvés),
- vezetett cselekvéssor (check-listák, gépi támogató eszközök),
- hibajelzések, javítási eljárások a javító személyzet számára;
- megfelelő kiképzés, szinten tartás.

SAFE-LIFE STRATÉGIA

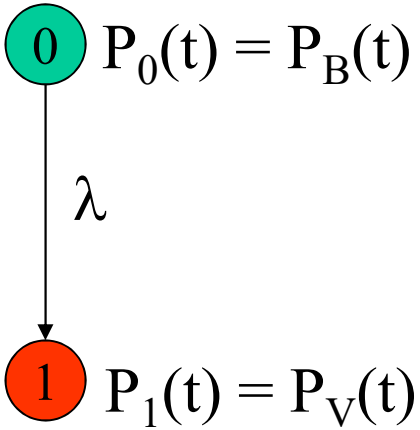
TÖKÉLETESSÉG, HIBAKIZÁRÁS

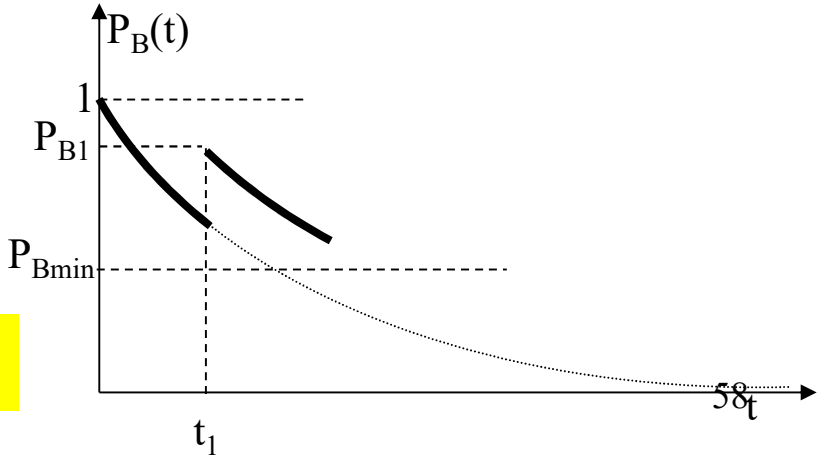
IDEÁLIS $l = 0$

VALÓSÁGOS $l \approx 0$

KORLÁTOZOTT ALKALMAZÁS
- EGYSZERŰ ELEMEK, RENDSZEREK
- RÖVID BIZTONSÁGOS ÉLETTARTAM

MEGELŐZŐ KARBANTARTÁS





WORST CASE FELTÉTELEZÉS

SAFE-LIFE STRATÉGIA

Bennfoglalt (inherens) hibabiztosság

Ennél a technikánál megengedjük, hogy ***egyetlen egység*** lásson el egy biztonságreleváns funkciót, feltéve, ha annak valószínűsíthető meghibásodási módjai nem veszélyesek.

Bármely olyan hibamódot, amelyet ***valószínűtlennek*** minősítenek (pl. belső fizikai tulajdonságok miatt), ilyen szempontból ***igazolni kell***.

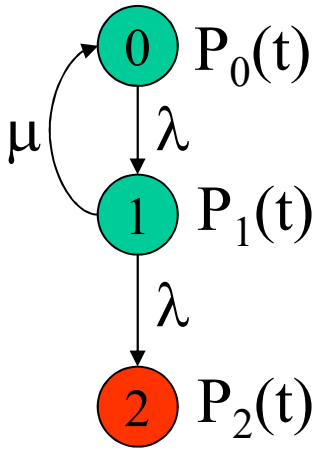
A bennfoglalt hibabiztosságot összetett és reaktív hibabiztosságú rendszerekben fel lehet használni, például az egységek közötti függetlenség biztosítására, illetve veszélyes hiba észlelésekor a rendszer leállításának kikényszerítésére.

FAULT-TOLERANT STRATÉGIA

A HIBA FELISMERÉSE ÉS HATÁSÁNAK MASZKOLÁSA

HARDVER-REDUNDANCIA / TARTALÉKOLÁS

$\mu >> \lambda$



$$P_B(t) = \sum_{i=0}^{1} P_i(t)$$

$$P_V(t) = P_2(t)$$

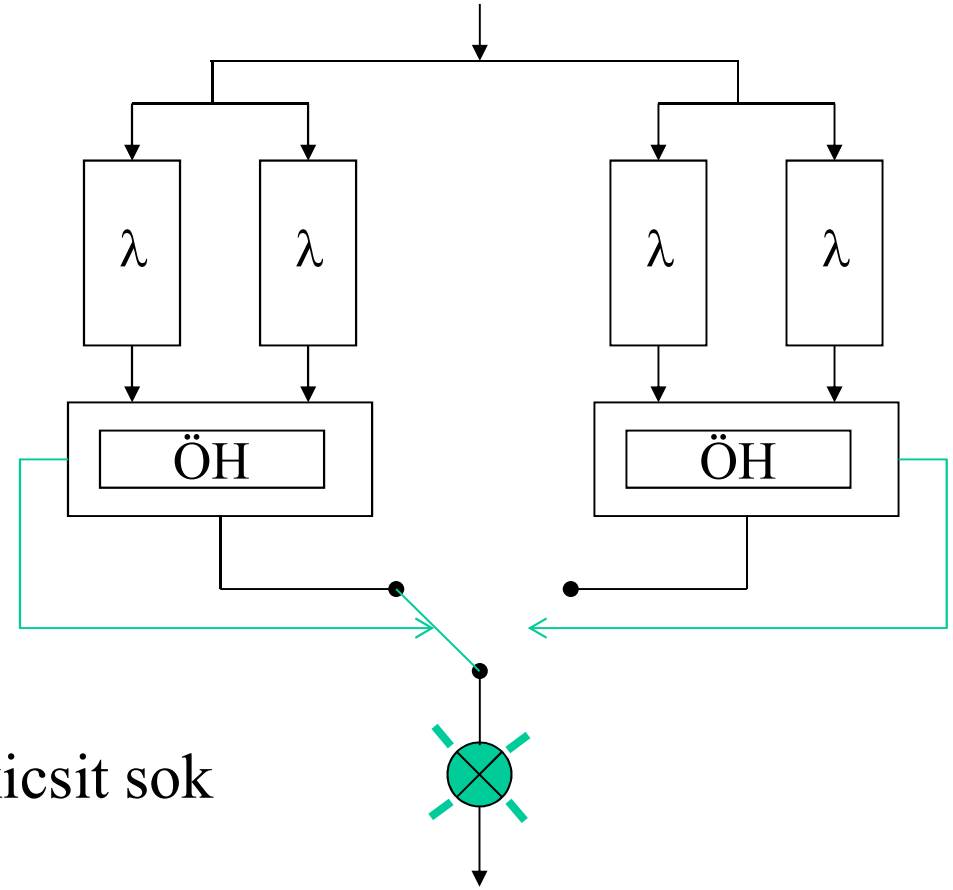
A biztonsági rendszerek működőképességének biztosítása

- teljes értékű tartalékolással (teljes funkcionalitás)
- csökkentett értékű tartalékolással (csökkentett funkcionalitás).

EGYÉB REDUNDANCIA FORMÁK

FAULT-TOLERANT STRATÉGIA

2x(2v2) RENDSZER

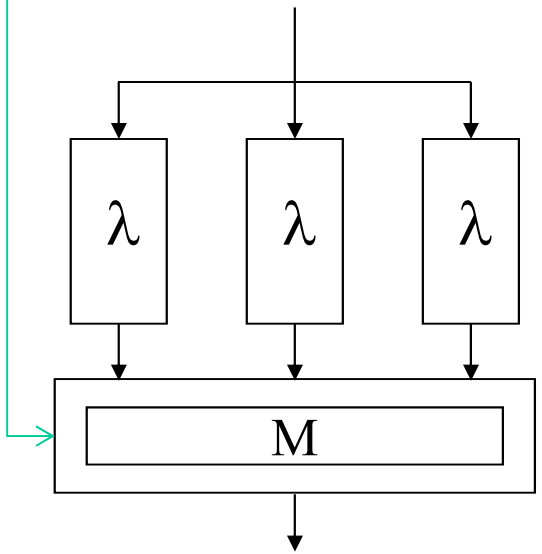


Jó, csak egy kicsit sok hardver kell.

FAULT-TOLERANT STRATÉGIA

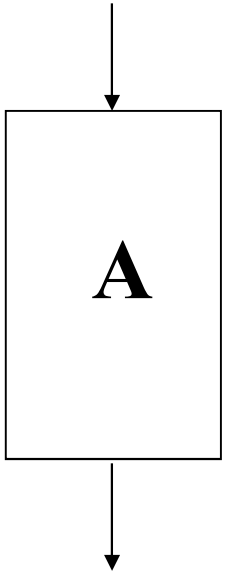
TÖBBSÉGI LOGIKA (SZAVAZÓ) ALKALMAZÁSA

3-ból 2 szavazólogika



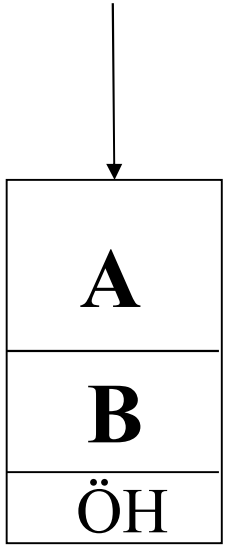
Biztonsági architektúrák

- 1 hardver, 1 szoftver
  - Lehet, h. a szoftver jól van megírva,
  - de a hardver véletlen hibái ellen semmi nem véd.



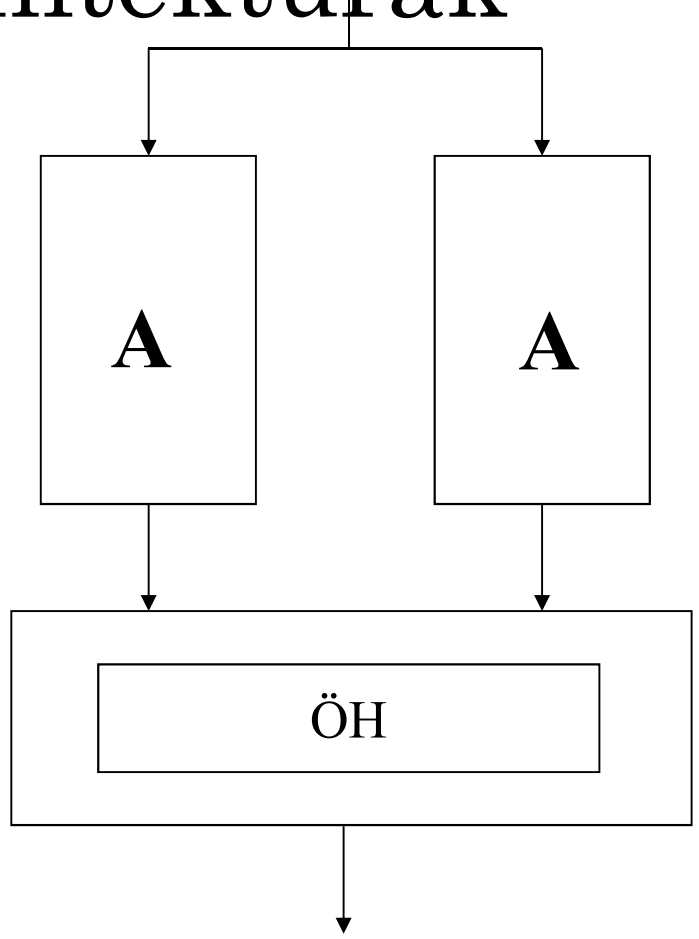
Biztonsági architektúrák

- 1 hardver, 2 szoftver
  - Két különböző (diverz) szoftver fut (A és B) ugyanazon a gépen.
  - Két szoftver futhat párhuzamosan, vagy egymás után.
  - Az összehasonlító felfedi, ha a két szoftver mást mond → felfedhetők a specifikációs és programozási hibák
  - Mivel a két program eltérő, ezért egy HW hiba nem egyformán hat a két szoftverre, így a véletlen HW hibák is felfedhetők
- Pl. Ebilock (svéd) elektronikus bb.



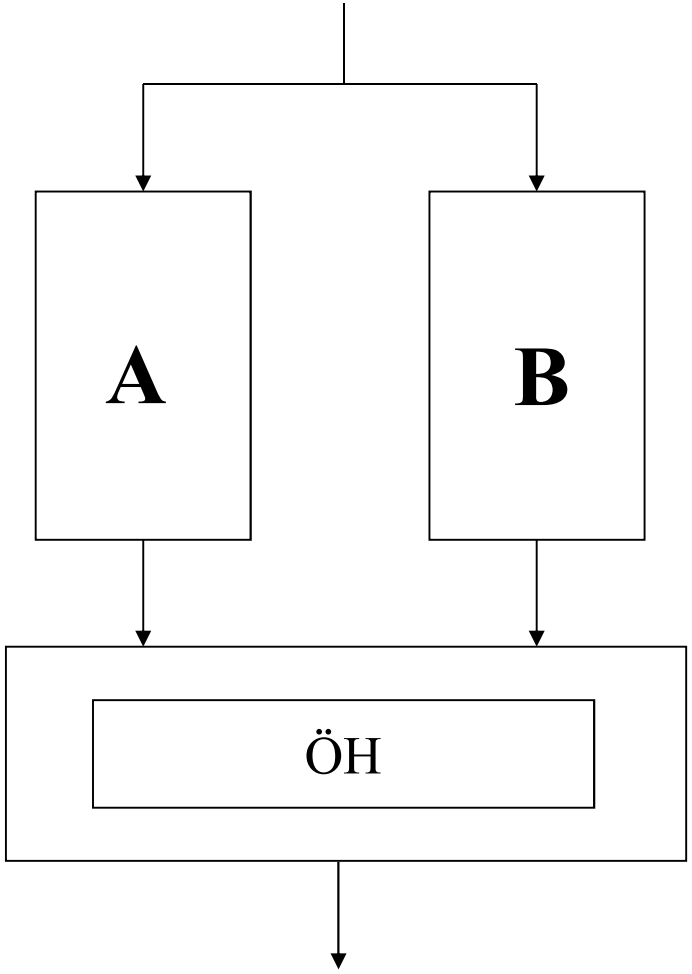
Biztonsági architektúrák

- 2 hardver, 1 szoftver
  - 2-ből 2 rendszer (2v2)
  - Véd a hardver véletlen meghibásodásai ellen
  - A szoftvert „eleve jóra” kell készíteni, mert az architektúra nem véd a specifikációs és programozási hibák ellen.
- Pl. Siemens SIMIS-elv



Biztonsági architektúrák

- 2 hardver, 2 szoftver
  - Az architektúra véd a véletlen hardver hibák ellen és
  - a szoftver hibák ellen.
  - A két csatornában eltérő specifikációval, eltérő programnyelven kifejlesztett programok futnak
- Pl. Alcatel (Thales) Elektra



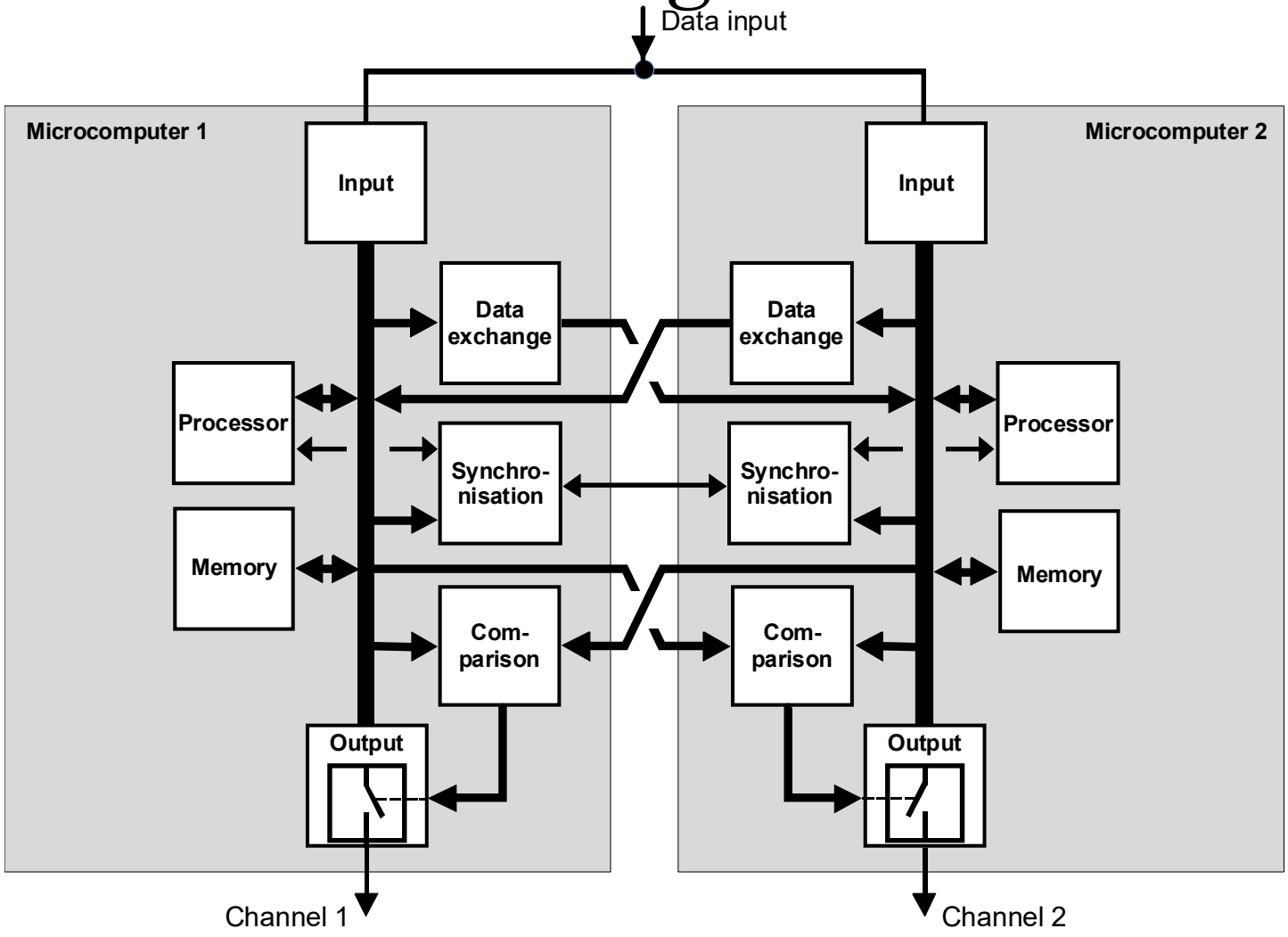
Rendelkezésre állás

- Az eddig bemutatott architektúrák biztonságosak ugyan, de már egy hiba esetén is működésképtelenek.
- Módszerek a rendelkezésre állás növelésére → Tartalékolás
  - Egycsatornás rendszer: redundancia
  - 2v2 → 2×(2v2) (pl. SIMIS IS: SIMIS PC)
  - 2v2 → 2v3 (pl. SIMIS IS: ECC számítógépek)

2v2

- 2 mikroszámítógép
- óraszinkron
- utasításszinkron
- a mikroszámítógépektől független 2 összehasonlító
- összehasonlítja a kimeneteket és a
- processzor tartalmakat (memóriát)

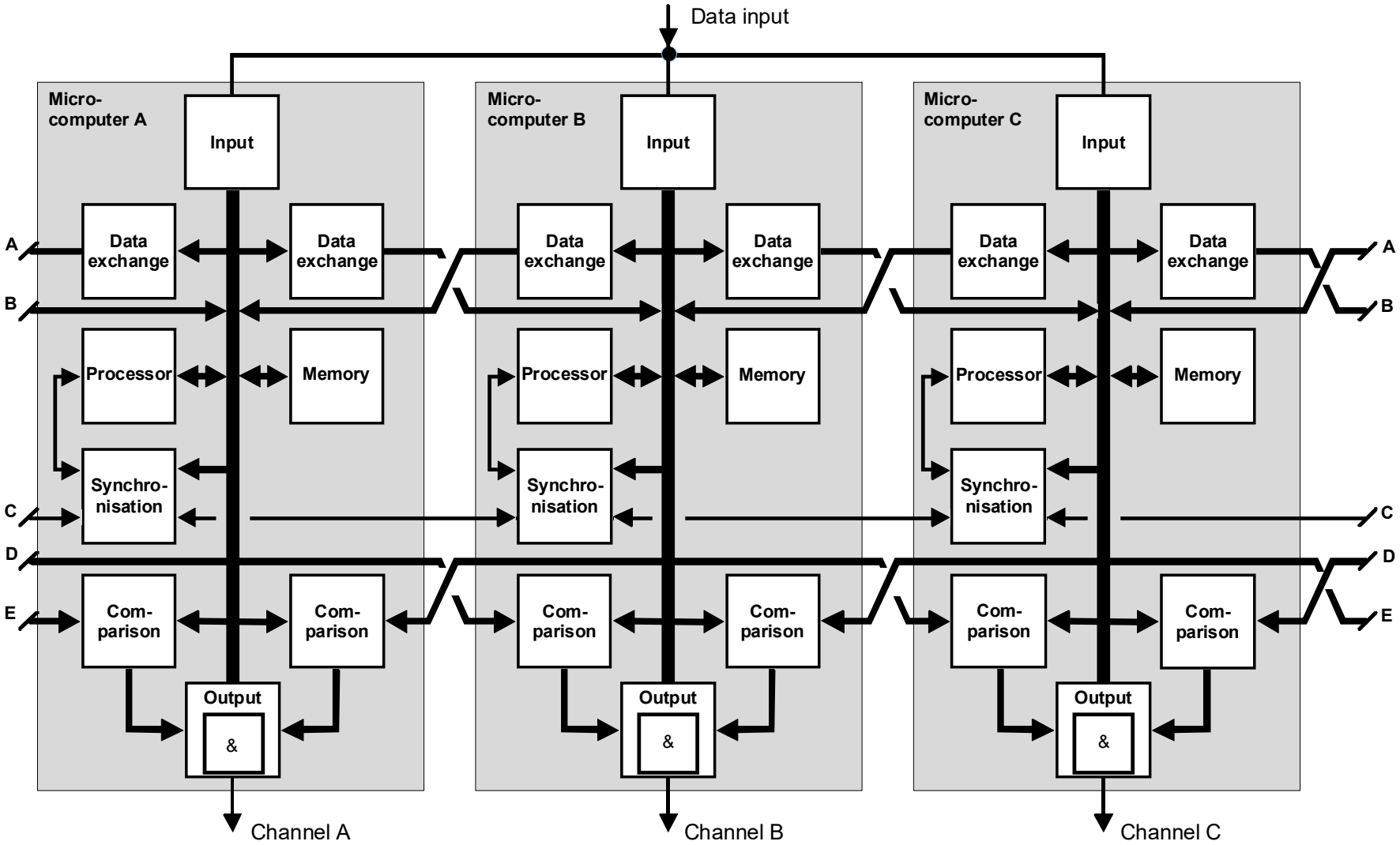
Számítógép konfigurációk
2v2 konfiguráció



2v3

- 3 mikroszámítógép
- 6 független összehasonlító egység
- a 3. csatorna is aktív
- hiba esetén a hibás csatorna/modul leáll
- tovább működik 2v2 rendszerként

2v3


Data input
Micro-computer A
Micro-computer B
Micro-computer C
Input
Data exchange
Processor
Memory
Synchro-nisation
Com-parison
Output
&
A
B
C
D
E
Channel A
Channel B
Channel C

A KÖZÚTI KÖZLEKEDÉSI AUTOMATIKA

A közúti forgalomirányítás célja

- A közlekedési folyamatok befolyásolása meghatározott célok elérése érdekében.

- A forgalomirányító rendszer tervezésének első lépése az elérendő célok meghatározása:
  - Forgalombiztonság javítása
  - Torlódás elkerülése
  - Az infrastruktúra jobb kapacitás kihasználása
  - Adott útvonalak tehermentesítése
  - Környezeti terhelés csökkentése
  - Makrogazdasági szempontok

- A célmeghatározás **problematikus** az egymásnak ellentmondó célok miatt:
  - egyéni érdek,
  - társadalmi érdek,
  - politikai érdek.

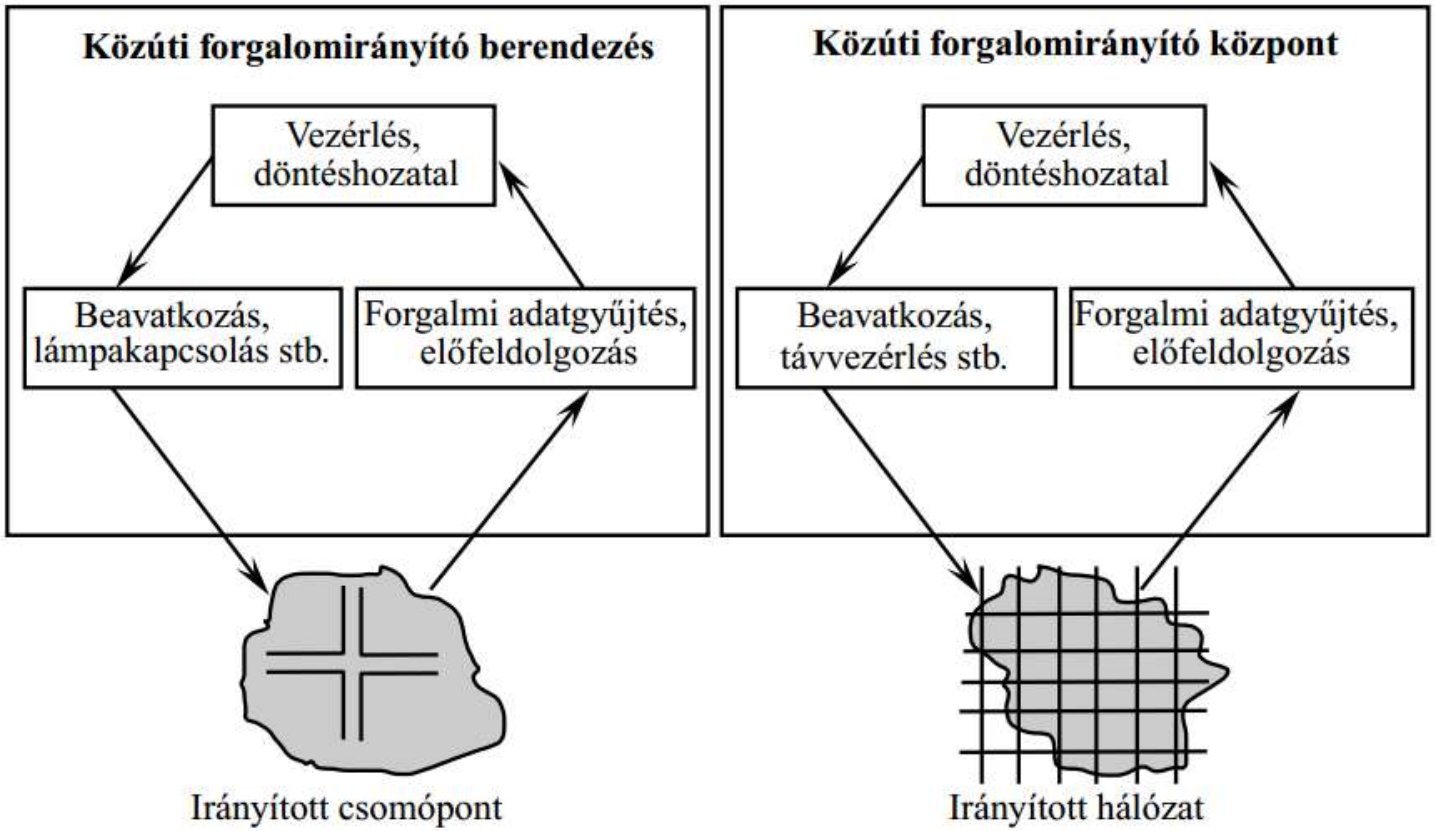
- A tervezés 2. lépése a célok matematikai leírása: **célfüggvény** felállítása

- A célfüggvény a célokat leíró paraméterek súlyozott összege:

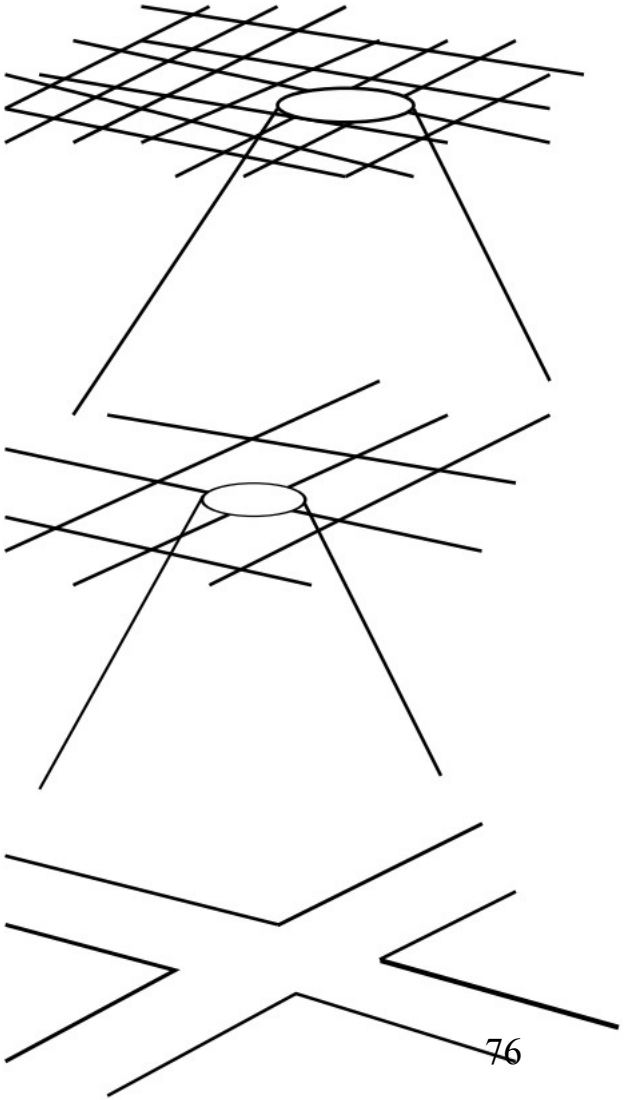
$$J(t) \rightarrow min$$

Információáramlás a forgalomirányításban

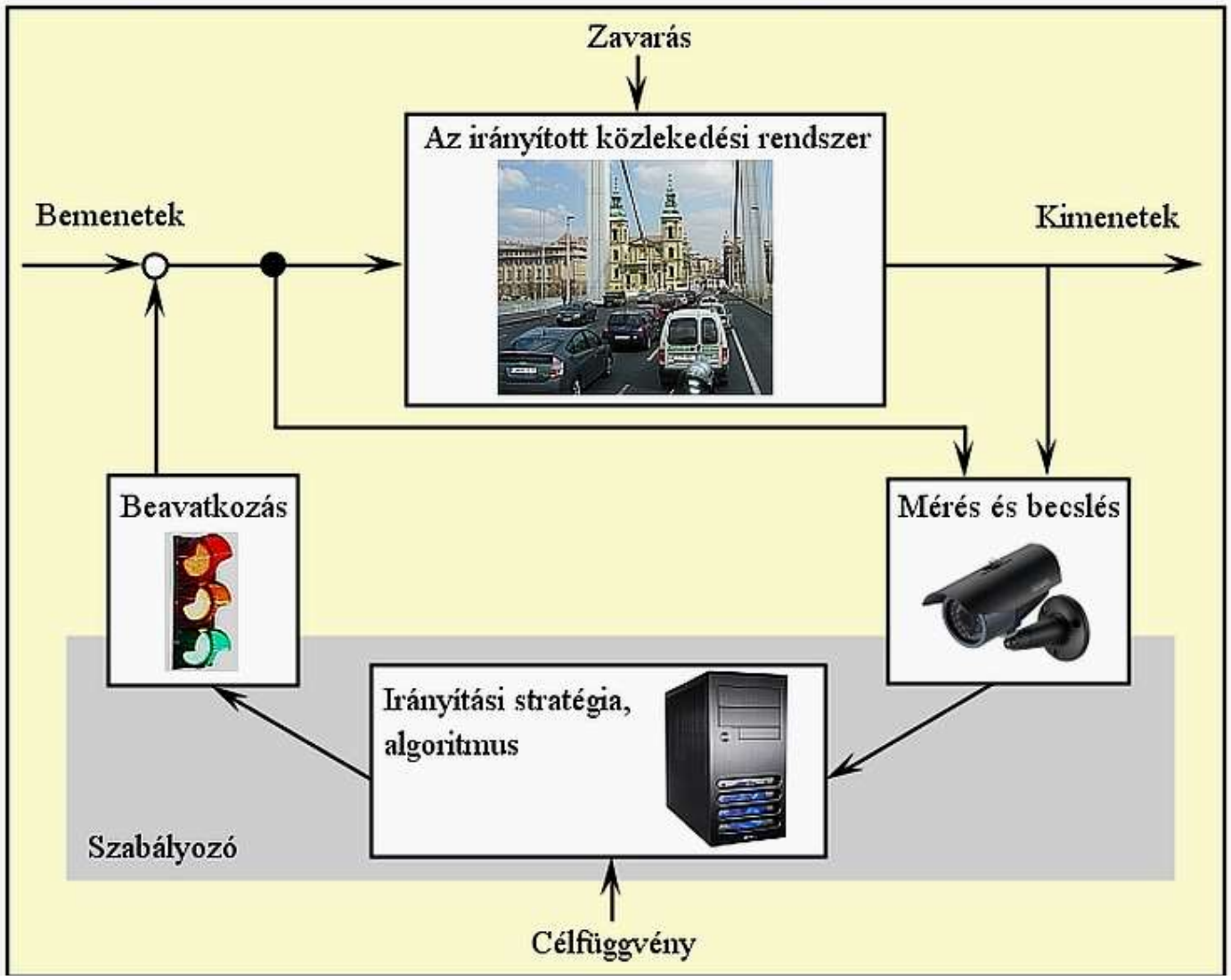
- Az általános szabályozási kör minden forgalomirányító rendszerben azonos



- A nagyobb irányítórendszereket szintekre oszthatjuk.
- Az egyes szinteken más-más célfüggvények érvényesülnek.
- A felsőbb szinteken: globális, stratégiai célok
- Az alsóbb szinteken: lokális célok
- A szintek közötti kapcsolatot biztosítani kell!



A közúti közlekedésirányítás szabályozási köre



Közúti forgalomirányító berendezések

- A csomóponti járműmozgások biztonságos irányítása
- Optimális jelzésterv: lokális/hálózati forgalomfüggő mód

- Moduláris felépítés:
  - 2 CPU kártya:
    az egyik ellenőrzi a másikat!
  - Lámpakapcsoló kártya
  - Detektorkártya
  - Hálózati tápellátást vezérlő kártya
  - Kommunikációs kártya

A forgalomirányító berendezés biztonsági funkciói

- Milyen hibák lehetségesek?
  HW és SW
- Jelzőfejek:
  - hamis jelzésképek
    - piros fénypont: áram ellenőrzés,
    - zöld fénypontok: „zöld együttégés” ellenőrzése feszültség vizsgálattal
  - Izzókiégés:
    - Piros / sárga / zöld fénypontok (áram/teljesítmény ellenőrzéssel)
- A jelzésterv folyamatos ellenőrzése a közbensőidő mátrix alapján
- A közbenső idő mátrix a gép EPROM-jába van égetve!

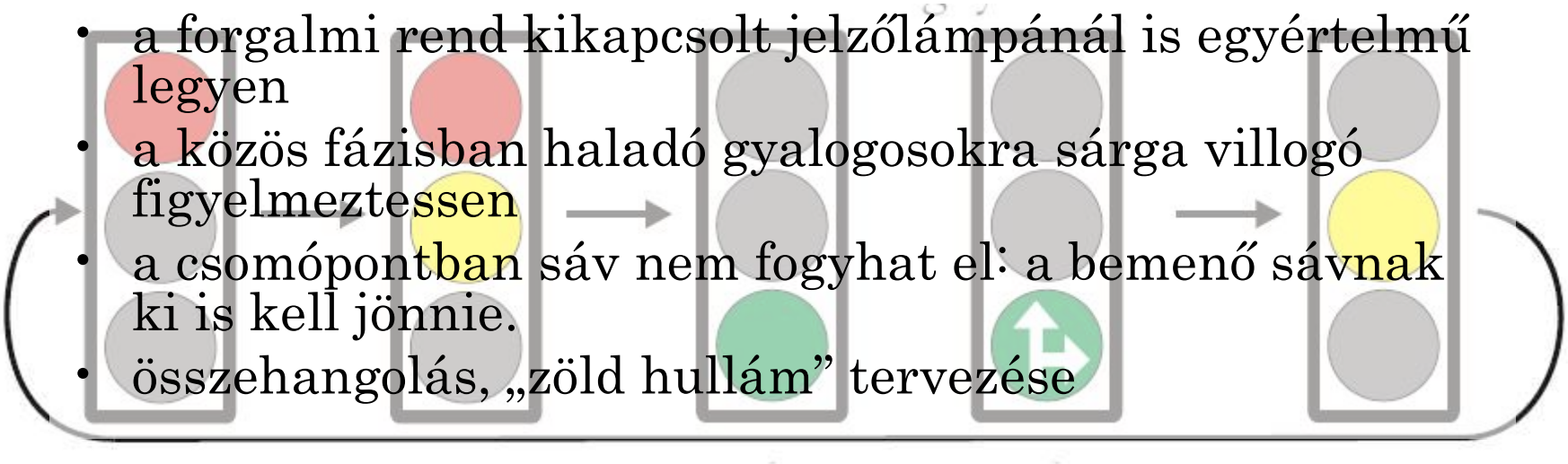
- A jelzők megbízhatósága biztonságkritikus!
- Szigorú előírások teljesítése!
  - Fényintenzitás (cd=lm/str)
  - Fénysugár nyílásszög
    - Főjelző: W (Wide)
    - Ismétlőjelző lehet N (Narrow)
  - Fantomfény kivédése
    - Színtelen előtétlencse
    - Fényelnyelő szűrő előtétlencse: a kívülről érkező fényt elnyeli

A közúti közlekedés modellezése

Csomópontok és Forgalmi folyamatok

Csomópontok

- a megállások száma *és/vagy* a várakozási idők összege minimális legyen
- az irányítás lehetőleg forgalomfüggő és összehangolt legyen
- a programváltási időpontok a forgalom időbeni lefolyását kövessék
- a forgalmi rend kikapcsolt jelzőlámpánál is egyértelmű legyen
- a közös fázisban haladó gyalogosokra sárga villogó figyelmeztessen
- a csomópontban sáv nem fogyhat el: a bemenő sávnak ki is kell jönnie.
- összehangolás, „zöld hullám” tervezése



Forgalmi folyamok

Dugók kialakulásának okai

- Baleset
- Ideiglenes terelések
- Fantom dugó

A közúti közlekedés modellezése

- Makroszkopikus modell
  - hálózat szintű vizsgálatra alkalmas
- Mezoszkopikus modell
  - összeköti a makro- és mikroszkopikus modelleket
  - dinamikus forgalomszétosztásra alkalmas
- Mikroszkopikus modell
  - járműkövetési-, sávválasztási-, illetve útvonal-választási modell
  - jármű-járművezető rendszer
- Szub-mikroszkopikus modell
  - emberi viselkedés vizsgálata

A közúti közlekedés modellezése

- Forgalomtervezés
  - adott területen végrehajtott változás hatásai
- Szimulációk
  - forgalmi szabályozások összehasonlítása
  - O-D (honnan-hová) viszonyok meghatározása
- Valósidejű forgalomszabályozás
  - valóságos forgalom irányítása

Véletlenszerű hibák elleni védelem

RAM paraméterek

Tartalom

- Megbízhatósági paraméterek
  - Hogyan jellemezhető a véletlenszerű hibák fellépése az alkatrészekben és a rendszerekben?
- Elemek megbízhatósága
  - Hogyan alakulnak egy alkatrész megbízhatósági paraméterei?
- Rendszerek megbízhatósága
  - Hogyan számítható ki a rendszerek megbízhatósága, ha ismerjük a rendszer struktúráját és az elemek megbízhatósági jellemzőit?

MEGBÍZHATÓSÁGI PARAMÉTEREK

MEGBÍZHATÓSÁGI PARAMÉTEREK

	Jelölés	Dimenzió
• Működőképesség valószínűsége	R(t)	-
• Meghibásodás valószínűsége	F(t)	-
• *(Meghibásodási sűrűség*	*f(t)*	*[1/t])*
• Meghibásodási ráta	l(t)	[1/t]
• Várható/közepes élettartam	m, T	[t]

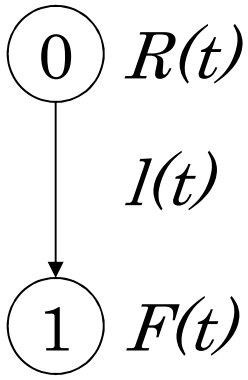
- Működőképesség
  - annak valószínűsége, hogy az adott rendszer, adott idő után, adott időintervallumban, a meghatározott körülmények között a feladatát kifogástalanul ellátja.
- Meghibásodás
  - olyan esemény, amelynek során legalább egy meghibásodási kritérium sérül.
- Meghibásodási kritériumok
  - jelzik a határt egy egység működőképes és nem működőképes állapota között.
- Működőképes/meghibásodott állapot
- Meghibásodások fajtái
  - Teljes vagy részleges
  - Váratlan vagy fokozatos (drift) jellegű

A meghibásodás fellépése véletlen esemény

Ha feltételezzük, hogy a rendszer várható élettartama T, akkor

$R(t)=P(t<T)$ és $F(t)=P(t\geq T)$.

$R(t)+F(t)=1$



$R(0)=1$ $\quad F(0)=0$

$R(\infty)=0$ $\quad F(\infty)=1$

R(t) monoton csökkenő,

F(t) monoton növekvő.

Gyakorlati meghatározás

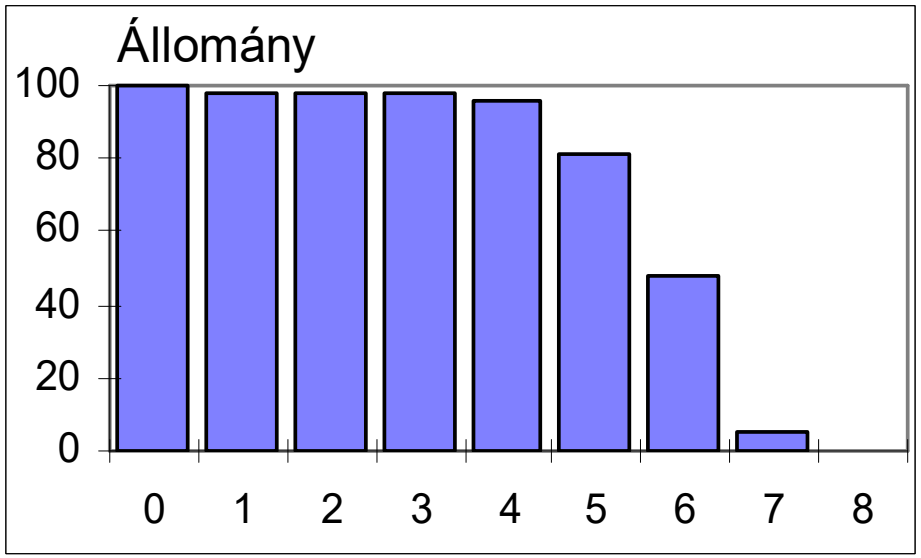
$$F(t)\cong\frac{N_0-N(t+\Delta t)}{N_0}$$

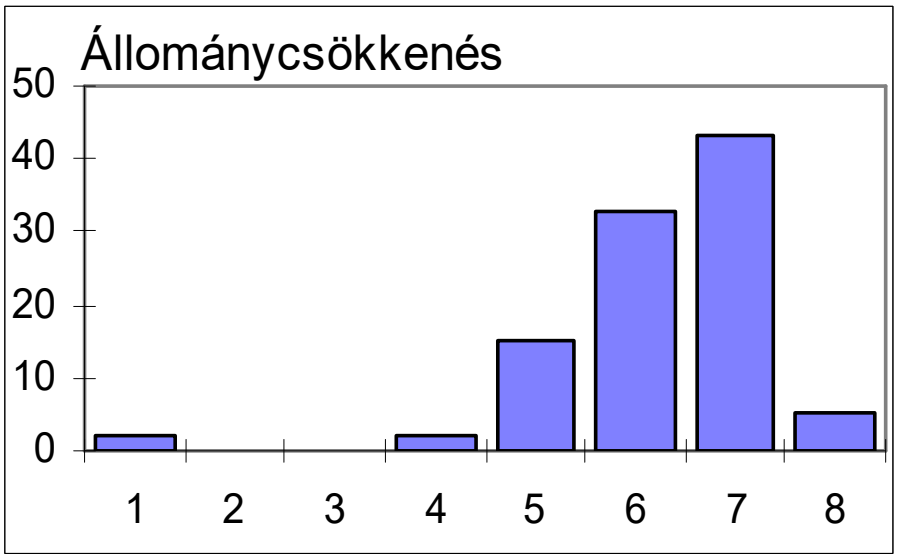
$$R(t)\cong\frac{N(t+\Delta t)}{N_0}$$

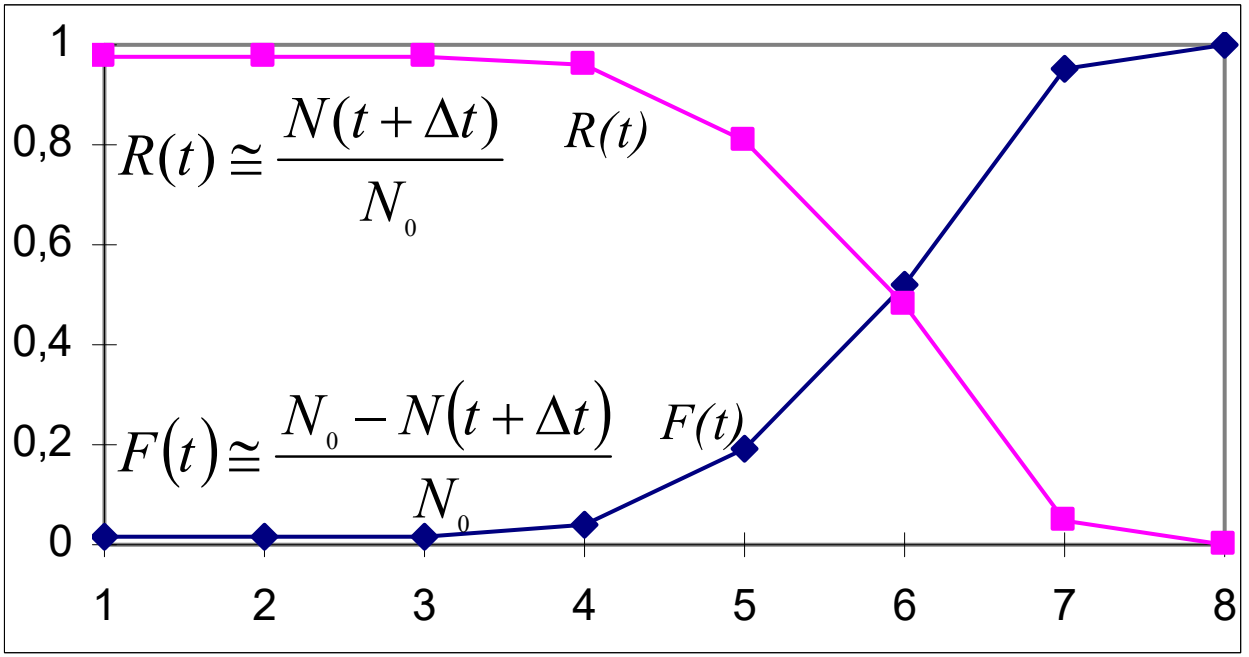
$$F(t)=\lim_{\substack{N_0\to\infty\\ \Delta t\to 0}}\frac{N_0-N(t+\Delta t)}{N_0}$$

$$R(t)=\lim_{\substack{N_0\to\infty\\ \Delta t\to 0}}\frac{N(t+\Delta t)}{N_0}$$

MEGBÍZHATÓSÁGI PARAMÉTEREK - PÉLDA







Meghibásodási ráta l(t): a l*(t)Dt* érték annak **feltételes valószínűsége**, hogy egy *t* időpontban még nem meghibásodott egység a [*t, t+Dt*] időintervallumban meghibásodik.

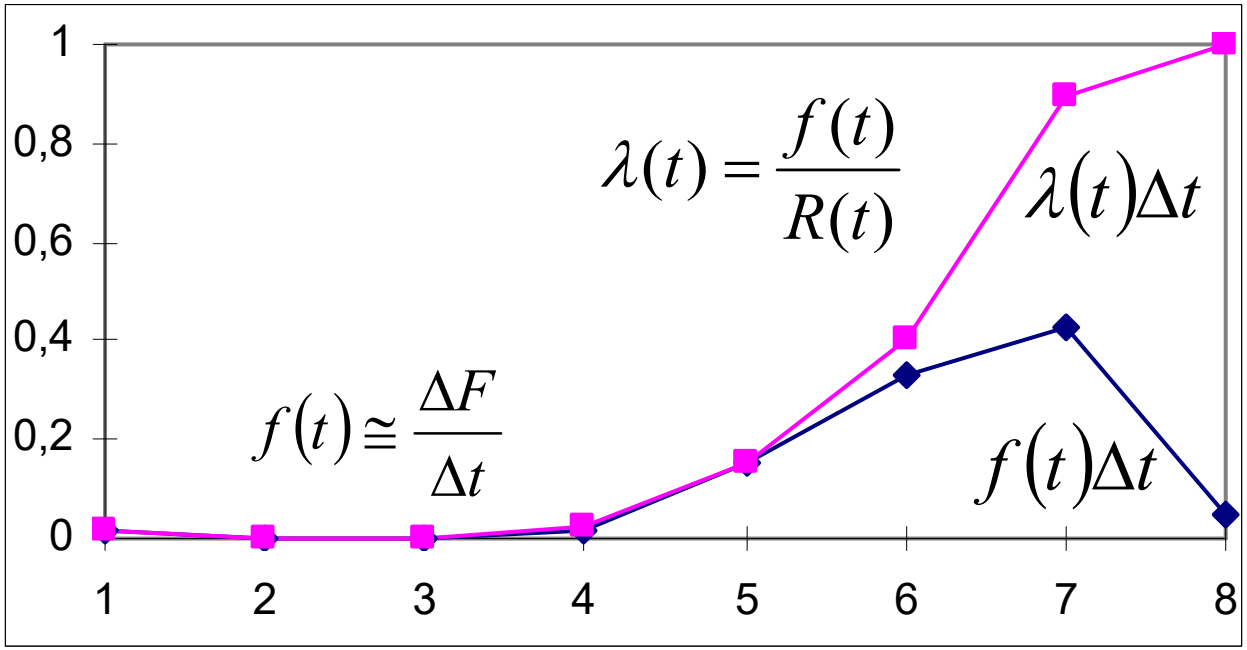
$$\lambda(t)\cdot\Delta t = P\left(t < T \le t+\Delta t \mid t < T\right)$$

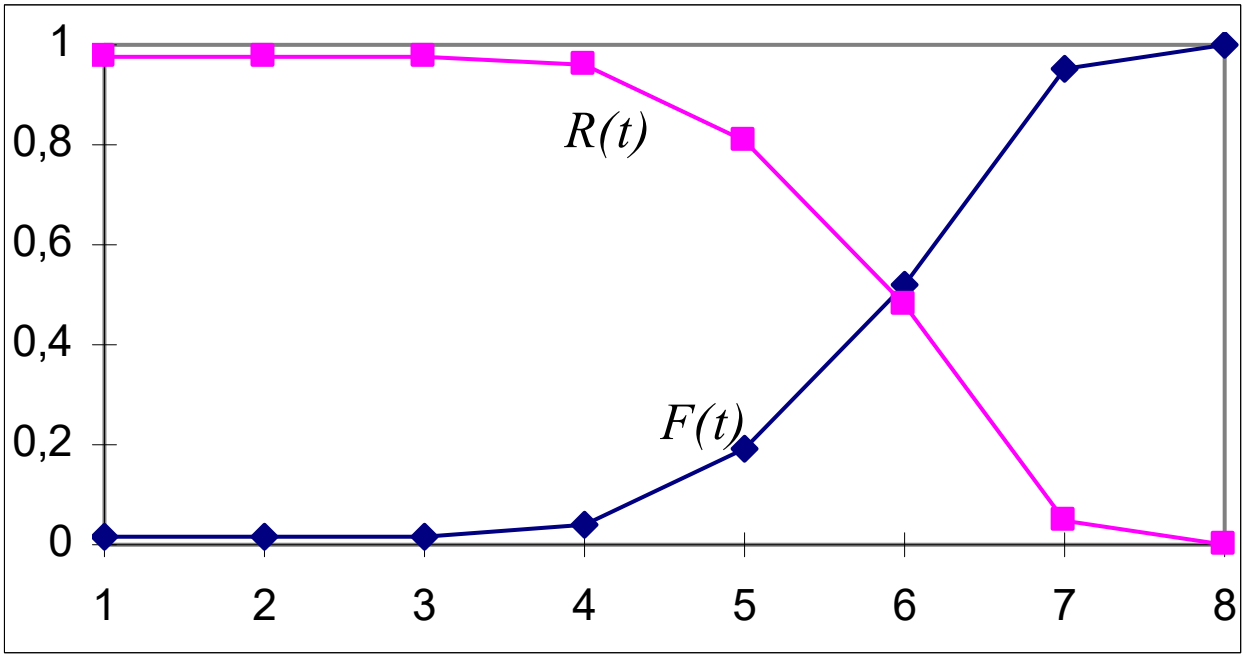
Kísérleti meghatározása: a megfigyelési intervallumban meghibásodott elemek számának, illetve a megfigyelési intervallum kezdetén működő egységek darabszámának és az időintervallumnak a hányadosa.

$$\lambda(t) \cong \frac{N(t)-N(t+\Delta t)}{N(t)\cdot\Delta t}$$

$$\lambda(t) = \frac{f(t)}{R(t)}$$

$$\lambda(t) = \lim_{\substack{\Delta t\to 0\\ N_0\to\infty}} \frac{N(t)-N(t+\Delta t)}{N(t)\cdot\Delta t}$$


1
0,8
0,6
0,4
0,2
0
1
2
3
4
5
6
7
8
$\lambda(t) = \frac{f(t)}{R(t)}$
$\lambda(t)\Delta t$
$f(t) \cong \frac{\Delta F}{\Delta t}$
$f(t)\Delta t$


1
0,8
0,6
0,4
0,2
0
1
2
3
4
5
6
7
8
R(t)
F(t)

Várható élettartam T (az első meghibásodásig eltelő átlagos időtartam): a t valószínűségi változó várható értéke.

$$m = \int_0^\infty t \cdot f(t)dt$$

$$\int_0^\infty uv'dt = uv - \int_0^\infty vu'dt$$

$$u = t; \qquad u' = 1$$

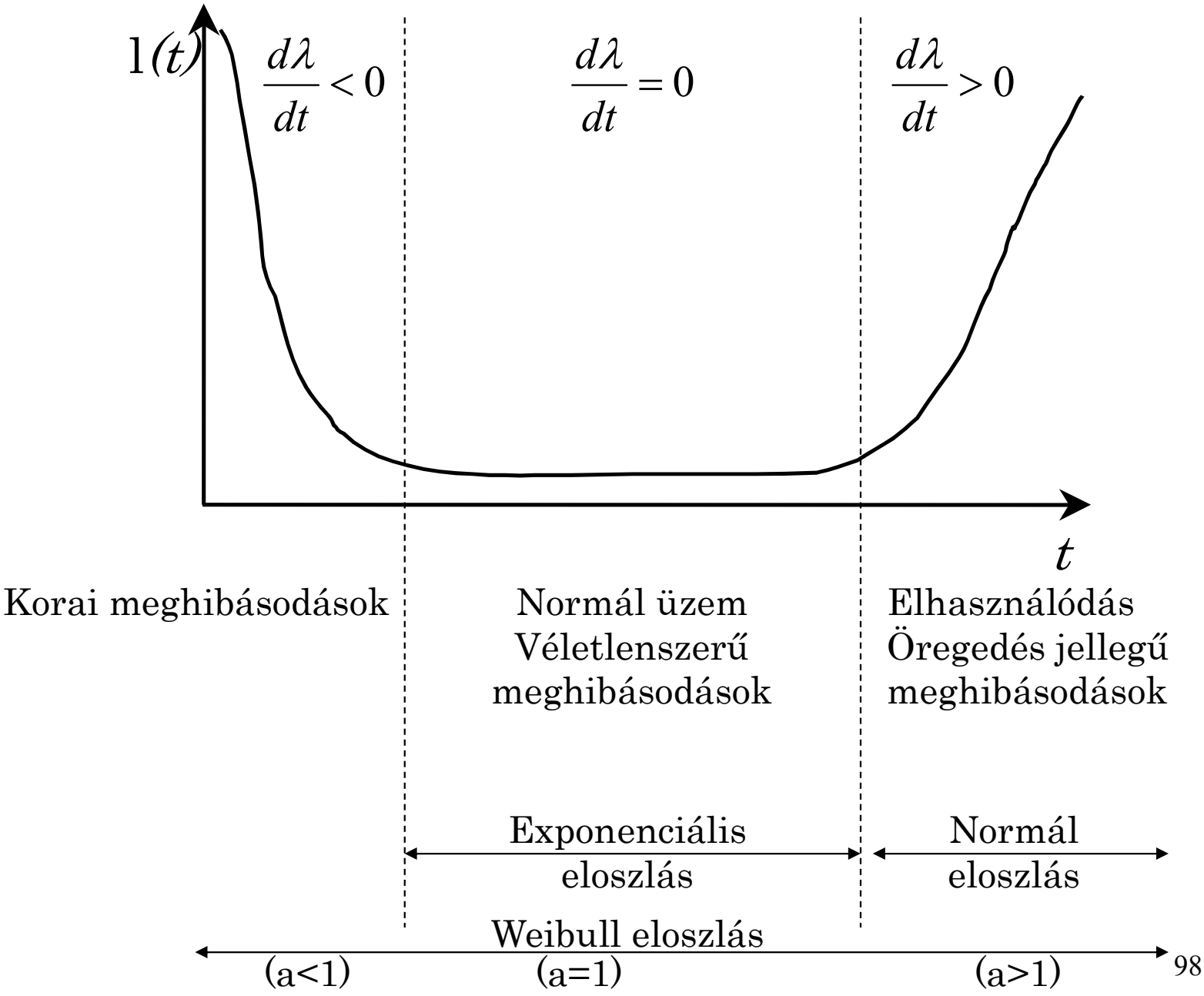
$$v' = f(t); \quad v = -R(t)$$

$$m = \left[-tR(t)\right]_0^\infty + \int_0^\infty R(t)dt$$

$$m = \int_0^\infty R(t)dt = T$$

ELEMEK MEGBÍZHATÓSÁGA

FÜRDŐKÁD-GÖRBE



EXPONENCIÁLIS ELOSZLÁS

A meghibásodás valószínűsége a véletlen változók növekvő értékével monoton módon, az „e” függvénynek megfelelően tart az „1” határértékhez.

A túlélési valószínűség függvény az „e” függvénynek megfelelően csökken, és tart a „0” határértékhez.

Az üzemidő során időegységenként azonos számú egység hibásodik meg, vagyis a meghibásodási gyakoriság a használati időtől független.

A meghibásodás-mentes működés valószínűsége egy $(t, t+\Delta t)$ időintervallumban független a korábban eltelt időtől, és csak a Δt időintervallum nagyságától függ, azaz

a jövőbeni meghibásodási viselkedés teljes mértékben független a rendszer előéletétől.

Az exponenciális eloszlás a fürdőkádgörbe középső, vízszintes szakaszára alkalmazható.

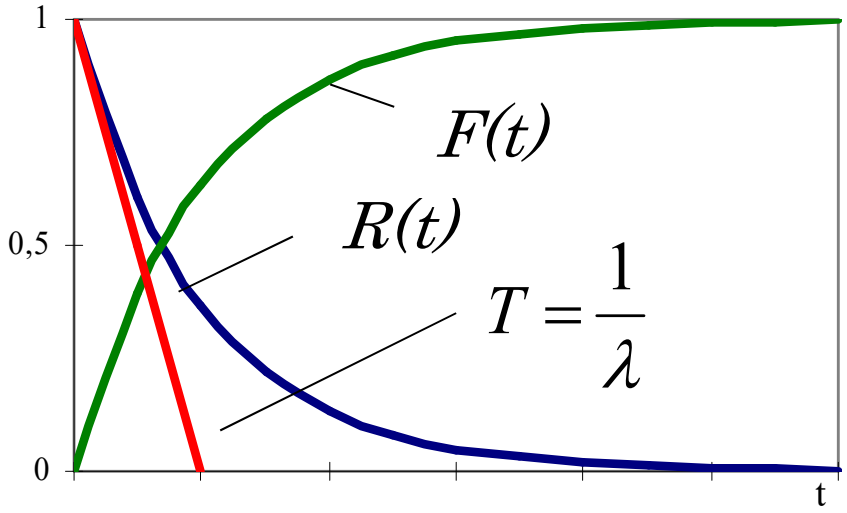
$$\lambda = \text{állandó!}$$

Ha több, egymástól független meghibásodási mechanizmussal kell számolni, akkor ezek szuperpozíciója szintén exponenciális eloszlást eredményez.

$$R(t) = e^{-\int_0^t \lambda(t)dt} = e^{-\lambda t}$$

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

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



λ = konstans

A meghibásodási gyakoriságot befolyásoló tényezők

A **mechanikai** környezet hatása: $\lambda' = K_e \lambda$

Környezeti körülmények	K_e
Telepített üzem szárazföldön	1,0
Hajók	1,2
vonatok	2,4
Dugattyús motoros repülőgépek	5,0
Reaktív hajtóműves repülőgépek	6,0
Rakéták a rakétatöltet égése közben	100
Űrjárművek a rakétatöltet égése közben	100

10°C szabály (kondenzátorok gyorsított vizsgálata alapján):
ha a hőmérséklet a megengedett határhőmérséklethez képest 10°C-kal emelkedik vagy csökken, az élettartam a felére csökken, illetve a kétszeresére növekedik.

RENDSZEREK MEGBÍZHATÓSÁGA

RENDSZERTULAJDONSÁGOK

Egy rendszer megbízhatósága függ:

- elemeinek megbízhatóságától és
- az elemek egymással való kapcsolatától.

A megbízhatóságot befolyásoló rendszerjellemzők:

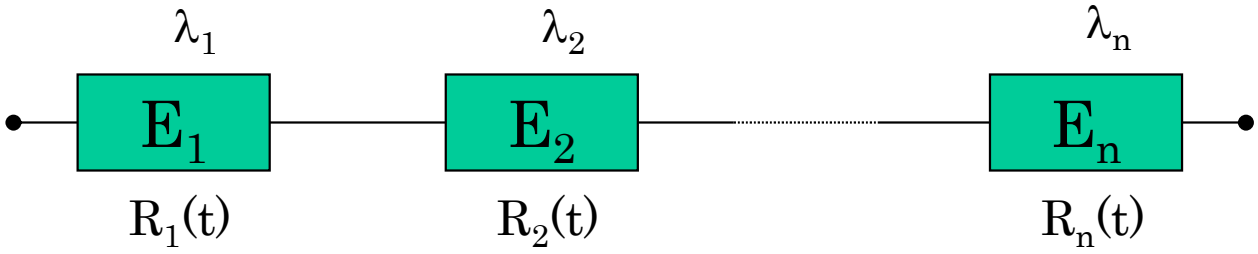
- a rendszer struktúrája (nem tévesztendő össze a villamos kapcsolásokkal!!!)
  - – soros rendszerek (strukturális redundancia nélküli rendszerek)
    egyetlen elem meghibásodása esetén a teljes rendszer meghibásodik;
  - – párhuzamos rendszerek
    mindaddig működőképes, amíg legalább egy eleme működőképes;
  - – egyéb redundáns struktúrájú rendszerek;
- a rendszer üzemmódja
  - – folyamatos;
  - – időszakos;
  - – alkalmanként működő;
- a rendszer javíthatósága
  - – nem javítható (a terméktől és/vagy annak alkalmazási körülményeitől függően)
    a javítás műszakilag lehetetlen, igen nehéz vagy nem gazdaságos;
  - – javítható
    a javítás történhet a meghibásodott elem helyreállításával vagy cseréjével.

Egy rendszer fizikai struktúrája és megbízhatósági szempontból vett struktúrája lehet azonos, de eltérő is.

Például a soros és a párhuzamos rezgőkör villamosan eltérő struktúrája ellenére megbízhatósági szempontból azonos struktúrájú: mindkettő soros rendszer.

Az előbbiekből adódik az a követelmény, hogy a megbízhatósági elemzéseket mindig a rendszer **megbízhatósági helyettesítő képének** vagy más alkalmas modelljének, pl. a hibafának a megalkotásával kezdjük.

SOROS RENDSZEREK MEGBÍZHATÓSÁGA



Soros rendszer definíciója:

- a rendszer véges számú elemből áll,
- egyetlen elem meghibásodása a teljes rendszer meghibásodásához vezet,
- csak teljes meghibásodásokat vesznek figyelembe, fokozatos meghibásodásokat nem,
- a meghibásodások egymástól függetlenek,
- az elemek meghibásodási gyakorisága időinvariáns (véletlen meghibásodások, az “e” eloszlás érvényes),
- a túlélés és a meghibásodás valószínűsége egymás komplementere,
- javítást nem terveznek,
- az anyag, konstrukció, gyártás szempontjából különböző elemeknek lehet azonos λ értékük.

SOROS RENDSZEREK MEGBÍZHATÓSÁGA

Soros rendszer működőképességének valószínűsége

(minden elem egyidejűleg működőképes):

$$R_s(t) = R_1(t) \cdot R_2(t) \cdot \ldots \cdot R_n(t) = \prod_{i=1}^{n} R_i(t) \qquad R_i(t) < 1$$

A soros rendszer eredő túlélési valószínűsége kisebb,
mint a legkisebb elemi túlélési valószínűség.

Soros rendszer meghibásodásának valószínűsége:

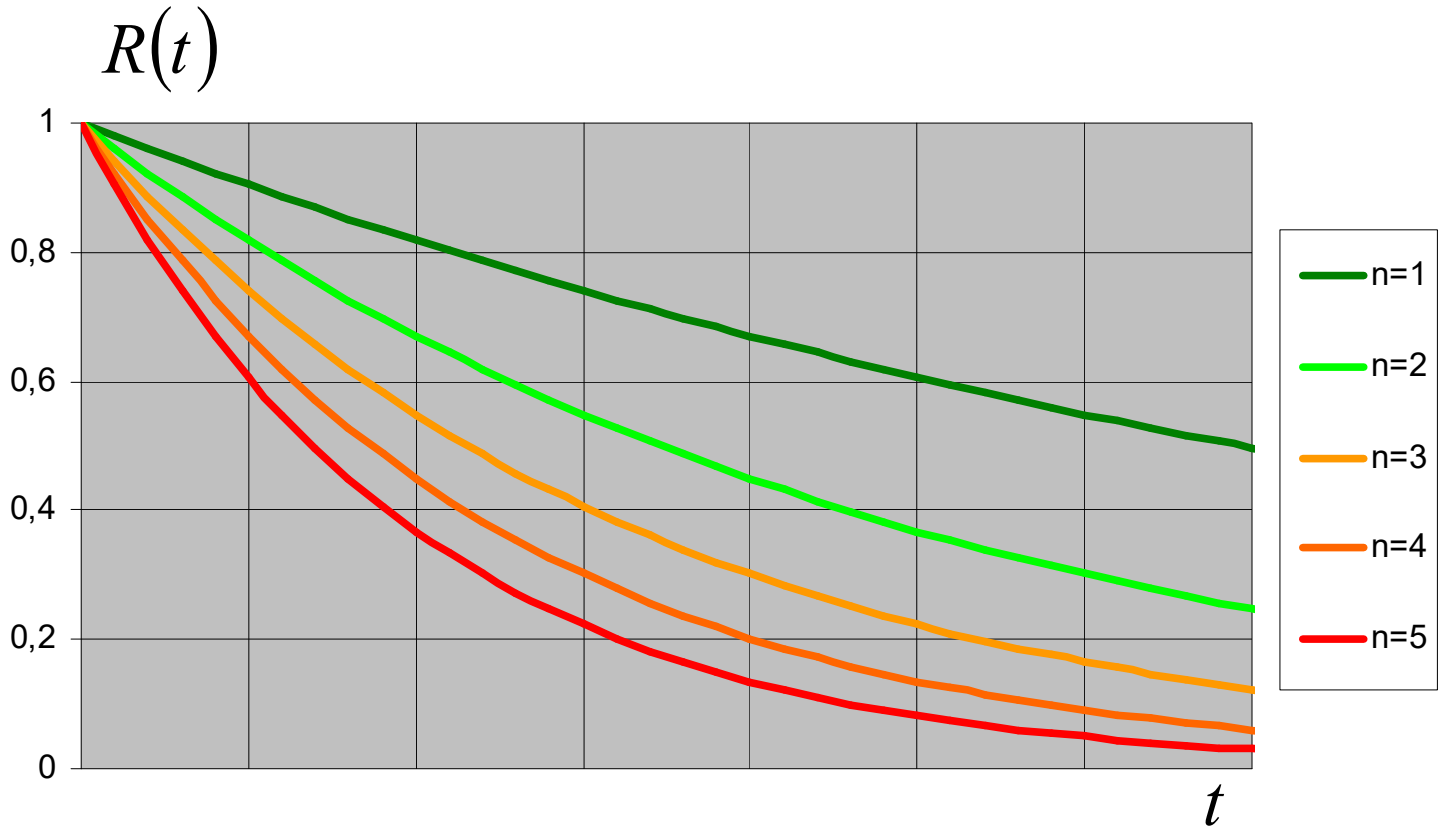
$$F_s(t) = 1 - \prod_{i=1}^{n} (1 - F_i(t))$$

A rendszer meghibásodási rátájának számítása:

$$R_s(t) = e^{-\lambda_1 \cdot t} \cdot e^{-\lambda_2 \cdot t} \cdot \ldots \cdot e^{-\lambda_n \cdot t} = e^{-\sum_{i=1}^{n} \lambda_i \cdot t} = e^{-\lambda_s \cdot t}$$

$$\lambda_s = \lambda_1 + \lambda_2 + \ldots + \lambda_n = \sum_{i=1}^{n} \lambda_i$$

A rendszer várható élettartama $T_s = \frac{1}{\lambda_s} = \frac{1}{\sum_{i=1}^{n} \lambda_i}$



P

$$\forall i : R_i(t_1) = 0{,}9$$

$$n = 10: \qquad R_S(t_1) = R_i(t_1)^{10} = 0{,}9^{10} = 0{,}348678$$

$$n = 100: \qquad R_S(t_1) = R_i(t_1)^{100} = 0{,}9^{100} = 2{,}66 \cdot 10^{-5}$$

1. példa

n=2 R_1=0,1 R_2=0,9 $R_s=R_1R_2$=0,1 0,9=0,09

n=2 R_1=0,5 R_2=0,5 $R_s=R_1\ R_2$=0,5 0,5=0,25

2. példa

n=2 R_1=0,6 R_2=0,8 $R_s=R_1\ R_2$=0,6 0,8=0,48

n=2 R_1=0,7 R_2=0,7 $R_s=R_1\ R_2$=0,7 0,7=0,49

A MEGBÍZHATÓSÁG NÖVELÉSÉNEK MÓDSZEREI

- Egyszerű rendszerkialakítás, kevés alkatrész (v.ö. bonyolult rendszerek)
- Kis meghibásodási gyakoriságú alkatrészek (magas előállítási költség)
- Azonos meghibásodási gyakoriságok
- Redundáns felépítés (gyenge elemekből jó rendszer)
- Előöregítés
- Tűréselemzés (Worst-Case, Monte Carlo)
- Hibafa elemzés (Fault Tree Analysis)
- Rövid üzemidő / Kis működésszám
- Csökkentett terhelés (derating)
- Túlterhelés elleni védelem
- A kockázatok elkerülése
- Karbantartási stratégiák, megelőző karbantartás
- Automatikus hibadiagnózis