Megbízhatóság és biztonság

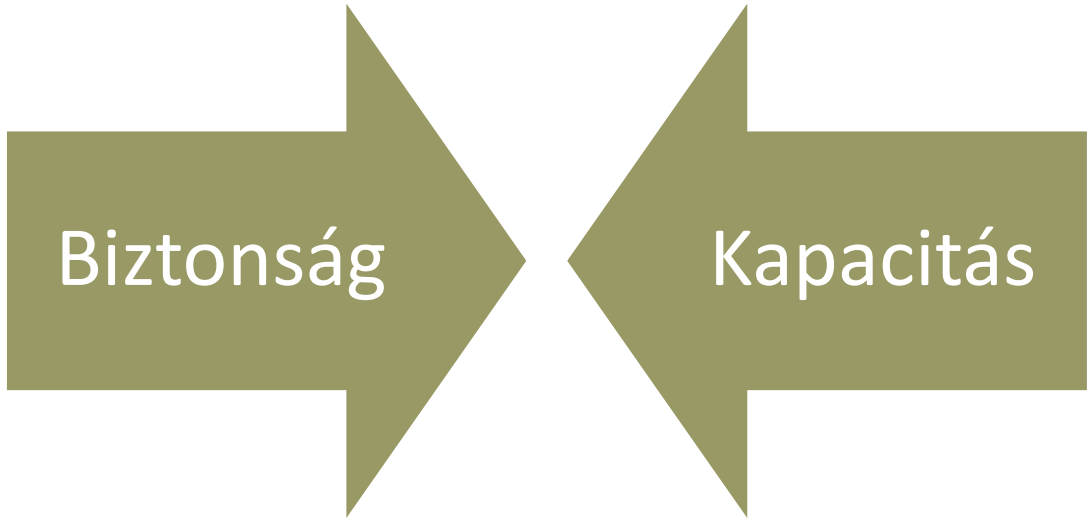
Dr. Sághi Balázs

BME Közlekedés- és Járműirányítási Tanszék

2017

A közlekedési rendszerekkel szemben támasztott elvárások

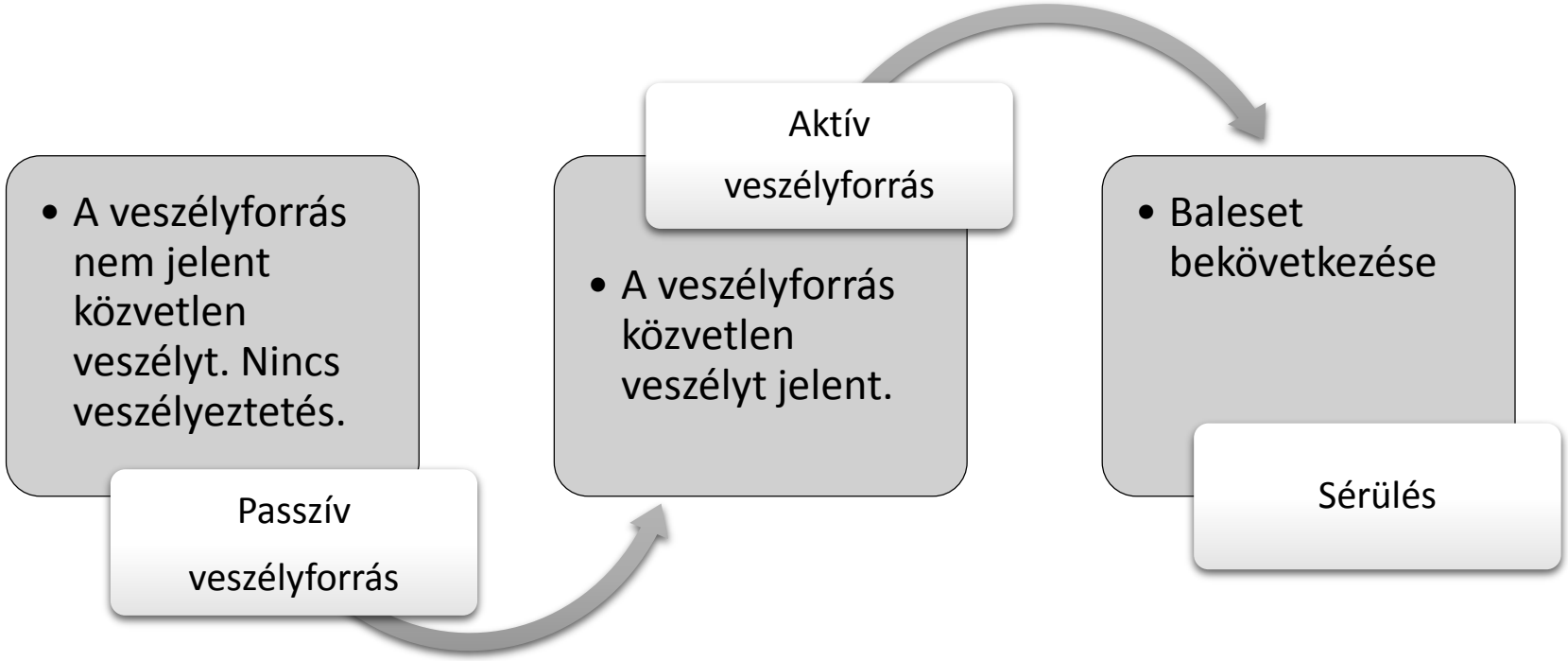
Elvárások



Probléma

- A kapacitás növekedése a biztonság csökkenését okozza
  - sebesség emelése,
  - forgalomsűrűség növekedése.

Biztonság, veszélyeztetés, baleset (baleseti eseménylánc)



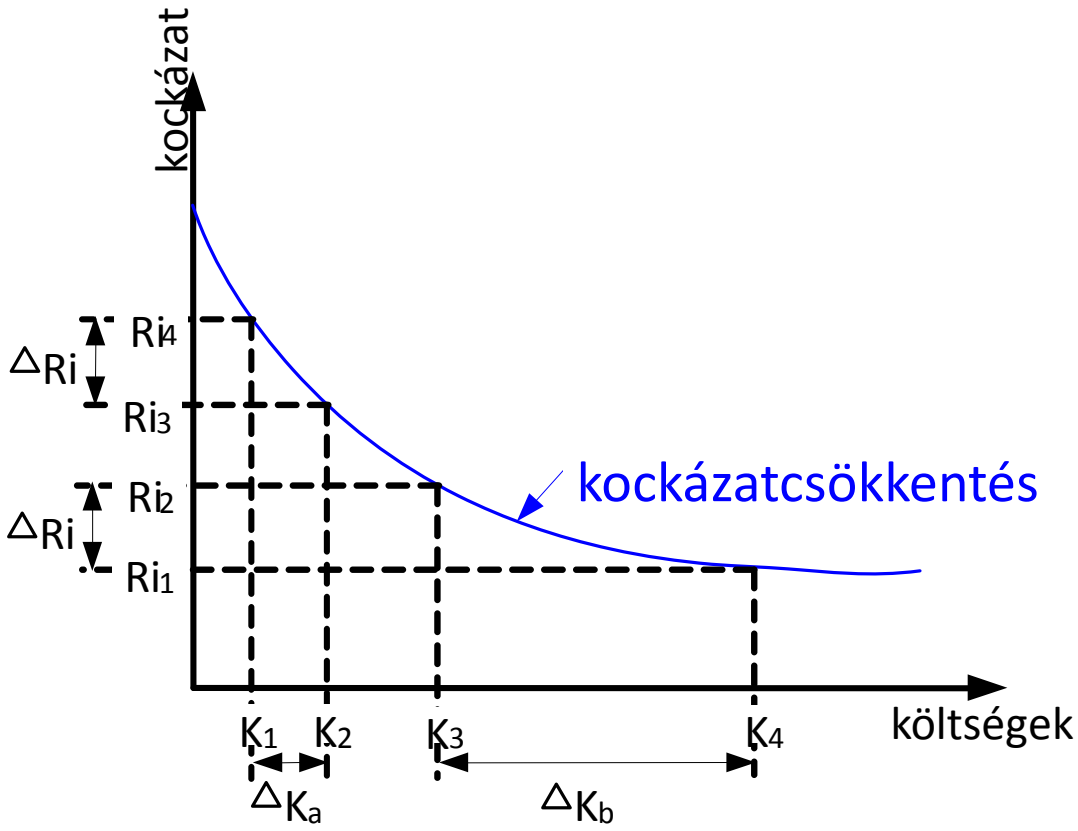
A kockázat fogalma

- A kockázat egy veszélyeztető hatás jelentőségét fejezi.
- Alapvetően emberi, szubjektív érzés
- Kockázati paraméterekkel írjuk le
  - Gyakoriság
  - Súlyosság
  - Egyéb paraméterek (pl. menekülési lehetőség)

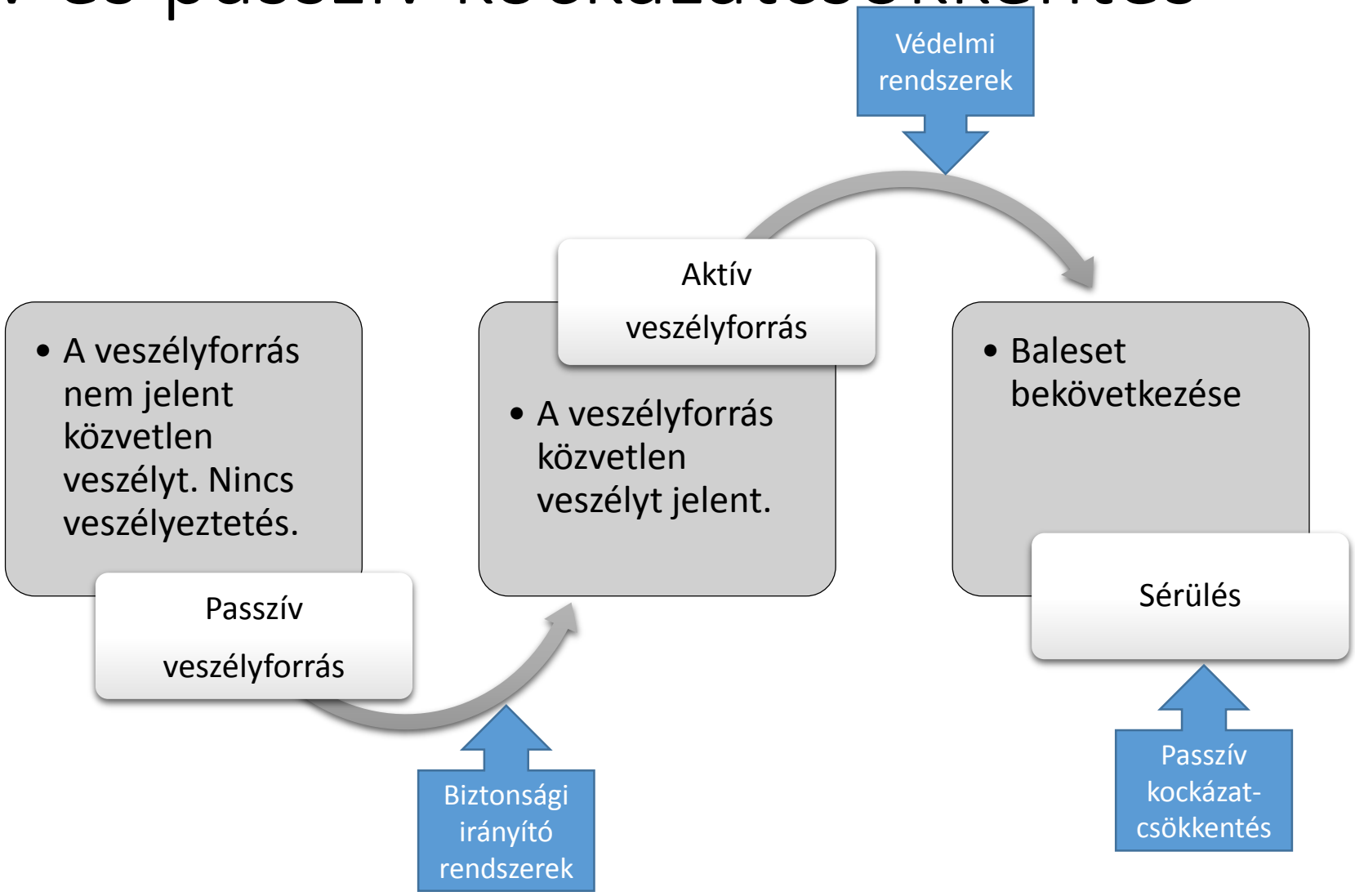
Gyakoriság		Súlyosság			
		Katasztro-fális	Kritikus	Csekély	Elhanya-golható
		4	**3**	**2**	**1**
gyakori	**A**				
valószínű	**B**				
néha	**C**				
alig	**D**				
valószínűtlen	**E**				
rendkívül valószínűtlen	**F**				

Társadalmilag elviselhető kockázat

- A kockázattűrést szubjektív szempontok befolyásolják
  - pl. felelősség
- A kockázat csökkentése költségekkel jár
  - abszolút biztonság nem létezik
- A ráfordítások és az elérhető eredmények megfelelő arányát keressük.



Aktív és passzív kockázatcsökkentés



Közlekedési szabályok

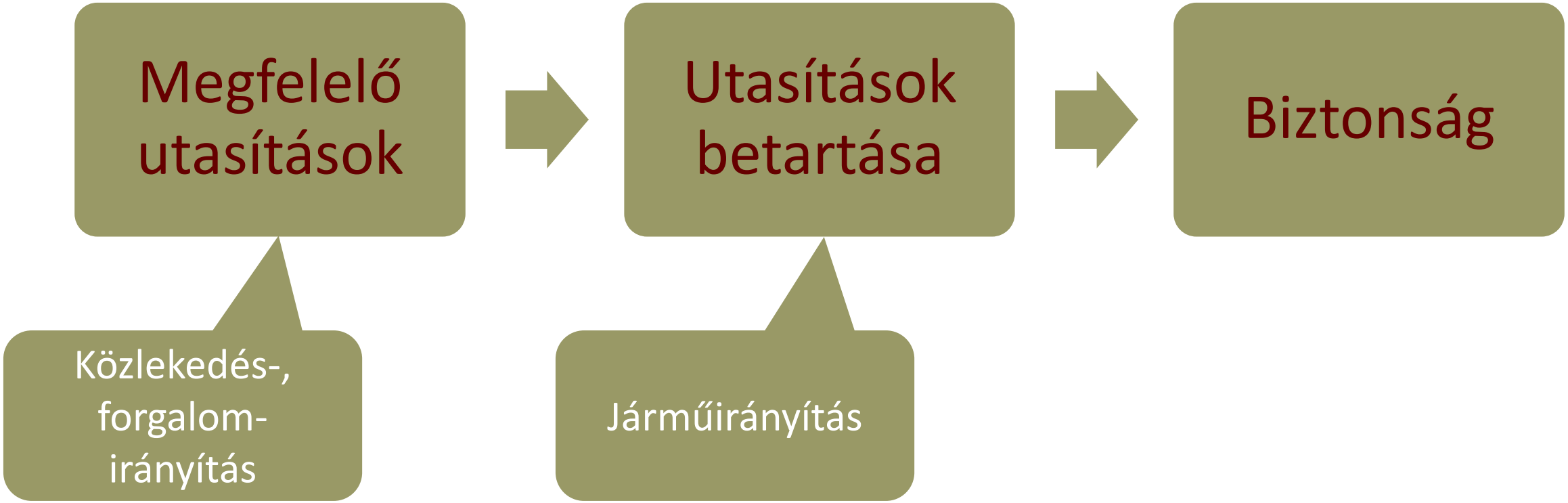
Folyamatosan, azonos módon alkalmazott

- pl. jobbkéz-szabály, jobbra-tartási kötelezettség
- Fontos a szabályok ismerete, ezért a rendszerhez való hozzáférést korlátozzuk, képzéshez kötjük.

Forgalom-, illetve szituációfüggően változó módon alkalmazott

- Forgalomirányítás
  - A járműveknek engedélyt/utasítást adunk bizonyos mozgásokra.
  - A járművek az engedélynek megfelelően mozoghatnak.
- A forgalomirányítás feladatai
  - a biztonságos járműmozgások feltételeinek megteremtése,
  - egyéb irányítási célok elérése (pl. energiafelhasználás csökkentése)

Irányítási utasítások és azok betartása



Irányítási utasítások és azok betartása Közúti közlekedés

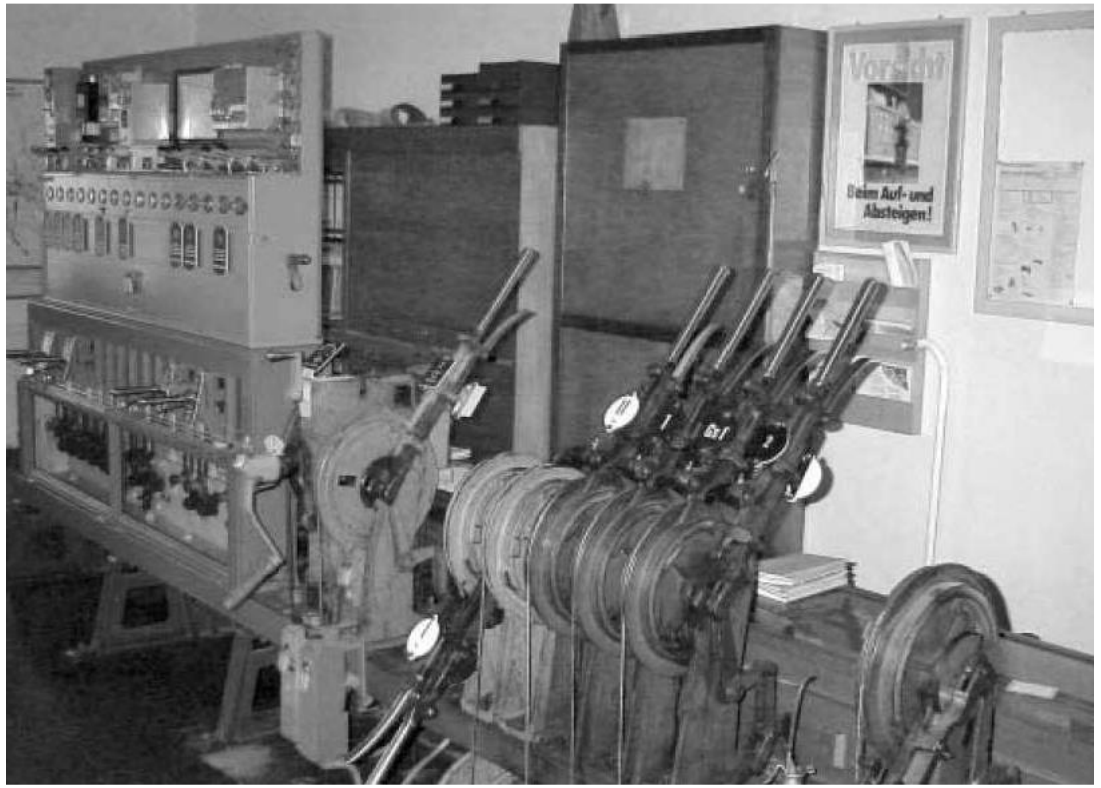
- Gépi úton ellenőrzött utasítások jelzések révén.
  - Ellenőrző mechanizmusok biztosítják, hogy ne jelenhessen meg olyan jelzés, amelynek következtében veszélyes forgalmi szituáció alakulhat ki,
  - még meghibásodás esetén se.
- Az utasítások betartása humán döntésen alapul.
  - Szabályozott rendszerhozzáférés
  - Újabban: támogató rendszerek a járműveken

Irányítási utasítások és azok betartása Légi közlekedés

- Utasítások adása humán döntés.
- Utasítások betartása humán döntés.
- Alapja:
  - támogató eszközök,
  - magas szintű képzés,
  - folyamatos tréning.

Irányítási utasítások és azok betartása Vasúti közlekedés

- Jelzésadás – menetengedély
  - Gépi úton ellenőrzött
  - Biztosítóberendezések
- Jelzések betartása
  - Korán megjelenik a gépi úton való kikényszerítés.
  - Vontmegállító, vonatbefolyásoló berendezések.



Gépi eszközök a közlekedésirányításban

- Probléma
  - Hogyan kérhető számon ezektől a berendezésektől az a „kompetencia”, ami a humán irányítók kiképzése és folyamatos tréningje biztosít?
- Általában
  - minél nagyobb egy humán irányító felelőssége, annál szigorúbb képzettségi követelményeket támasztunk.
- Műszaki rendszerek esetén
  - minél nagyobb az adott műszaki rendszer szerepe a kockázatcsökkentésben, annál kevésbé engedhető meg, hogy ne lássa el a feladatát,
  - azaz a biztonság annál magasabb szintjét kell elérni.

Biztonsági rendszerek belső biztonsága

Biztonsági funkciók

- A biztonsági irányító rendszerek és védelmi rendszerek funkcionalitása
- Biztonsági funkciók révén csökkentik a kockázatot az irányított folyamatban.
- Biztonsági funkcióik védekeznek a külső veszélyforrások ellen.

Biztonsági integritás

- A berendezések belső biztonsága
- Az irányított folyamat megfelelően védve legyen az irányítórendszer saját, belső veszélyforrásaitól.
- Mekkora legyen a védekezés mértéke?

Összefoglalás

- A közlekedési folyamatok kockázatai a társadalmilag elviselhetőnél magasabbak,
- ezért kockázatcsökkentő műszaki rendszereket alkalmazunk.
- Ezek a rendszerek biztonságkritikus rendszerek, mert ha nem látják el a feladatukat, veszélyeztetések alakulhatnak ki.
- A biztonságkritikus rendszerekkel szemben ezért magasabb követelményeket támasztunk.

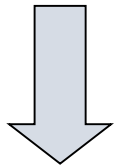
Veszélyforrások, veszélyeztetések

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

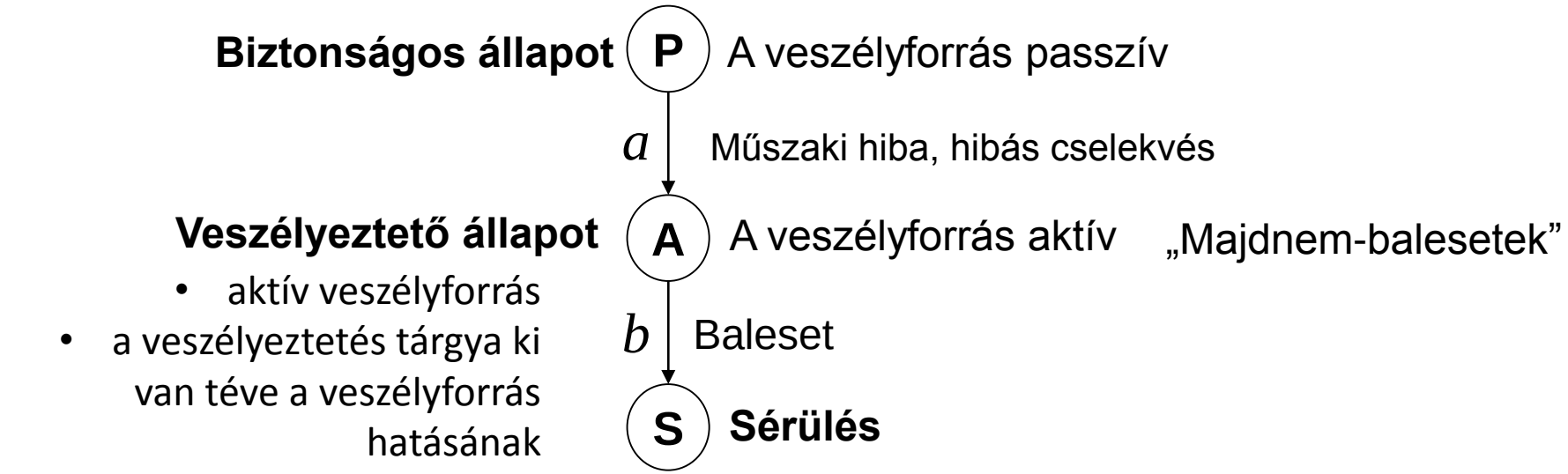
veszélyforrás

okozhatja.

Biztonság és veszélyeztetés – Baleseti eseménylánc

Biztonság:
a veszélyeztetettségtől mentes állapot valószínűsége (P)

Balesetmentesség:
a sérüléstől mentes állapot valószínűsége (P, A)



Veszélyforrások a közlekedésben (1)

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 (2)

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**

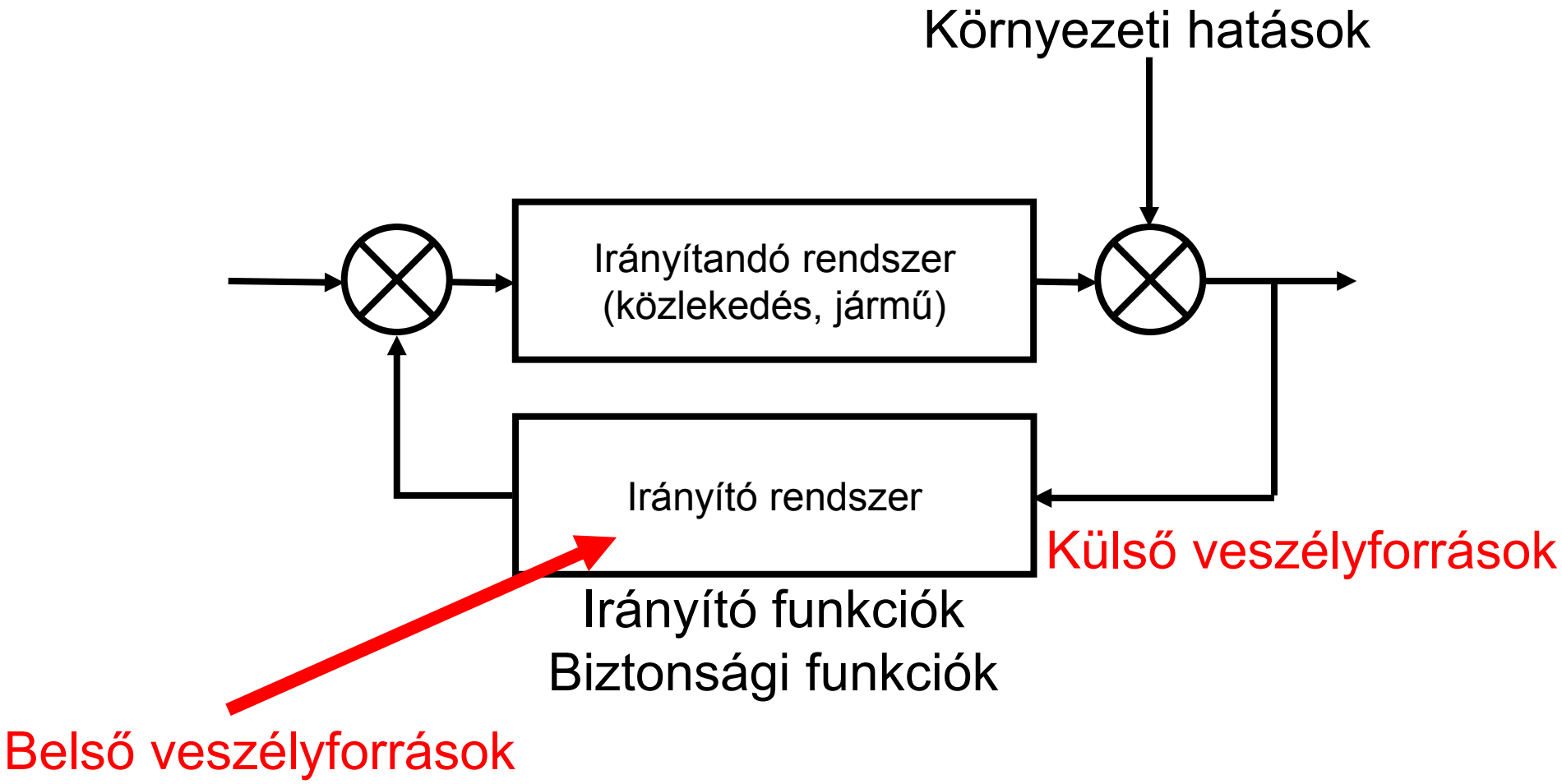
Lehetséges veszélyforrások (külső és belső)

- A rendszer valamely elemének
  - szisztematikus hibája – emberi eredetű
    - HW
    - SW
  - véletlenszerű meghibásodása
    - HW
- A rendszer
  - funkcionalitása;
  - normál üzeme;
  - hibaállapotai;
  - szükségüzeme;
  - helytelen használata;
  - csatlakozó felületei;
  - üzemeltetése, karbantartása és ellátási kérdései;
  - selejtezése

- Hibás emberi cselekvés
  - a rendszer létrehozása folyamán
  - a rendszer üzemeltetése folyamán
    - utas
    - személyzet (működtetés, karbantartás)
- Környezeti hatás
  - mechanikai
  - villamos környezet
  - időjárás, természeti
  - egyéb

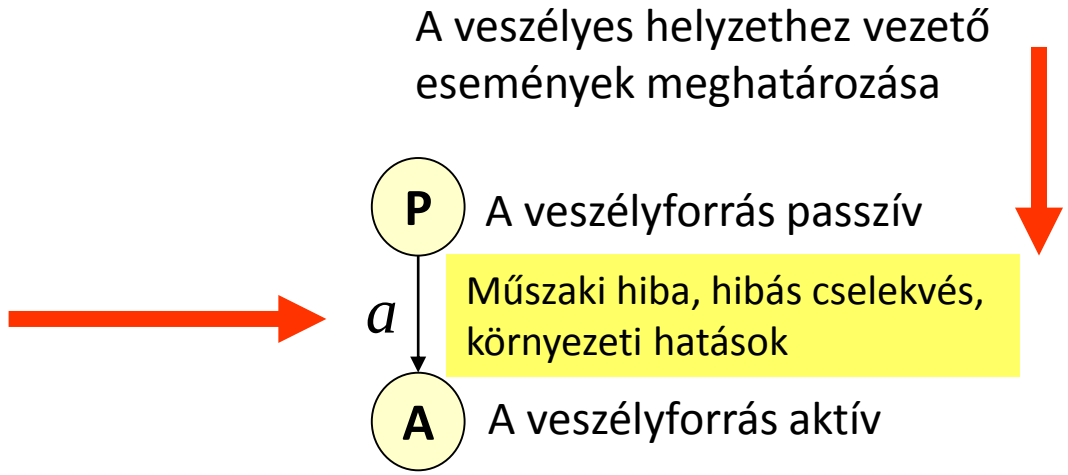
- Szándékos veszélyeztetés >> security

Az irányító rendszer szerepe



Veszélyek számbavétele

- Lehetséges módszerek (szisztematikus eljárások)
  - ellenőrző lista alapján
  - a vizsgált rendszer alrendszerekre bontásával
  - a funkciók számbavétele alapján
- Azonosított veszélyek listája
  - azonosító (pl. sorszám)
  - a veszélyforrás megnevezése
  - **a veszélyeztetés okai**
  - a keletkező elsődleges baleset
  - a lehetséges következmény baleset



BIZTONSÁGI KOCKÁZAT

Biztonsági kockázat

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

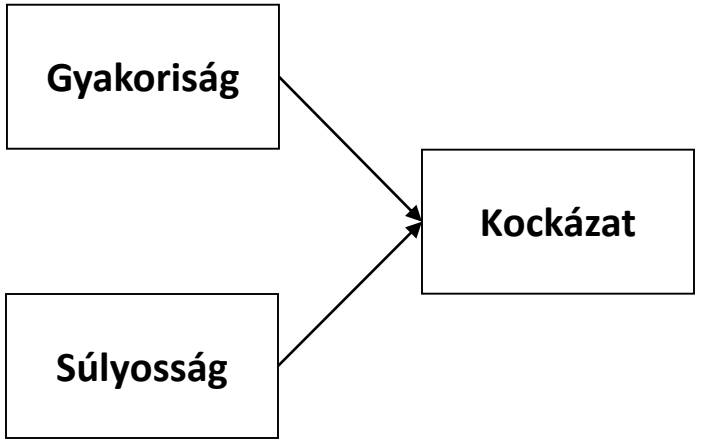
Biztonsági kockázat:

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

kombinációja, amelyet további

- **kockázati paraméterek**

is befolyásolhatnak.



A kockázat **meghatározható**

- mennyiségileg / kvantitatív módon
- kockázatosztályozással / kvalitatív eljárással

Kvantitatív kockázat-meghatározás

Példa a kockázat számszerű kifejezésére (1)

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 (2)

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

Mekkora a villámcsapásból adódó halálozás kockázata?

Évente a lakosság $25/50\,000\,000=5x10^{-7}$ részét éri villámcsapás.

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

A **lakosság egészére** vonatkozó kockázat: **$5x10^{-7}$ halál/ember-év**

Károk, sérülések

- személyi
- anyagi
- környezeti

Példa 1:

Áldozat = halálozás
= 10 súlyos sérülés
= 100 könnyű sérülés

Példa balesetbiztosításból:

A testrészek egészségkárosodása (térítési százalékkal):

- mindkét szem látóképességének elvesztése, mindkét felkar – alkar vagy kéz – elvesztése, egyik kar vagy kéz, valamint comb vagy lábszár együttes elvesztése (felső végtag plusz alsó végtag csonkolása), mindkét comb elvesztése: 100%,
- mindkét lábszár elvesztése: 90%,
- egyik comb elvesztése, egyik felkar elvesztése: 80%,
- egyik lábszár elvesztése, egyik alkar elvesztése, beszélőképesség teljes elvesztése, mindkét fül hallóképességének teljes elvesztése: 70%,
- jobbkezes jobb kezének, balkezes bal kezének elvesztése (csuklón alul): 65%,
- jobbkezes bal kezének, balkezes jobb kezének elvesztése (csuklón alul): 50%,
- egyik láb teljes elvesztése (boka alatt): 40%,
- egyik szem látóképességének teljes elvesztése: 35%,
- egyik fül hallóképességének teljes elvesztése: 25%.

Egyéni és kollektív kockázat

- Példa egyéni kockázatra
  - kőomlás egy vonalszakaszon 10 évenként
  - hétvégi oda-vissza utazás (100/év)
  - a vonat 4 s alatt halad el a veszélyeztetett helyen

$$Ri_i = HR_i \cdot Da_i = \frac{1 esemény}{10\,év \cdot 365\,\frac{nap}{év}} \cdot \frac{4\frac{s}{esemény \cdot utazás} \cdot 100\frac{utazás}{év}}{24 \cdot 60 \cdot 60\,\frac{s}{nap}} \cdot 1\,\frac{halálozás}{személy}$$

$$Ri_i = 1{,}2 \cdot 10^{-6}\,\frac{halálozás}{személy \cdot év}$$

Kollektív kockázat

- az egyéni kockázatok összege
- Példa
  - a vonaton 650-en utaznak

$$Ri_o = \sum Ri_i = 650 személy \cdot 1{,}2 \cdot 10^{-6} \frac{halálozás}{személy \cdot év}$$

$$Ri_o = 7{,}8 \cdot 10^{-4} \frac{halálozás}{év}$$

Kockázatosztályozás

- A kockázati paraméterek
  - súlyosság,
  - gyakoriság,
  - kontrollálhatóság stb.

  kategóriákba sorolása.
- A kategóriák közötti kombinációk kialakítása
- A kombinációk csoportosítása

Kárkihatási kategóriák (példa, vasúti közlekedés) (Súlyosság)

Kategó-ria	**Leírás**	**Következmények** (csak személyekre)
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

Kárkihatási kategóriák (példa) (Súlyosság)

Kategó-ria	Leírás	Következmények	
		a **személyeket** illetően	a **szolgáltatásokat** illetően
4	Kataszt-rofális	Halálesetek és/vagy több súlyos sérült	
3	Kritikus	Egy haláleset vagy több súlyos sérült	Egy alapvető rendszer teljes elvesztése
2	Csekély	Egy súlyos sérült, több kisebb sérülés	Súlyos károk egy vagy több rendszerben
1	Elhanya-golható	Lehetséges kisebb egyedi sérülések	Károk a rendszerben

Veszélybekövetkezési gyakoriságok (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	$<10^{-9}$

Kockázatosztályozás (vasúti példa)

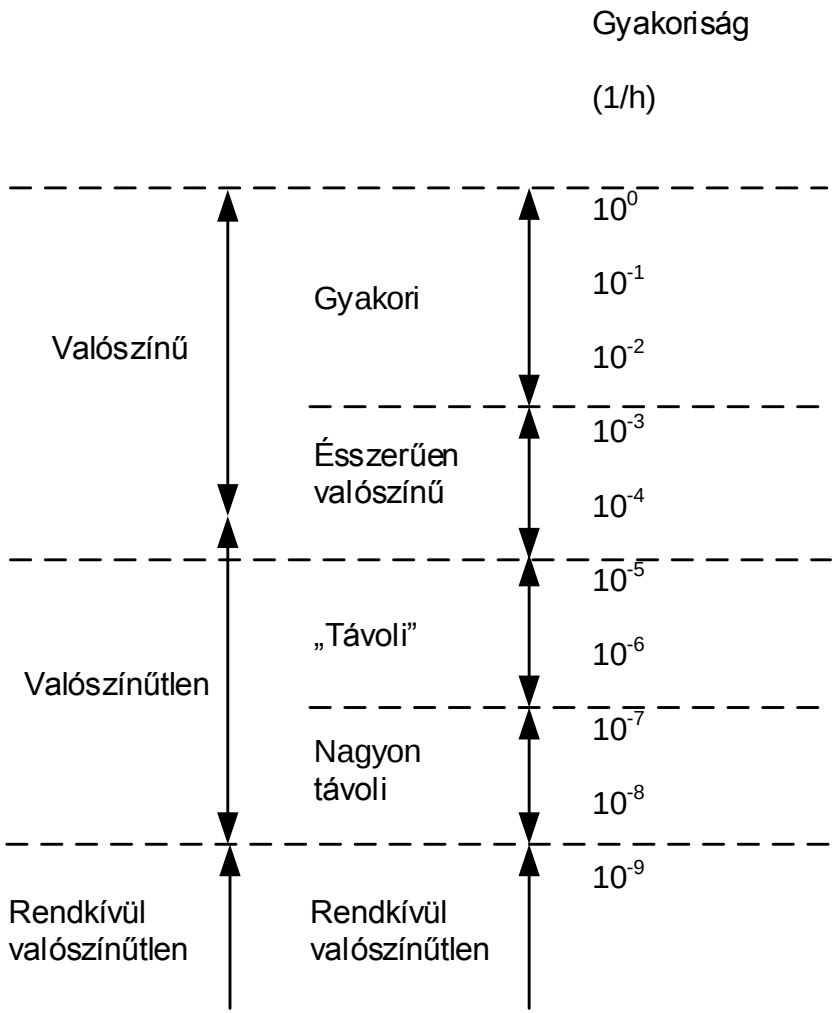
Valószínűségi szint		Kárkihatási kategóriák			
		Katasztro-fális	Kritikus	Csekély	Elhanya-golható
		4	3	2	1
gyakori	A				
valószínű	B		K4		
néha	C				K2
alig	D		K3		
valószínűtlen	E				
rendkívül valószínűtlen	F			K1	

Kockázati kategóriák:
K1 (alacsony) – K4 (magas)

Súlyossági kategóriák a légiközlekedésben

Kategória	Értelmezés
Katasztrofális	Megakadályozza a biztonságos továbbrepülést, és a leszállást
Veszélyes	(…)
Lényeges	(…)
Kicsi	Nem csökkenti érdemben a repülés biztonságát, kisebb funkcionális visszaesés, szükséges lehet a személyzet beavatkozása, de túlterhelést még nem jelent számukra
Hatástalan	(…)

Gyakoriságok – polgári repülés



Súlyossági kategóriák (Járműipar, AAAM, ISO 26262)

- AIS 0 : nincs sérülés
- AIS 1 : könnyű sérülés (bőrsérülés, izomfájdalom stb.)
- AIS 2 : mérsékelt sérülés (mélyebb vágás, max 15 perc eszméletvesztés
- AIS 3 : súlyos, de nem életveszélyes (csonttörés [nem koponya], ízületi sérülés…)
- AIS 4 : súlyos, életveszélyes, valószínű túléléssel (súlyos csontsérülések, 12 óra eszméletvesztés)
- AIS 5 : kritikus sérülés, életveszélyes, bizonytalan túléléssel (12+ óra eszméletvesztés, belső vérzés …)
- AIS 6 : extrém kritikus, halálos sérülés, haláleset

Súlyosság

- AIS → ISO 26262 súlyossági kategóriák

	Class of severity (see Table 1)			
	S0	**S1**	**S2**	**S3**
Reference for single injuries (from AIS scale)	— AIS 0 and less than 10 % probability of AIS 1-6 — Damage that cannot be classified safety-related	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Példák súlyossági kategóriákra Vezetési szcenáriók alapján

- S0: könnyű ütközés, súrolás, parkolóhelyre be- és kiállás során keletkező sérülések, útelhagyás ütközés, borulás nélkül
- S1: oldalsó ütközés (pl. fának) nagyon kis sebességgel, oldalsó, hátsó, első ütközés másik személyautóval nagyon kis sebességgel
- S2: ütközés kis sebességgel, gyalogos/biciklis ütközés kanyarodás során (városi kereszteződés)
- S3: ütközés közepes sebességgel stb.

Gyakoriság

- Kategóriák: E0, E1, E2, E3, E4
- E0: nagyon valószínűtlen; pl. jármű és repülőgép ütközése, természeti katasztrófák (földrengés, hurrikán stb.)
- A többi kategóriát olyan esetekre alkalmazzuk, amikor a szituáció fennállásának időtartama vagy gyakorisága miatt veszélyeztetés alakulhat ki.
  - A fennállás időaránya a teljes időalaphoz képest
  - A fellépés gyakorisága időegység alatt
  - A kettő kombinációja

Gyakoriság

- Időtartam aránya szerint

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Duration (% of average operating time)	Not specified	<1 % of average operating time	1 % to 10 % of average operating time	>10 % of average operating time

- Fellépési gyakoriság szerint

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Frequency of situation	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average

Kontrollálhatóság

- Annak valószínűsége, hogy egy átlagos (reprezentatív) járművezető meg tudja-e tartani/vissza tudja-e szerezni az irányítást, illetve a környező érintett személyek el tudják-e kerülni a veszélyeztetést

Driving factors and scenarios	Class of controllability (see Table 3)			
	C0	C1	C2	C3
	Controllable in general	99 % or more of all drivers or other traffic participants are usually able to avoid harm	90 % or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm

Kontrollálhatóság példák

- C0 (mindenki): a rádió hangerő váratlan felerősödése, figyelemelterelő jelzések
- C1 (99%+): a vezetőülés pozíciójának helytelen állítása (lefékezés, megállás), kormány blokkolása induláskor
- C2 (90%+): ABS hiba vészfékezésnél, lámpák kikapcsolása sötét úton
- C3 (90%-): fékhiba, hibás légzsák nyitás nagy sebességnél

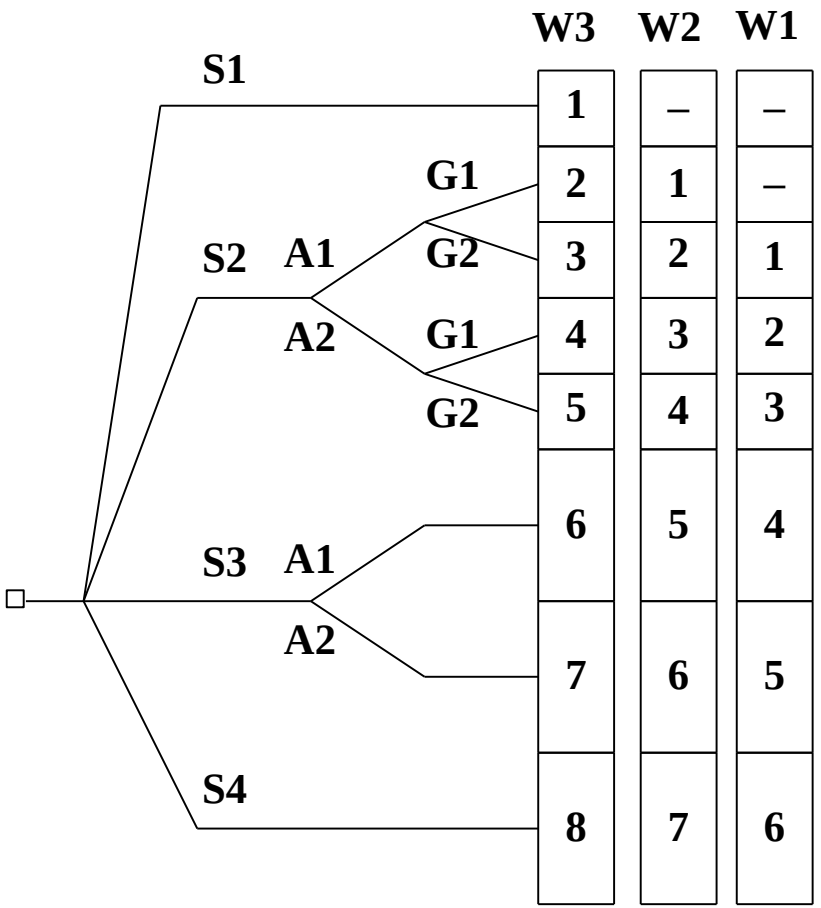
Kategóriák kombinációja

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Kockázati kategóriák:
elhanyagolható (QM),
A (alacsony) – D (magas)

Kockázati gráf - Követelményosztályok (DIN 19250)

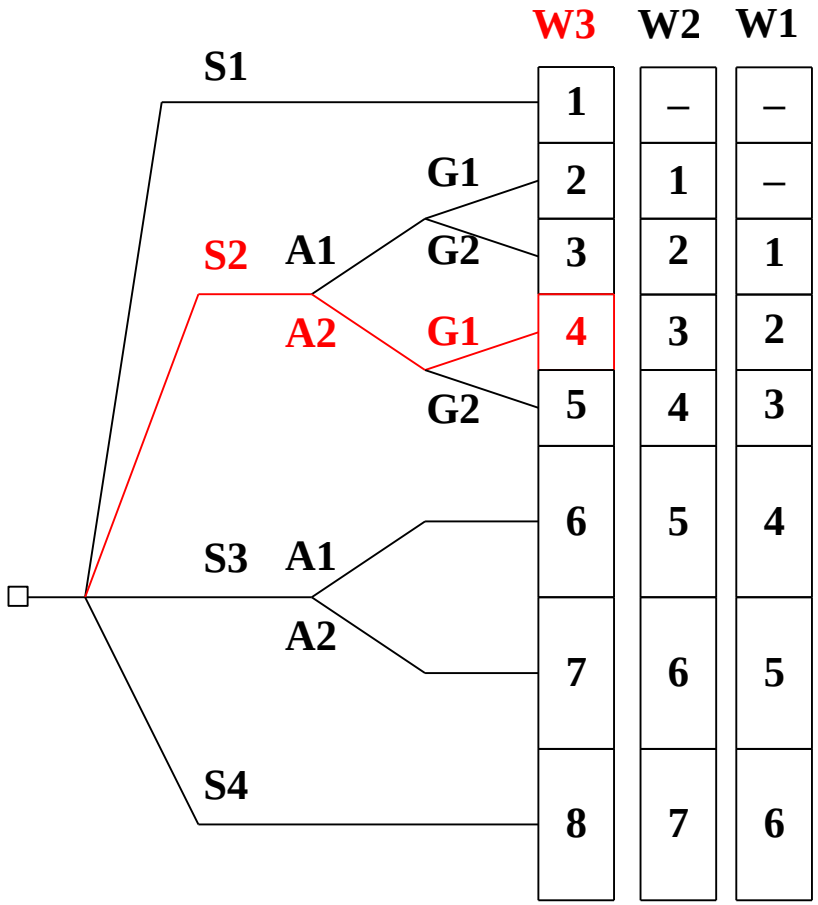
Kockázati paraméter		Értelmezés
Következmény (súlyosság)	S1	Kisebb sérülés
	S2	Súlyosabb sérülés egy vagy több személynél, vagy egy személy halála
	S3	Több személy halála
	S4	Nagyon sok személy halála, katasztrófa
A veszélyes zónában tartózkodás	A1	Ritkától átlagos gyakoriságig
	A2	Gyakori tartózkodástól állandó tartózkodásig
A veszély elkerülésének lehetősége	G1	Lehetséges bizonyos körülmények között
	G2	Majdnem lehetetlen
A nem kívánt esemény gyakorisága	W1	Nagyon kis valószínűség
	W2	Kis valószínűség
	W3	Nagy valószínűség



Kockázati kategóriák:
1 (alacsony) – 8 (magas)

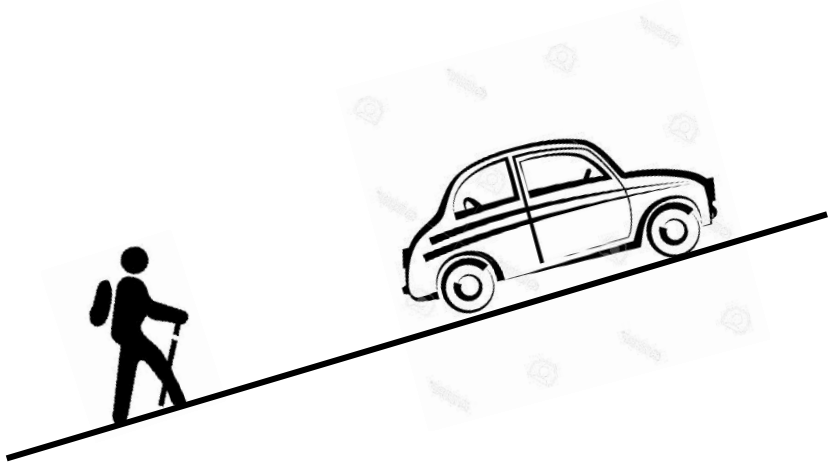
Kockázati gráf - példa
Ajtócsukó automatika – szándékolatlan működés

Kockázati paraméter		Értelmezés
Következmény (súlyosság)	S1	Kisebb sérülés
	S2	**Súlyosabb sérülés egy vagy több személynél, vagy egy személy halála**
	S3	Több személy halála
	S4	Nagyon sok személy halála, katasztrófa
A veszélyes zónában tartózkodás	A1	Ritkától átlagos gyakoriságig
	A2	**Gyakori tartózkodástól állandó tartózkodásig**
A veszély elkerülésének lehetősége	**G1**	**Lehetséges bizonyos körülmények között**
	G2	Majdnem lehetetlen
A nem kívánt esemény gyakorisága	W1	Nagyon kis valószínűség
	W2	Kis valószínűség
	W3	**Nagy valószínűség**



Példa (járműipar)

- A jármű emelkedőn áll
- A visszagurulás gátló meghibásodik
  - pl. pirosnál, emelkedőn
  - parkolóban lejtőn
  - stb.



Súlyosság, gyakoriság

S0: nincs sérülés

S1: könnyebb sérülés

S2: súlyos, életveszélyes, valószínű túlélés

S3: súlyos, életveszélyes, bizonytalan túlélés, halálos sérülés

E1: soha, ritkábban, mint évente

E2: az üzemidő 1%-nál kisebb, néhányszor egy évben

E3: üzemidő 1-10%, párszor havonta

E4: üzemidő 10%-nál több, szinten minden vezetés során

Kontrollálhatóság

Van vezető a járműben

C0: általánosan kontrollálható

C1: a vezetők/résztvevők több, mint 99%-a elkerüli a sérülést

C2: a vezetők/résztvevők több, mint 90%-a elkerüli a sérülést

C3: kevesebb, mint 90% képes elkerülni a sérülést

Nincs vezető a járműben

C0: általánosan kontrollálható

C1: a vezetők/résztvevők több, mint 99%-a elkerüli a sérülést

C2: a vezetők/résztvevők több, mint 90%-a elkerüli a sérülést

C3: kevesebb, mint 90% képes elkerülni a sérülést

Kategóriák kombinációja

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Nincs vezető

Van vezető

KOCKÁZATCSÖKKENTÉS, KOCKÁZATTŰRÉS

Kockázatmentesség

- Szubjektív és objektív kockázat
  - Szubjektív kockázat
    - a lehetséges kártól való félelem mértéke
    - személyenként/szituációnként változó
  - Objektív kockázat
    - Probléma: többnyire csak hiányos, becsült bemeneti adatok
- Egyéni és társadalmi igény (vágy): a kockázatoktól való mentesség
  - A potenciális veszélyeztető hatás megszüntetése
    - Pl. kisfeszültség alkalmazása, alacsony sebesség stb.
    - Probléma: kapacitás-szűkülés
  - A veszélyforrás helyének/hatókörének elkerülése
    - Csak bizonyos típusú veszélyforrások esetén megoldható
    - A közlekedésben globálisan nem megvalósítható
- A tökéletes kockázatmentesség globálisan nem megvalósítható

Kockázatcsökkentés

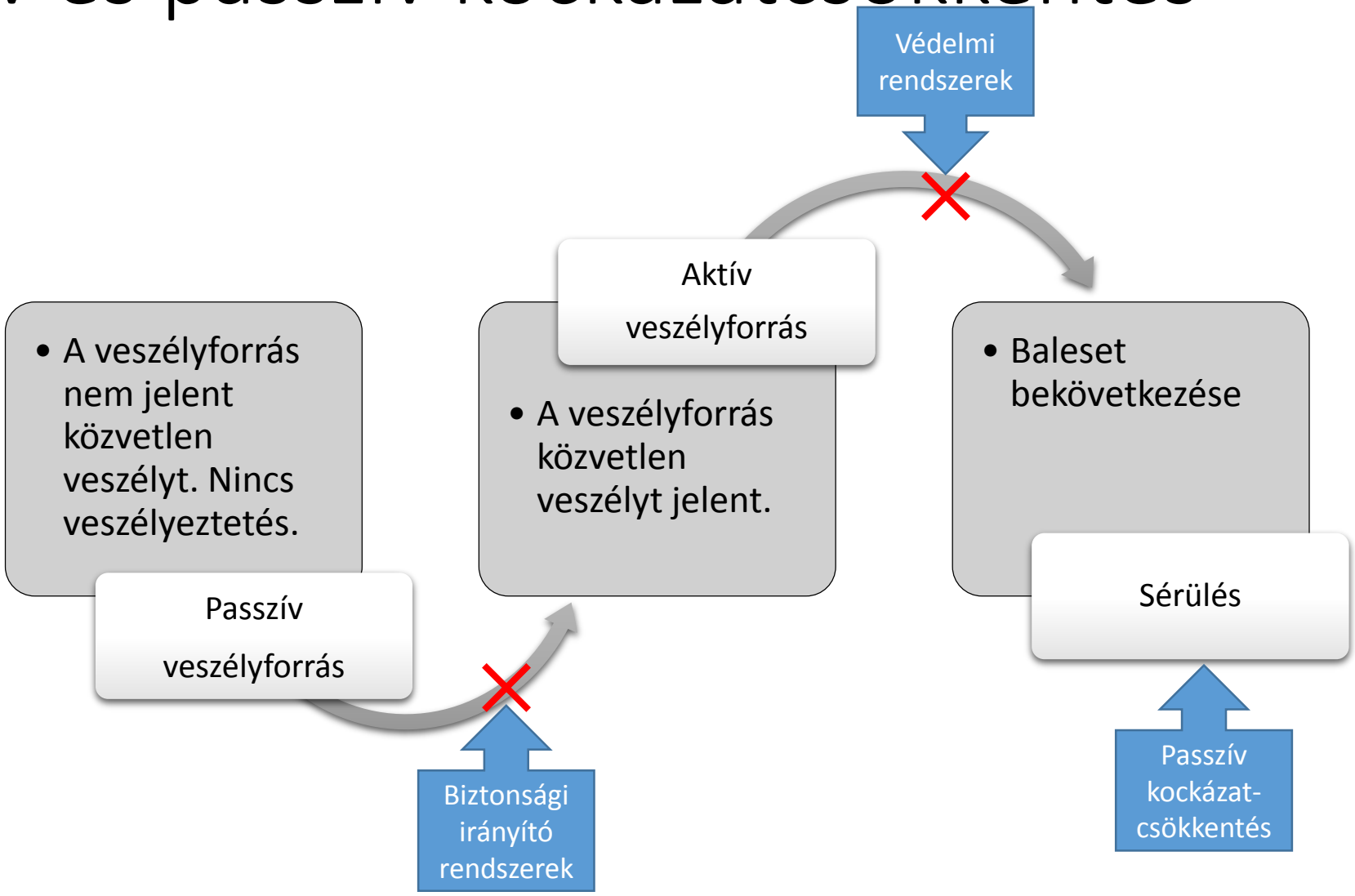
- Műszaki és szervezési intézkedések összessége
- A rendszer / környezet megfelelő
  - kialakítása (tervezése),
  - üzemeltetése.
- A veszélyeztető hatású rendszer használatának szabályozása
  - Oktatás, képzés, jogosultság, belépési engedély stb.
- Folyamatirányító rendszer alkalmazása
  - Pl. forgalomirányító berendezések

Kockázatcsökkentő/biztonsági intézkedések

- aktív kockázatcsökkentés/biztonság – a balesetek megelőzése
  - a biztonságos állapottól való eltérés megakadályozása
    → biztonsági irányítórendszer
  - a veszélyeztetések idejekorán való felismerése – folyamatos ellenőrzés
    - műszaki berendezések állapota
    - emberi tevékenység (éberség stb.)

    ÉS megfelelő reakció kiváltása
    → védelmi rendszer
- passzív kockázatcsökkentés/biztonság – a balesetek következményeinek enyhítése

Aktív és passzív kockázatcsökkentés



Elfogadható kockázati szint, kockázattűrés

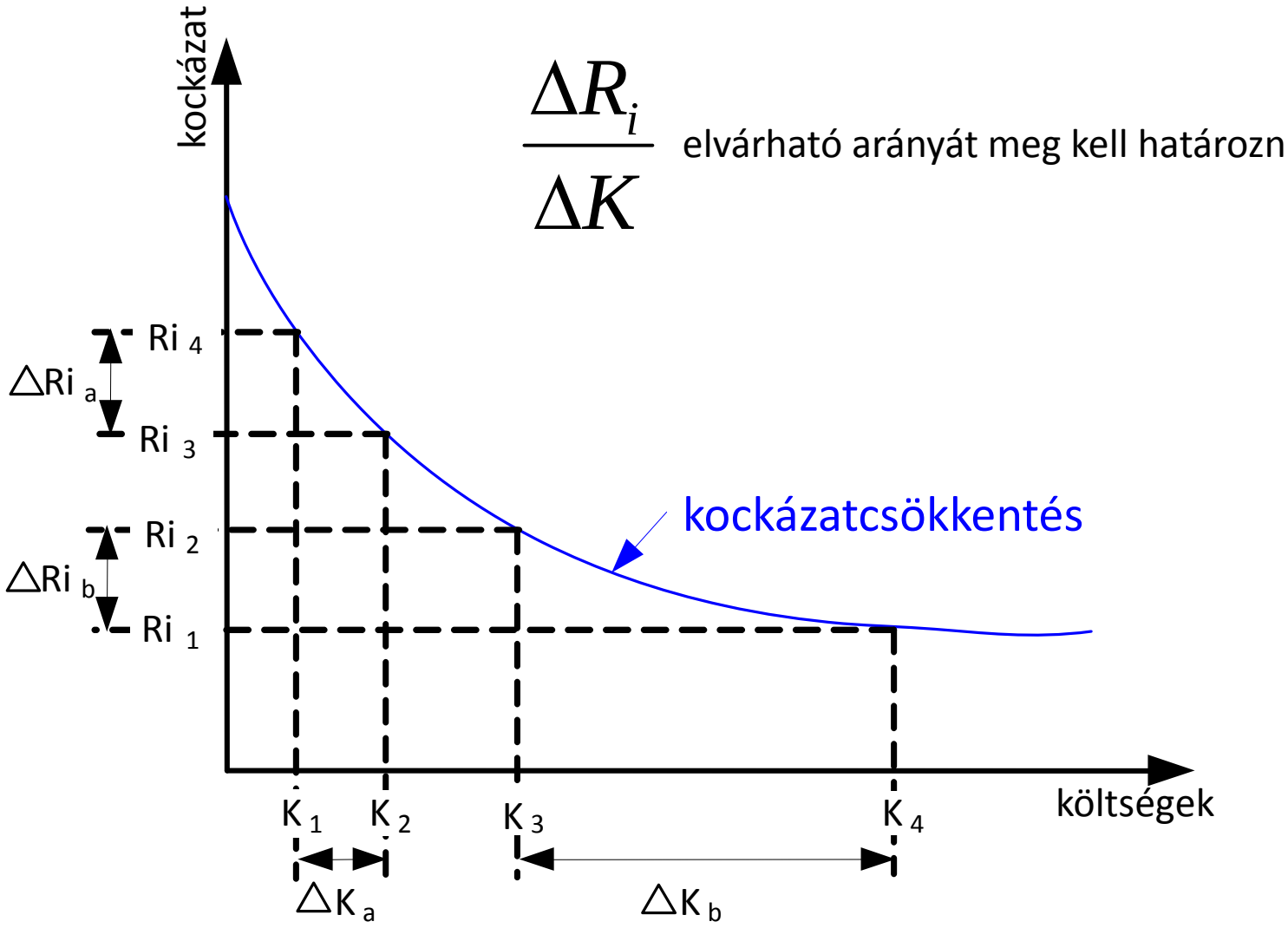
- Meddig kell csökkenteni a kockázatot? Mi az elfogadható kockázati szint?
- Befolyásoló tényezők
  - Társadalmi elfogadottság – érdekcsoportok, érdekképviselet – érdekegyeztetés
    - a kockázat okozója
    - a kockázat elszenvedője
    - a hatóság
  - költségek – elérhető eredmény
- Az elfogadható kockázati szint függ pl.
  - a sérülések súlyosságától
  - a veszélynek kitett személyek számától
  - a veszélynek kitett személyek jellege
  - a veszélyeztető hatás időtartamától
  - a felelősség arányától

Kockázati határ – elfogadható kockázat

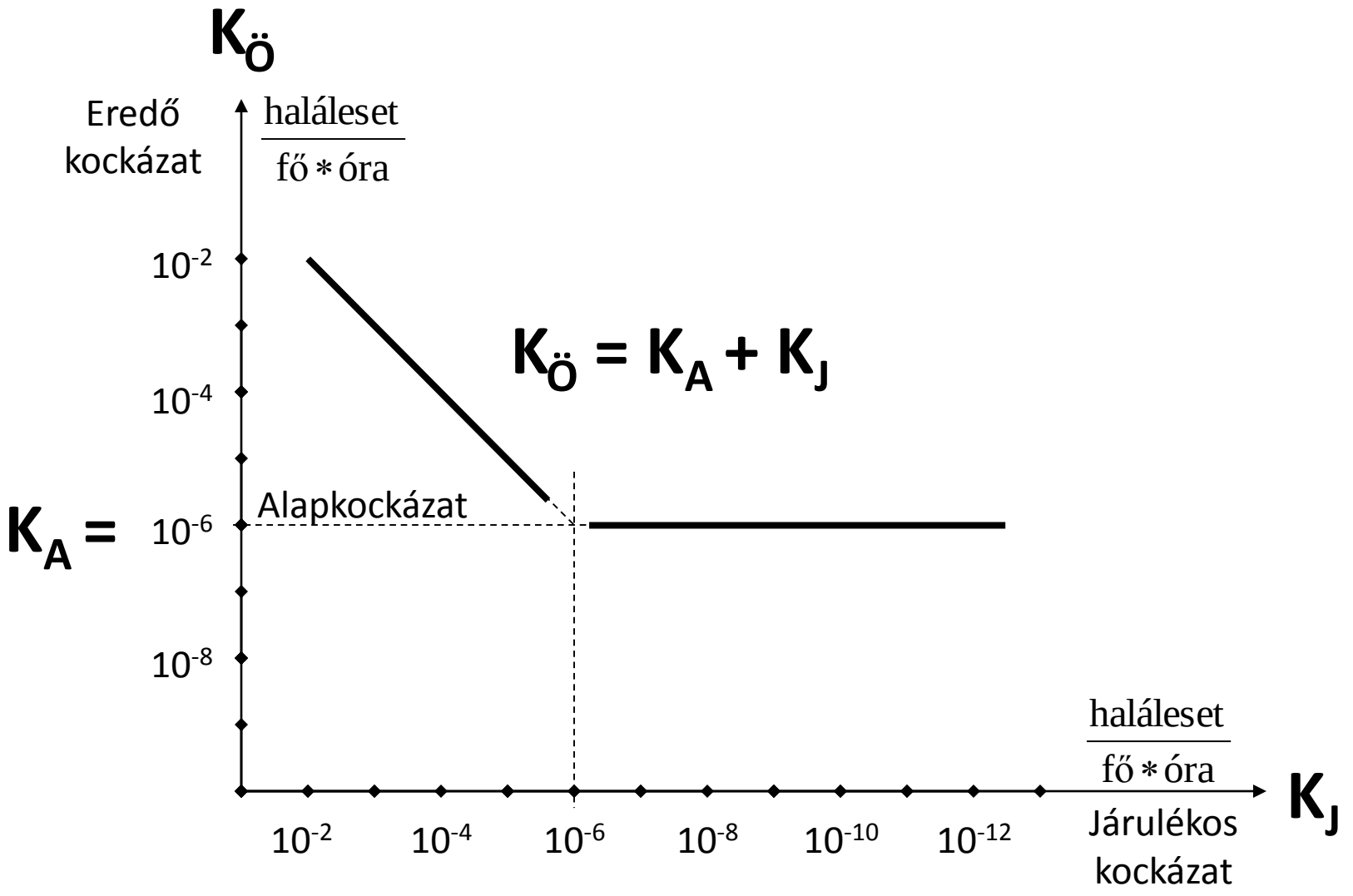
- társadalmi konszenzus
- a kielégítő (megengedhető) valószínűség határértékét
  - az arányosság elvének megfelelően,
  - a védendő javak értéke alapján

  határozzák meg
- határérték meghatározása
  - a veszély fellépési valószínűségére/gyakoriságára
  - a kárértékre
  - a reprezentatív kárkategóriák fellépési valószínűségére

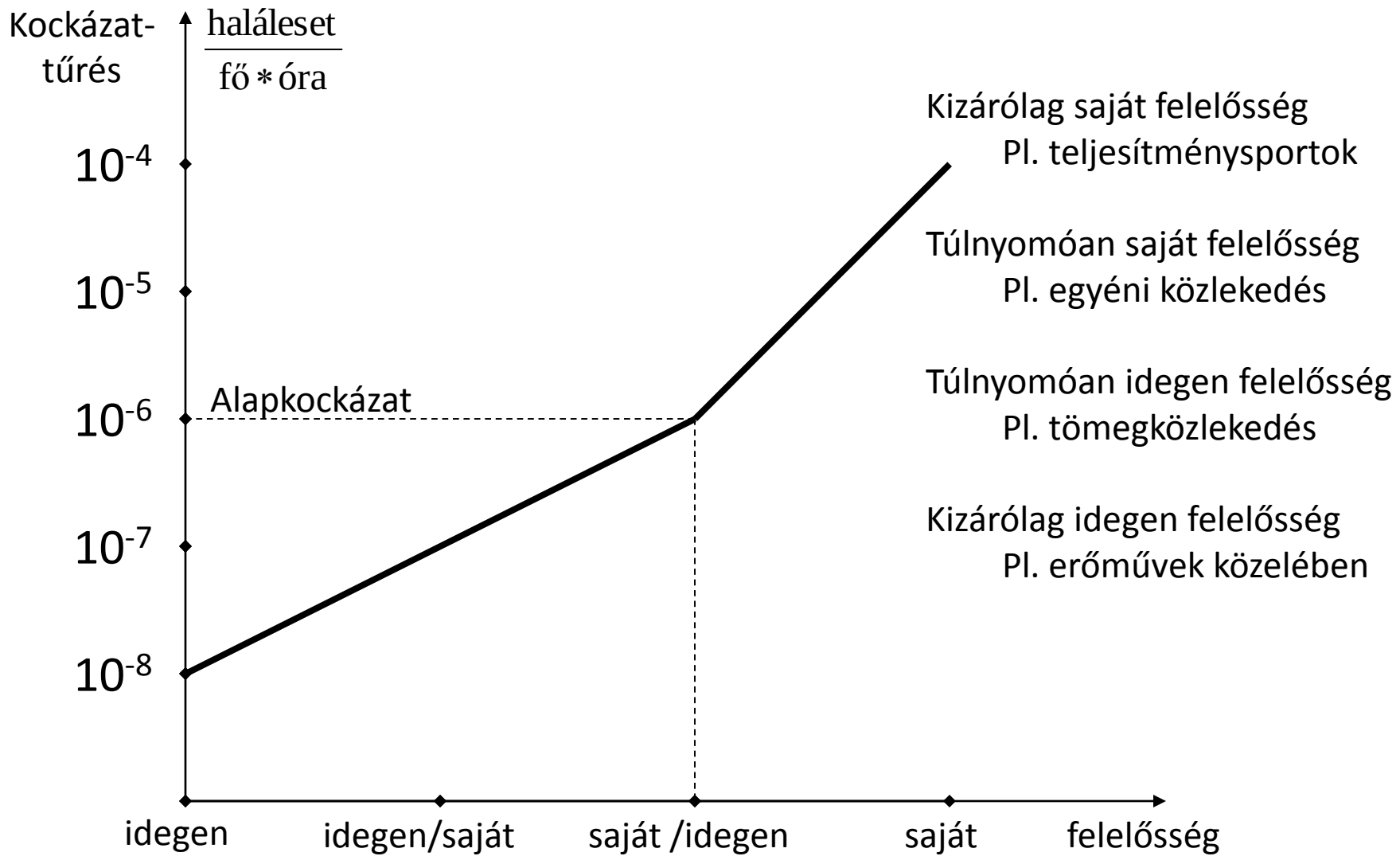
A kockázatcsökkentés hatékonysága



Alap- és járulékos kockázat



A kockázattűrés függése a felelősségtől



Kockázattűrési megközelítések

- MEM
  - Minumum Endogeneous Mortality
  - minimális természetes „halandóság”
  - 5-15 év között az értéke 2×10^{-4} haláleset/fő/év
  - Feltételezése szerint egyidejűleg max. 20 műszaki rendszer veszélyeztethet egy egyént
  - egy rendszerre 10^{-5} haláleset/fő/év jut
  - azaz 10^{-9} haláleset/fő/óra.

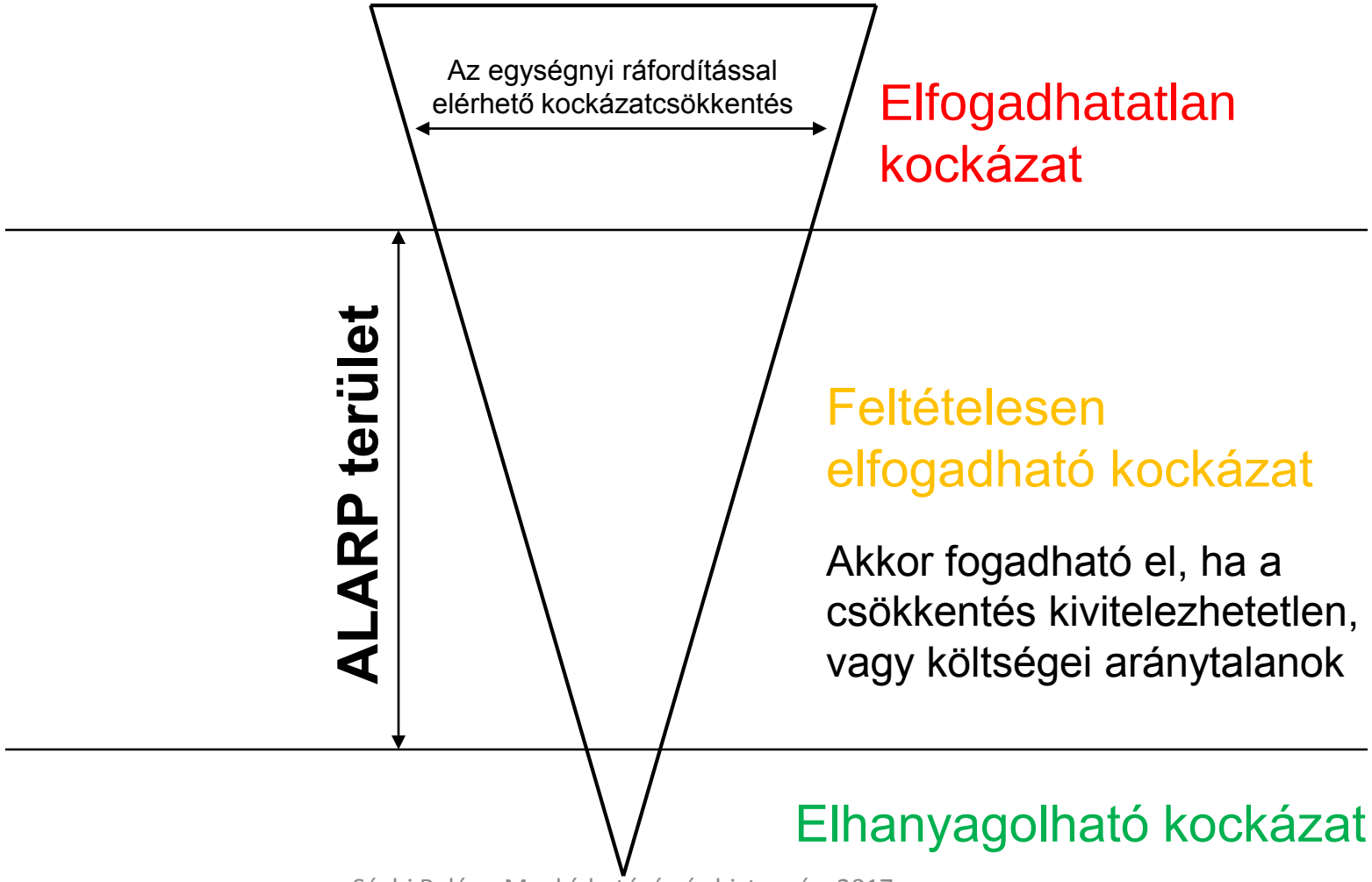
Kockázattűrési megközelítések

- GAME / GAMAB
  - Globalement Au Moins Equivalent
  - Egy új rendszer nem lehet rosszabb, mint a régiek
  - Statisztikai adatok

  - Mi van új rendszer esetén?

Kockázatcsökkentés – Az ALARP elv

As **L**ow **A**s **R**easonably **P**racticable
Olyan alacsony, amennyire ésszerűen megvalósítható



Elfogadható kockázat gyakran az elemzésből származik (pl. ágazati szabványokban)

	Következmény			
Gyakoriság	Katasztrofális	Kritikus	Marginális	Elhanyagolható
Gyakori	**A**	**A**	**A**	**B**
Valószínű	**A**	**A**	**B**	**C**
Esetenként	**A**	**B**	**C**	**C**
Távoli	**B**	**C**	**C**	**D**
Valószínűtlen	**C**	**C**	**D**	**D**
Hihetetlen	**D**	**D**	**D**	**D**

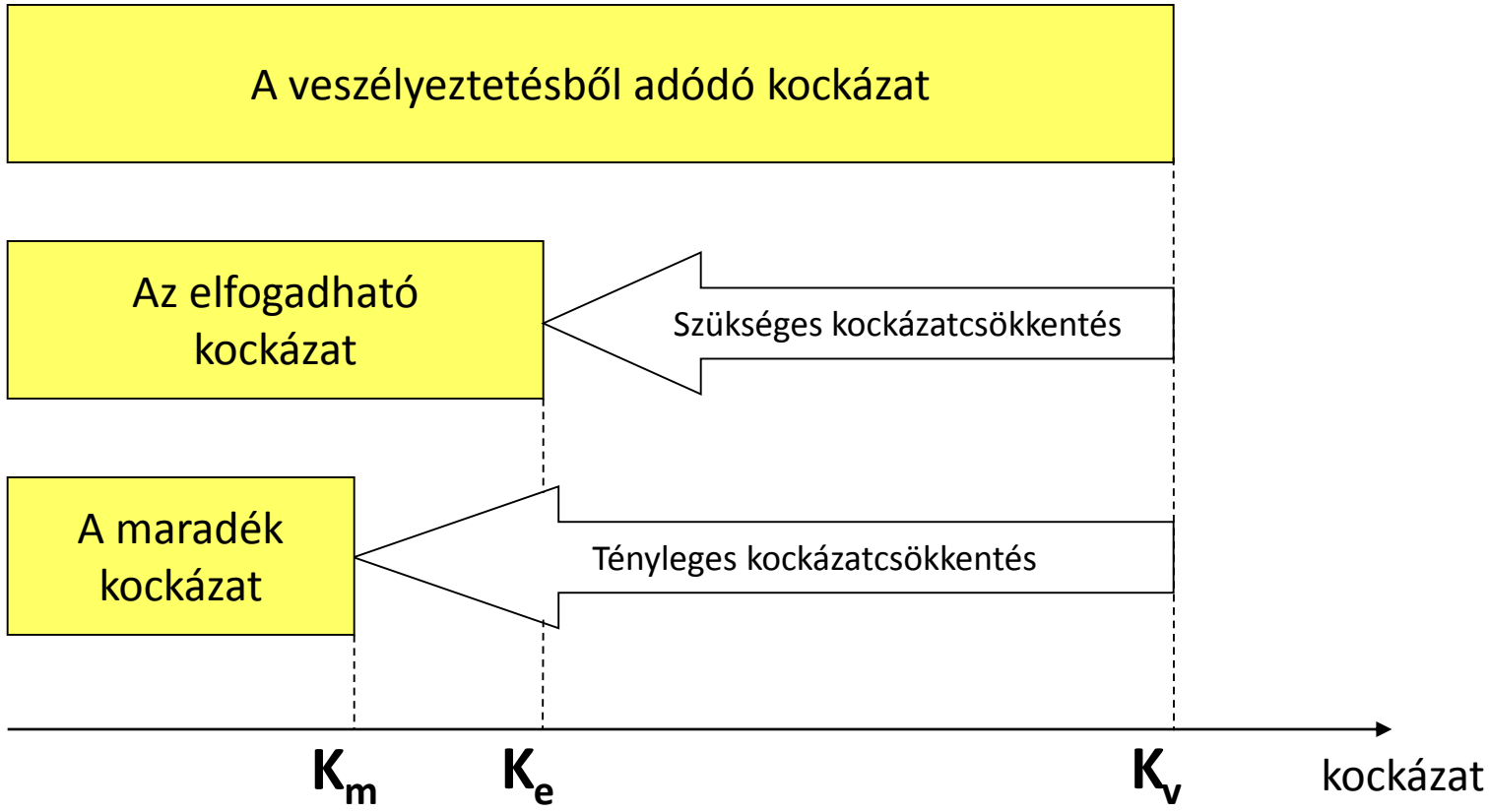
Kockázati osztály	**Értelmezés**
A	Nem tolerálható
B	Nem kívánatos, csak akkor fogadható el, ha a kockázatcsökkentés nem lehetséges
C	A *projekt biztonsági áttekintő bizottsága* ajánlásával elfogadható
D	Normál projekt áttekintés alapján elfogadható

Elfogadható kockázati szint

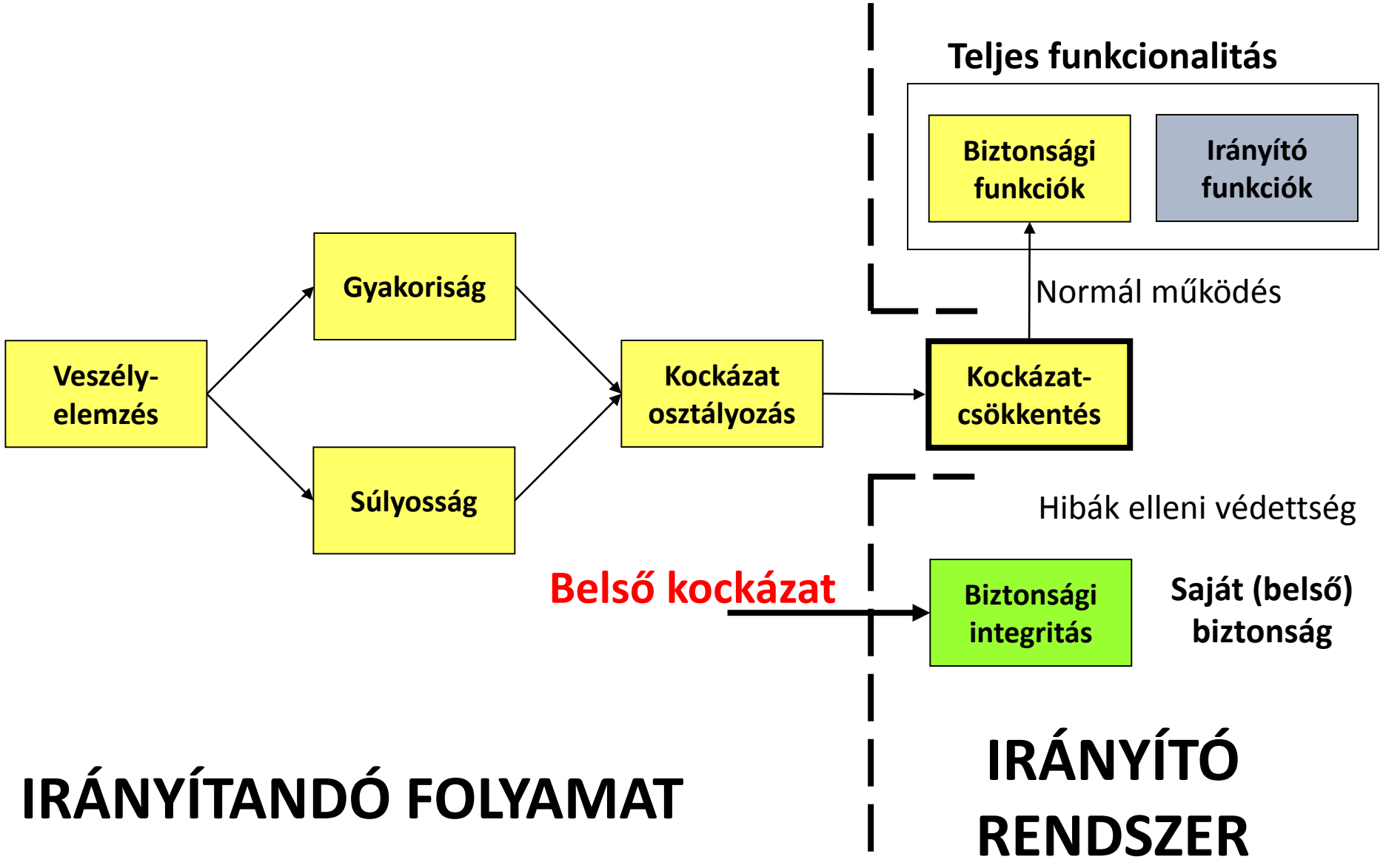
Valószínűségi szint		Kárkihatási kategóriák			
		Kataszt-rofális 4	Kritikus 3	Csekély 2	Elhanya-golható 1
gyakori	A	K4			
valószínű	B				
néha	C		K3		
alig	D			K2	
valószínűtlen	E				K1
rendkívül valószínűtlen	F				

- 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 – Kockázatmenedzselés



Biztonsági funkciók – Biztonsági integritás



Biztonsági rendszerekben fellépő hibák

Szisztematikus hibák (emberi eredetűek)

- 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

Véletlenszerű hibák (hardver meghibásodások)

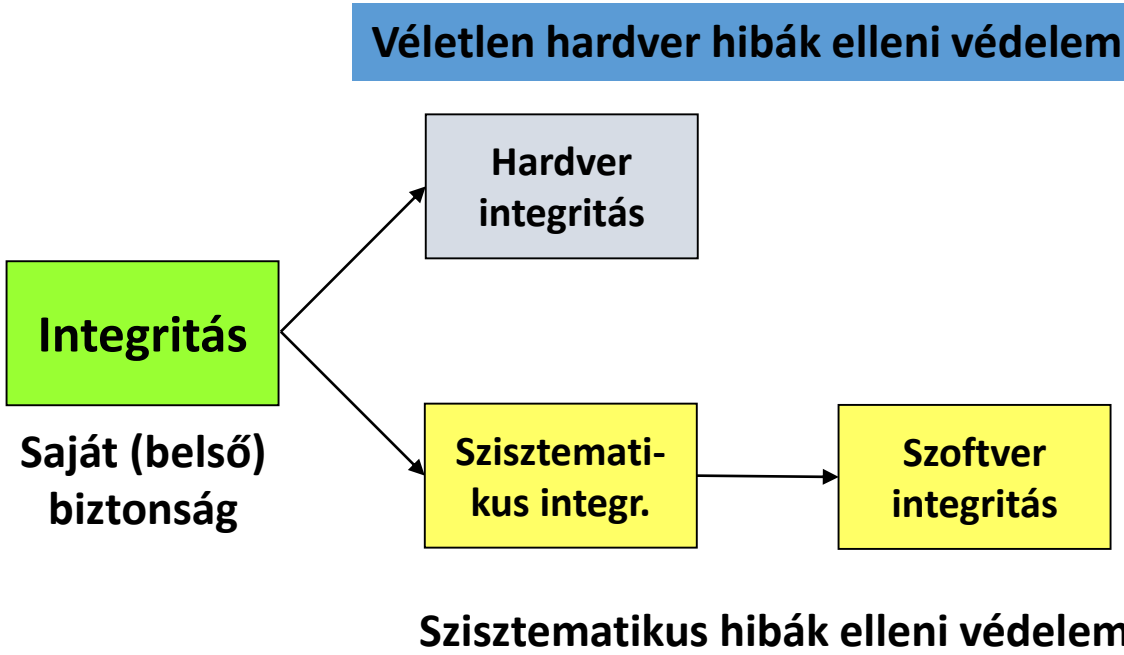
Befolyásoló tényezők:

- 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.

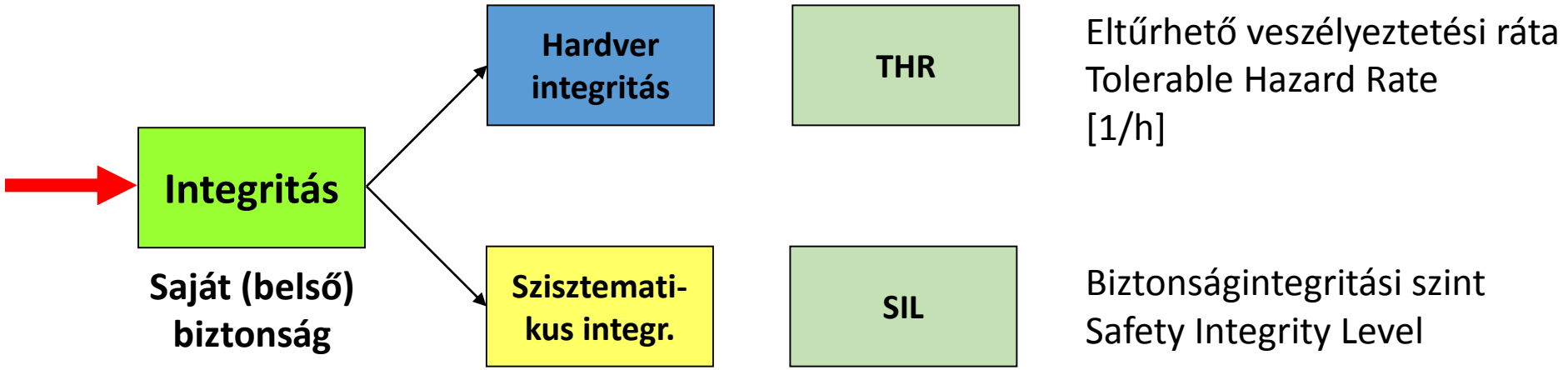


A **szisztematikus integritás** a biztonsági integritásnak
a veszélyes szisztematikus hibákra vonatkozó része.

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

Biztonsági integritási szintek és hibakezelés

Véletlen hardver hibák elleni védelem
A biztonsági szintnek megfelelő
megbízhatóság elérése, biztonsági stratégiák



Szisztematikus hibák elleni védelem
A biztonsági szintnek megfelelő fejlesztési módszerek alkalmazása
Minőségbiztosítás a teljes életciklusban

A biztonsági integritási szintek száma és értelmezése

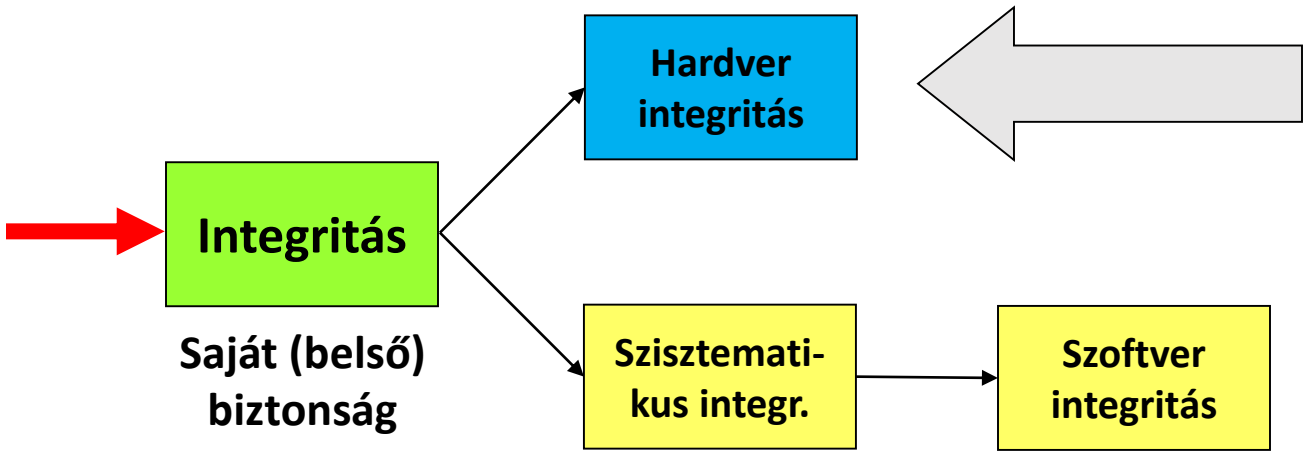
A biztonsági integritási szintek száma a különböző alkalmazási területeken:
1 … 8

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 integritási szintek és hibakezelés

Véletlen hardver hibák elleni védelem:
- A biztonsági szintnek megfelelő megbízhatóság elérése, biztonsági stratégiák



Hibadetektálás
Hibatűrés
Biztonsági állapot

A hibák
- **elkerülése**
- **eltávolítása**

Diverz kialakítás

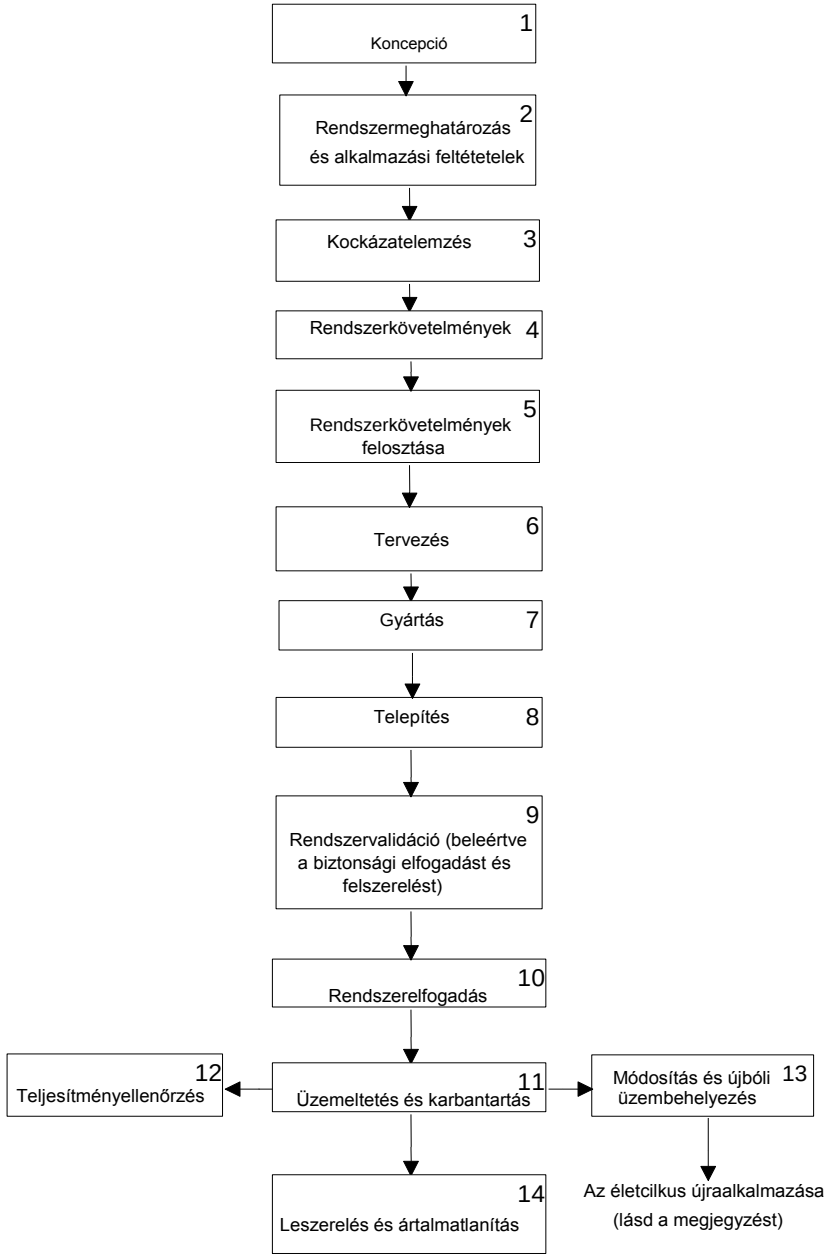
Szisztematikus hibák elleni védelem:

- **Minőségbiztosítás a teljes életciklusban (szervezett folya**
- **A biztonsági szintnek megfelelő fejlesztési módszerek alkalmazása**
- **Mó**

A szisztematikus hibák elleni védelem

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

Folyamat szabályozása (példa)

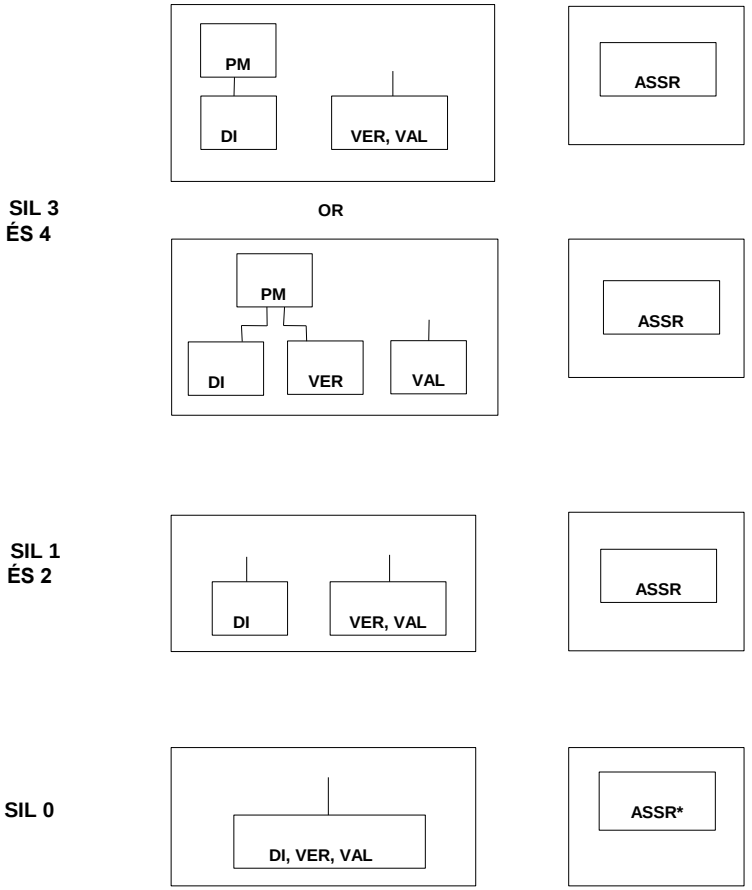


MEGJEGYZÉS: Az a fázis, amelynél a módosítás a rendszer életciklusába belép, függ a módosítandó rendszertől és a szóban forgó módosítás jellegétől.

SIL-intézkedések, példa (EN 50129)

Technikák/Intézkedések	SIL 1	SIL 2	SIL 3	SIL 4
1. A biztonsági szervezet tagjainak képzése	HR: Kezdeti képzés minden biztonságorientált tevékenységnél		HR: Minden biztonságorientált tevékenységgel kapcsolatban ismétlődő képzés vagy a tevékenység rendszeres teljesítése	
2. A résztvevők személyi függetlensége	lásd a 6. ábrát: a függetlenség megszervezése			
3. A biztonsági szervezet személyzetének képesítése (lásd az 1. sz. megjegyzést) 4. (lásd a megjegyzést)	HR: műszaki oktatás vagy elegendő tapasztalat		HR: magasabb szintű műszaki oktatás vagy szélesebb körű tapasztalat	

Személyi függetlenség (példa)



Magy.:
PM = Project Manager
DI = Tervező, megvalósító
VER = Verifikáló
VAL = Validáló
ASSR = Asszesszor

= lehet egyazon személy

=lehet egyazon szervezet

* =SIL0-ra csak akkor kell asszesszor, egy átfogó rendszer biztonságára lehet hatással

SIL-intézkedések, példa (EN 50129)

Technikák/Intézkedések	SIL 1	SIL 2	SIL 3	SIL 4
1. A biztonságorientált és nem biztonságorientált rendszerek szétválasztása	R: jól meghatározott interfészek a biztonságorientált és nem biztonságorientált rendszerek között		HR: jól meghatározott interfészek a biztonságorientált és nem biztonságorientált rendszerek között és interfész-elemzés	
2. Grafikus leírás beleértve pl. blokkdiagramokat	HR		HR	
3. Strukturált specifikáció	HR: manuális, hierarchikus szétválasztás alfeladatokra, interfészleírások		HR: hierarchikus szétválasztás formális módszerek alkalmazásával, automatikus konzisztencia-ellenőrzés, finomítás a funkcionális szintig	
4. Formális vagy félformális módszerek			R: számítógéppel támogatott	
5. Számítógéppel támogatott specifikációs eszközök		R: eszközök kiválasztása bármely konkrét tervezési módszer előnyben részesítése nélkül	R: modellorientált eljárások hierarchikus felosztással, minden objektum, kapcsolatainak, közös adatbázisának, automatikus konzisztencia-ellenőrzésének leírása	
6. Ellenőrzőlisták	R: előkészített ellenőrzőlisták minden biztonsági életciklus-fázisra		R: előkészített részletes ellenőrzőlisták minden biztonságorientált életciklus-fázisra	
7. Veszélynapló	HR: A Veszélynaplót fel kell fektetni és karban kell tartani a rendszer teljes életciklusa során			

Módszerek hozzárendelése az ASIL-hez (példa)

Table 2 — Properties of modular system design

	Properties	ASIL			
		A	B	C	D
1	Hierarchical design	+	+	++	++
2	Precisely defined interfaces	+	+	+	+
3	Avoidance of unnecessary complexity of hardware components and software components	+	+	+	+
4	Avoidance of unnecessary complexity of interfaces	+	+	+	+
5	Maintainability during service	+	+	+	+
6	Testability during development and operation	+	+	++	++

Table 4 — Methods for deriving test cases for integration testing

	Methods	ASIL			
		A	B	C	D
1a	Analysis of requirements	++	++	++	++
1b	Analysis of external and internal interfaces	+	++	++	++
1c	Generation and analysis of equivalence classes for hardware-software integration	+	+	++	++
1d	Analysis of boundary values	+	+	++	++
1e	Error guessing based on knowledge or experience	+	+	++	++
1f	Analysis of functional dependencies	+	+	++	++
1g	Analysis of common limit conditions, sequences, and sources of dependent failures	+	+	++	++
1h	Analysis of environmental conditions and operational use cases	+	++	++	++
1i	Analysis of field experience	+	++	++	++

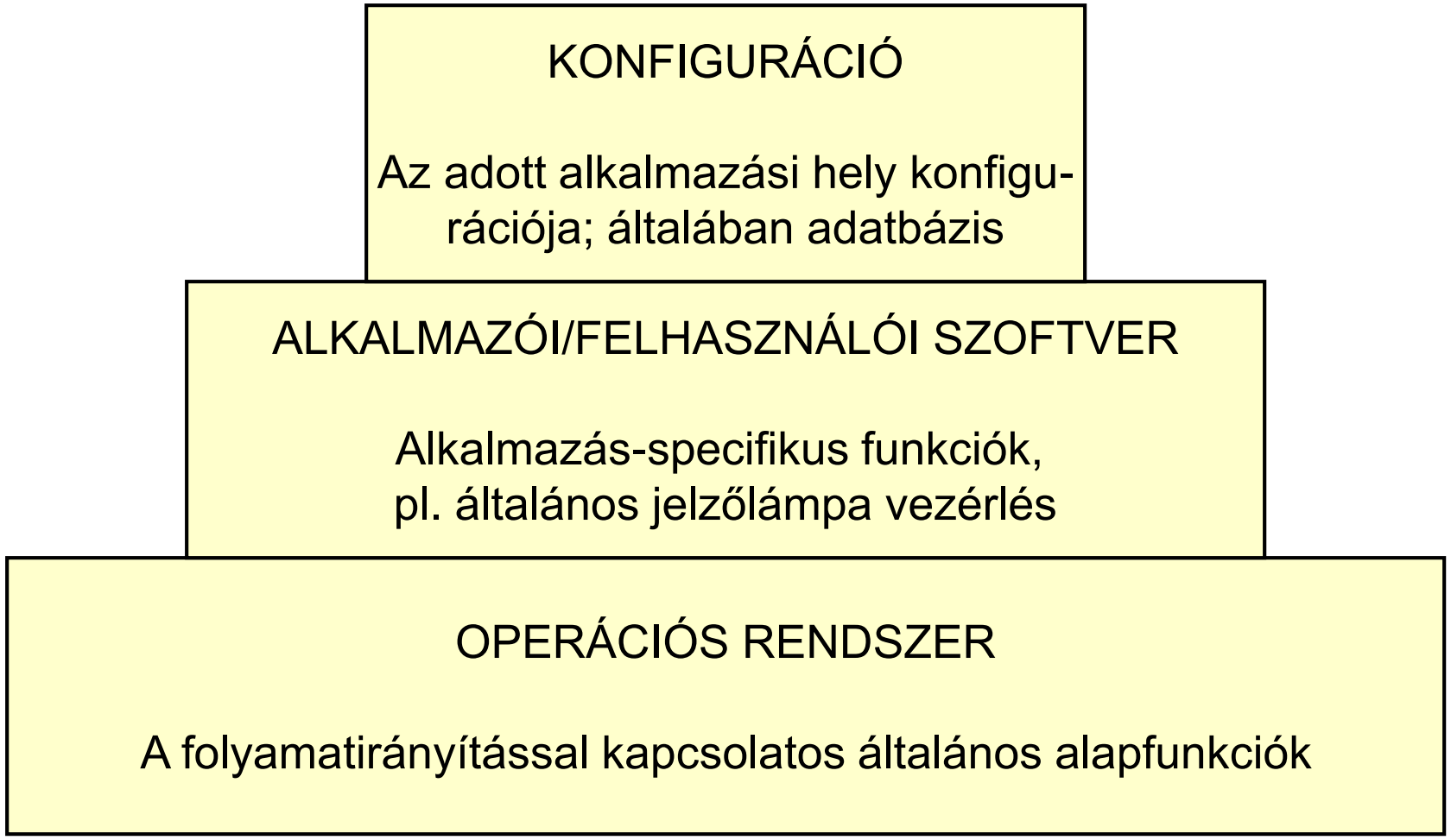
Biztonsági folyamatirányító

rendszerek szoftvere

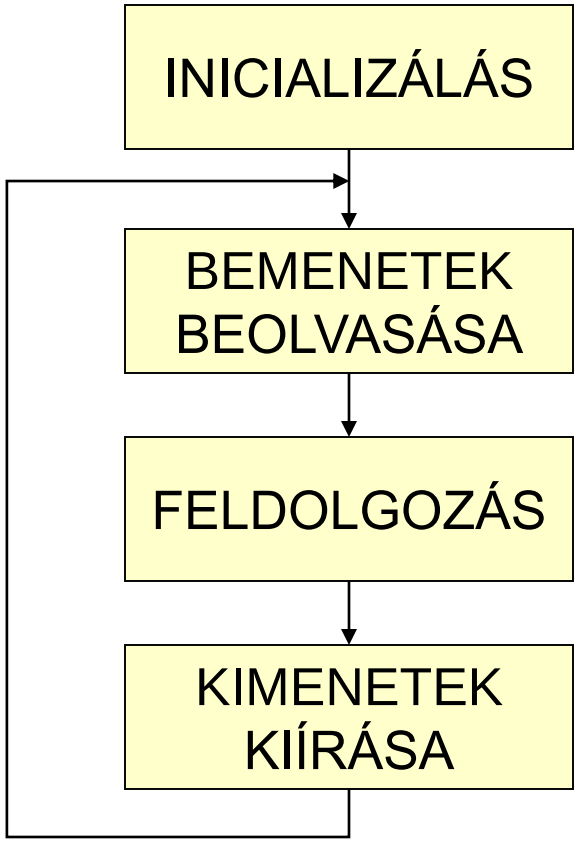
Programozott irányítórendszerek

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

Tagolt szoftverfelépítés



A folyamatirányító számítógépek



- Operációs rendszer feladatai
  - ciklikus működés
  - Többcsatornás működés támogatása
- Futás közbeni tesztek
  - Minden ciklusban v. ritkábban
  - Kommunikáció tesztelése
- Cél
  - elsődlegesen hardverhibák feltárása,
  - ritkábban szoftverhibák feltárása.
- A detektált hibákra megfelelően reagálni is kell

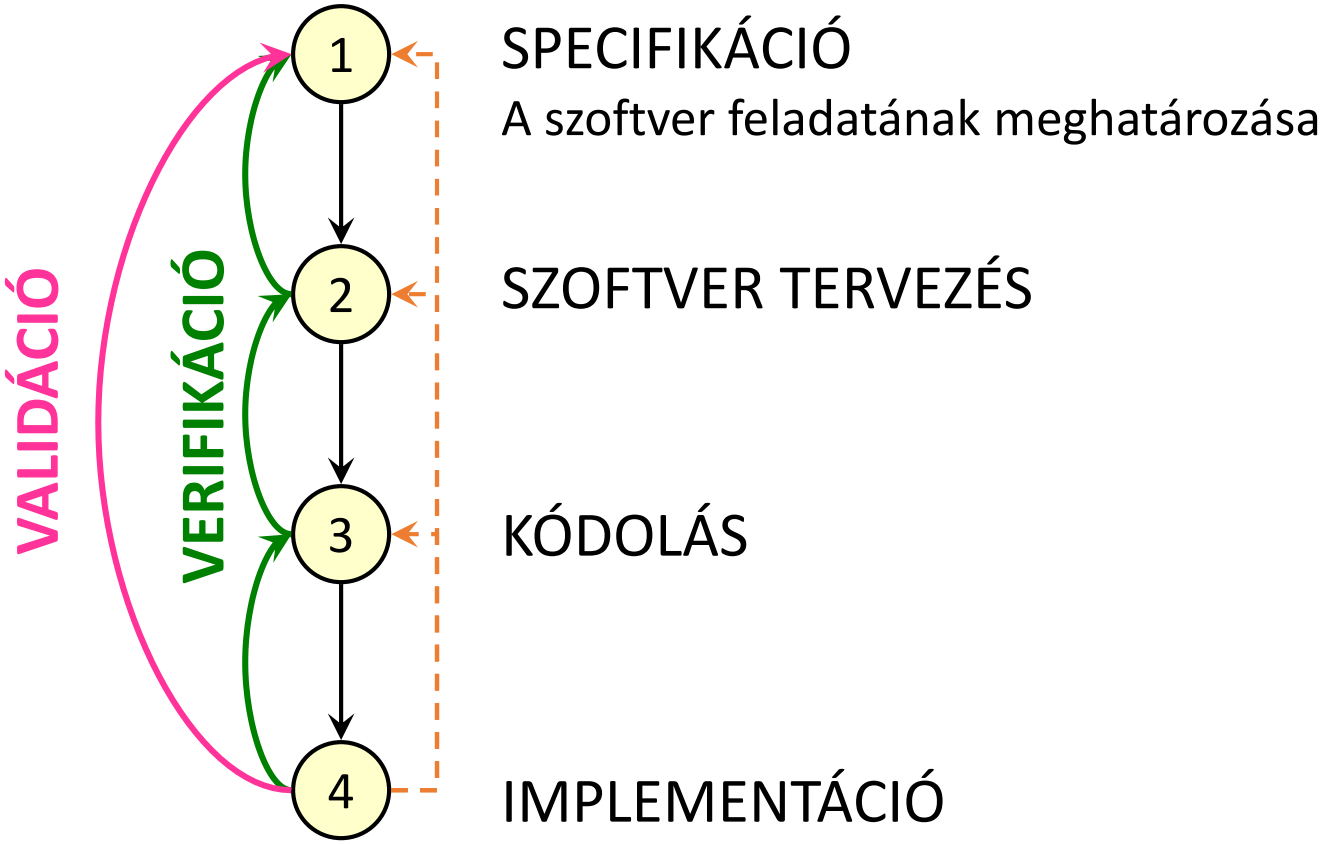
Szoftverek megbízhatósága

- A szoftver akkor működőképes – és így biztonságos –, ha a követelményeket (specifikáció) jól fogalmaztuk meg, és a megvalósítás (implementáció) is helyes.

- A szoftverek megbízhatósága (helyes működésének valószínűsége) **független az időtől** (amennyiben nem változtattuk meg).

- Szoftverek esetében nem beszélhetünk meghibásodásról:
  - A szoftver megbízhatóságát „csak” az eredeti, szisztematikus, specifikációs, tervezési és megvalósítási hibák csökkentik.
  - A szoftvert tároló alkatrész meghibásodása hardver-meghibásodás.
  - DE! Emberi beavatkozással egy jó szoftvert is el lehet rontani, például:
  - **Újra-bekerülési hiba**: átlagosan minden harmadik hibajavítással újabb hibát idézünk elő.

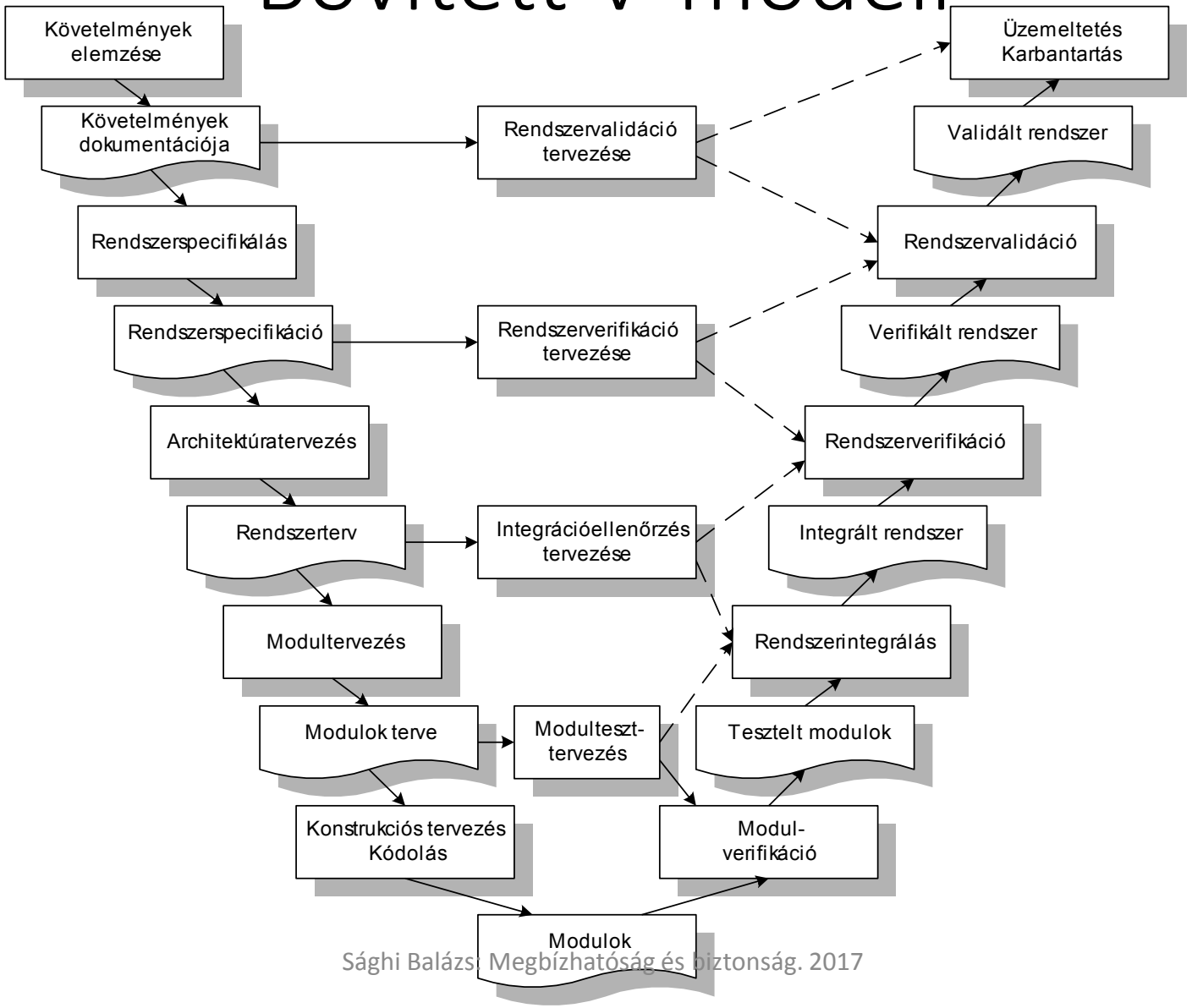
Szoftver-életciklus



KARBANTARTÁS

- Hibák javítása
- Módosítások

Bővített V-modell



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**.

Szoftverírás (1)

- Programozási technikák
  - Top-down
  - Bottom-up
  - Az előző kettő kombinációja
- Programozási koncepciók
  - **Defenzív programozás**: számítok arra, hogy a programozás során hibákat fogok elkövetni.
    - Passzív ellenőrzések: pl. ellenőrző összegek, hihetőség-vizsgálat
    - Aktív ellenőrzések: adatáramlástól független ellenőrzés, így tesztelhetők a ritkán aktív lefutási ágak is.
  - CASE: Computer Aided Software Engineering
    - Automatikus programgenerátorok: a generátor program helyességét kell bizonyítani.

Szoftverírás (2)

- Programnyelv, fejlesztői környezet
  - Olyan programozási nyelv szükséges, amely a valósidejű (real-time) működést támogatja.
  - Programozási nyelv szintje
    - Alacsony szintű programnyelv (pl. Assembly):
      - gépközeli, rugalmas,
      - de a szoftveríró nincs rákényszerítve a strukturált programozásra.
    - Magas-szintű programnyelv:
      - a nyelv szabályai rákényszerítenek a biztonságos programírás szabályaira,
      - de nem gépközeli, ezért a folyamat-vezérlést nehezebb programozni,
      - fordítóprogram (compiler) szükséges: ennek helyes működését is igazolni kell!
  - Programnyelv választásának kritériumai
    - A programozó mennyire jártas az adott nyelven való programozásban?
    - Mennyi tapasztalat van az adott programnyelvvel?
    - Van-e elterjedt, nagy valószínűséggel hibamentes fordítóprogram?
    - Mekkora az adott programnyelv/fejlesztőkörnyezet támogatottsága (pl. szimulációs háttér)?

Szoftver tesztelés (1)

- Az eredeti hibák kiküszöbölésének leggyakoribb eljárása a **hibaeltávolítás**. Lépései:
  - tesztelés
  - diagnózis
  - javítás.

- **Tesztelés**
  - Statikus: a rendszer működtetése nélküli tesztelés. Ez végrehajtható
    - a rendszeren magán vagy
    - a rendszer alkalmas modelljén végrehajtott vizsgálatokkal.

    Formái:
    - statikus analízis (program-átvizsgálás, szimbolikus végrehajtás, adatfolyam analízis stb.)
    - helyességbizonyítás (induktív bizonyítás)

Szoftver tesztelés (2)

- Dinamikus tesztelés: a rendszer működtetése révén
  - Tesztbemenetek kiválasztásának kritériumai
    - A tesztelés célja szerint
      - konformitás tesztek: a specifikáció teljesítésének vizsgálata
      - hibakereső tesztek: hibák feltárására
    - Rendszermodell szerint
      - funkcionális teszt (black box, feketedoboz): csak a be/kimenetek viselkedését vizsgálom.
      - strukturális teszt (white/glass box, „fehér/üveg doboz”): a teljes belső szerkezet figyelembevételével tesztel.
      - kombináció (grey box, „szürke doboz”): nagy vonalakban (nem részletekbe menően) teszi láthatóvá a tesztelendő egység belső struktúráját is.
  - Tesztbemenetek generálása
    - Determinisztikus tesztek: a tesztmintákat előre meghatározzák
    - Valószínűségi (véletlen vagy statisztikus) tesztek: a tesztmintákat valószínűségi eloszlás alapján választják ki.

Szoftver tesztelés (3)

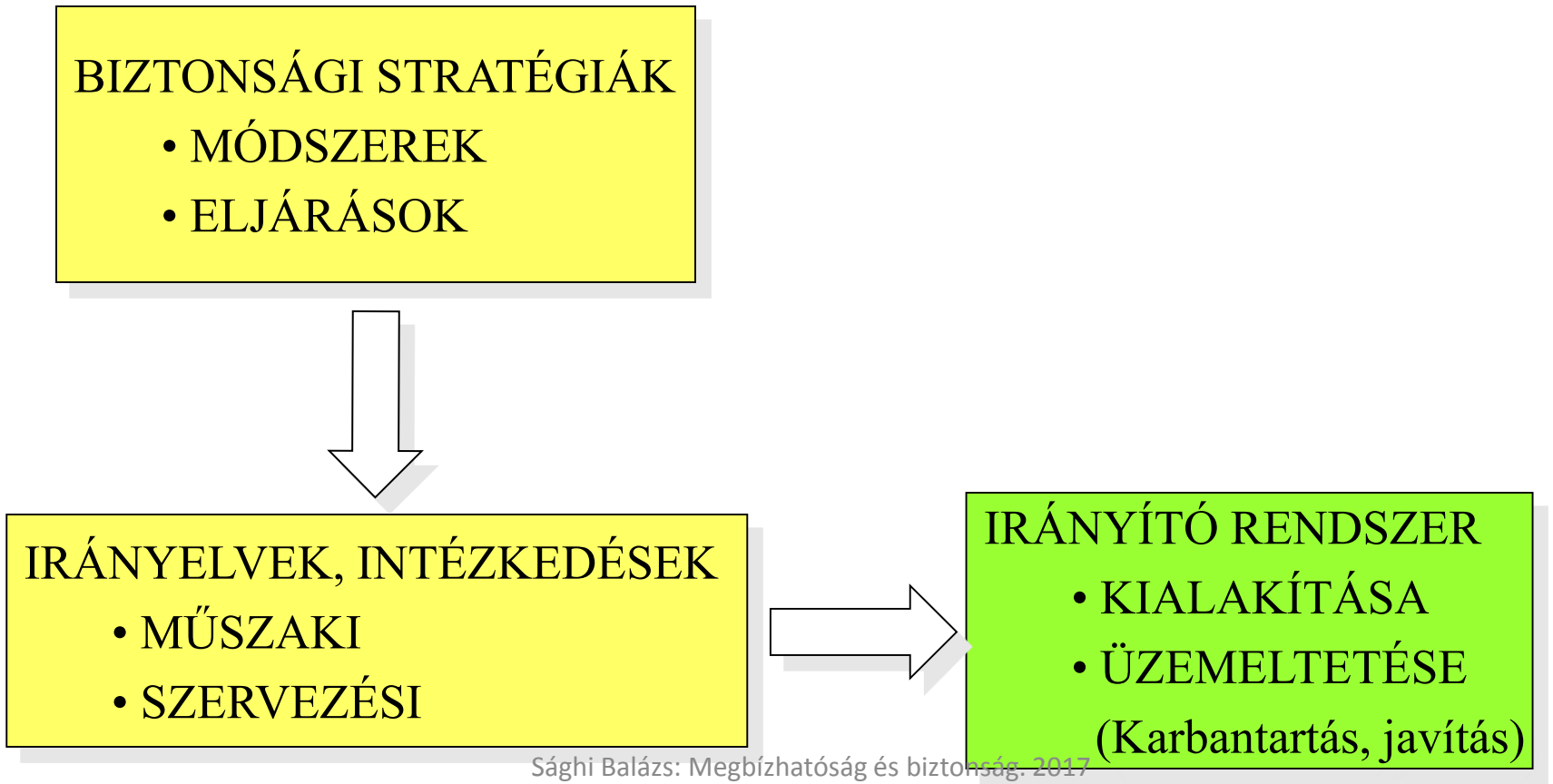
- A tesztkimenetek figyelésével dönthető el, hogy a teszt-feltételek teljesültek-e.
  - Összes tesztkimenet figyelése
  - A tesztkimenetek kompakt reprezentációja

- Referencia
  - Kimeneti eredmények szimulálása
  - Referenciarendszer („golden unit”)
  - Specifikáció
  - Prototípus
  - Másik implementáció

- Tesztelési fokozatok
  - Modulteszt
  - Több modul kapcsolatának tesztelése
  - Integrációs teszt: teljes kapcsolatrendszer + kommunikáció
  - Rendszerteszt: célhardveren való tesztelés
  - Átvételi teszt: a megrendelő végzi
  - Javítás utáni teszt

BIZTONSÁGI STRATÉGIÁK (1)

AZ IRÁNYÍTÓ RENDSZER VÉLETLENSZERŰ MEGHIBÁSODÁSAI ELLENI VÉDELEM ESZKÖZEI



BIZTONSÁGI STRATÉGIÁK (2)

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)

SAFE-LIFE STRATÉGIA

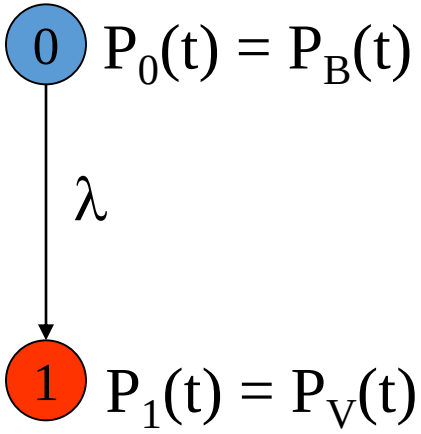
TÖKÉLETESSÉG, HIBAKIZÁRÁS

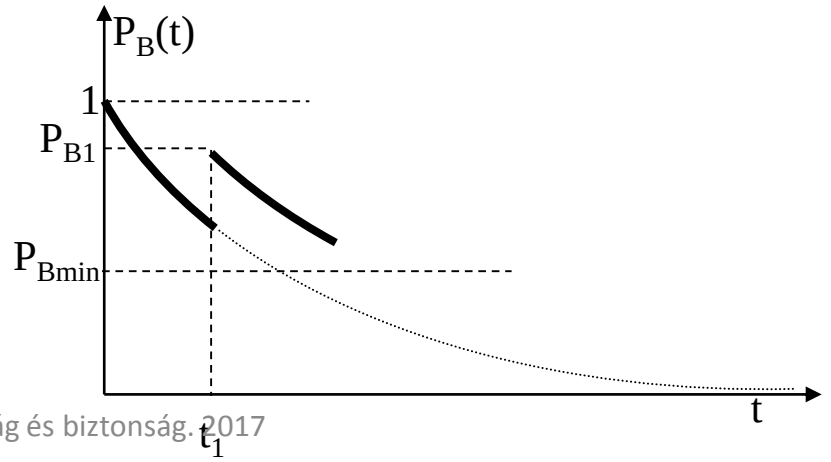
IDEÁLIS $\lambda = 0$

VALÓSÁGOS $\lambda \cong 0$

KORLÁTOZOTT ALKALMAZÁS
- EGYSZERŰ ELEMEK, RENDSZEREK
- RÖVID BIZTONSÁGOS ÉLETTARTAM

MEGELŐZŐ KARBANTARTÁS





WORST CASE FELTÉTELEZÉS

Bennfoglalt (inherens) hibabiztosság

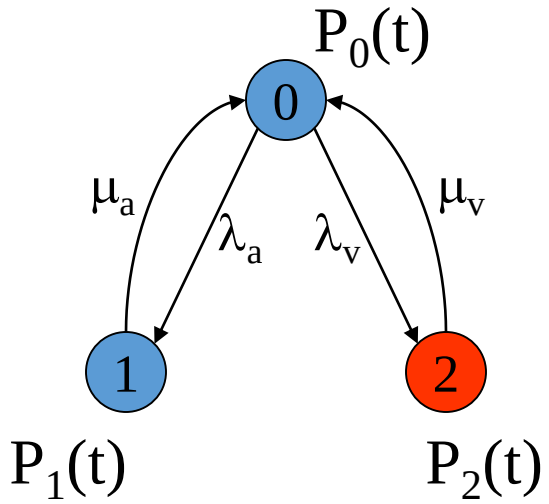
Ennél a technikánál megengedjük, hogy ***egyetlen egység*** lásson el egy biztonságreleváns funkciót, feltéve, ha annak valószínűsíthető meghibásodási módjai nem veszélyesek.

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.

FAIL-SAFE STRATÉGIA (1)

AKADÁLYOZÓ ÁLLAPOT, VESZÉLYEZTETŐ ÁLLAPOT



$$P_B(t) = P_0(t) + P_1(t)$$
$$P_V(t) = P_2(t)$$

$$\lambda_v << \lambda_a$$
$$\mu_v << \mu_a$$

AKADÁLYOZÓ ÁLLAPOT

- hibafelismerés, lekapcsolás
- hibakatalógus $\Rightarrow$ hibaszituációk

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

VESZÉLYEZTETŐ ÁLLAPOT

- tudatos kockázatvállalás - hibakizárás
  kockázat-tűrés!!!
- nem tudatos kockázatvállalás
  ismeretlen alkatrészek, szoftverek

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

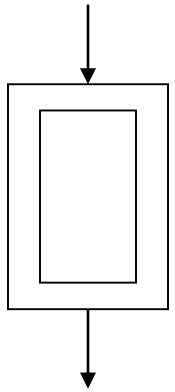
FAIL-SAFE STRATÉGIA (2)

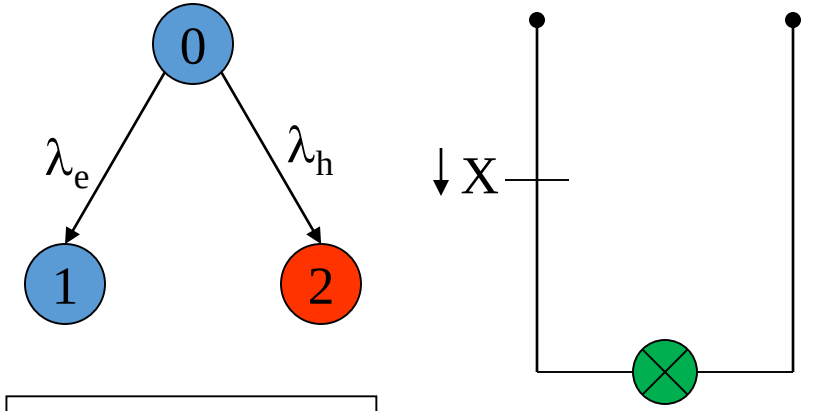
VALÓDI FAIL-SAFE RENDSZEREK

Önellenőrző tulajdonság:
kapcsolóelemek +
kapcsolástechnika
Egycsatornás kialakítás

ASZIMMETRIKUS MEGHIBÁSODÁSI TULAJDONSÁG

Valódi FS





Kapcsolóelemek
- **biztonsági jelfogók**
- **speciális elektronika**

$$\lambda = \lambda_e + \lambda_h$$
$$\lambda_h << \lambda_e$$

$$\lambda_v << \lambda_a$$

FAIL-SAFE STRATÉGIA (4)

EGY HIBA ELV

- a rendszert 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, T_a időn belül fel kell ismerni, és a rendszert akadályozó állapotba kell vezérelni, hogy az esetleges további hibák hatástalanok legyenek:

$$T_a = \frac{1}{1000a}, \quad \text{ahol} \quad a = \lambda_1 + \lambda_2$$

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

Reaktív hibabiztosság

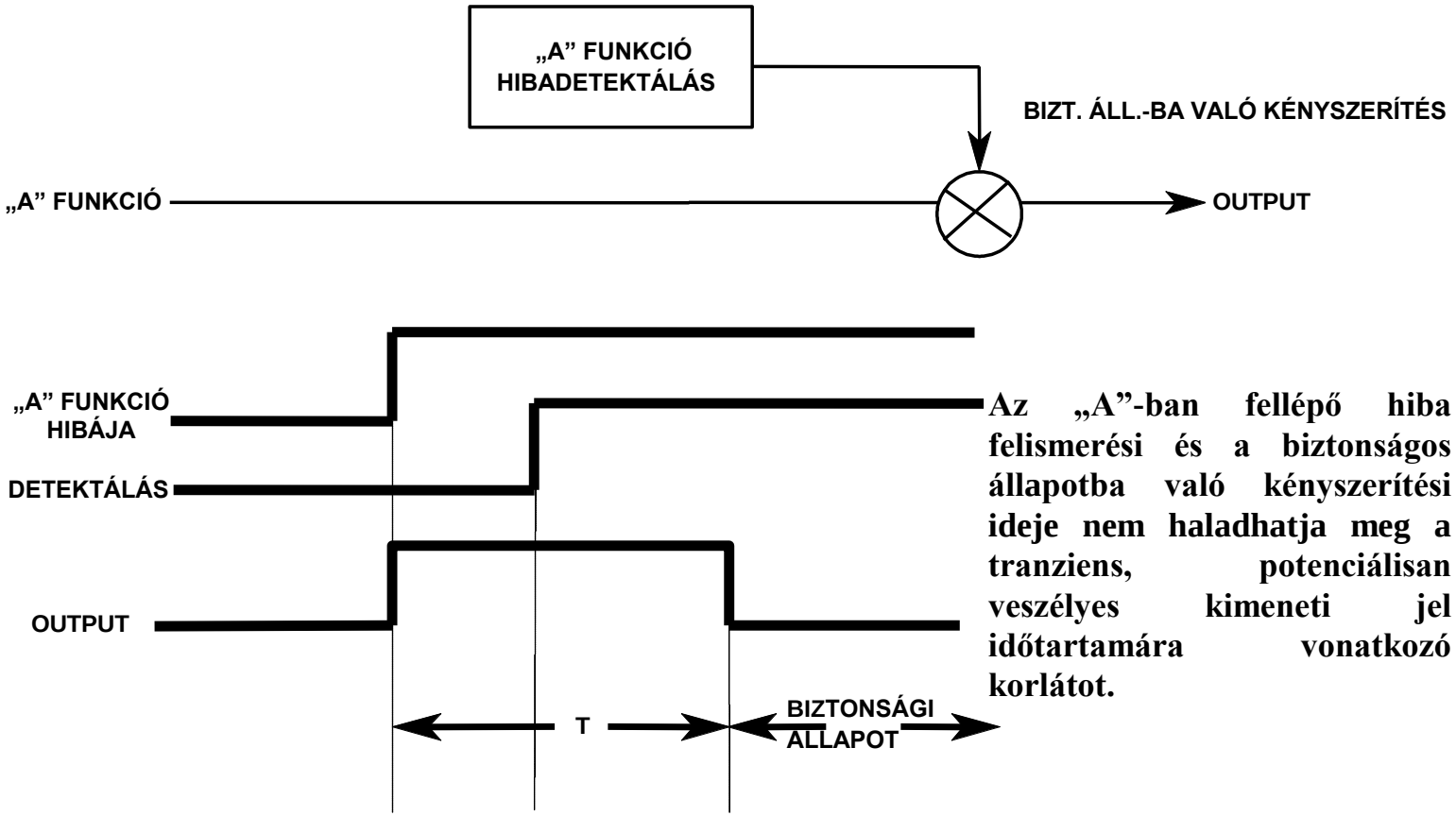
VALÓDI FAIL-SAFE RENDSZEREK

Ennél a technikánál megengedjük, hogy egy biztonságreleváns funkciót ***egyetlen egység*** lásson el, feltéve, hogy annak biztonságos működése bármely veszélyes hiba behatárolásával és hatálytalanításával biztosítható (például kódolással, többszörös számítással vagy összehasonlítással, illetve folyamatos ellenőrzéssel).

Bár a tényleges biztonságreleváns funkciót csak egyetlen egység látja el, az ellenőrző/tesztelő/hibadetektáló funkciót ***másik egységként*** kell tekinteni, amely független a közös eredetű hibák elkerülése végett.

Reaktív hibabiztosság

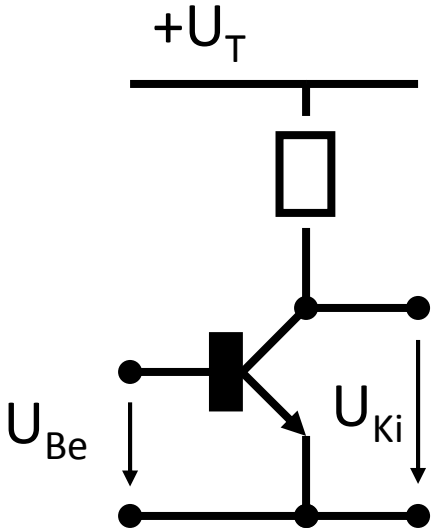
VALÓDI FAIL-SAFE RENDSZEREK

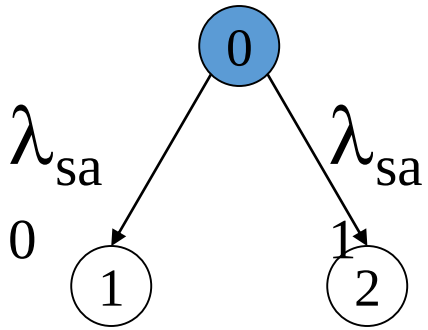


Az „A”-ban fellépő hiba felismerési és a biztonságos állapotba való kényszerítési ideje nem haladhatja meg a tranziens, potenciálisan veszélyes kimeneti jel időtartamára vonatkozó korlátot.

FAIL-SAFE STRATÉGIA (5)

FÉLVEZETŐ ELEMEK PROBLÉMÁJA





$$\lambda_{sa0} \approx \lambda_{sa1}$$

Szimmetrikus meghibásodási tulajdonság
Nincs veszélytelen hibaállapot

Stuck at 1 – sa1

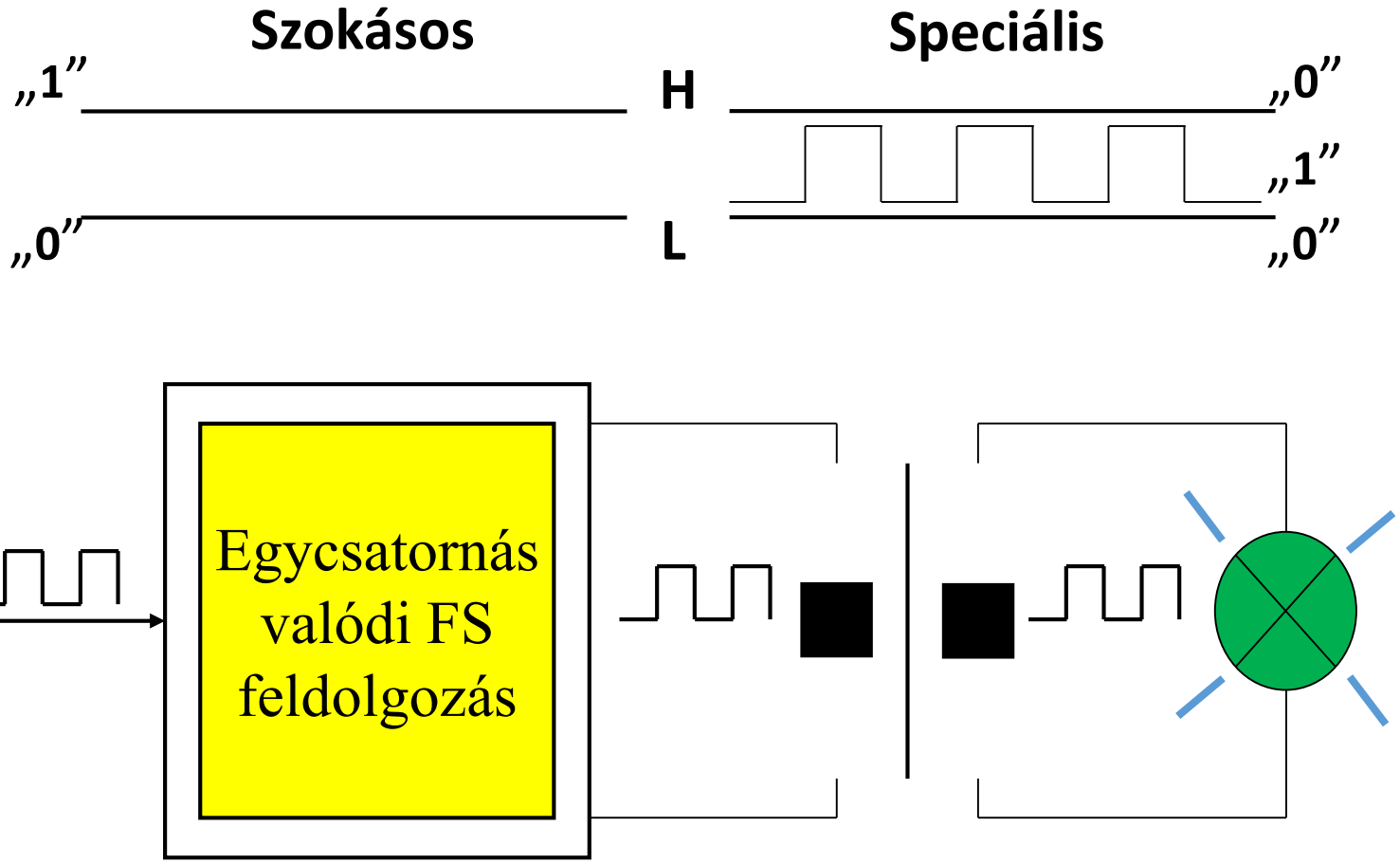
Stuck at 0 – sa0

Megoldás:

- speciális,valódi FS elektronika
- többcsatornás kialakítás

FAIL-SAFE STRATÉGIA (6)

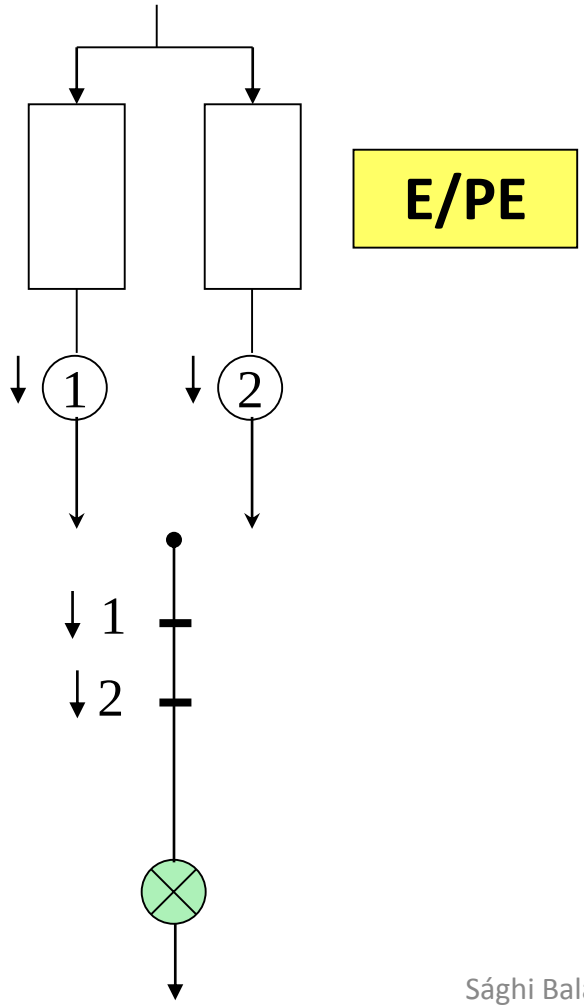
Speciális, huzalozott félvezető logika



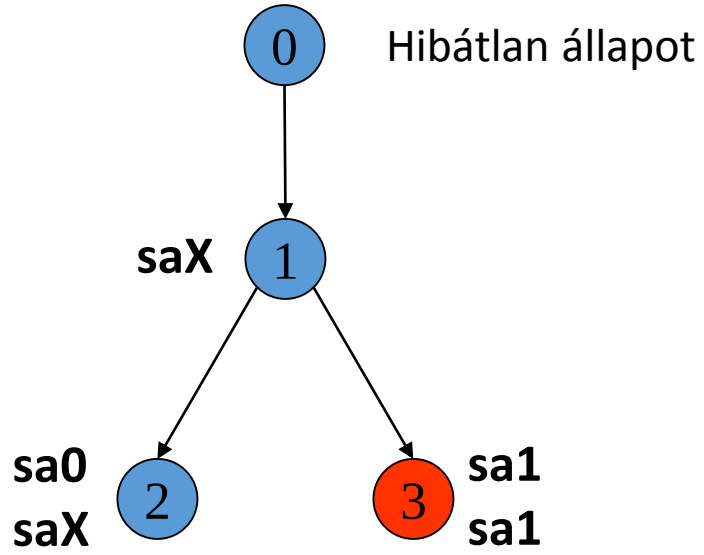
Korlátozott alkalmazhatóság

Duál elektronikai felépítés

KÉTCSATORNÁS KIALAKÍTÁS – NEM FAIL-SAFE



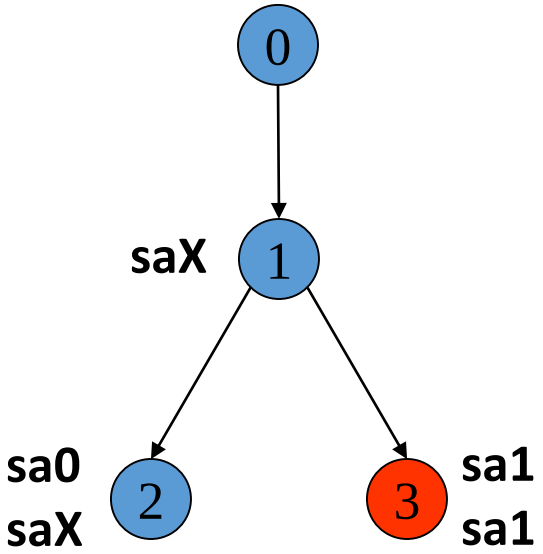
E/PE

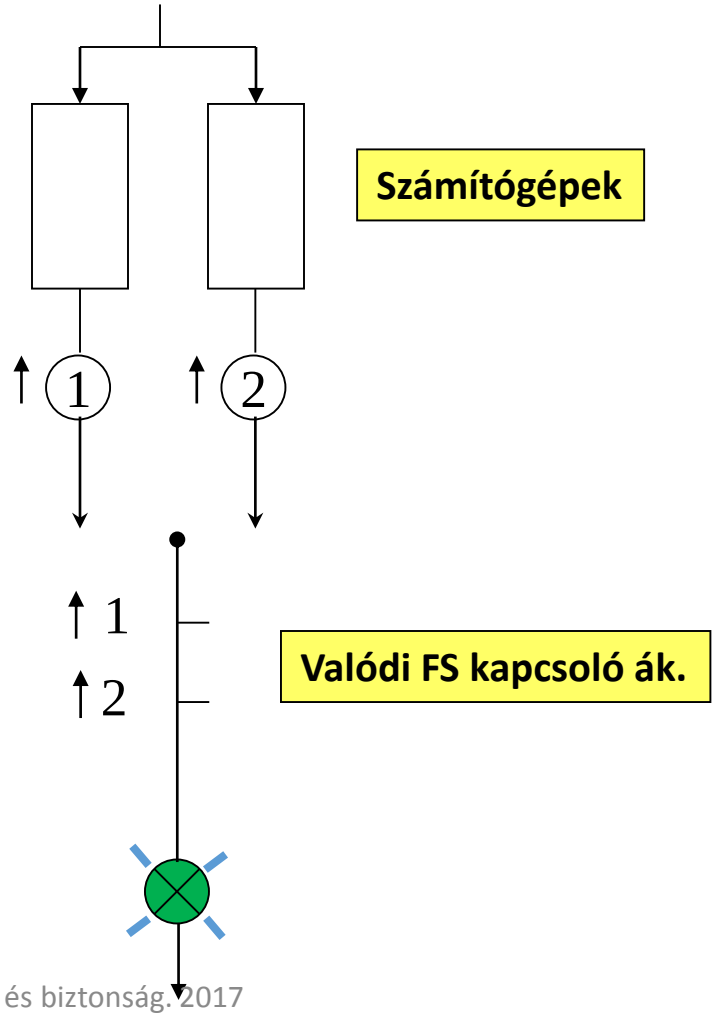


FAIL-SAFE STRATÉGIA (7)

TÖBBCSATORNÁS KIALAKÍTÁS

Információfeldolgozás:
nem fail-safe
2 v2
2-ből 2 rendszer

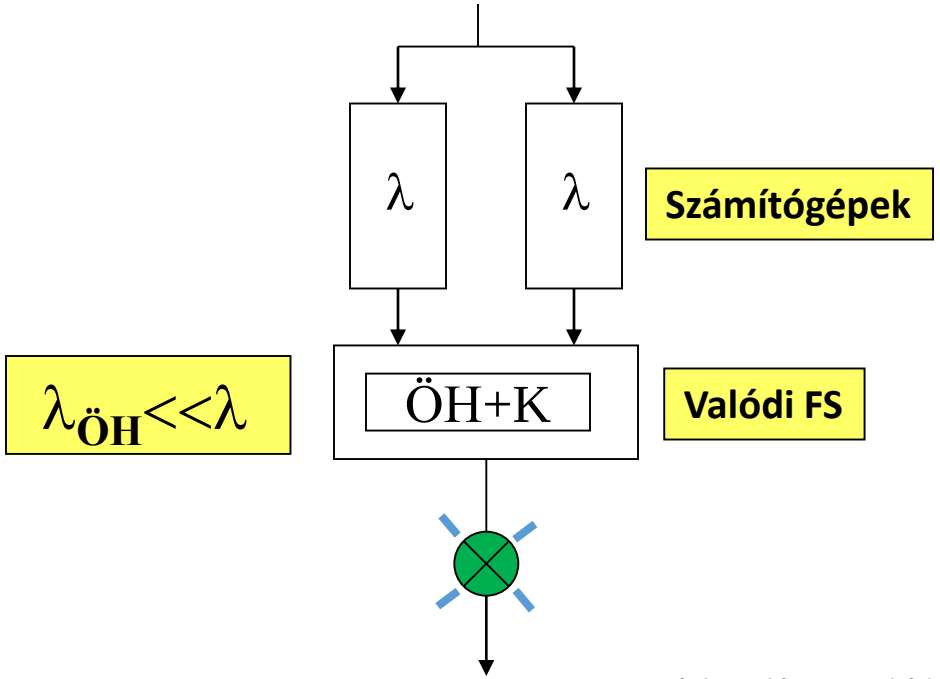


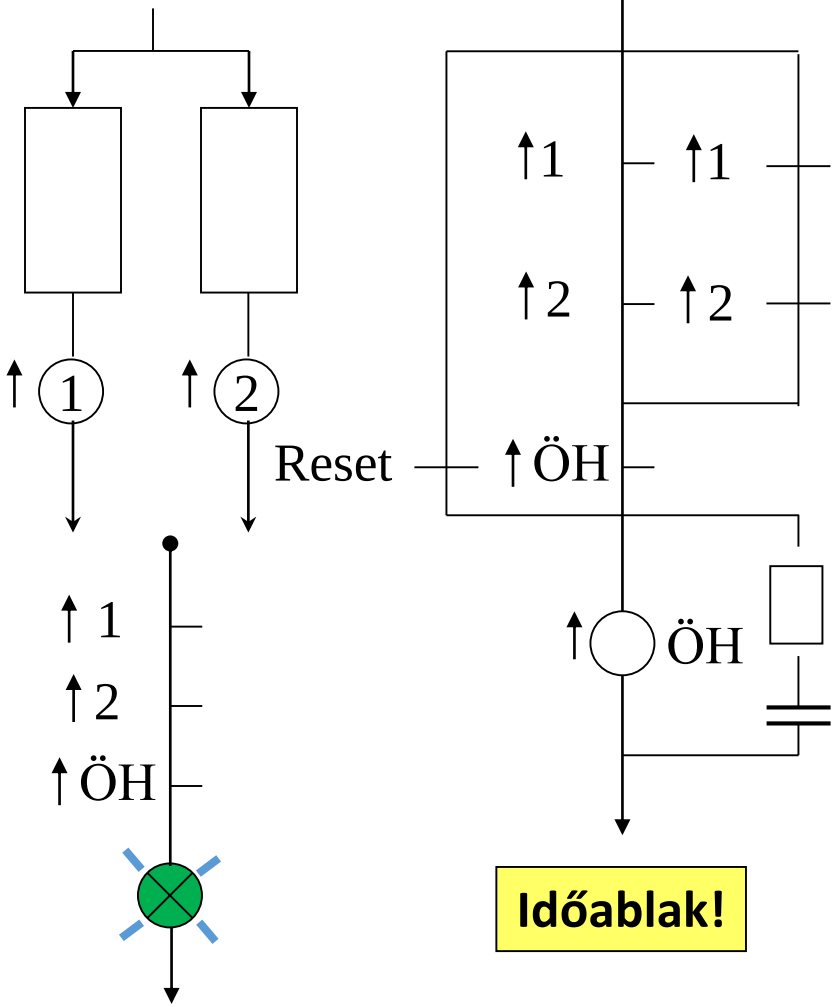


FAIL-SAFE STRATÉGIA (8)

KVÁZI FAIL-SAFE RENDSZEREK

Információfeldolgozás:
nem fail-safe
Többcsatornás kialakítás
Valódi FS összehasonlító





Összetett (kompozit) hibabiztosság

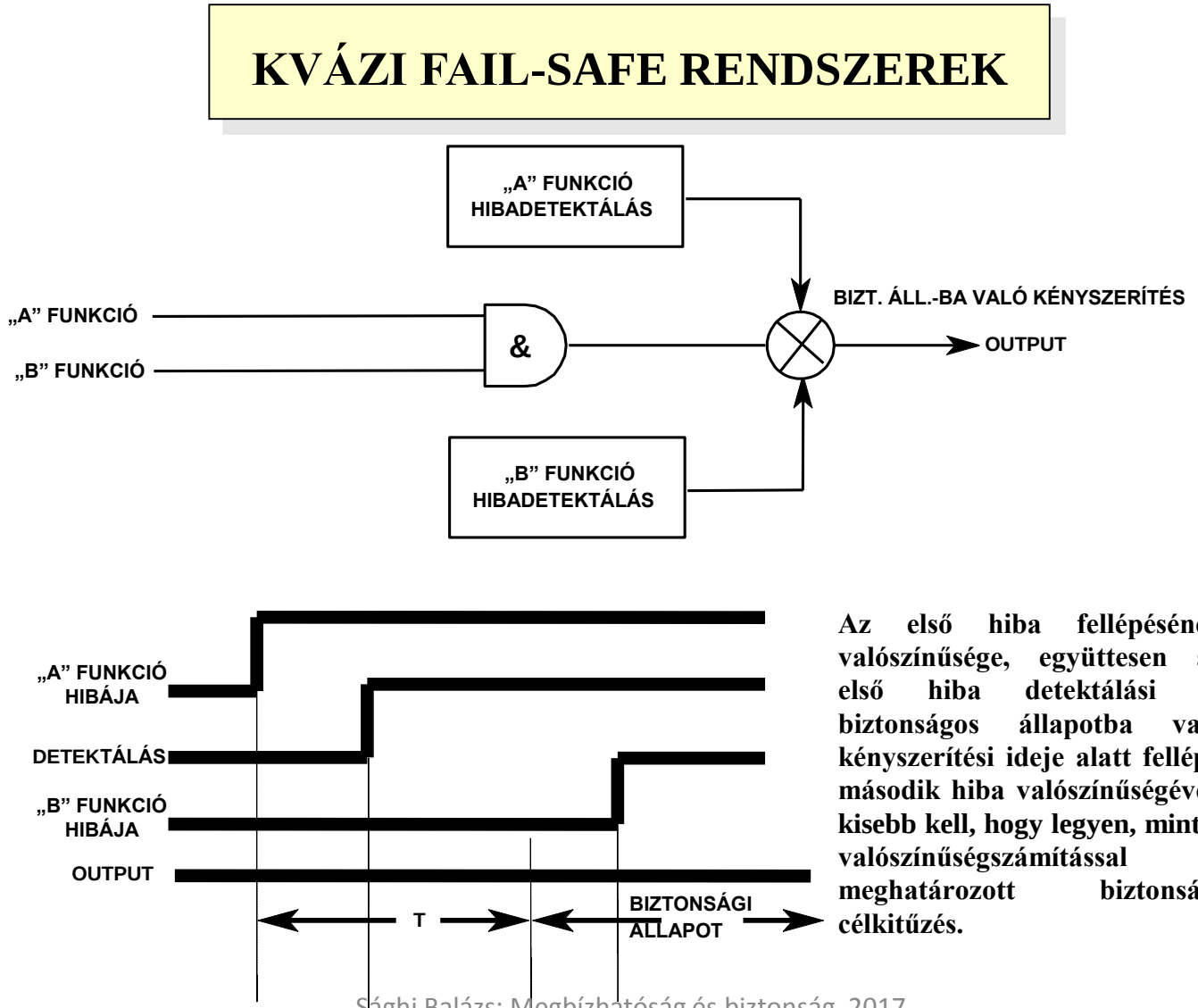
KVÁZI FAIL-SAFE RENDSZEREK

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.

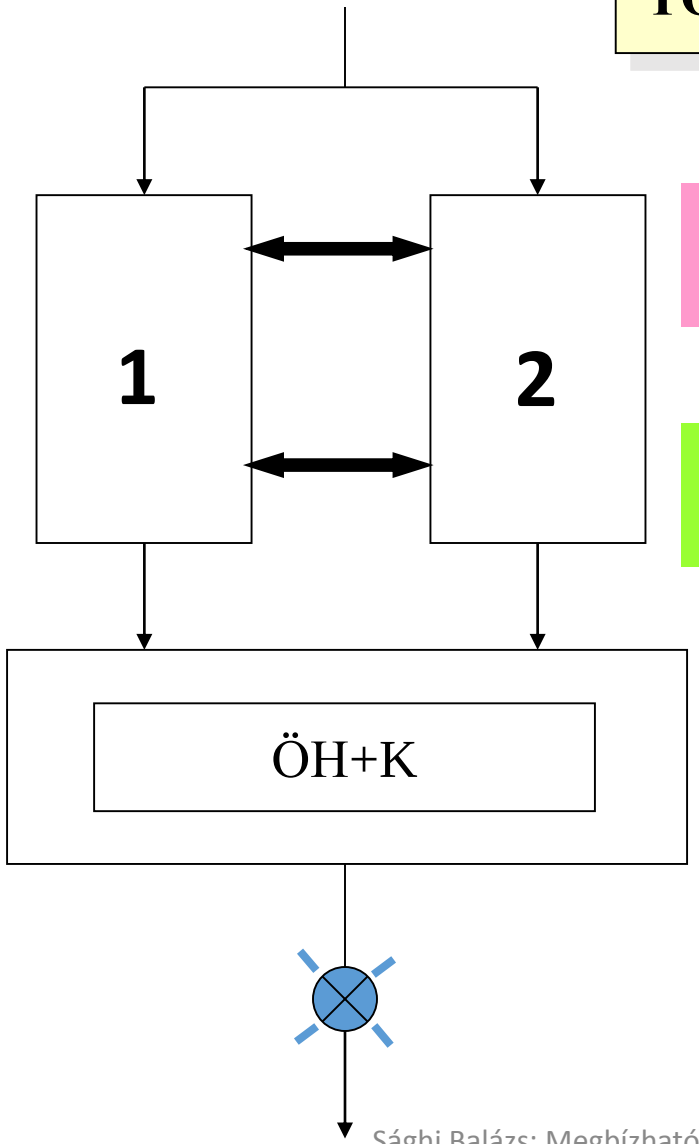
Összetett (kompozit) hibabiztosság



Az első hiba fellépésének valószínűsége, együttesen az első hiba detektálási és biztonságos állapotba való kényszerítési ideje alatt fellépő második hiba valószínűségével, kisebb kell, hogy legyen, mint a valószínűségszámítással meghatározott biztonsági célkitűzés.

FAIL-SAFE STRATÉGIA (9)

TÖBBSZINTŰ ÖSSZEHASONLÍTÁS



A beolvasott adatok cseréje és összehasonlítása

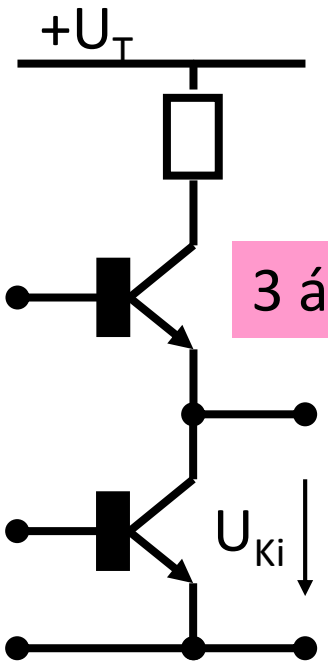
A feldolgozott adatok cseréje és összehasonlítása

FS összehasonlító és kapcsoló

FAIL-SAFE STRATÉGIA (10)

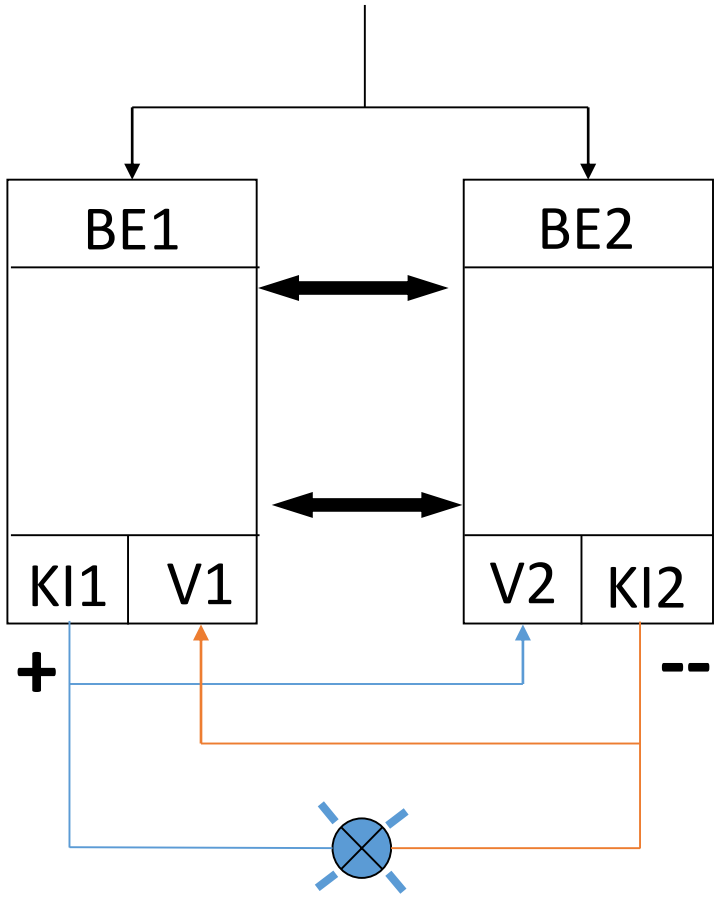
ÖSSZEHASONLÍTÁS
KÖZVETLEN VEZÉRLÉSSEL ÉS VISSZAOLVASÁSSAL

Totem-pole kapcsolás



3 állapotú kimenetek

Tristate



A nem intermittens kimenetek ellenőrzése

FAIL-SAFE STRATÉGIA (13)

A humán hibagyakoriság mérséklése

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

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

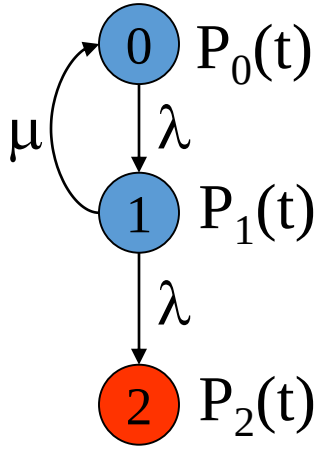
- a biztonsági feladatot ellátó irányító rendszer minél ritkábban kerüljön akadályozó állapotba, és minél rövidebb ideig tartózkodjon ebben az állapotban;
- a rutinműveletektől való mentesítés (kevesebb cselekvés),
- vezetett cselekvéssor (check-listák, gépi támogató eszközök),
- hibajelzések, javítási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

FAULT-TOLERANT STRATÉGIA (1)

A HIBA FELISMERÉSE ÉS HATÁSÁNAK MASZKOLÁSA

HARDVER-REDUNDANCIA / TARTALÉKOLÁS

$\mu >> \lambda$



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

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

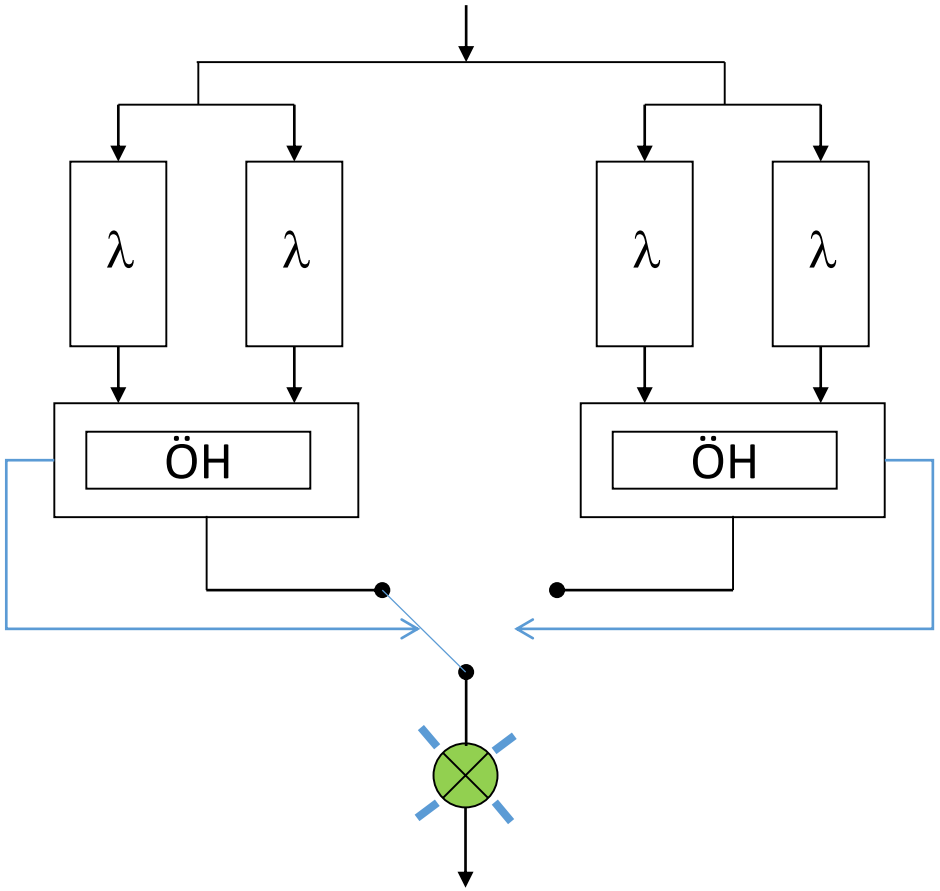
A biztonsági rendszerek működőképességének biztosítása

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

EGYÉB REDUNDANCIA FORMÁK

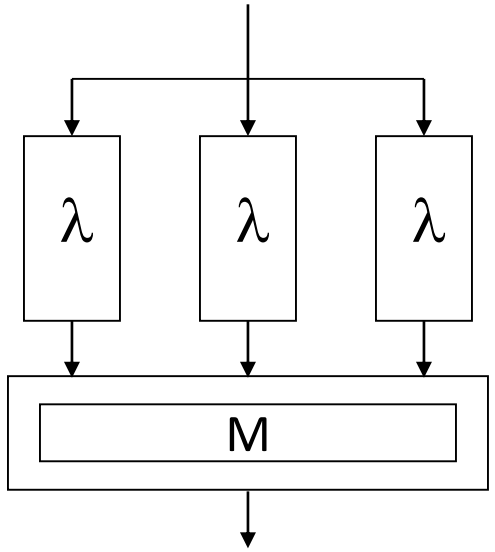
FAULT-TOLERANT STRATÉGIA (2)

2x(2v2) RENDSZER



FAULT-TOLERANT STRATÉGIA (3)

TÖBBSÉGI LOGIKA (SZAVAZÓ) ALKALMAZÁSA



3-ból 2 szavazólogika

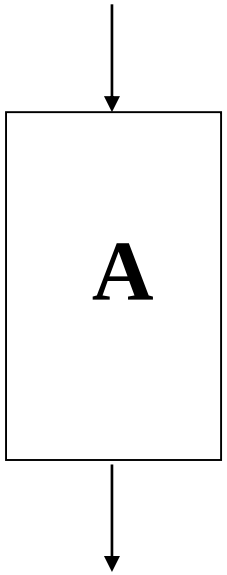
Diverz rendszerkialakítás

- 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)

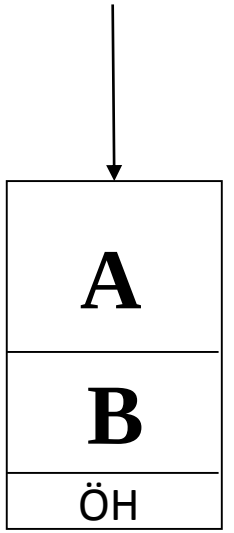
Biztonsági architektúrák

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



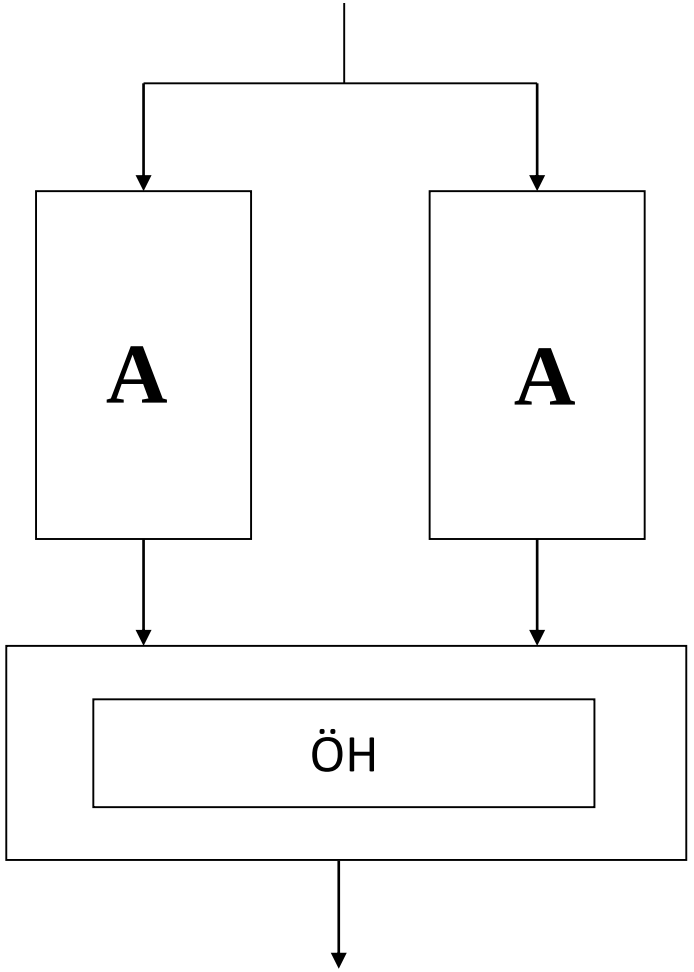
Biztonsági architektúrák

- 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.

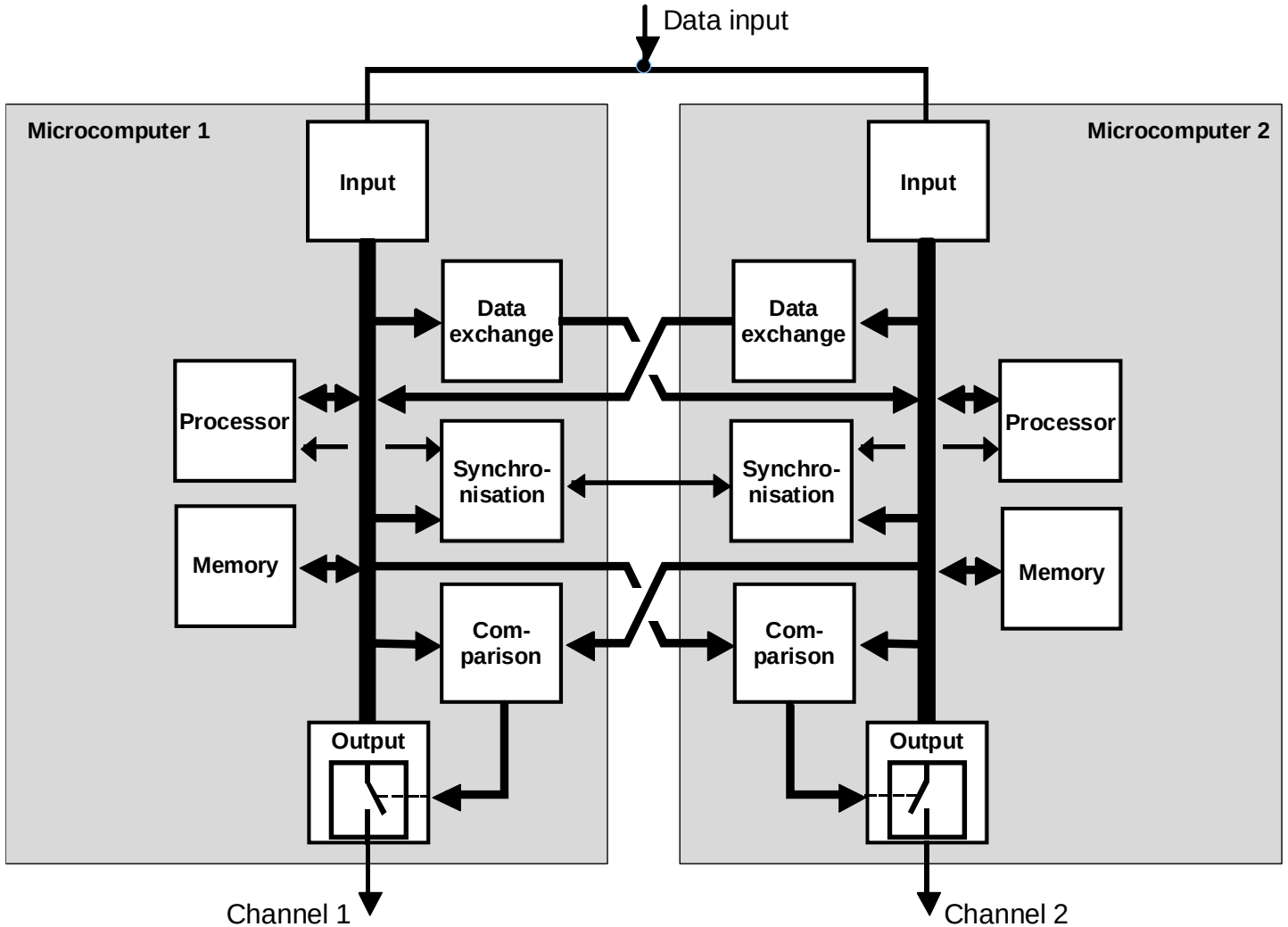


Biztonsági architektúrák

- 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

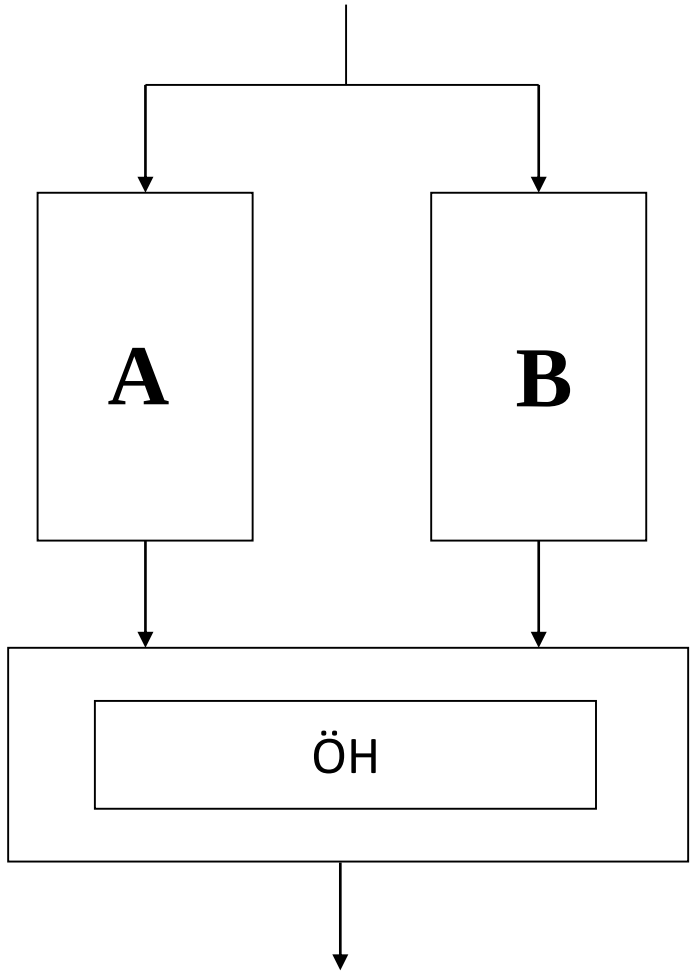


Számítógép konfigurációk
2v2 konfiguráció



Biztonsági architektúrák

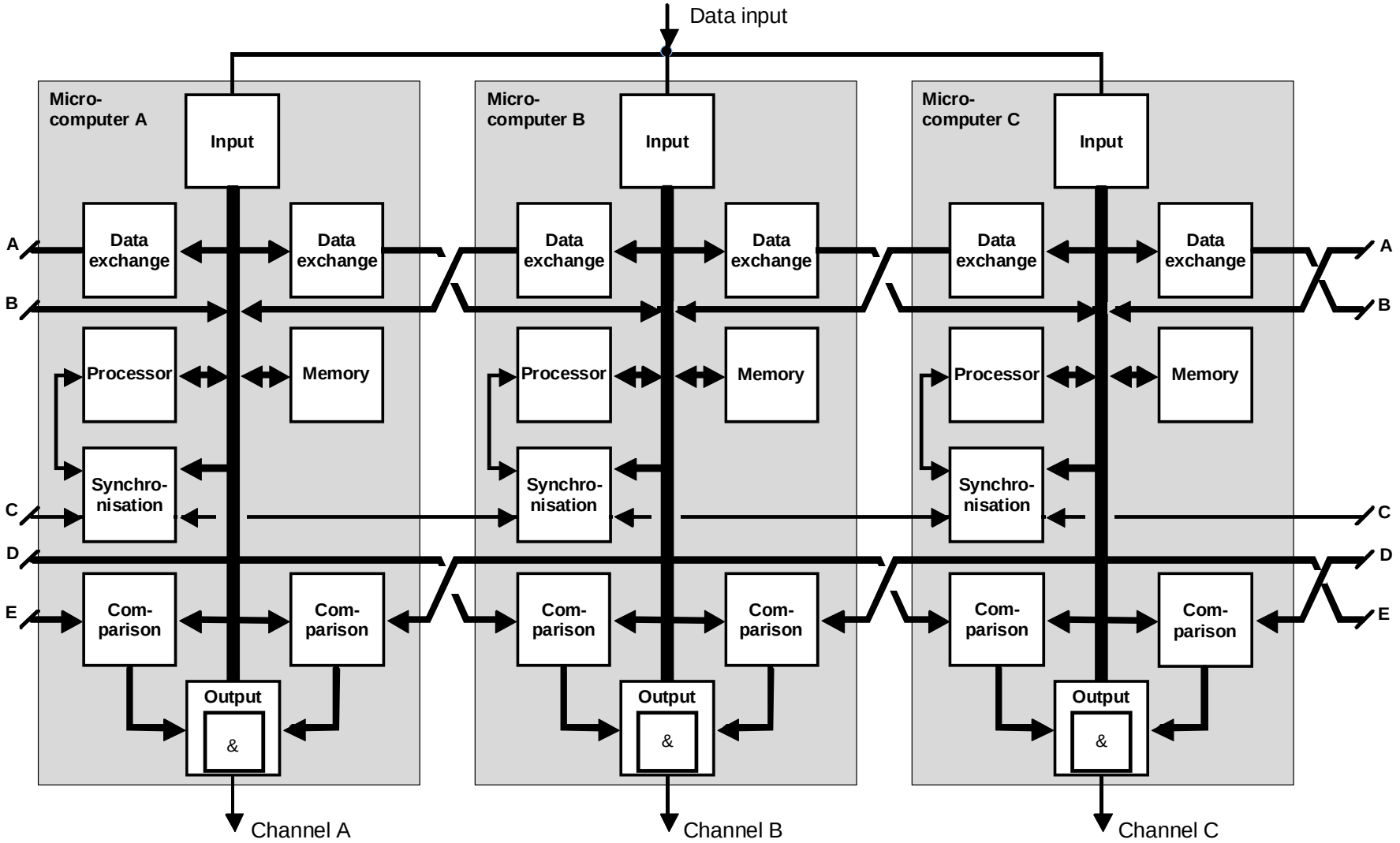
- 2 hardver, 2 szoftver
  - Az architektúra véd a véletlen hardver hibák ellen és
  - a szoftver hibák ellen.
  - A két csatornában eltérő specifikációval, eltérő programnyelven kifejlesztett programok futnak
- Pl. Thales Elektra



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)

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

Komplex mintapélda biztonsági architektúrára

Kereskedelmi komponensek

Diverz (A/B)
- PC hardver (Intel/AMD)
- Oper. rendszer (Win2000/Linux)
- fordítóprogramok

→ diverz programfutás