Védelem a véletlenszerű egyedi hibák veszélyeztető hatása ellen

Biztonsági stratégiák

Dr. Sághi Balázs diasorra alapján összeállította,
készítette Dr. Baranyi Edit

BIZTONSÁGI STRATÉGIÁK

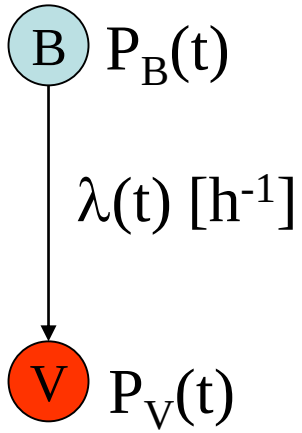
KÖZLEKEDÉSI AUTOMATIKA

FOLYAMATIRÁNYÍTÓ RENDSZEREK KIALAKÍTÁSA

BIZTONSÁGI VONATKOZÁSOK

BIZTONSÁG ↔ VESZÉLYEZTETÉS $b = \overline{v}$

A BIZTONSÁG MÉRTÉKE $P_B(t) = 1 - P_V(t)$

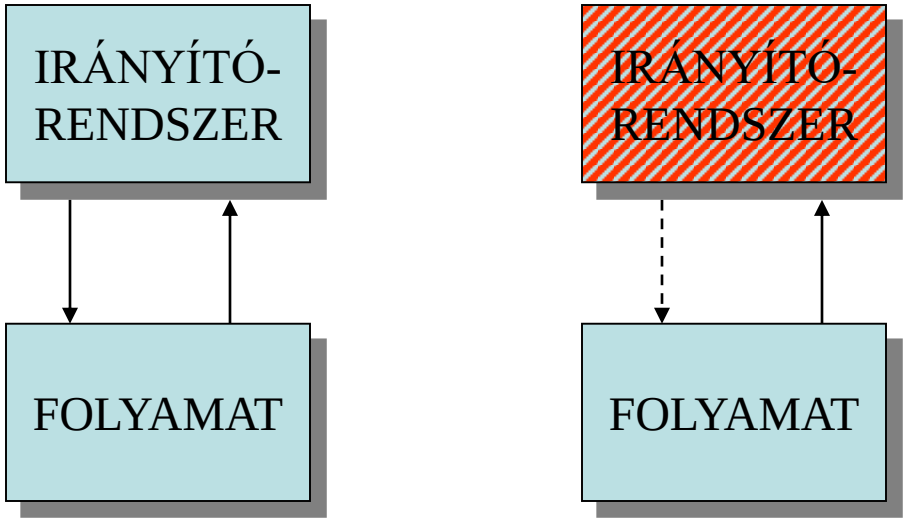


A BIZTONSÁG KÍVÁNT FOKA $P_B(t) \geq P_{Bmin} \leftrightarrow P_V(t) \leq P_{Vmax}$

VESZÉLYFORRÁSOK

- KIKÜSZÖBÖLÉSE
- HATÁS KIKÜSZÖBÖLÉSE
- HATÁS MÉRSÉKLÉSE

AZ IRÁNYÍTÓ RENDSZER VÉLETLENSZERŰ MEGHIBÁSODÁSA



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)

AZ IRÁNYÍTÓRENDSZER KARBANTARTÁSI, JAVÍTÁSI LEHETŐSÉGEI

FAIL-SAFE STRATÉGIA

Hibabiztos:

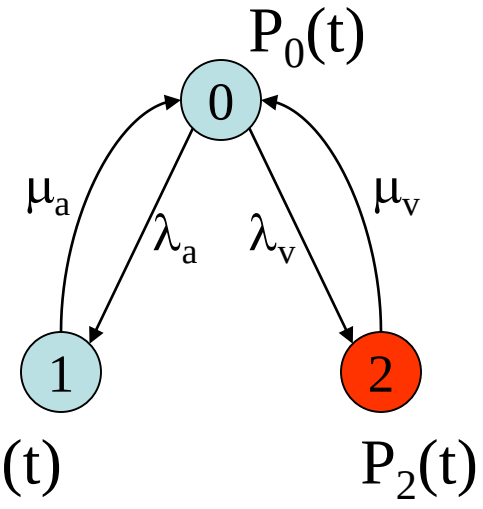
• hiba esetén biztonságos (akadályozó) állapotba jut, és a javításig ott is marad

FAIL-SAFE STRATÉGIA

Példa

FAIL-SAFE STRATÉGIA

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

Intézkedések
a nem tudatos kockázatvállalás mérséklésére

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

FAIL-SAFE STRATÉGIA

Önellenőrzés

- A hibafelismerő mechanizmus saját hibáját is ismerje fel, és
- ez a felismert hiba is

  akadályozó állapotot kell, hogy kiváltson!

FAIL-SAFE STRATÉGIA

EGY HIBA ELV

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

• a hibafelismerő mechanizmus kialakításánál akkor elegendő egyidejűleg egy hibát feltételezni ha,

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

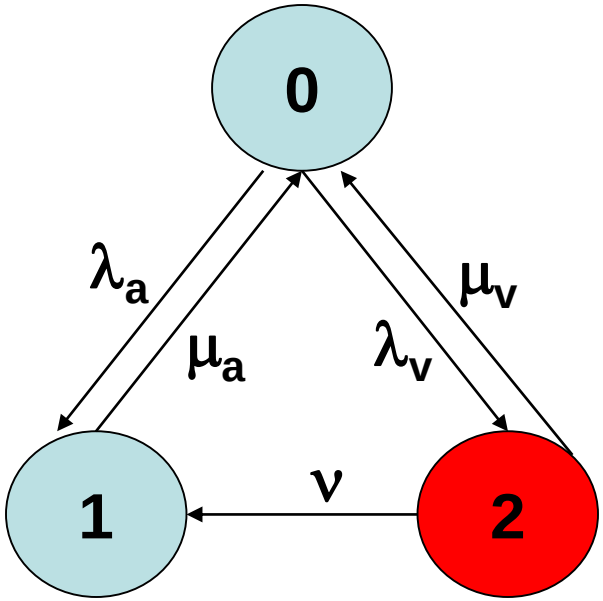
• a fellépő hibát még egy újabb hiba fellépése előtt, T_a időn belül fel kell ismerni, és a rendszert akadályozó állapotba kell vezérelni, hogy az esetleges további hibák hatástalanok legyenek:

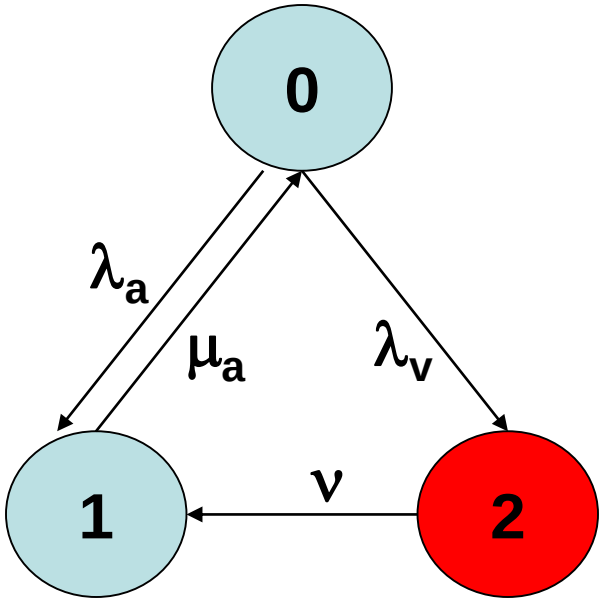
$$T_a = \frac{1}{1000a}, \quad \text{ahol} \quad a = \lambda_1 + \lambda_2$$

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

FAIL-SAFE STRATÉGIA

A veszélyeztető állapot átvezetése akadályozó állapotba





Egy hiba elv - kikapcsolási idő

$\nu >> \mu_v$ **esetén**

FAIL-SAFE STRATÉGIA

Valódi fail-safe rendszerek

Alapfeltétel:

- aszimmetrikus meghibásodási tulajdonság

Megvalósítás:

- egycsatornás kivitel

Kvázi fail-safe rendszerek

Alkalmazás:

- szimmetrikus meghibásodási tulajdonság esetén

Megvalósítás:

- többcsatornás kivitel fail-safe összehasonlítóval

FAIL-SAFE STRATÉGIA

Valódi fail-safe rendszerek

Alapfeltétel:

- aszimmetrikus meghibásodási tulajdonság

Megvalósítás:

- egycsatornás kivitel

FAIL-SAFE STRATÉGIA

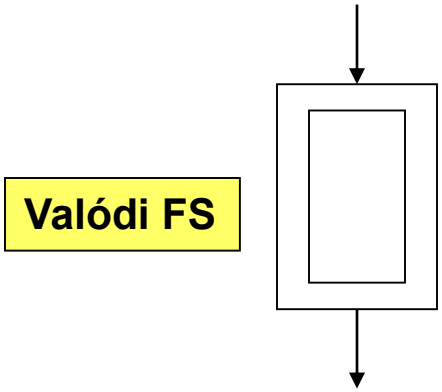
VALÓDI FAIL-SAFE RENDSZEREK

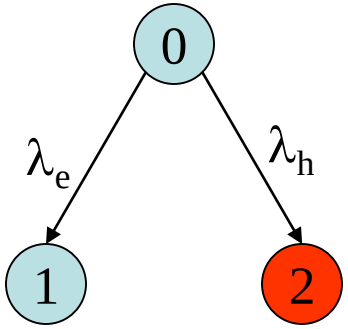
Önellenőrző tulajdonság:
- kapcsolóelemek +
- kapcsolástechnika

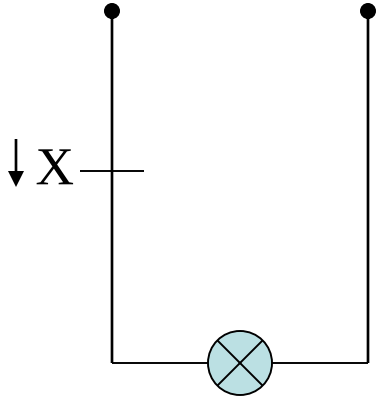
Egycsatornás kialakítás

ASZIMMETRIKUS MEGHIBÁSODÁSI TULAJDONSÁG

≠ parciális meghibásodási ráták







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

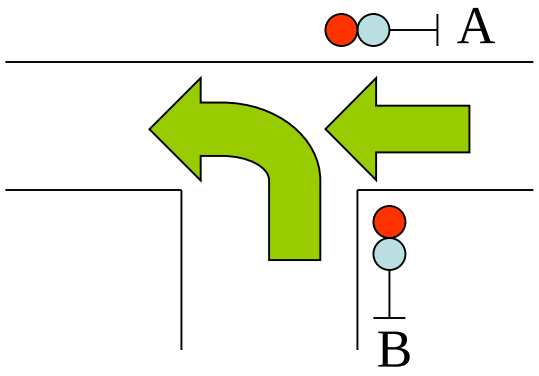
$\lambda = \lambda_e + \lambda_h$

$\lambda_h << \lambda_e$

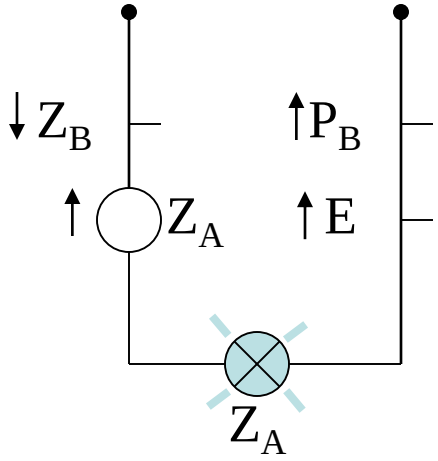
$\lambda_v << \lambda_a$

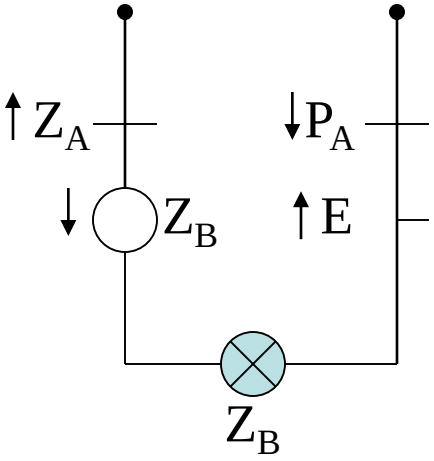
FAIL-SAFE STRATÉGIA

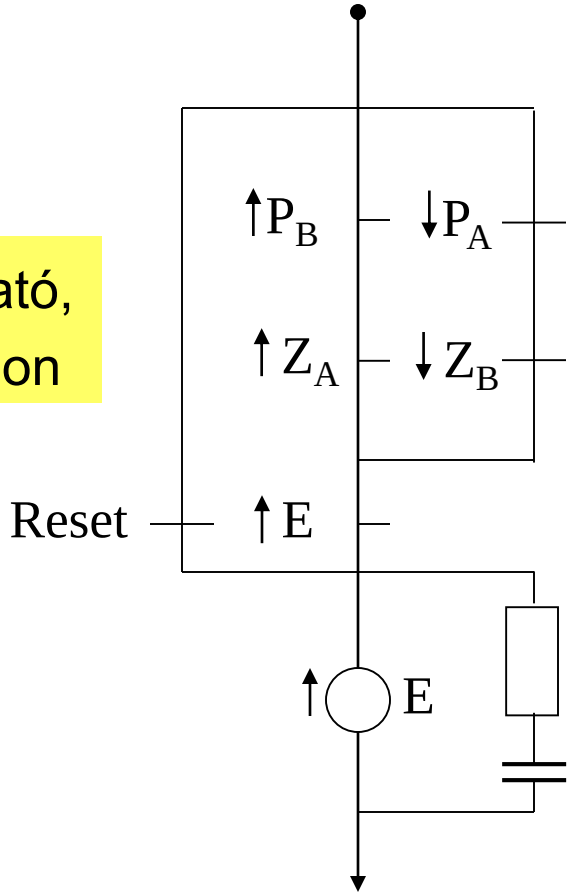
PÉLDA



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

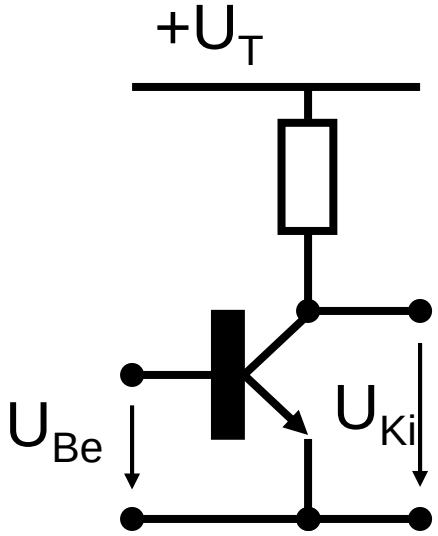


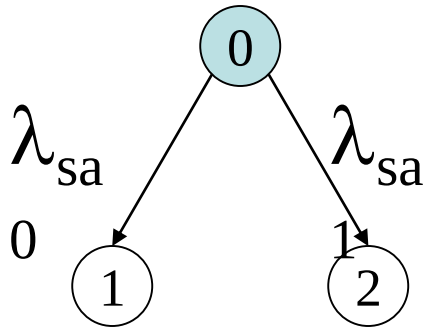




FAIL-SAFE STRATÉGIA

FÉLVEZETŐ ELEMEK PROBLÉMÁJA





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

Szimmetrikus meghibásodási tulajdonság
Nincs veszélytelen hibaállapot

Stuck at 1 – sa1

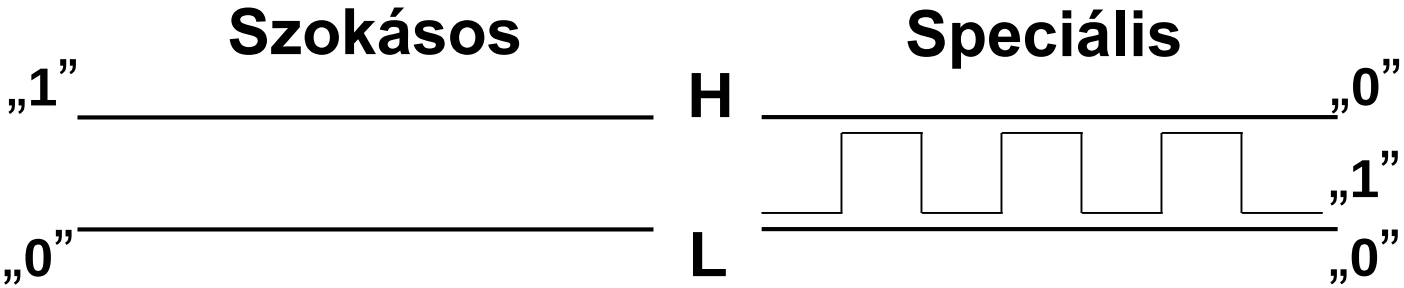
Stuck at 0 – sa0

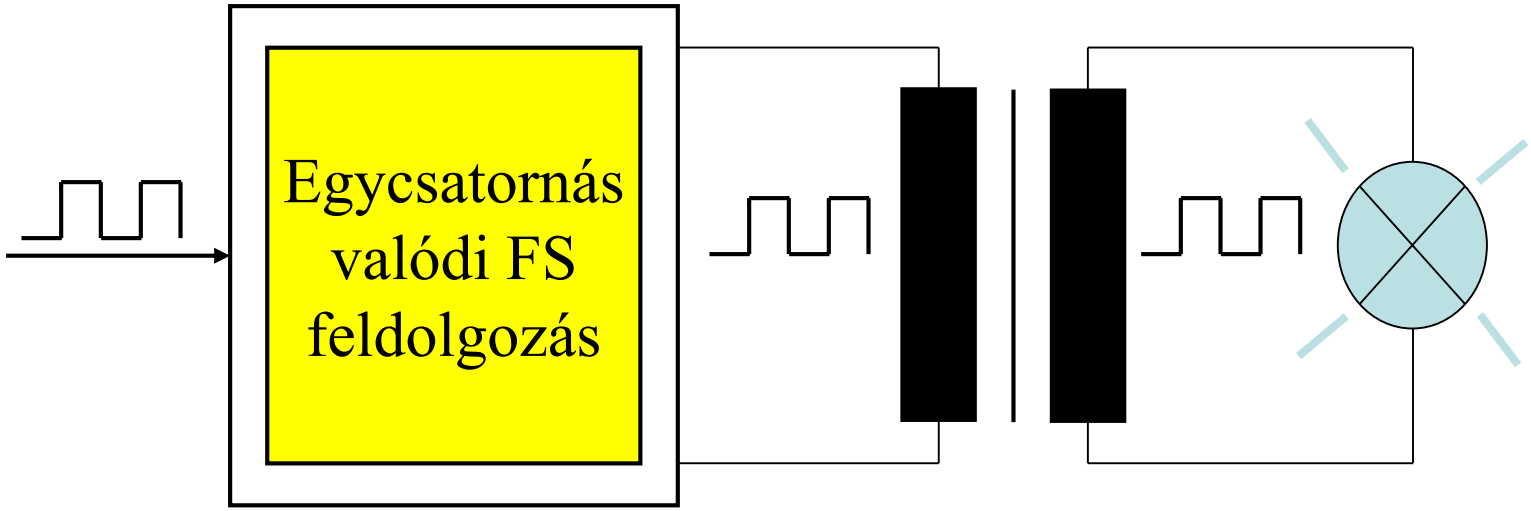
Megoldás:

- speciális,valódi FS elektronika
- többcsatornás kialakítás

FAIL-SAFE STRATÉGIA

Speciális, huzalozott félvezető logika





Korlátozott alkalmazhatóság

Reaktív hibabiztosság

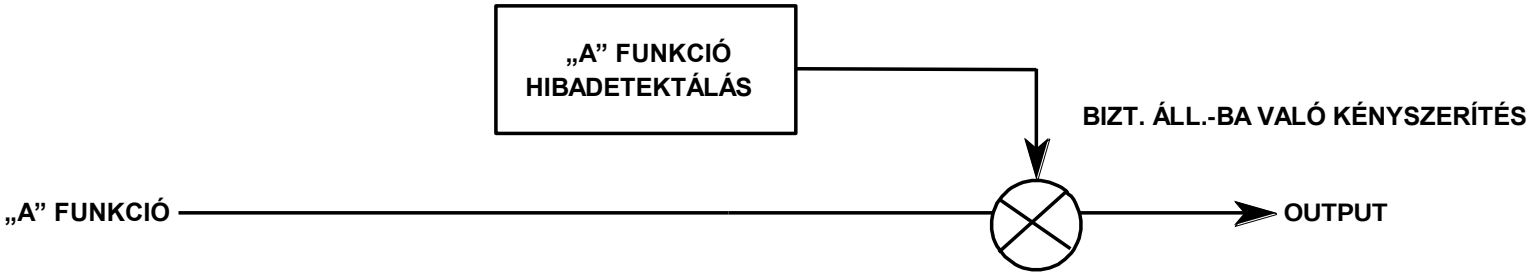
VALÓDI FAIL-SAFE RENDSZEREK

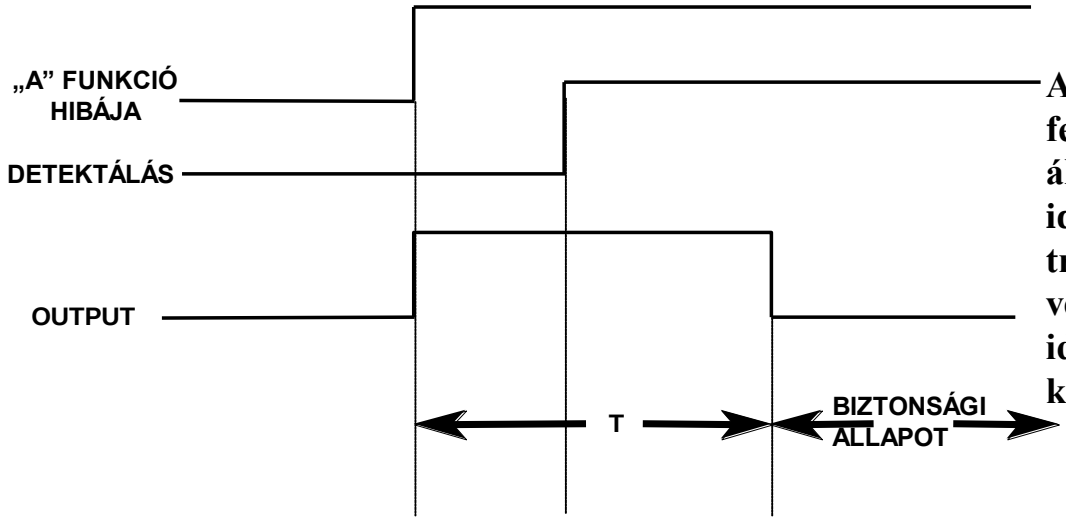
Ennél a technikánál megengedjük, hogy egy biztonságreleváns funkciót ***egyetlen egység*** lásson el, feltéve, hogy annak biztonságos működése bármely veszélyes hiba behatárolásával és hatálytalanításával biztosítható.

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

Kvázi fail-safe rendszerek

Alkalmazás:

- szimmetrikus meghibásodási tulajdonság esetén

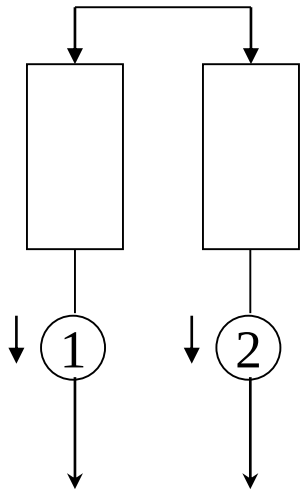
Megvalósítás:

- többcsatornás kivitel fail-safe összehasonlítóval

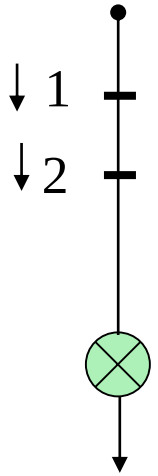
FAIL-SAFE STRATÉGIA

Duál elektronikai felépítés

KÉTCSATORNÁS KIALAKÍTÁS A KIMENETEK „ÉS” KAPCSOLATÁVAL



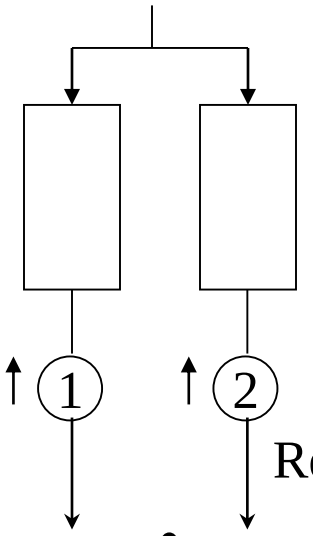
Információfeldolgozás:
nem fail-safe
2 v 2 (2-ből 2) rendszer

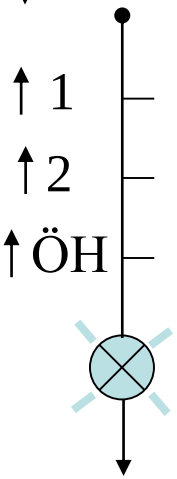


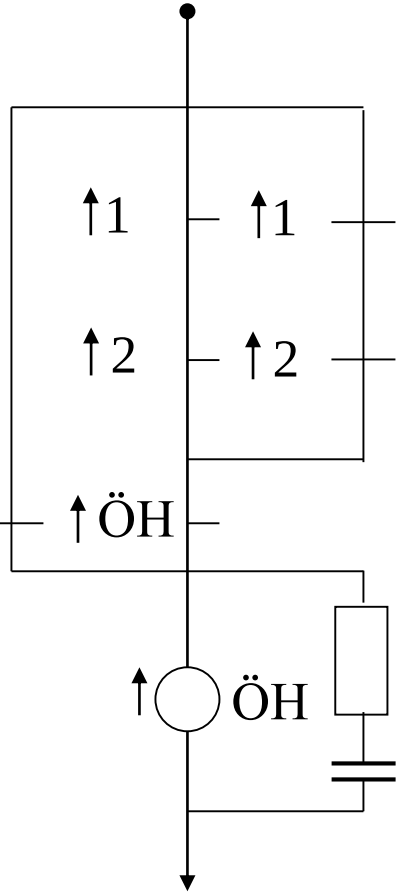
FAIL-SAFE STRATÉGIA

KVÁZI FAIL-SAFE RENDSZEREK

Információfeldolgozás:
nem fail-safe 2 v 2 (2-ből 2) rendszer
Kimenet:
valódi fail-safe összehasonlító

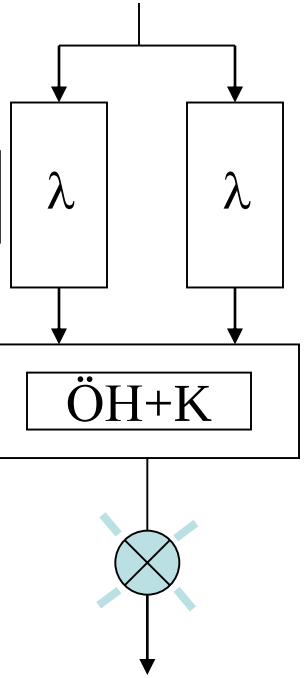






Időablak!

$\lambda_a = 2\lambda+\lambda_{ÖH}$



Számítógépek

$\lambda_{ÖH} << \lambda$

Valódi FS

Közös módusú hibák!!!

Diverz kialakítás???

Összetett (kompozit) hibabiztosság

KVÁZI FAIL-SAFE RENDSZEREK

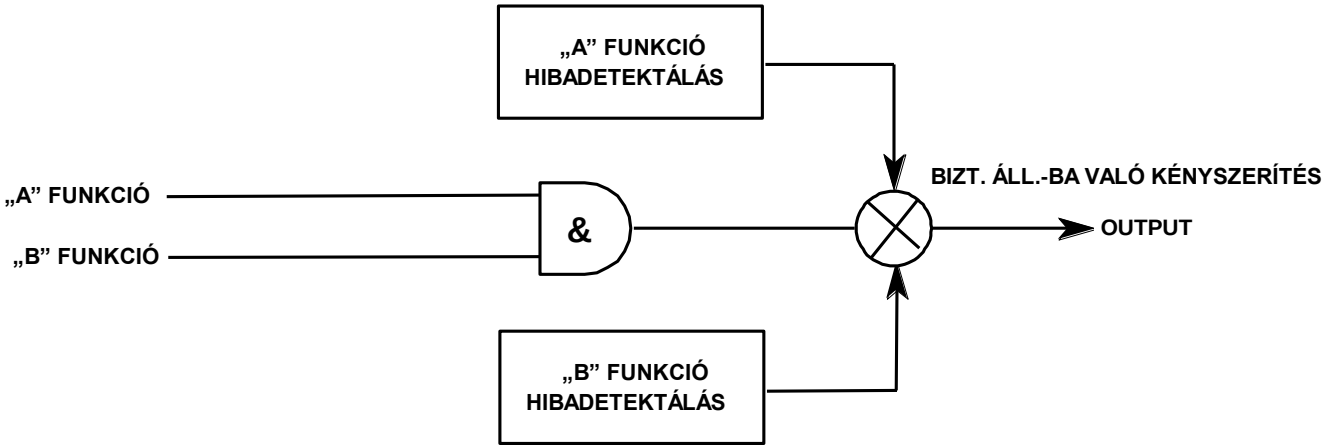
Minden egyes biztonságreleváns funkciót ***legalább két egység*** lát el. Ezeknek az egységeknek függetlenek kell lenniük minden más egységtől a ***közös eredetű hibák elkerülése*** végett.

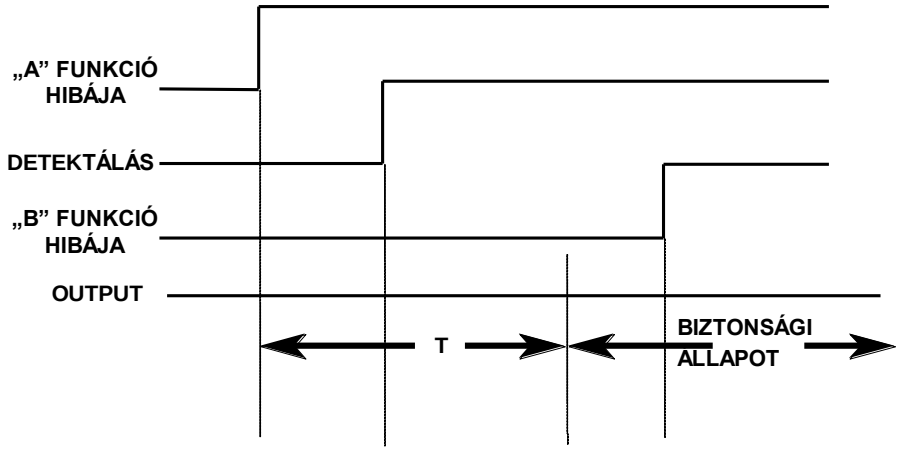
A nem akadályozó (restrictive) jellegű működések csak akkor hajtódhatnak végre, ha a szükséges számú egység “egyetért”.

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

KVÁZI FAIL-SAFE RENDSZEREK

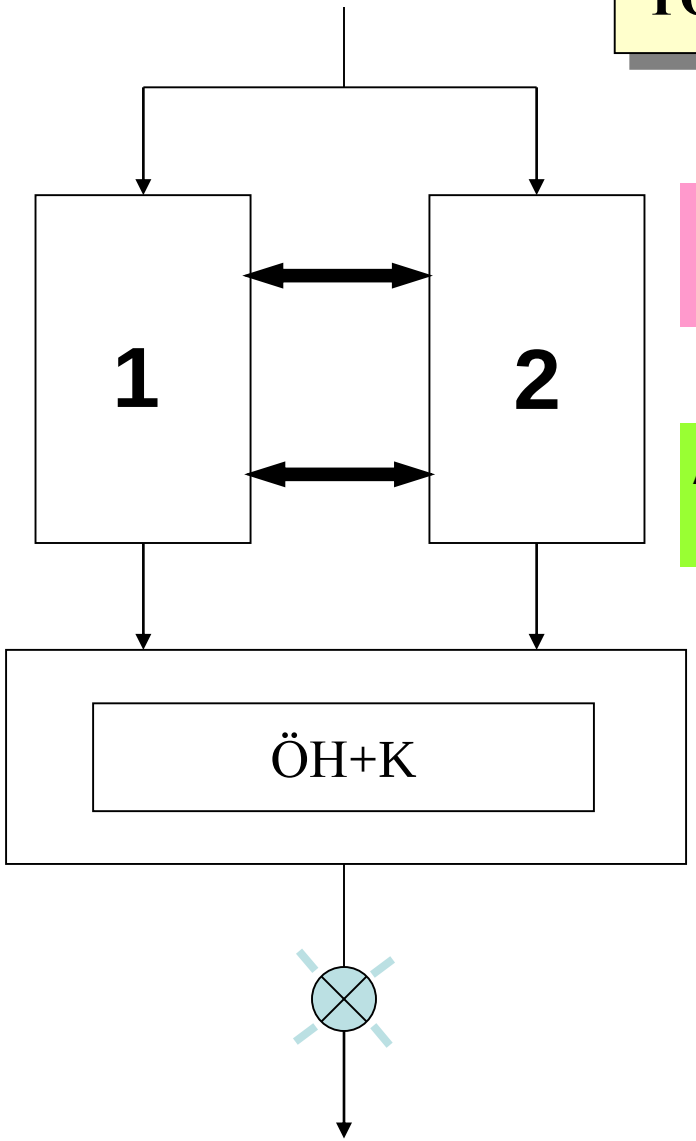




Az első hiba fellépésének valószínűsége, együttesen az első hiba detektálási és biztonságos állapotba való kényszerítési ideje alatt fellépő második hiba valószínűségével, kisebb kell, hogy legyen, mint a valószínűségszámítással meghatározott biztonsági célkitűzés.

FAIL-SAFE STRATÉGIA

TÖBBSZINTŰ ÖSSZEHASONLÍTÁS



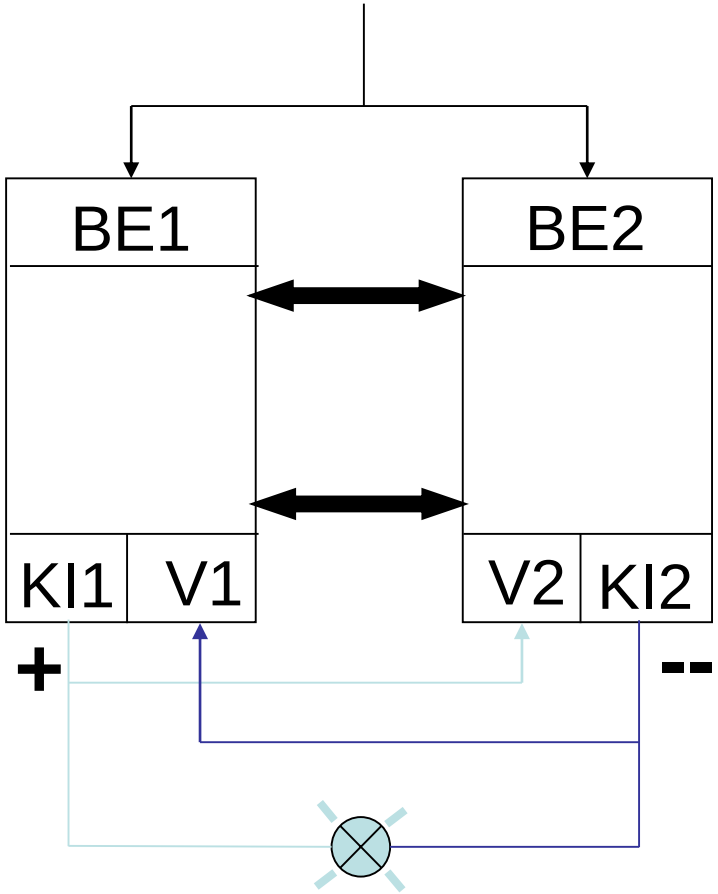
A beolvasott adatok cseréje és összehasonlítása

A feldolgozott adatok cseréje és összehasonlítása

FS összehasonlító és kapcsoló

FAIL-SAFE STRATÉGIA

ÖSSZEHASONLÍTÁS
KÖZVETLEN VEZÉRLÉSSEL ÉS VISSZAOLVASÁSSAL



FAIL-SAFE STRATÉGIA

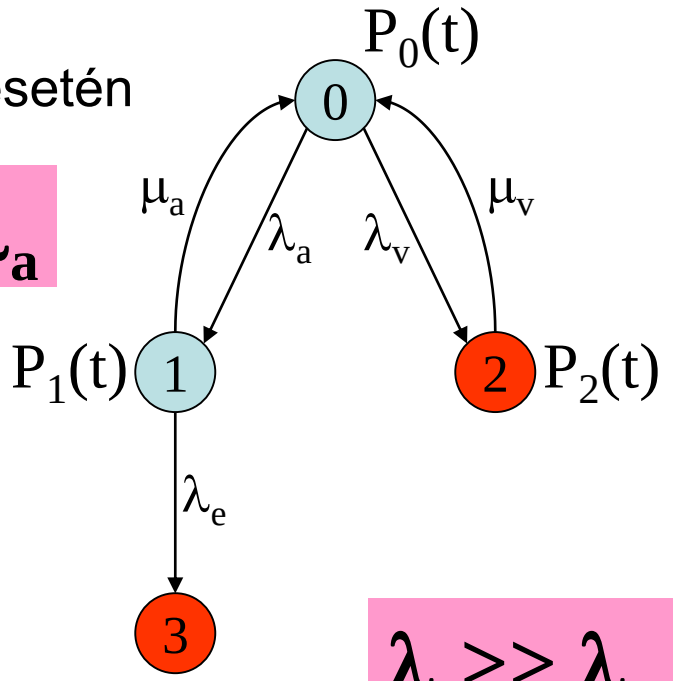
Ember-gép rendszer

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

λ_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”).



$\lambda_e >> \lambda_a$

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

μ_a

FAIL-SAFE STRATÉGIA

A humán hibagyakoriság mérséklése

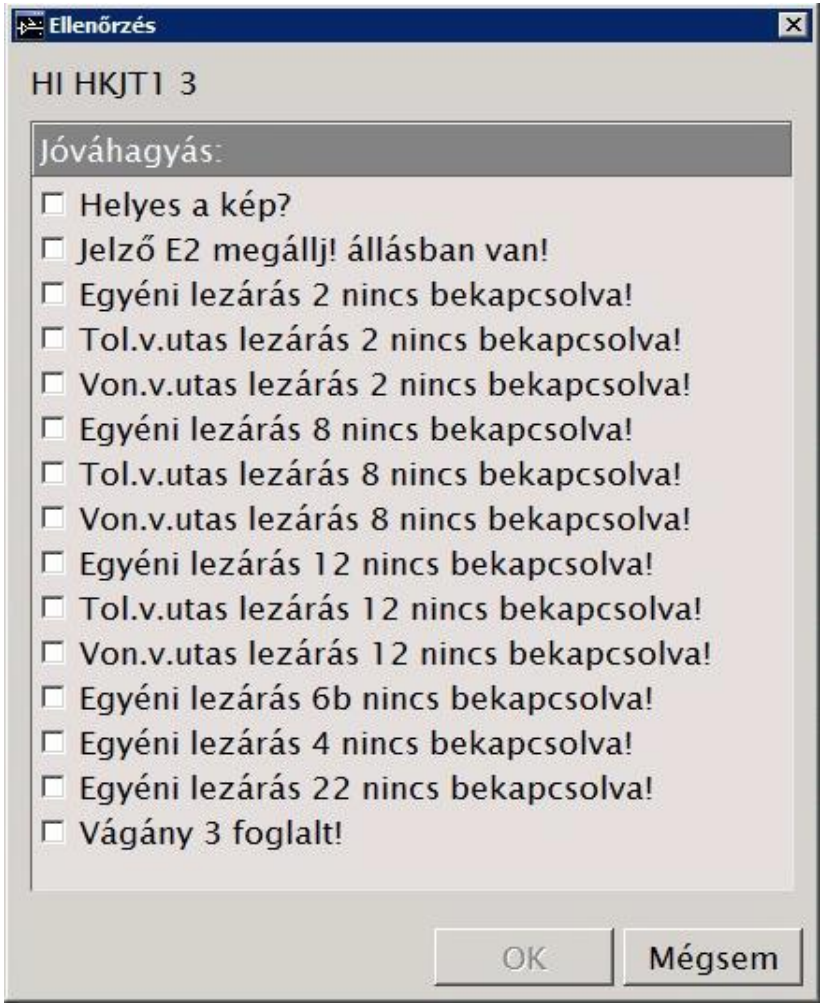
A hibás emberi cselekvés gyakorisága $\lambda_e = 10^{-3} \ldots 10^{-4}$ / cselekvés.

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.

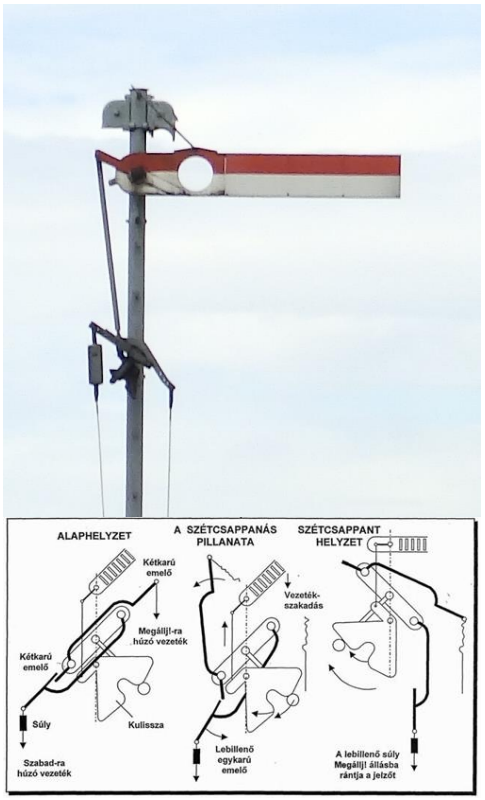
FAIL-SAFE STRATÉGIA

A humán hibagyakoriság mérséklése
Hívójelzés kivezérlése



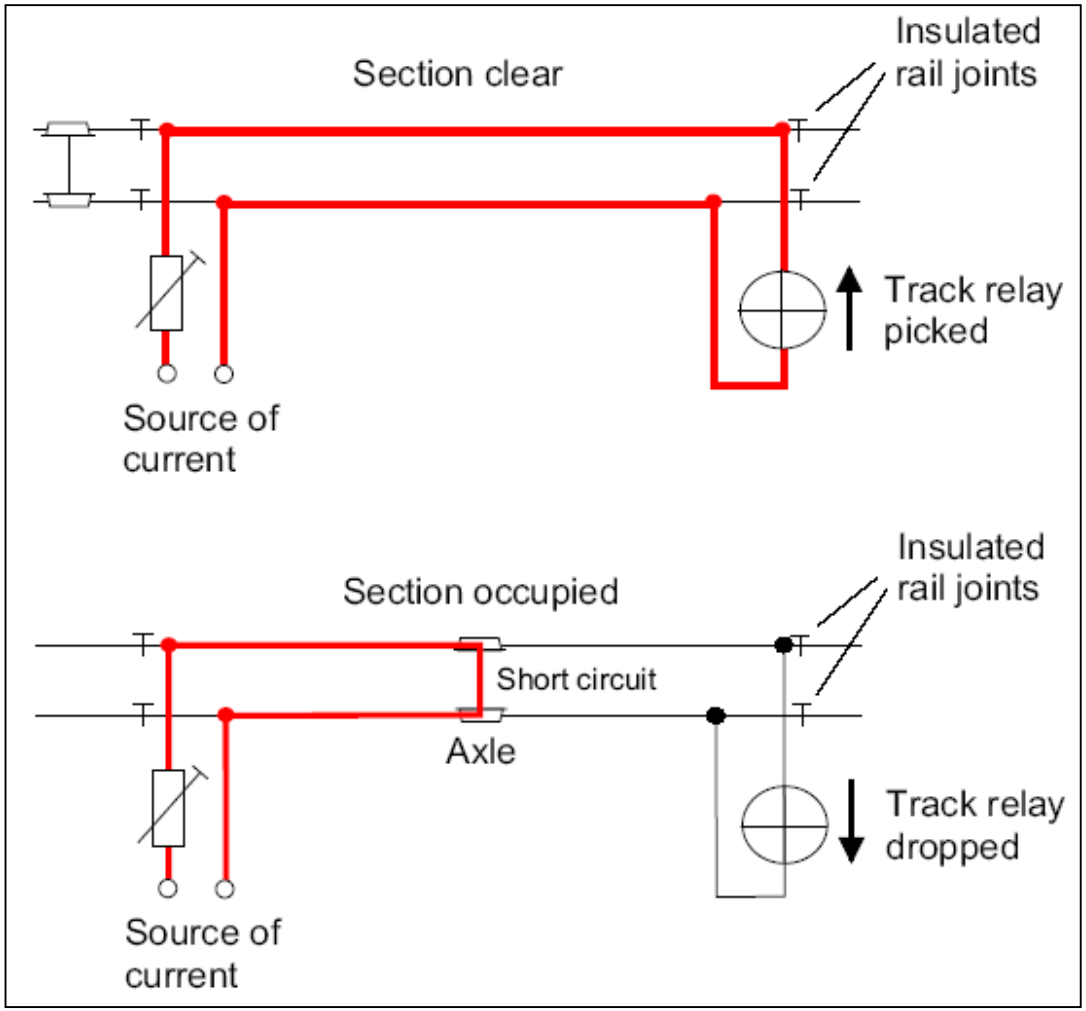
FAIL-SAFE STRATÉGIA

Példa



FAIL-SAFE STRATÉGIA

Példa



A rendszer, alrendszer, berendezés architektúrája (szabvány példa)

Technikák, intézkedések	SIL 1	SIL 2	SIL 3	SIL 4
1. A biztonságorientált és nem biztonságorientált rendszerek szétválasztása	R	R	HR	HR
2. Egyszerű elektronikai felépítés ön-teszteléssel és ellenőrzéssel	R	R	--	--
3.Duál elektronikai felépítés	R	R	--	--
4. Összetett fail-safe jellegen alapuló duál elektronikai felépítés fail-safe összehasonlítással	R	R	HR	HR
5. Belső fail-safe jellegen alapuló egyszerű elektronikai felépítés	R	R	HR	HR
6. Reaktív fail-safe jellegen alapuló egyszerű elektronikai felépítés	R	R	HR	HR
7. Diverziter elektronikai struktúra fail-safe összehasonlítással	R	R	HR	HR
8. Az architektúra igazolása a hardver mennyiségi megbízhatósági elemzésével	HR	HR	HR	HR

SAFE-LIFE STRATÉGIA

A hibakizárás stratégiája

SAFE-LIFE STRATÉGIA

TÖKÉLETESSÉG, HIBAKIZÁRÁS

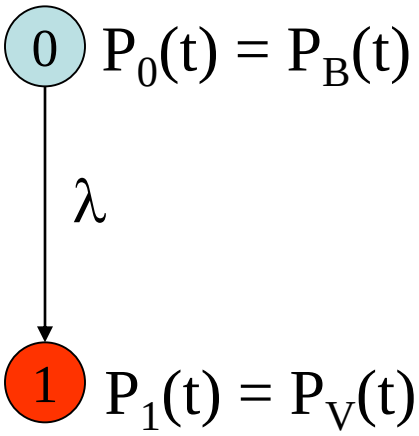
IDEÁLIS $\lambda = 0$

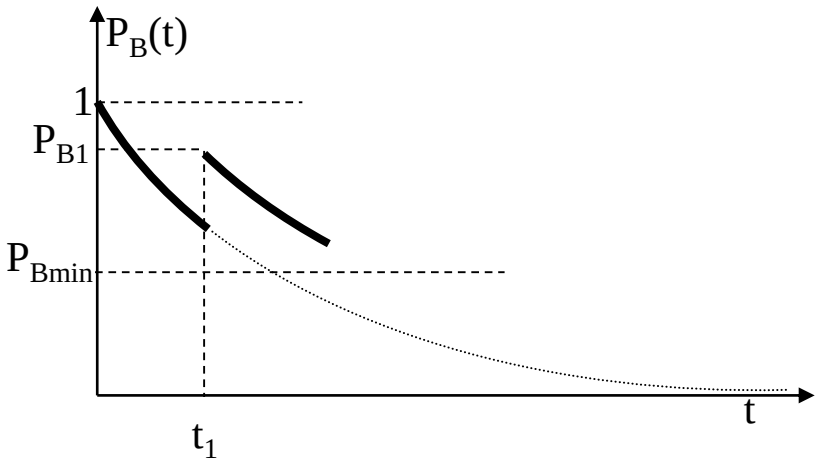
VALÓSÁGOS $\lambda \cong 0$

KORLÁTOZOTT ALKALMAZÁS

- EGYSZERŰ ELEMEK, RENDSZEREK
- RÖVID BIZTONSÁGOS ÉLETTARTAM

MEGELŐZŐ KARBANTARTÁS





WORST CASE FELTÉTELEZÉS

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.

SAFE-LIFE STRATÉGIA

Példa

Egymotoros kisrepülő – nem állhat le

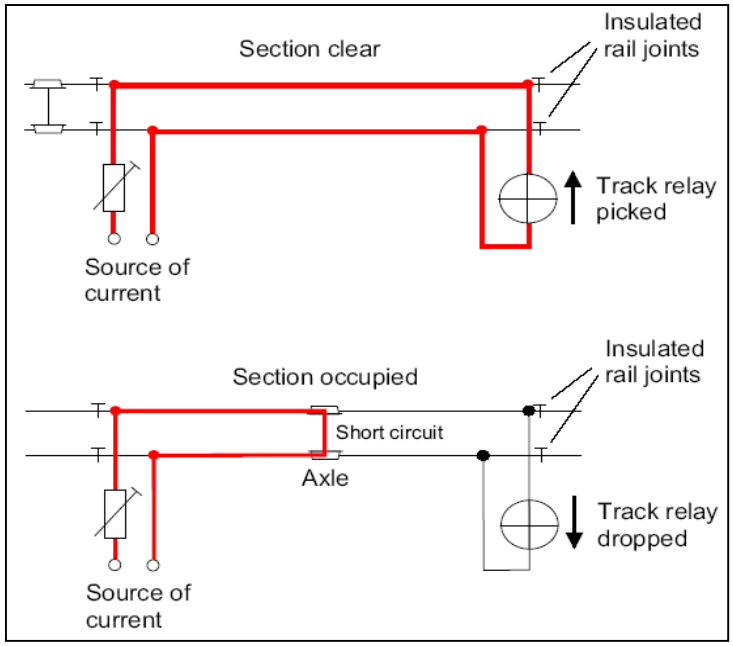
Motor olaj – cserélni kell xxx km után

Gumiabroncs – megfelelő mélység szükséges

SAFE-LIFE STRATÉGIA

Példa

Szigeteltsín áramkör
(biztonsági jelfogó)



SAFE-LIFE STRATÉGIA

Példa

Mechanikus biztosítóberendezés

FAULT-TOLERANT STRATÉGIA

Hibatűrő rendszer:

• hiba esetén is működőképes **és** biztonságos marad

Megvalósítás:

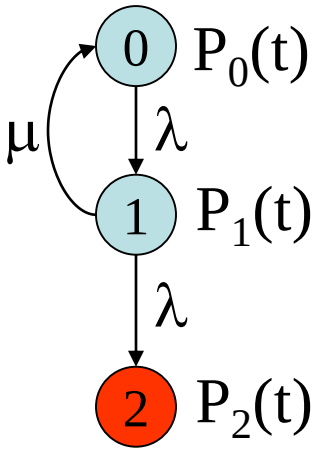
• több (legalább 3) csatornás kivitel **és** többségi elvű szavazás

FAULT-TOLERANT STRATÉGIA

A HIBA FELISMERÉSE ÉS HATÁSÁNAK MASZKOLÁSA

HARDVER-REDUNDANCIA / TARTALÉKOLÁS

$\mu >> \lambda$



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

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

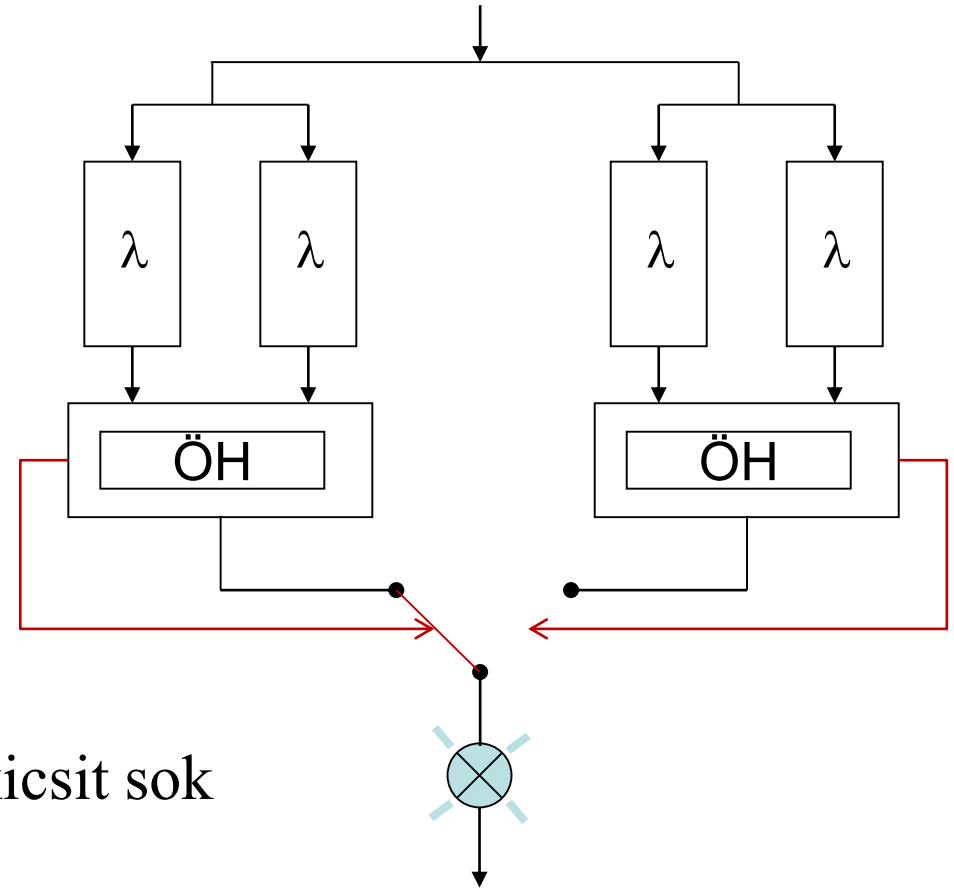
A biztonsági rendszerek működőképességének biztosítása

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

EGYÉB REDUNDANCIA FORMÁK

FAULT-TOLERANT STRATÉGIA

2x(2v2) RENDSZER

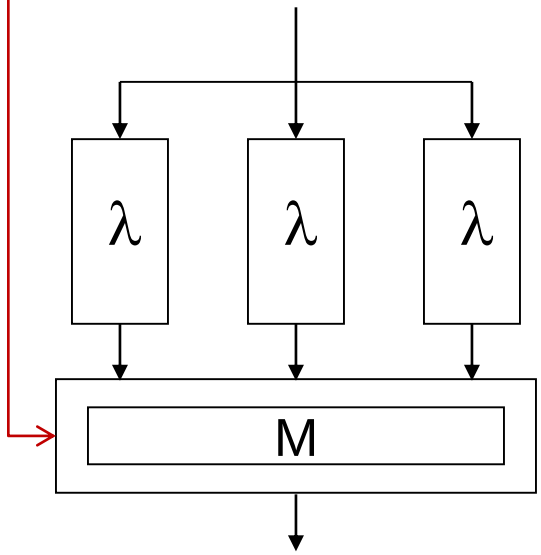


Jó, csak egy kicsit sok hardver kell.

FAULT-TOLERANT STRATÉGIA

TÖBBSÉGI LOGIKA (SZAVAZÓ) ALKALMAZÁSA

3-ból 2 szavazólogika



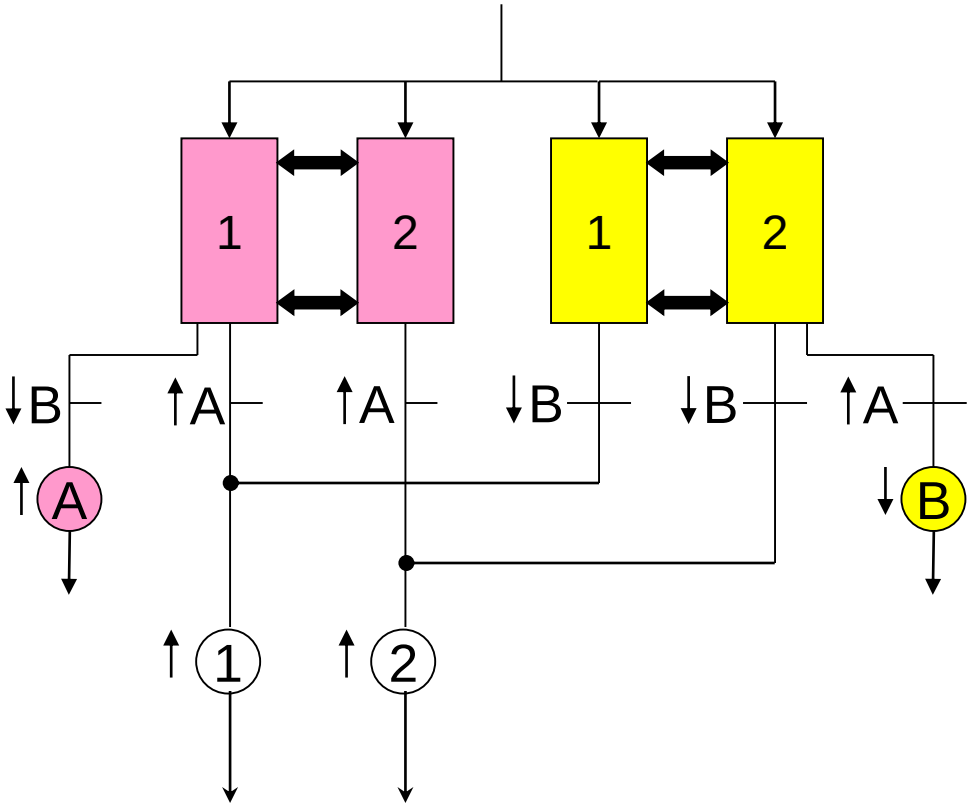
Diverz rendszerkialakítás

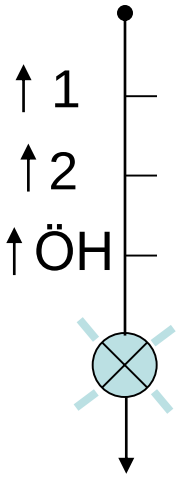
- Megvalósítható
  - hardveresen (különböző alkatrészek)
  - szoftveresen (különböző szoftverek ugyanarra a feladatra)
    - eltérő specifikáció
    - eltérő programozó csapatok
    - eltérő programnyelv stb.
- A szisztematikus hiba megjelenésekor (üzem közben) észlelhető
- Megfelelő hibareakciót kell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

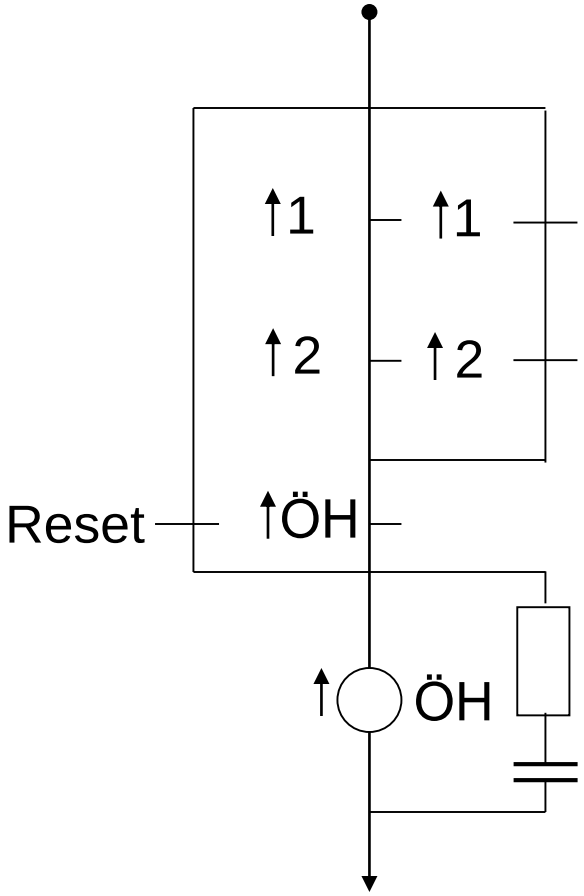
- Előny
  - védelem a szisztematikus hibák veszélyes hatása ellen
  - „polcról levett” komponensek (COTS, Commercial Off-The-Shelf) alkalmazhatósága
- Hátrány
  - A hibadetektálás az üzem közbenre tolódik (kisebb rendelkezésreállás)
  - A különböző csatornák szinkronizálása nehéz
  - Drága (fejlesztés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

FAULT-TOLERANT STRATÉGIA

2x(2v2) RENDSZER



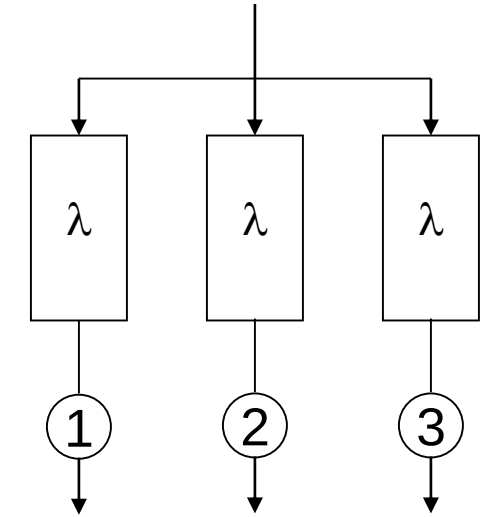




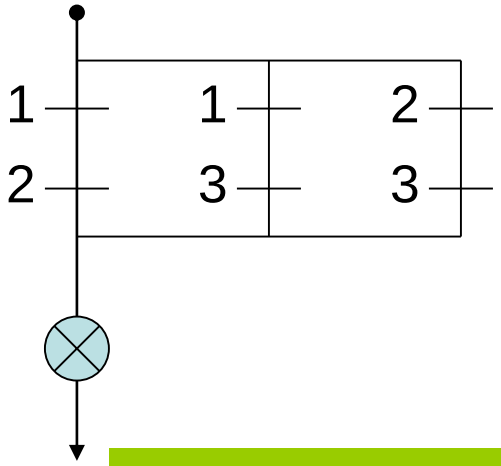
Bekapcsolási sorrend

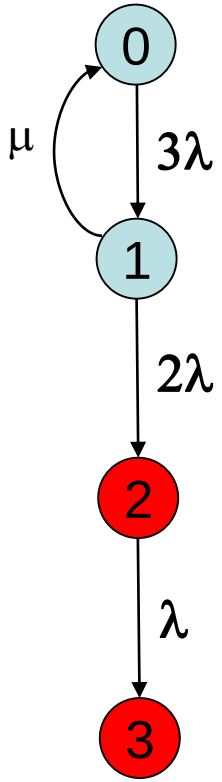
FAULT-TOLERANT STRATÉGIA

TÖBBSÉGI LOGIKA (SZAVAZÓ) ALKALMAZÁSA



3-ból 2



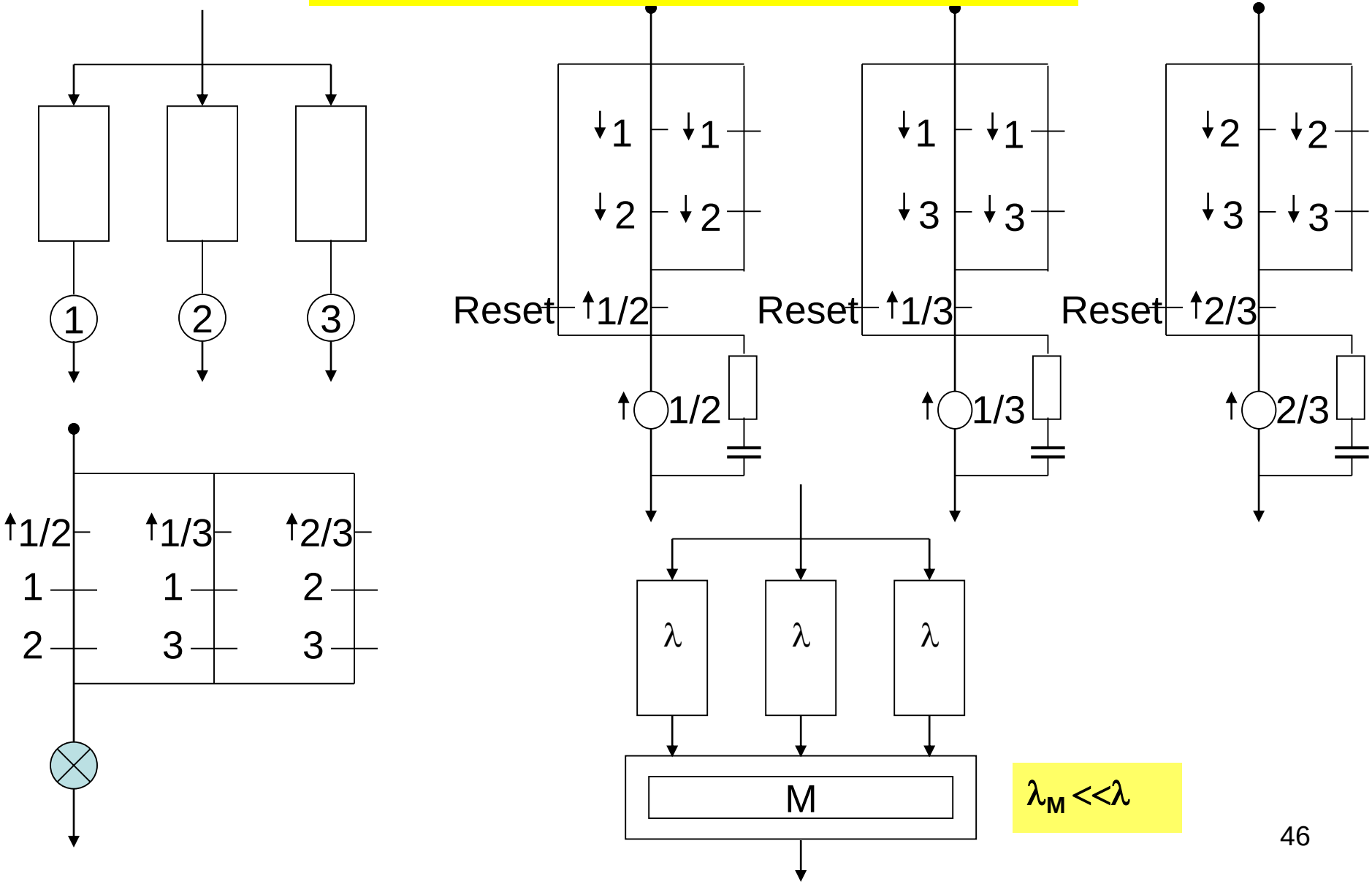


Diverz kialakítás???

Közös módusú hibák!!!

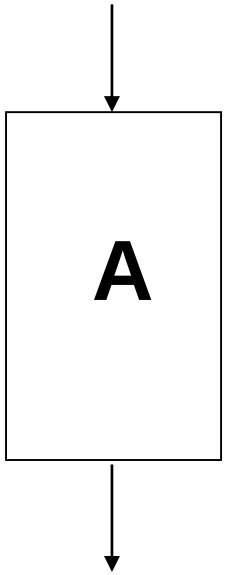
FAULT-TOLERANT STRATÉGIA

TÖBBSÉGI LOGIKA KIKAPCSOLÁSSAL



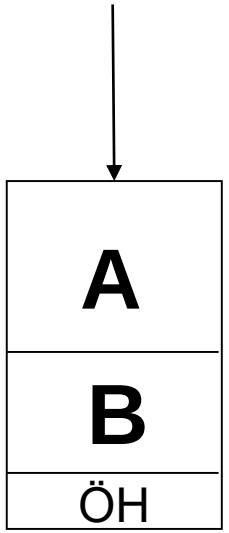
Biztonsági architektúrák

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



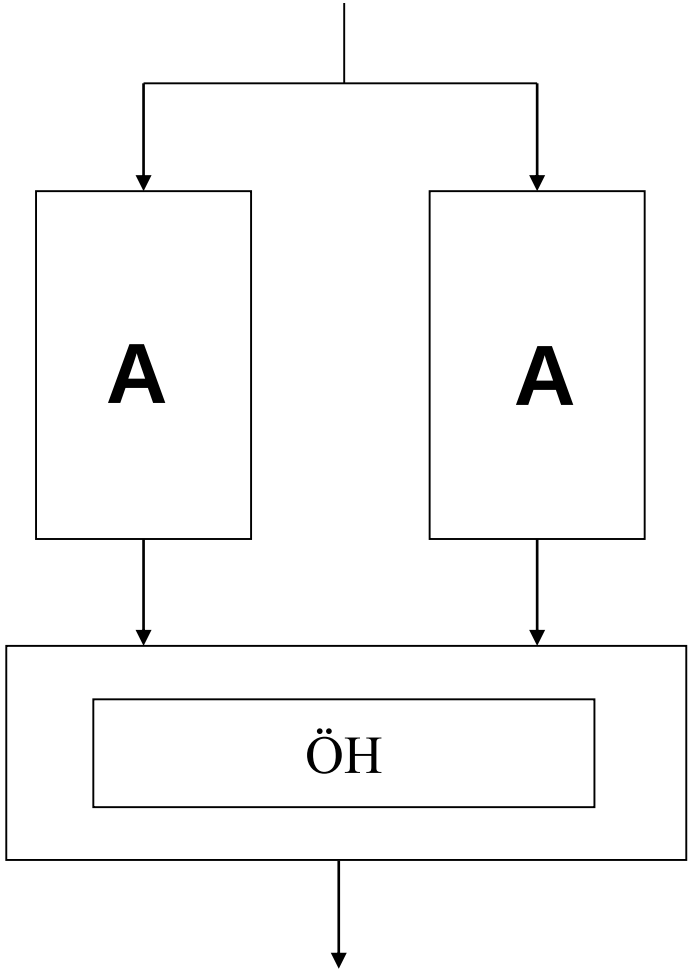
Biztonsági architektúrák

- 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.



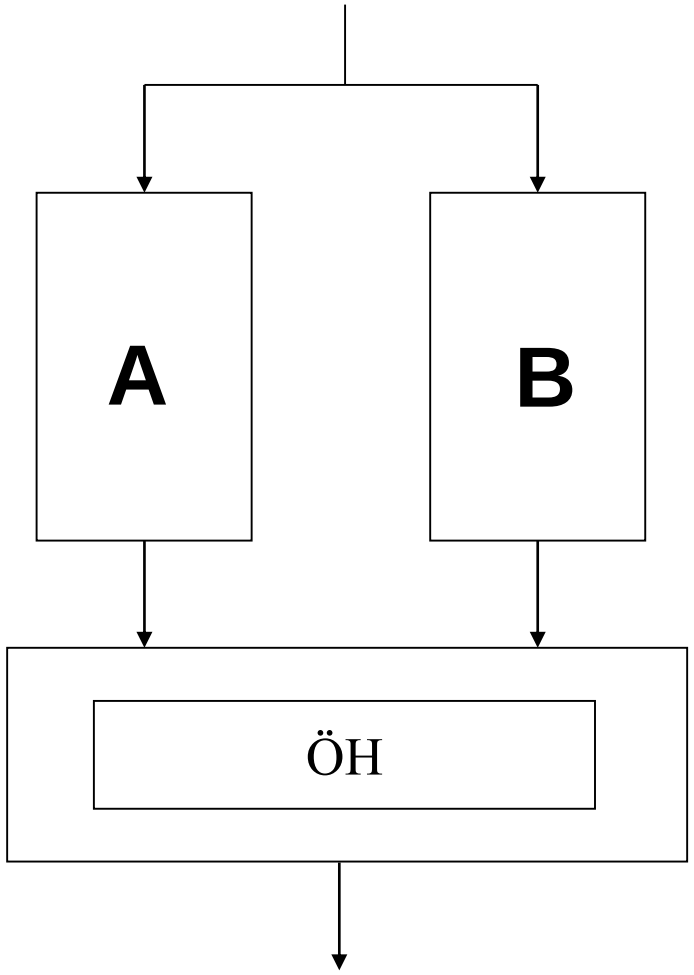
Biztonsági architektúrák

- 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



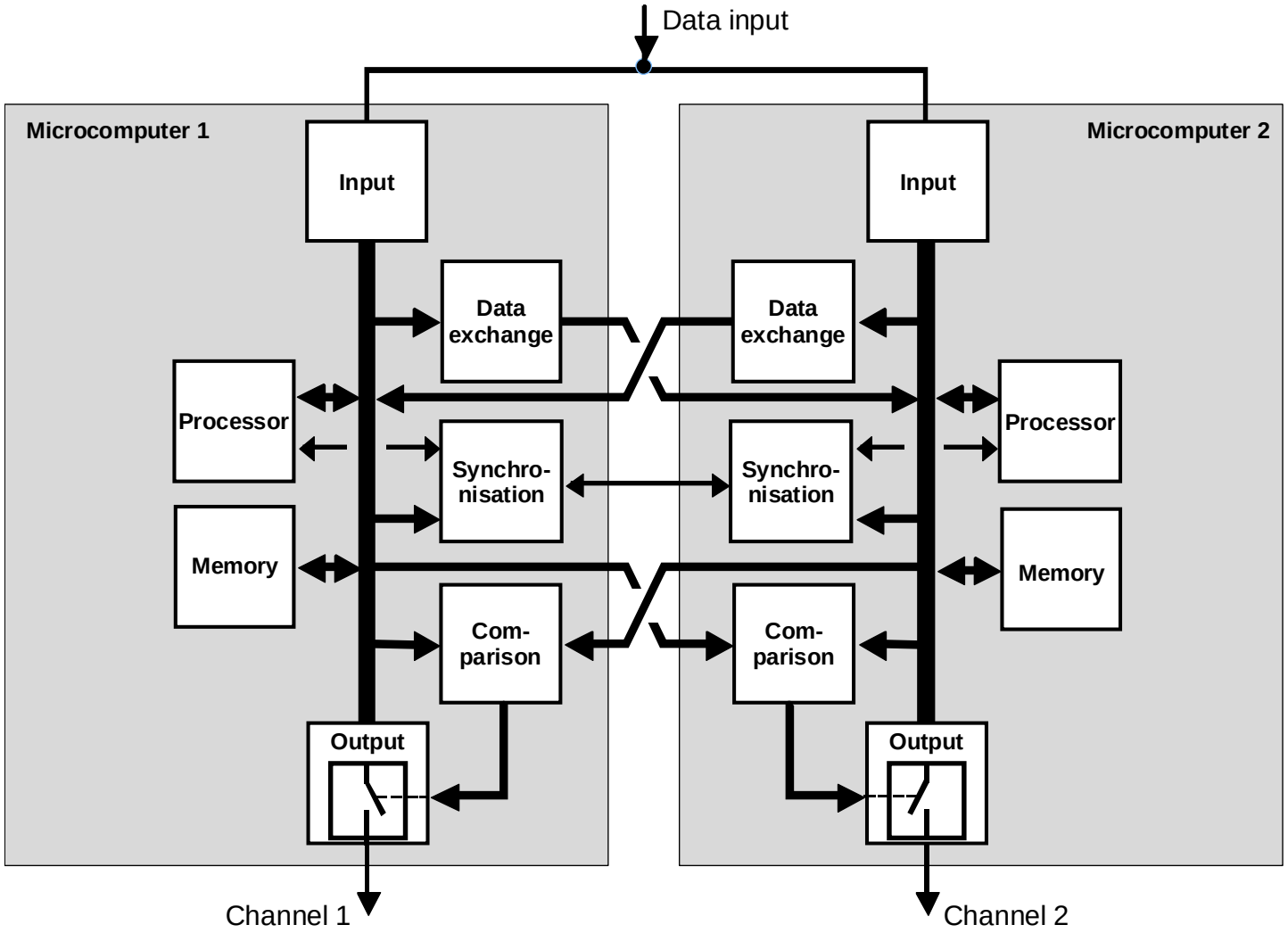
Rendelkezésre állás

- 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)

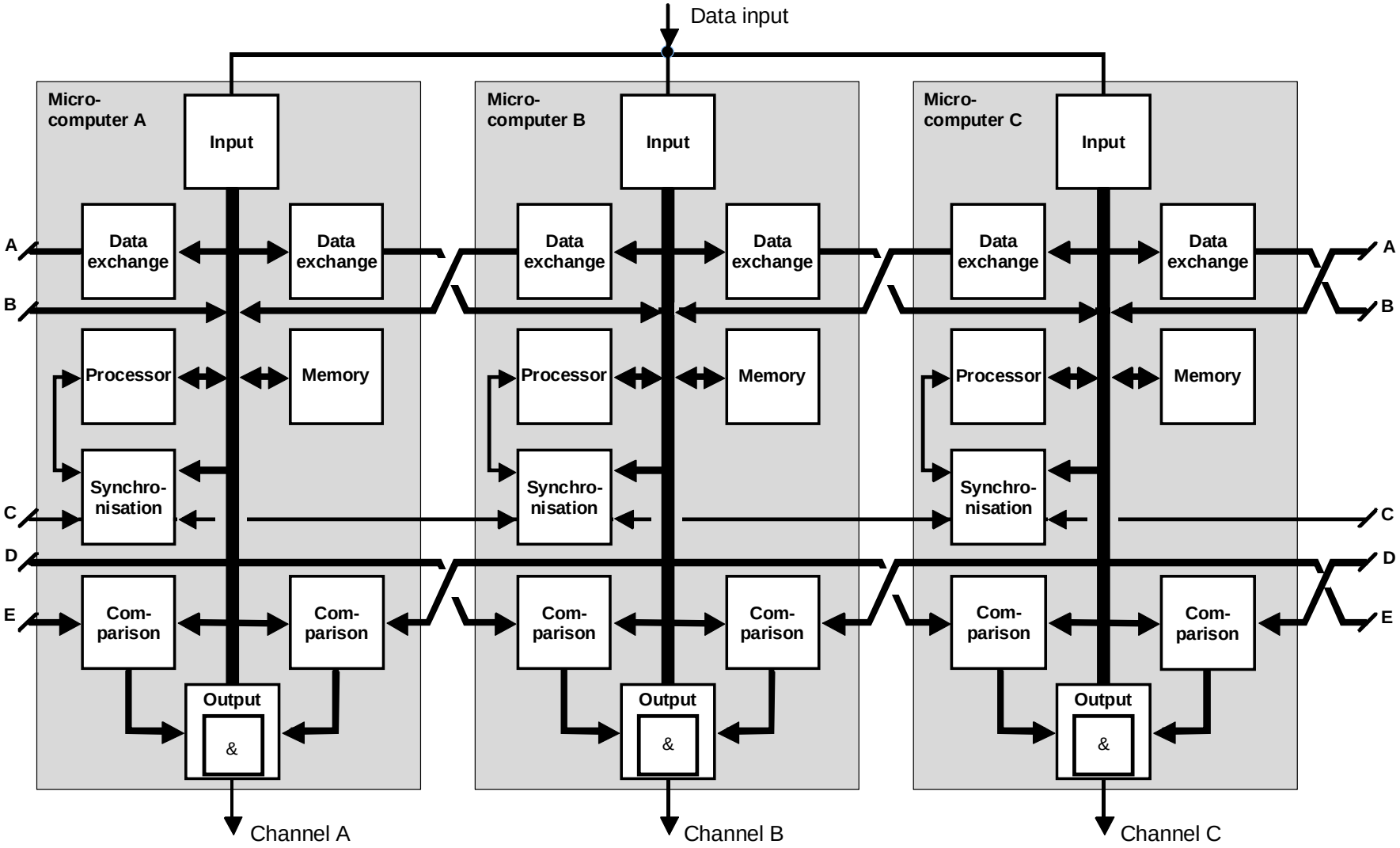
Számítógép konfigurációk
2v2 konfiguráció



2v3

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

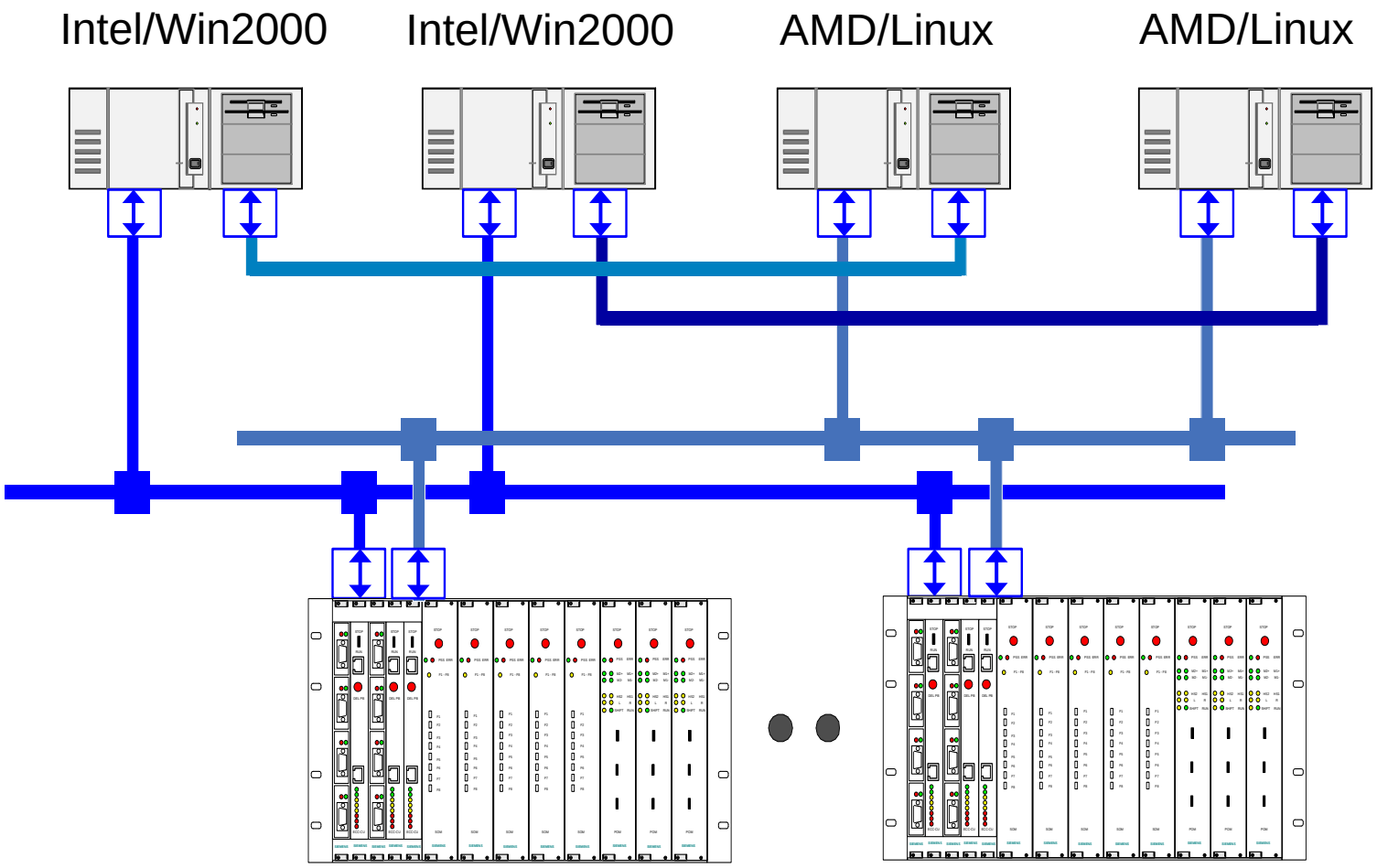
2v3


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

SIMIS PC

- 2×(2v2) diverz számítógéprendszer
- Kereskedelmi forgalomban kapható számítógépek és operációs rendszerek
  - AMD, Intel alaplap/processzor
  - Win2000, Linux operációs rendszerek
  - a diverzitás, és az ECC-kben való összehasonlítás miatt lehetséges ezek alkalmazása
- Összehasonlítás az ECC-kben történik (időablakkal)

SIMIS PC



SIMIS PC
2 x 2-ből 2 rendszer

EIM ECC
3-ból 2 rendszer

ELEKTRA Rendszerfelépítés

- Két diverz szoftver csatorna
- A két csatornában lévő gépeknek egyenként van 2-es vagy 3-as redundanciájuk