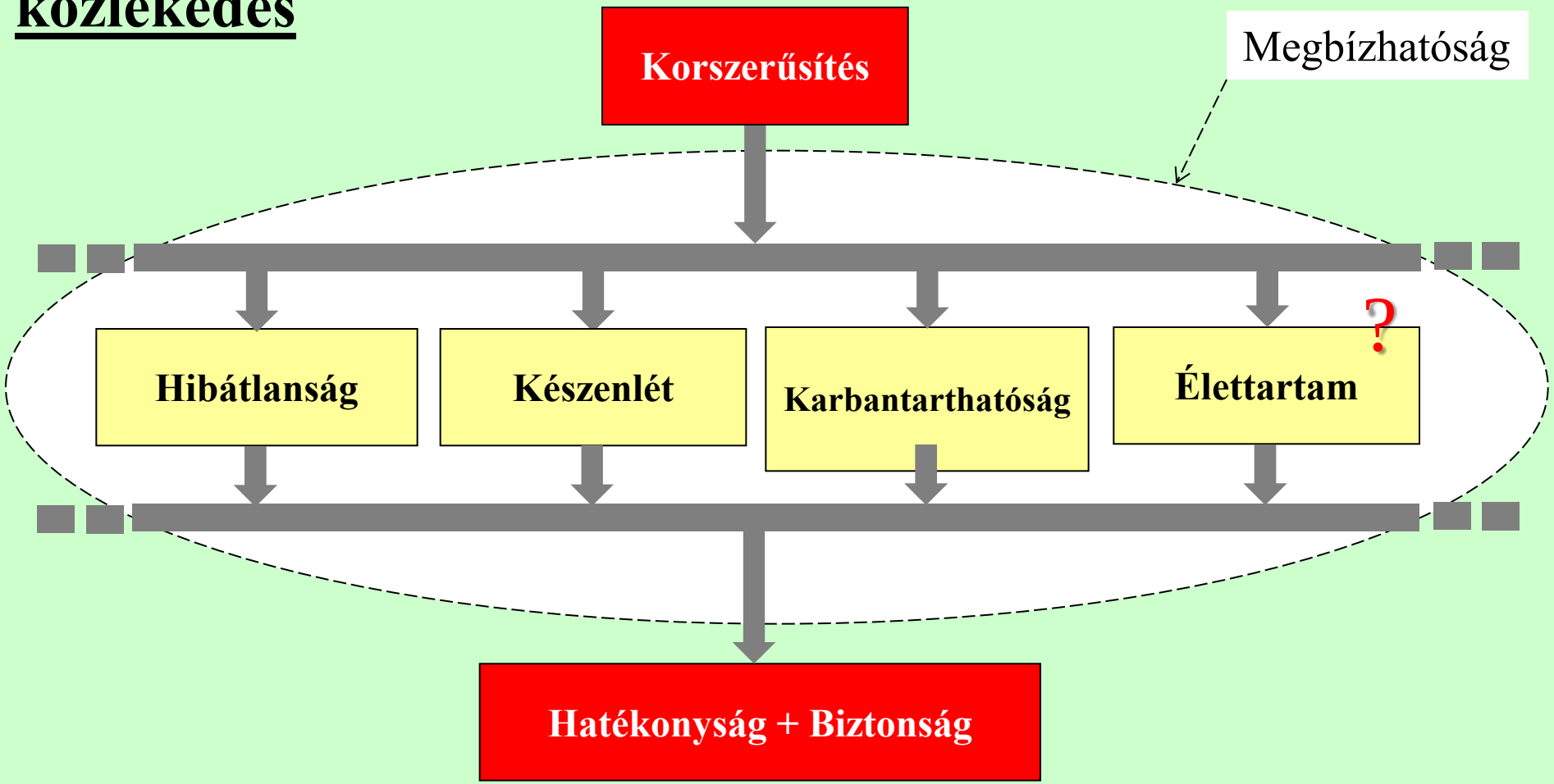
Katedra riadiacich a informačných systémov
Elektrotechnická fakulta
Žilinská univerzita, Univerzitná 1, 010 26 Žilina

Biztosítóberendezési rendszerek biztonsága
Nézetek és valóság, ...

prof. Ing. Karol Rástočný, PhD.
doc. Ing. Izabela Krbilová, PhD.

A BB technika korszerűsítése → hatékony és biztonságos közlekedés



A BBT korszerűsítése → elektronizálás→ más hozzáállás a fejlesztéshez, az üzemeltetéshez és a karbantartáshoz

Az előadás tárgya

Gyakran hallott kijelentések

- A rendszer nagy megbízhatóságú, tehát biztonságos ....
- A BB rendszer működött egy évig próbaüzemben, és nem keletkezett semmilyen veszélyeztető állapot, tehát a rendszer biztonságos ....
- Ha biztonságról van szó, az ár nem számít...
- A rendszer SILx szintű
- A BB életkora nem befolyásolja a biztonságot, csak a megbízhatóságot ....
- ...

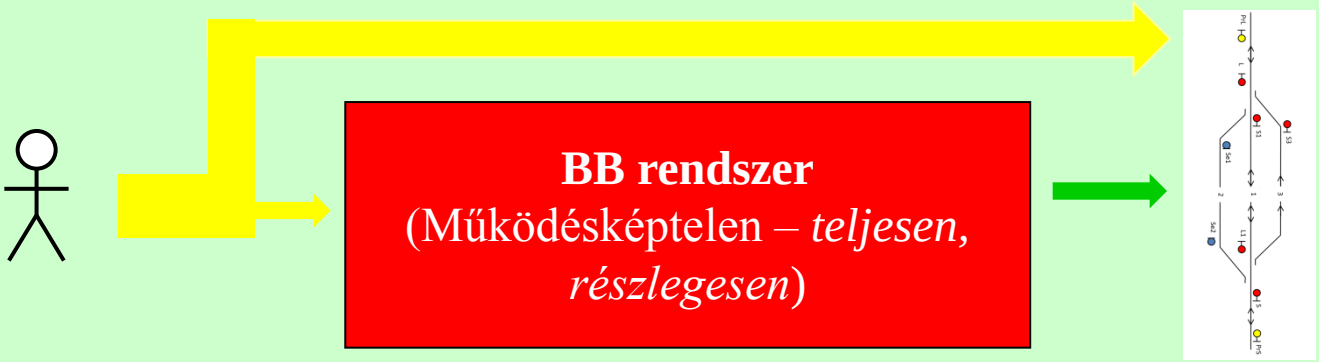
Kérdések

- Mit jelentenek ezek a kijelentések?
- Egyáltalán helyesek ezek a kijelentések?
- Ha érvényesek ezek a kijelentések, akkor milyen körülmények között?

Integritás és készenlét vs biztonság

Elsődleges biztonság

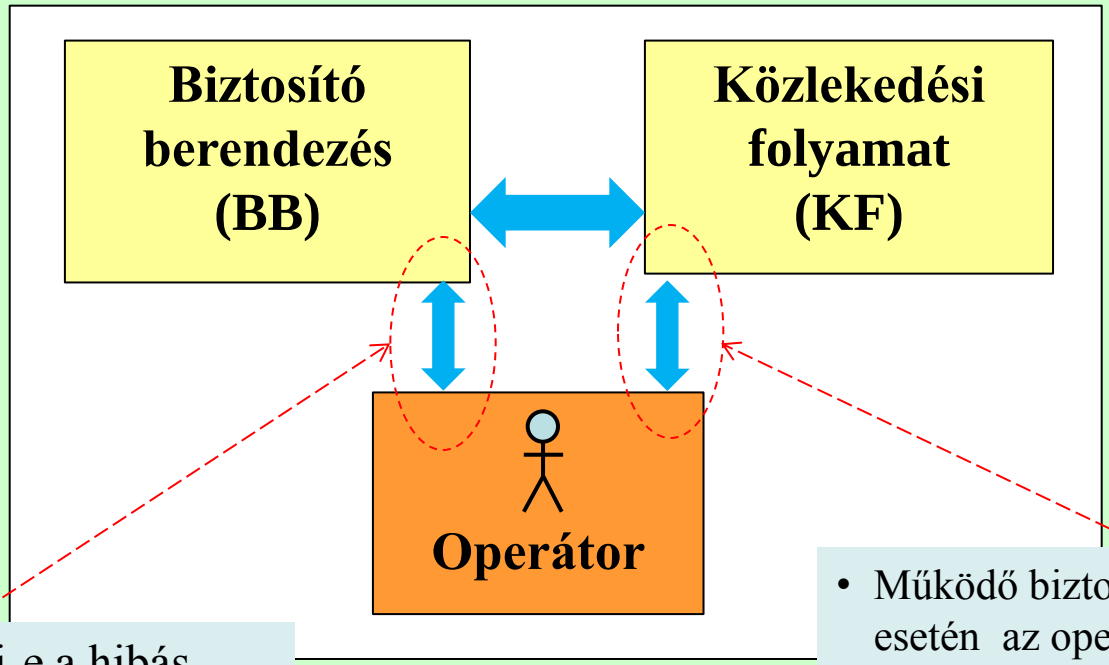
Másodlagos biztonság



Biztonságintegritás →az elsődleges biztonság befolyásolása
Készenlét → a másodlagos biztonság befolyásolása

A hibás kezelés befolyása a biztonságra

Az operátor kapcsolata a BB-vel és a közlekedési folyamattal – **modell architektúra**

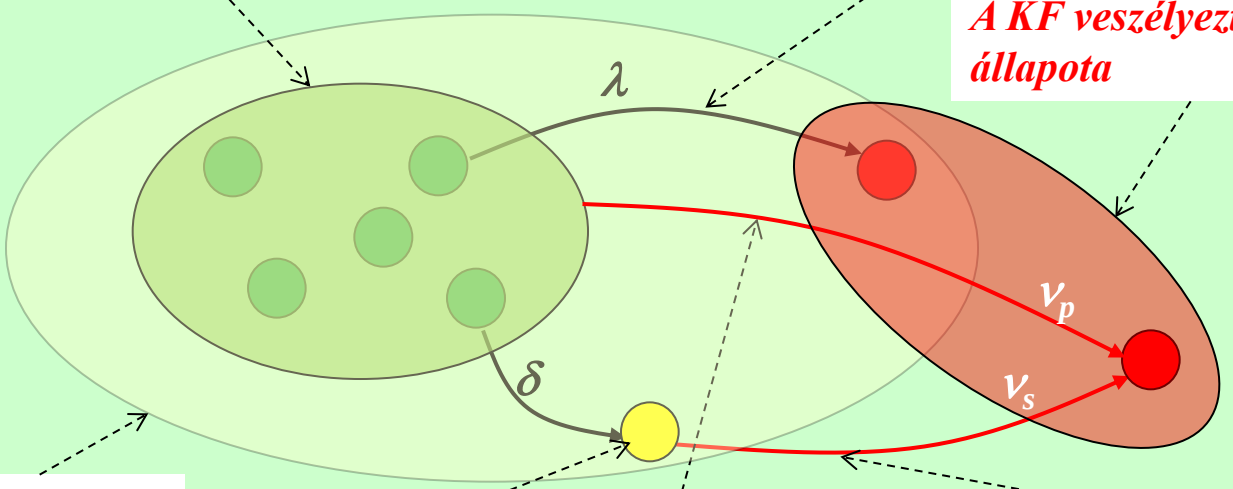


- Veszélyeztetheti-e a hibás kezelés a közlekedés biztonságát?
- A kapott visszajelentések biztonságilag relevánsak-e?

- Működő biztosítóberendezés esetén az operátor befolyásolja-e a KF biztonságát?
- Mekkora a BB felújítási ideje?
- Milyen gyakoriak a biztonságkritikus kezelések?

A hibás kezelés befolyása a biztonságra

Kapcsolat az operátor, a BB és a KF között – állapotmodell



A BB működőképes

Átmenet veszélyeztető állapotba BB hiba miatt

A KF veszélyeztetett állapota

A BB állapotai

A hiba detektálása és negációja után a BB biztonságos állapotban van

Átmenet veszélyeztető állapotba az operátor hibájának következtében (másodlagos veszélyeztetés)

Átmenet veszélyeztető állapotba az operátor hibájának következtében (elsődleges veszélyeztetés)

Kockázatelemzés a BB életciklusában

- Koncepció
- A rendszer definíciója és az alkalmazás feltételei
- Kockázatelemzés
- Rendszerkövetelmények
- A rendszerkövetelmények lebontása
- Tervezés és megvalósítás
- ....

.....

Veszélyeztetések azonosítása

.....

A veszélyeztetések következményeinek azonosítása

Kockázatszámítás (becslés)
(minden egyes veszélyeztetésre)

THR meghatározása
(minden egyes veszélyeztetésre)

A SIL táblázat interpretációja és alkalmazása

A kockázatelemzéstől a BB tervezéséig

Veszélyeztetések listája

Azonosító	Leírás	THR [h^{-1}]
H1	Jármű kisiklása a váltón	1.10^{-9}
H2	.....	....

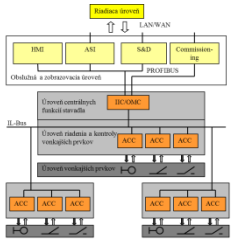
Kockázat-elemzés

A biztonsági funkciók definiálása

Azonosító	Leírás	THR [h^{-1}]
F1	A váltó szakasz szabad állapotának ellenőrzése	2.10^{-10}
F2	.....	....

Veszélyeztetések kezelése

- **BB architektúra definiálása**
- **A funkciók hozzárendelése a BB egyes részeihez**
- **THR hozzárendelése a BB egyes részeihez**



A SIL táblázat interpretációja és alkalmazása

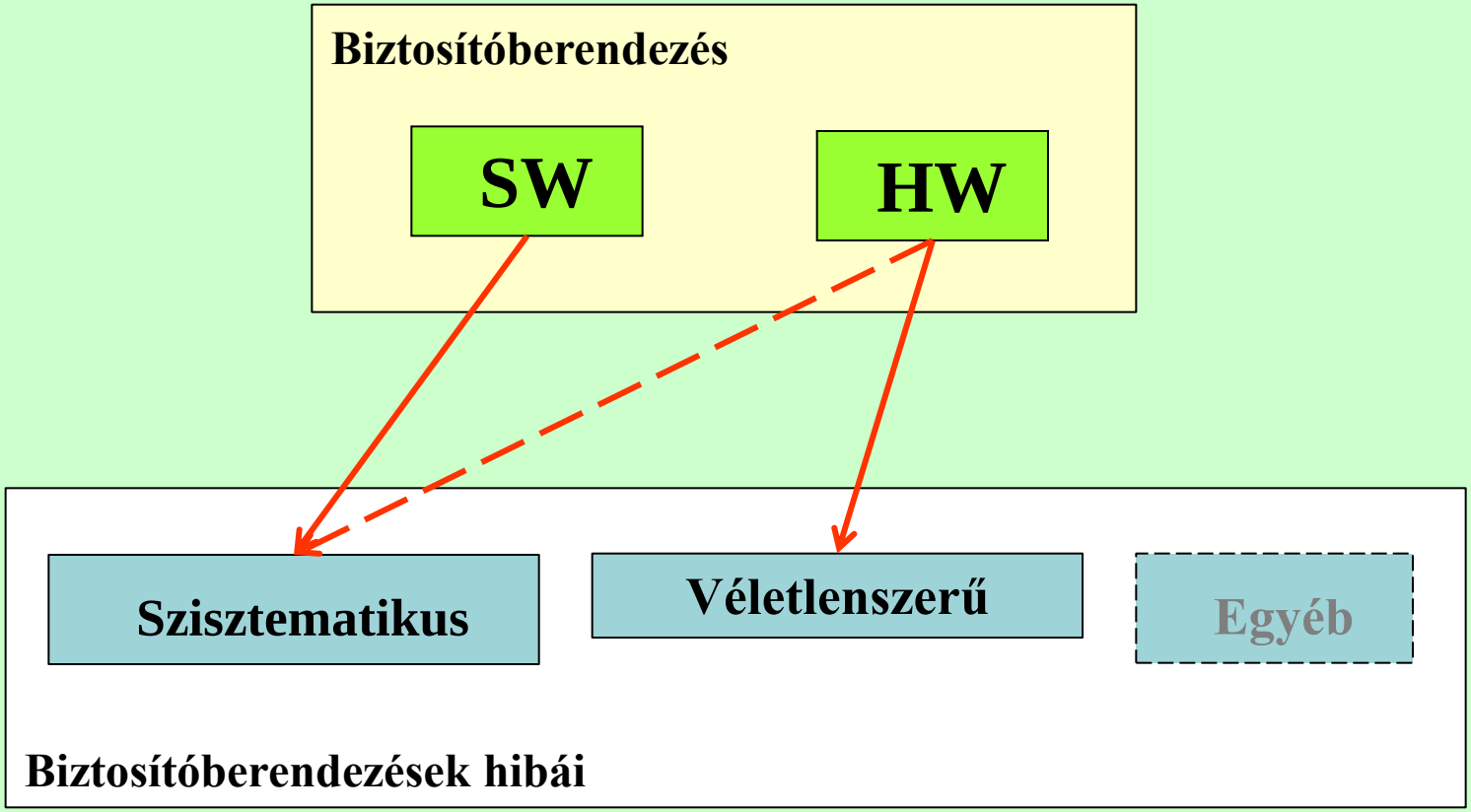
SIL táblázat (STN EN 50129)

Tolerable **H**azard **R**ate **THR per hour and per function**	**S**afety **I**ntegrity **L**evel
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

SIL táblázattal összefüggő kérdések:

- Lehet kvantifikálni az összes veszélyes hibák előfordulását?
- Mi az értelme és érvényesség terjedelme a SIL táblázatban megadott értékeknek?
- Hogyan van definiálva a biztonsági funkció?

Az elektronikus BB-k hibáinak besorolása



Biztonságintegritás verzus hibák

Biztonságintegritás

Szisztematikus hibák elleni biztonságintegritás

Véletlenszerű hibák elleni biztonságintegritás

Követelmény-specifikáció

Tesztelés

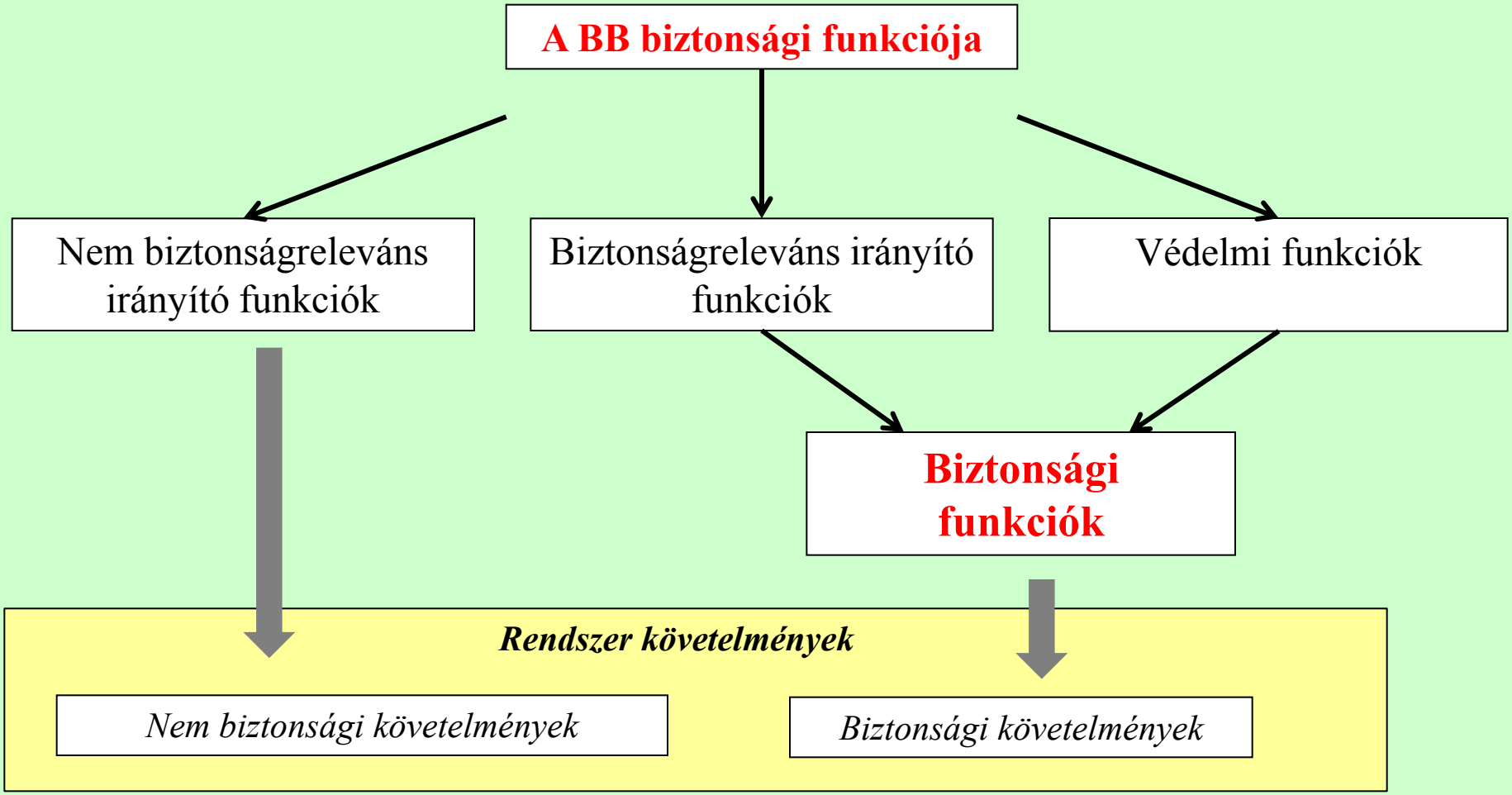
&

Tesztelés
+
Számítás
(SIL táblázat használata)

A követelmények teljesítésének igazolása

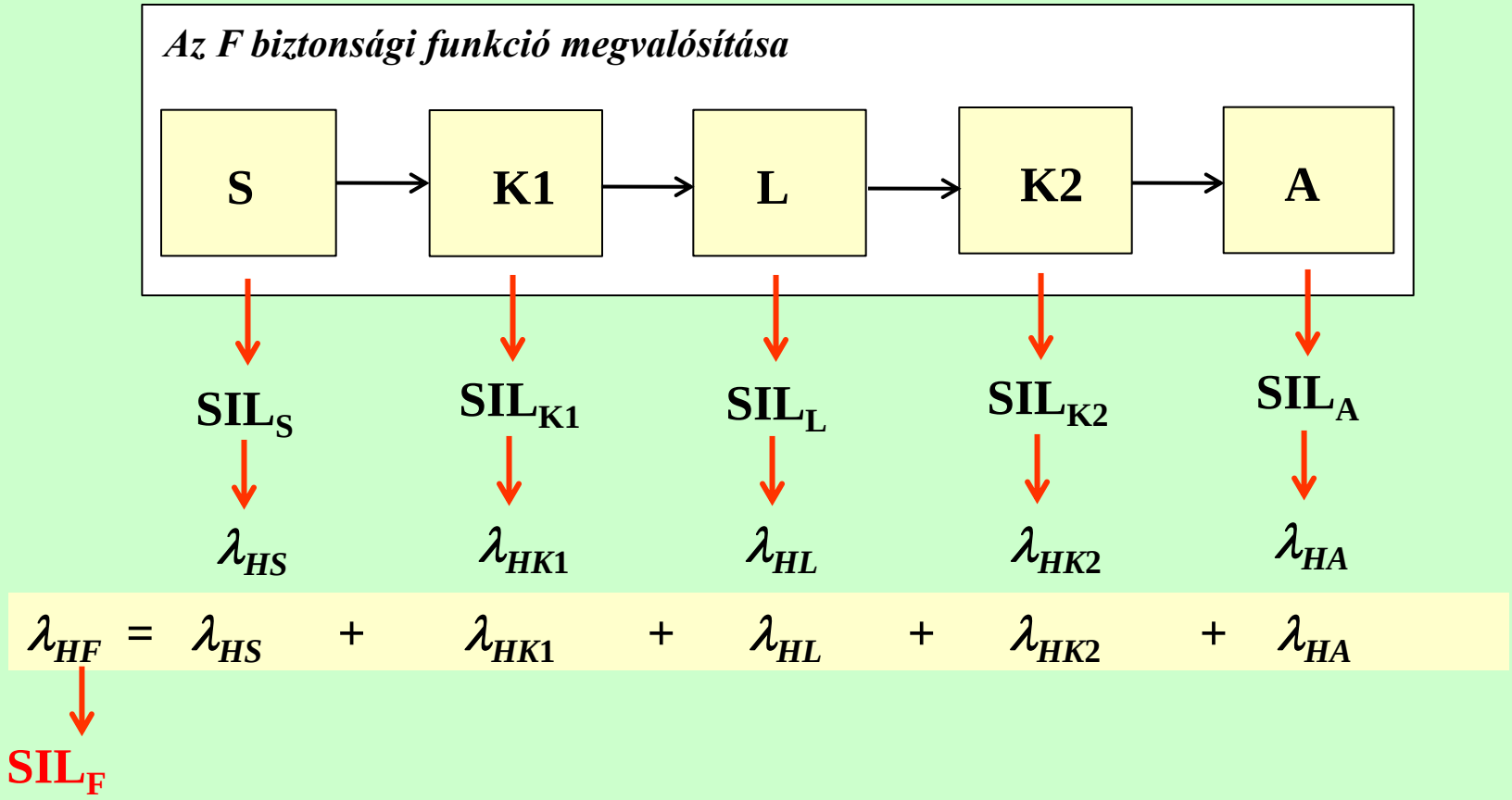
Biztonsági funkció

A BB biztonsági funkciója



Következtetés:
A biztonsági funkciókat a kockázatelemzés alapján kell specifikálni

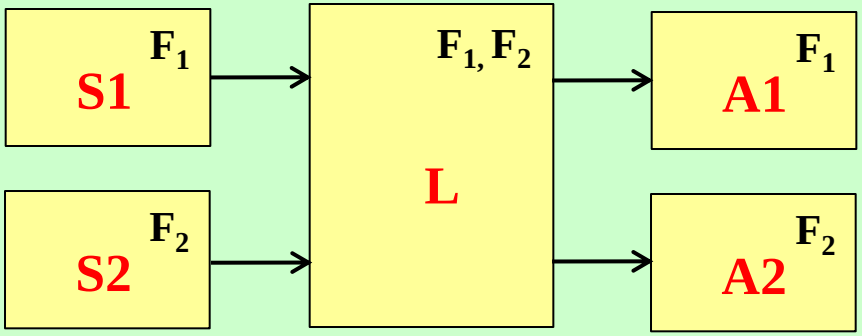
Biztonsági funkcióhoz SIL hozzárendelése



Megjegyzés:

Ha a biztonsági funkcióra a követelmény pld. SIL4, és az összes rendszerelem teljesíti a SIL 4-et, az még nem jelenti azt, hogy a biztonsági funkció is SIL4 lesz.

SIL bezpečnostných funkcií

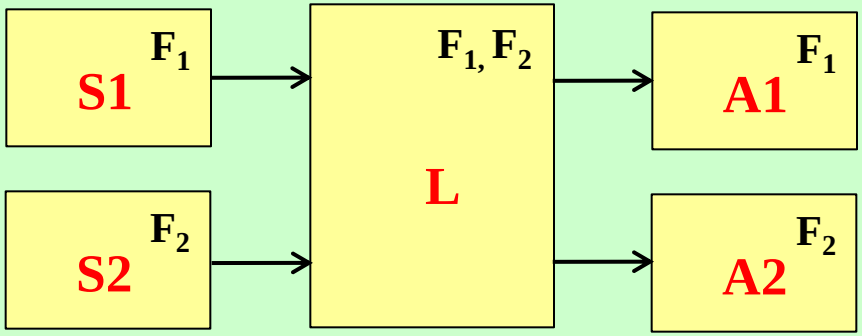


- F_1 ..... THR_{F1}
- F_2 ..... THR_{F2}

$$\lambda_{HF1} = \lambda_{HS1} + \lambda_{HL} + \lambda_{HA1} \qquad \lambda_{HF1} \leq THR_{F1}$$

$$\lambda_{HF2} = \lambda_{HS2} + \lambda_{HL} + \lambda_{HA2} \qquad \lambda_{HF2} \leq THR_{F2}$$

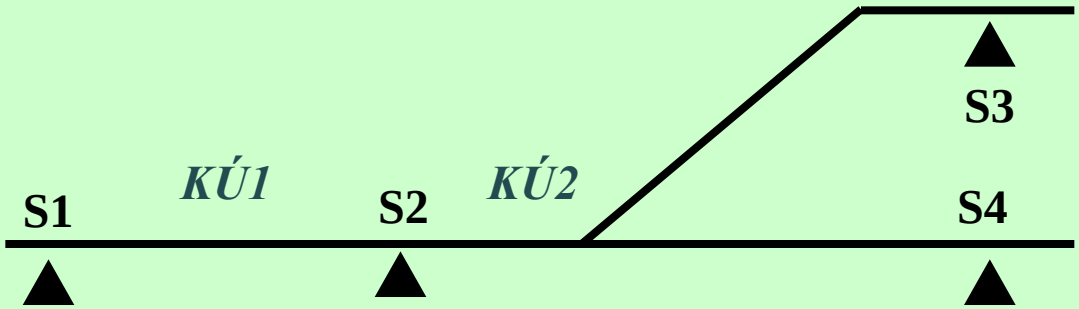
SIL zabezpečovacieho systému



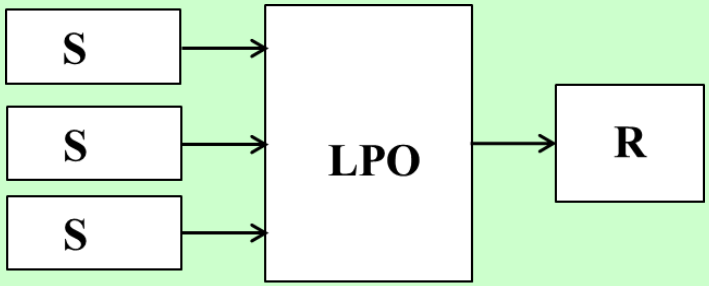
$$\lambda_{HS} = \lambda_{HS1} + \lambda_{HS2} + \lambda_{HL} + \lambda_{HA1} + \lambda_{HA2}$$

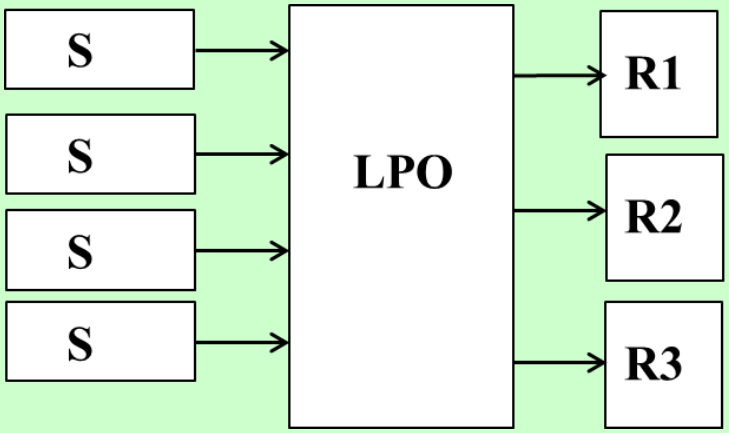
Egyszerűsített példa

Feladat: az állomásfej vágányszakaszai (KÚZ) szabad állapotának ellenőrzése

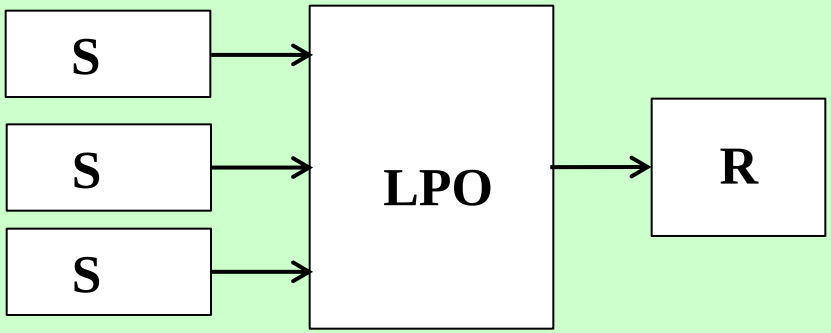


Tételezzük fel tengelyszámláló alkalmazását (PO)





Műszaki megoldás (1)



Tengelyszámláló SIL

$\lambda_{HS} = 0{,}5.10^{-9}\ h^{-1}$

$\lambda_{HLPO} = 2.10^{-9}\ h^{-1}$

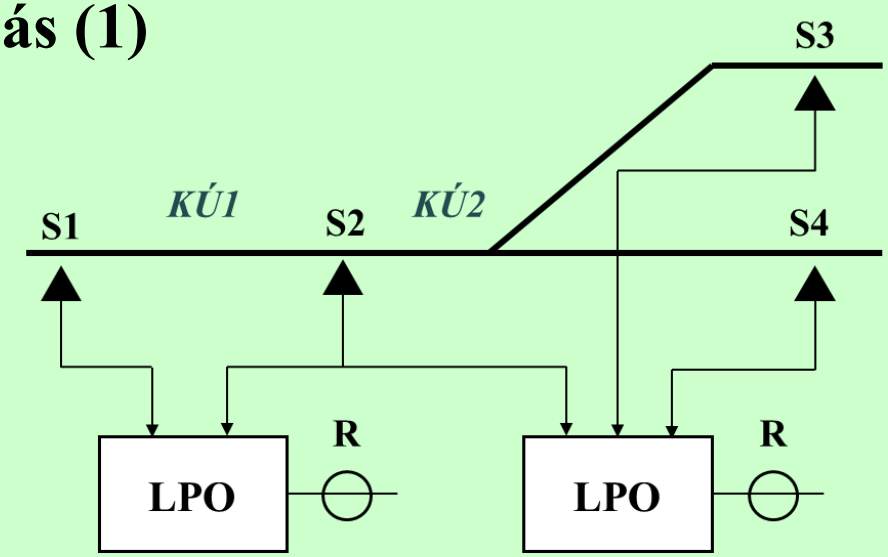
$\lambda_{HR} = 1.10^{-9}\ h^{-1}$

$$\lambda_{HPO} = 3.\lambda_{HS} + \lambda_{HLPO} + \lambda_{HR}$$

$$\lambda_{HPO} = 4{,}5.10^{-9}\ h^{-1}$$

Biztonsági funkció

Műszaki megoldás (1)



Biztonsági funkció: *A KÚ1 szakasz foglaltságellenőrzése*

$\lambda_{HF1} = 2.\lambda_{HS} + \lambda_{HLPO} + \lambda_{HR}$

$\lambda_{HF1} = 4.10^{-9}\ h^{-1}$

Biztonsági funkció: *A KÚ2 szakasz foglaltságellenőrzése*

$\lambda_{HF\,2} = 3.\lambda_{HS} + \lambda_{HLPO} + \lambda_{HR}$

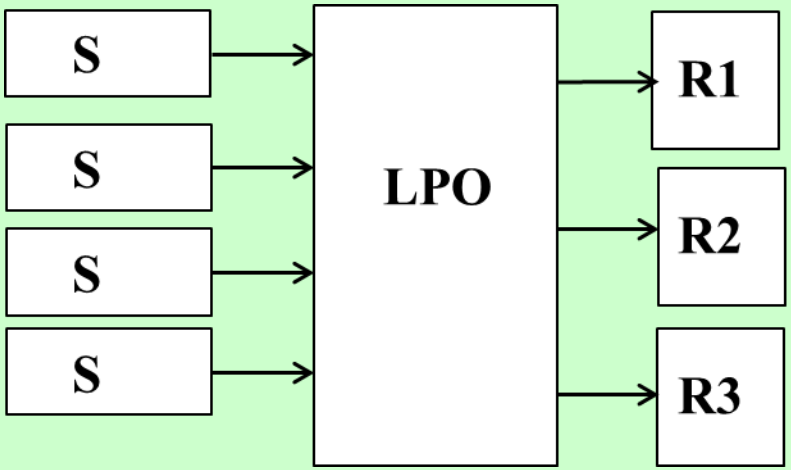
$\lambda_{HF2} = 4{,}5.10^{-9}\ h^{-1}$

Biztonsági funkció: *A KÚZ szakasz foglaltságellenőrzése*

$\lambda_{HF\,Z} = 4.\lambda_{HS} + 2.\lambda_{HLPO} + 2.\lambda_{HR}$

$\lambda_{HFZ} = 8.10^{-9}\ h^{-1}$

Műszaki megoldás (2)



Tengelyszámláló SIL

$\lambda_{HS} = 0{,}5.10^{-9}\ h^{-1}$

$\lambda_{HLPO} = 2.10^{-9}\ h^{-1}$

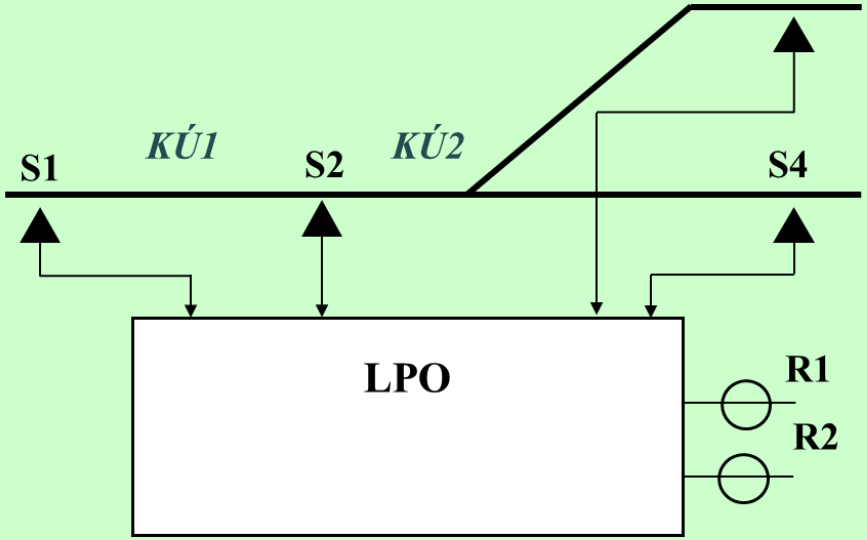
$\lambda_{HR} = 1.10^{-9}\ h^{-1}$

$$\lambda_{HPO} = 4.\lambda_{HS} + \lambda_{HLPO} + 3.\lambda_{HR}$$

$\lambda_{HPO} = 7.10^{-9}\ h^{-1}$

Biztonsági funkció

Műszaki megoldás (2)



Biztonsági funkció: ***A KÚ1 szakasz foglaltságellenőrzése***

$$\lambda_{HF1} = 2.\lambda_{HS} + \lambda_{HLPO} + \lambda_{HR}$$

$$\lambda_{HF1} = 4.10^{-9}\ h^{-1}$$

Biztonsági funkció: ***A KÚ2 szakasz foglaltságellenőrzése***

$$\lambda_{HF\,2} = 3.\lambda_{HS} + \lambda_{HLPO} + \lambda_{HR}$$

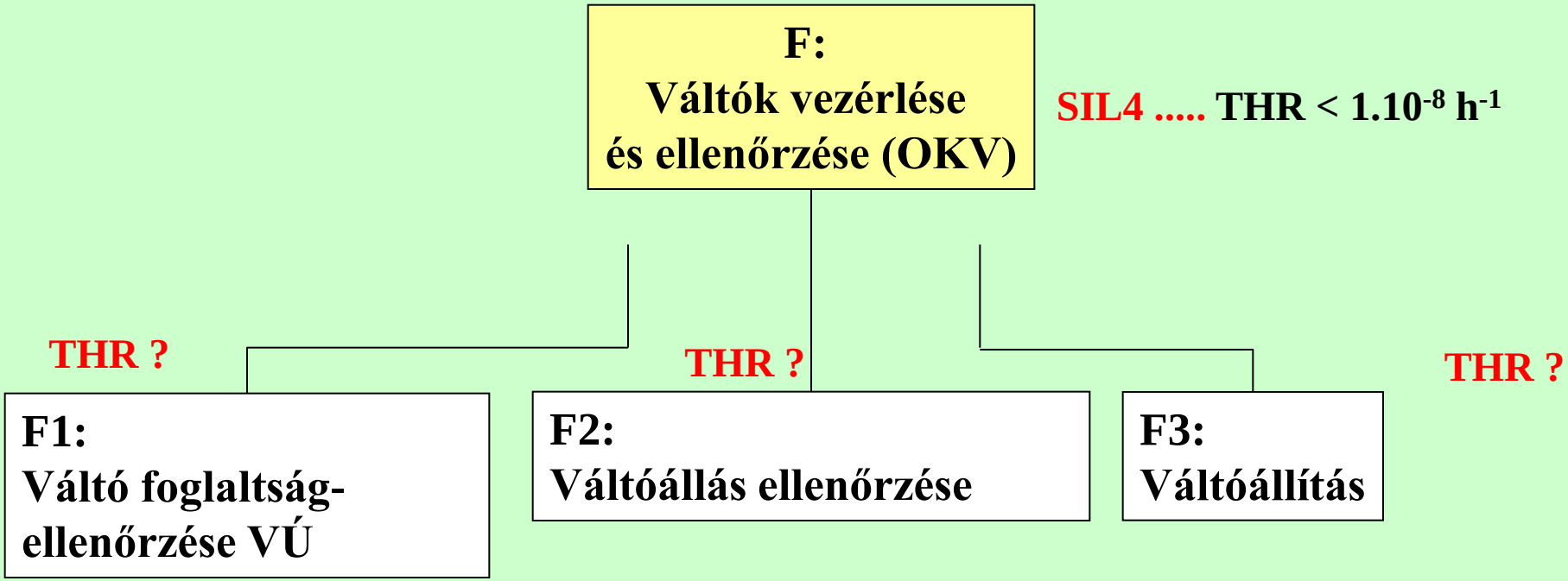
$$\lambda_{HF2} = 4{,}5.10^{-9}\ h^{-1}$$

Biztonsági funkció: ***A KÚZ szakasz foglaltságellenőrzése***

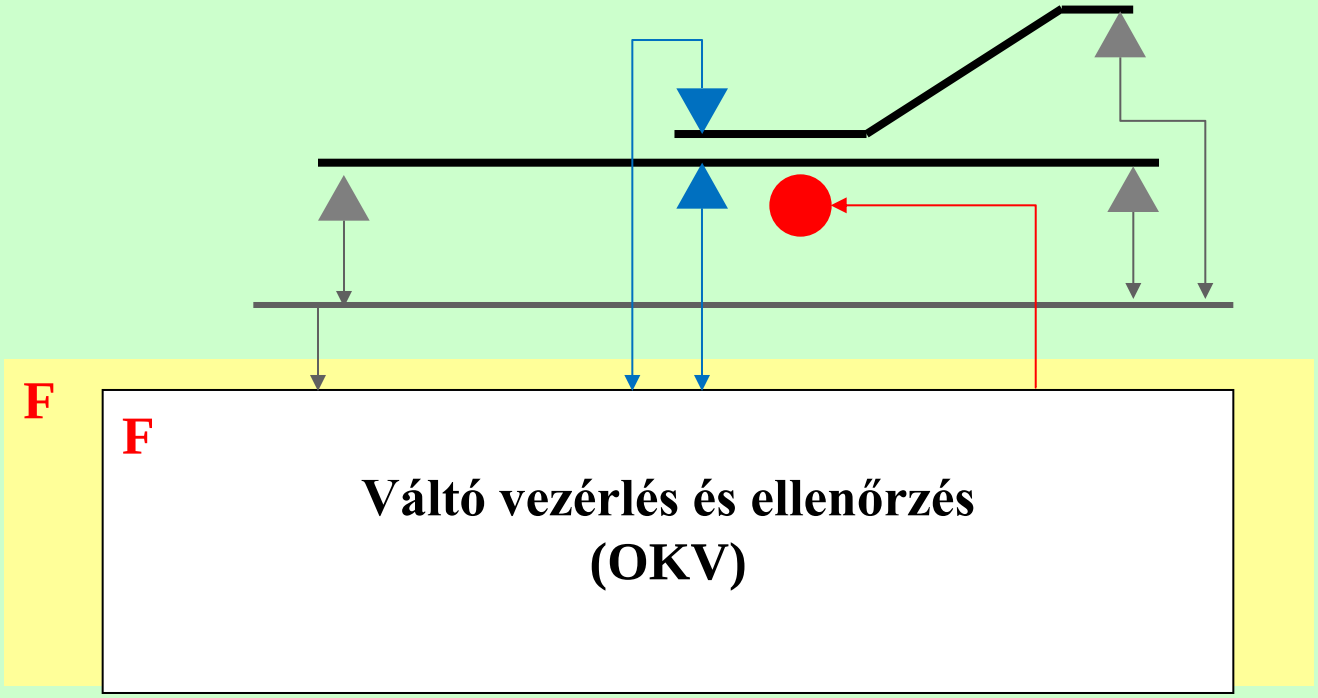
$$\lambda_{HF\,Z} = 4.\lambda_{HS} + 1.\lambda_{HLPO} + 2.\lambda_{HR}$$

$$\lambda_{HFZ} = 6.10^{-9}\ h^{-1}$$

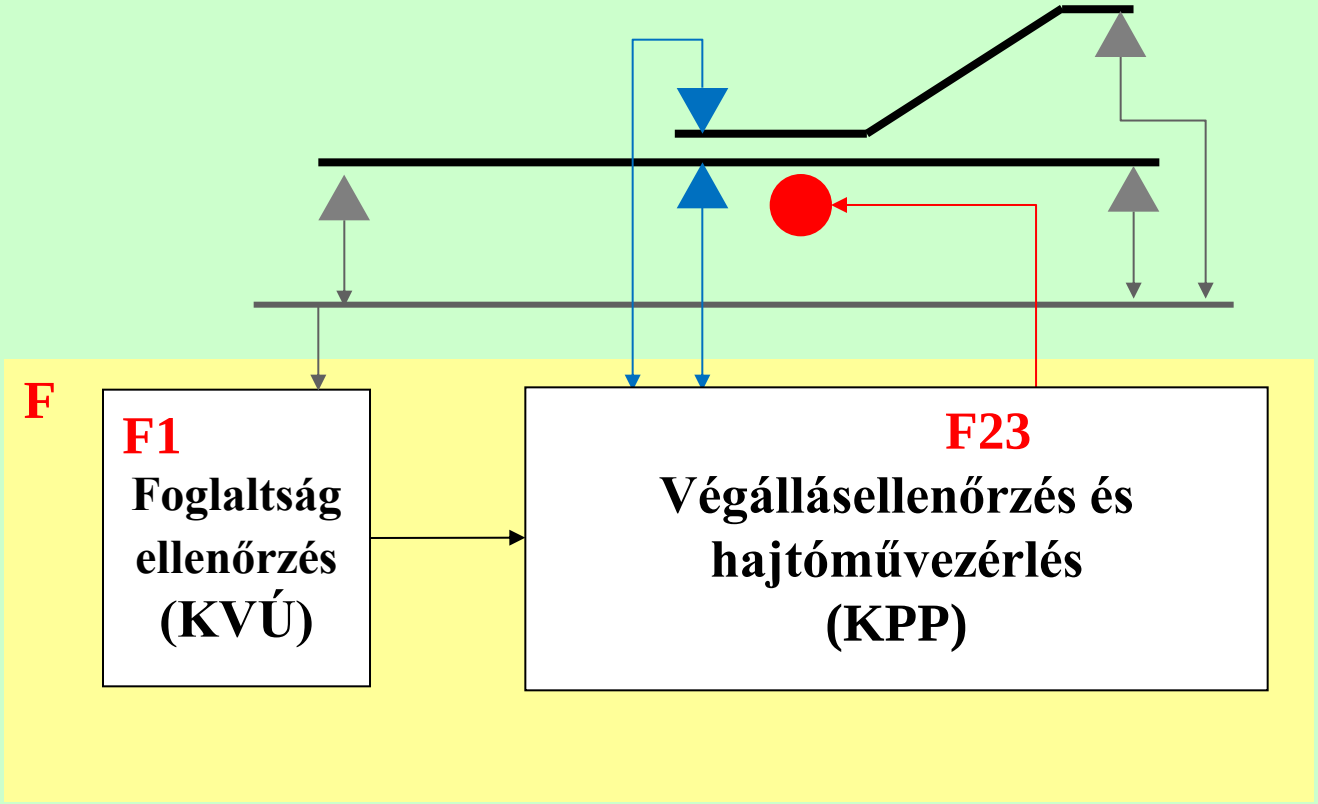
Egyszerűsített példa a biztonsági funkciók megvalósítására



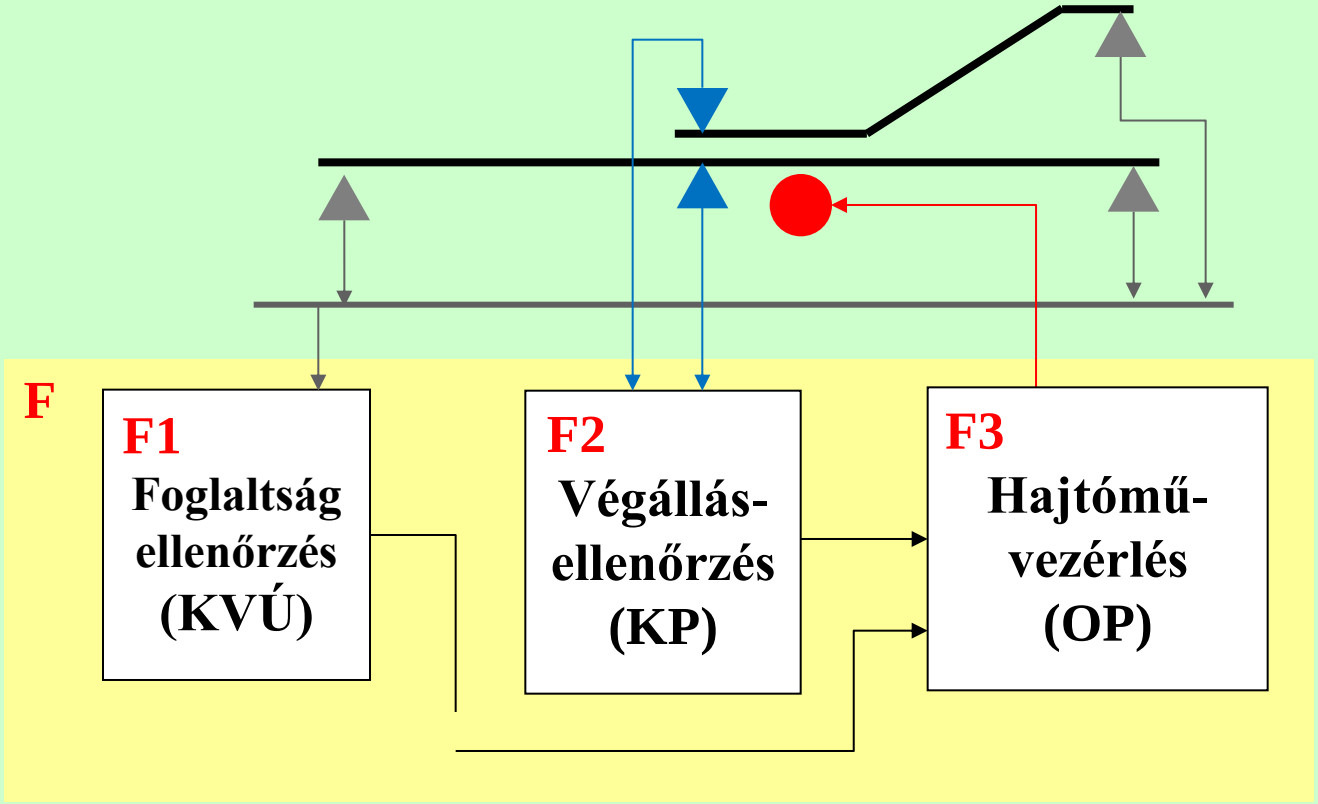
Példa a biztonsági funkciók megvalósítására



Példa a biztonsági funkciók megvalósítására



Példa a biztonsági funkciók megvalósítására



A biztonsági funkció definiálásának objektivitása

Idealizált követelmény

- **Az utasnak azonos biztonságot kellene nyújtani, függetlenül attól, hogy melyik ország melyik vasútvonalán utazik.**

Alapelv

Az a kockázat, aminek az utas ki van téve, nem kellene, hogy

- **nagyobb legyen, mint az általánosan tolerálható kockázat;**
- **attól függjön, hogy milyen vasúti műszaki rendszert vesz igénybe az utas.**

Hogyan lehet ezt elérni?

- **A biztonsági kockázat meghatározása az egyéni kockázat alapján**

A svájci vasút példája (SBB)

Alapelv

Ár **Biztonság**

- A biztonság igazolásánál ki kell mutatni, hogy **semmilyen nem tolerálható kockázat nem keletkezik**, és **minden megfelelő** kockázatcsökkentő **eljárást** alkalmaztak.

Kiindulás (főleg statisztikai adatok)

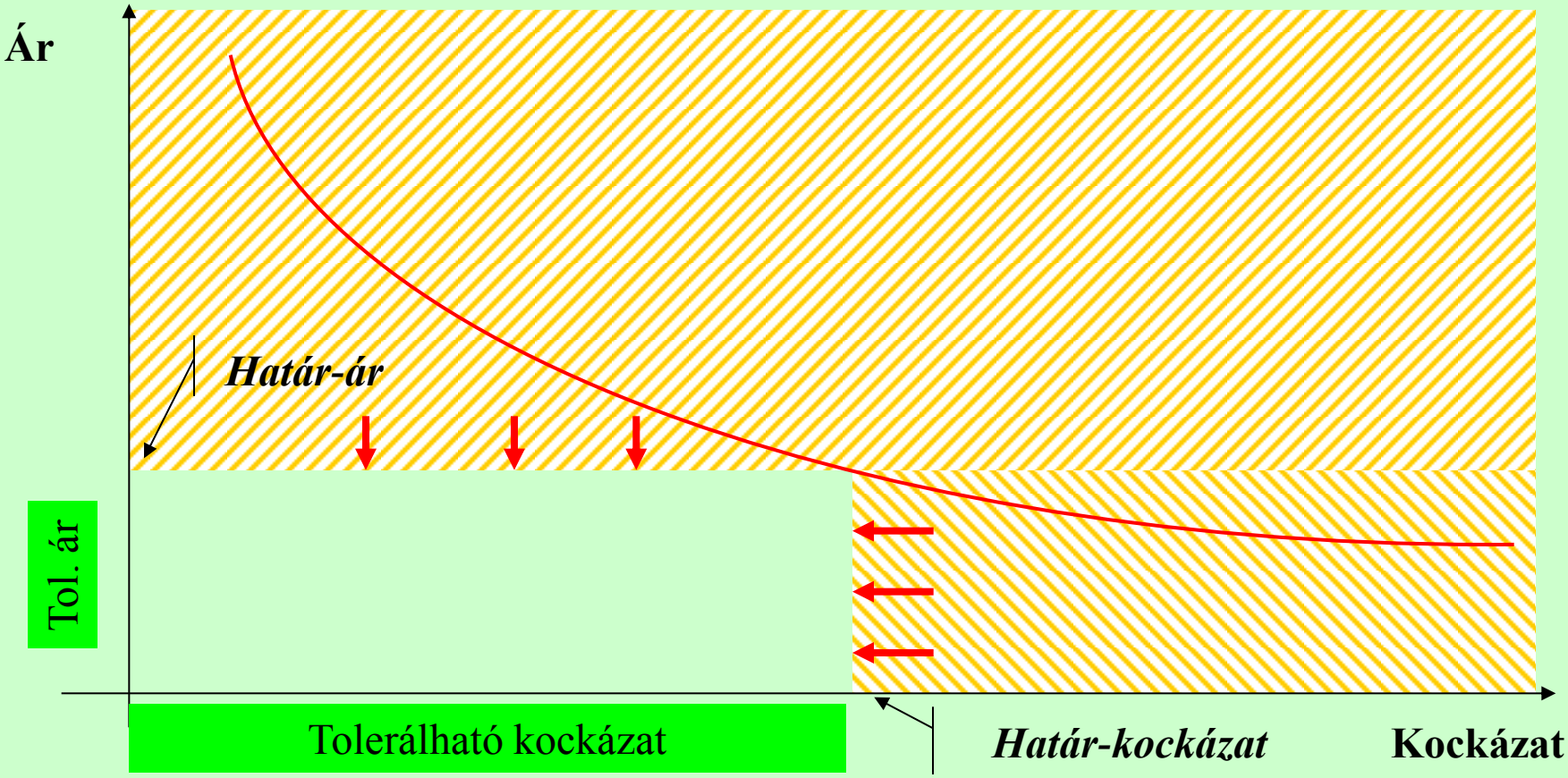
- MEM kritérium: $R_i = 1.10^{-5}$ haláleset/ személyenként és évenként
- Egy utas átlagos útja vonattal: 47 min; vonatsebesség 50,5 km.h^{-1}
- Átlagos üzemi feltételek: 125,8 vonat/nap, 129 utas/vonat
- Az utas átlagos kockázata R_k=1.02 FWI/év (**F**atalities and **W**eighted **I**njuries: FWI = halálos sérülések száma + 0,1. súlyos sérülések száma + 0,01. könnyű sérülések száma)
- Az egyén legfeljebb 1000 óra/év időben használja a vasutat.

Következtetés

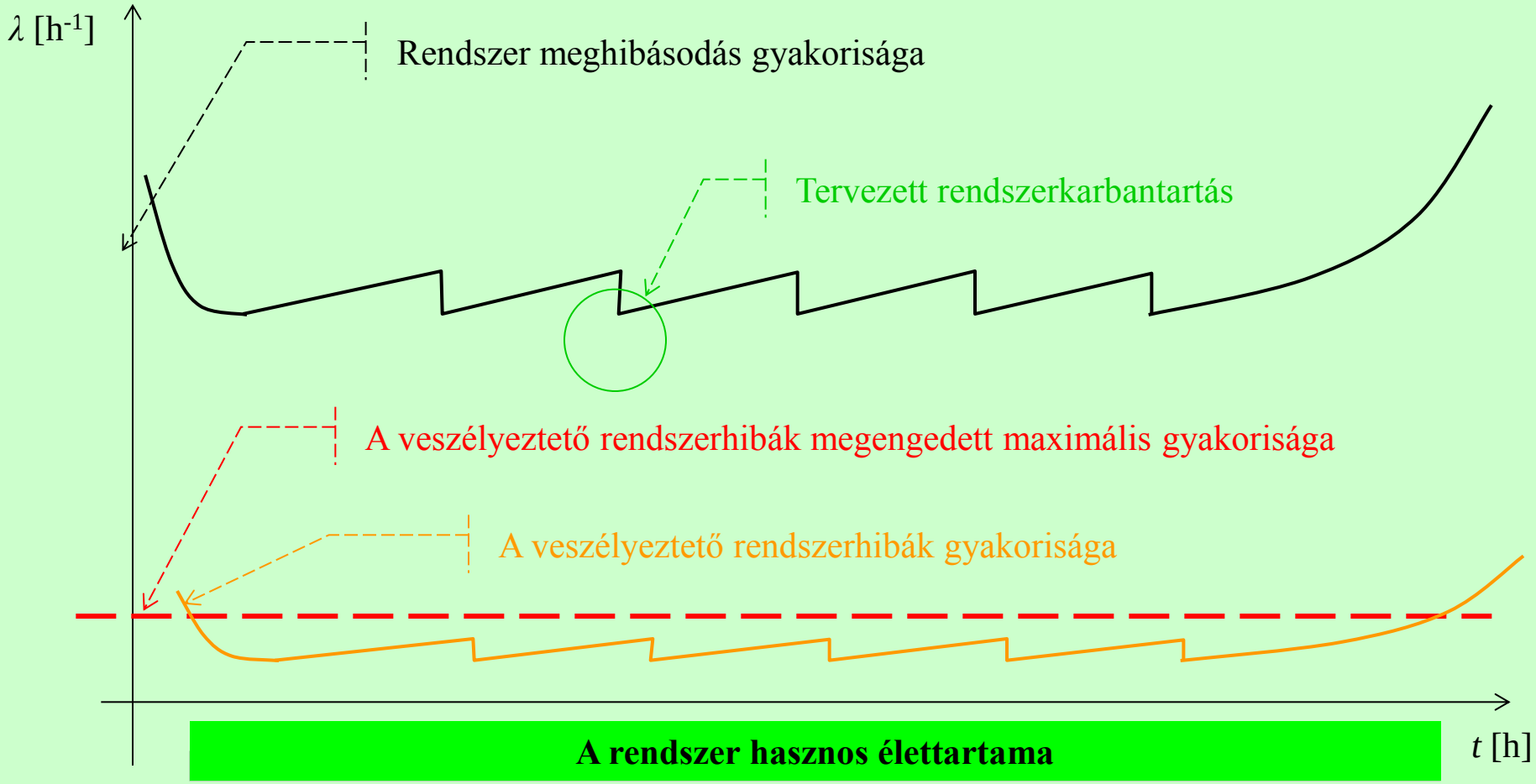
- Az utas átlagos tolerálható kockázata: **R_{iAC}=1.5 FWI/személy és év**

Ár verzus biztonság (kockázat)

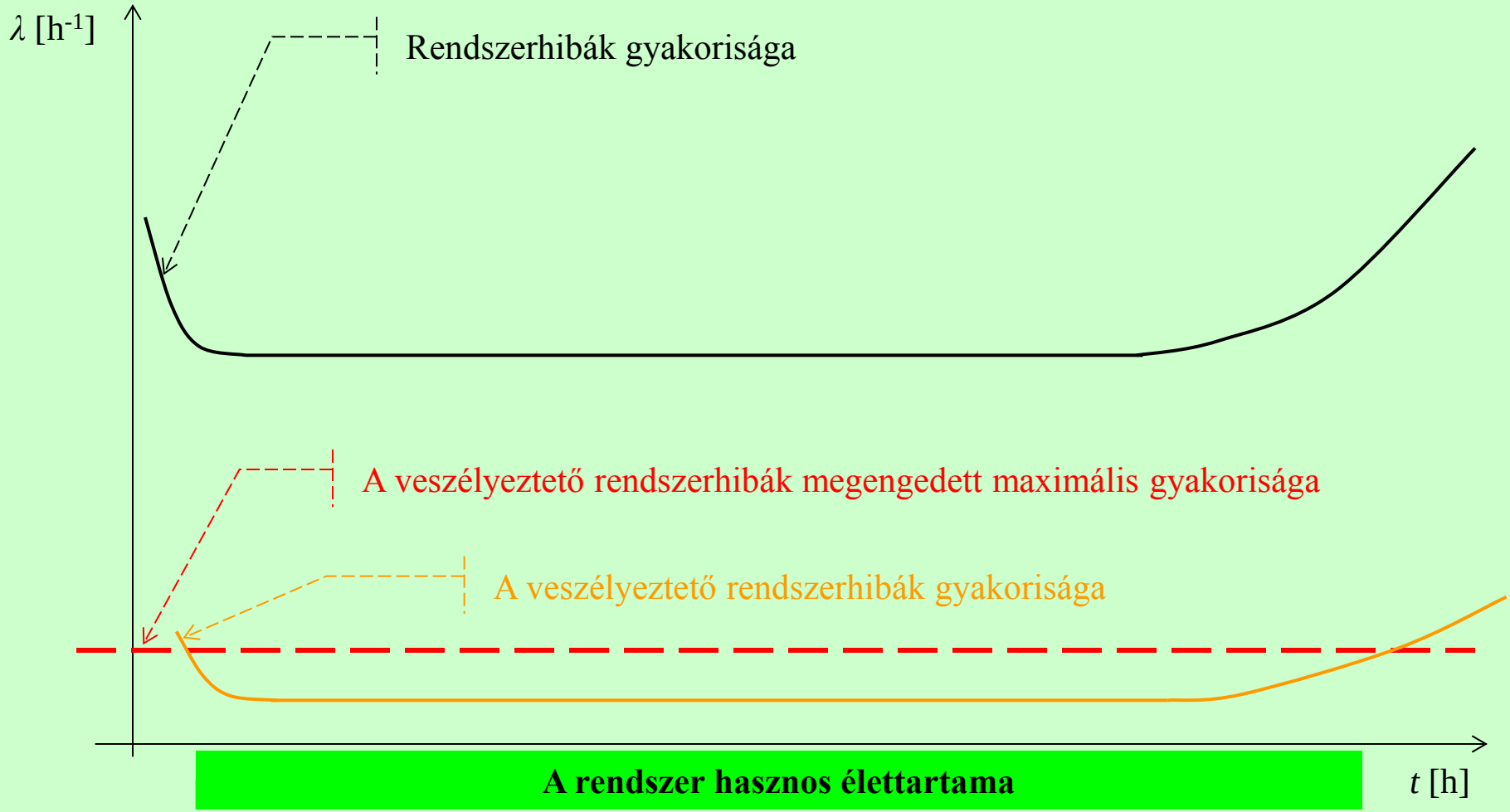
Fiktív összefüggés a rendszer ára és kockázata kozott



Biztosítóberendezés elektromechanikus elemekkel



Biztosítóberendezés elektronikus elemekkel (1)



Biztosítóberendezés elektronikus elemekkel (2)

- **A külsőtéri elemek élettartama (jelzők, váltóhajtóművek, ...)**
  - Elvben a relés rendszerekkel azonos
- **A belsőtéri elemek élettartama (logika)**
  - Relés rendszerek – elvben a kábelezés élettartama korlátozza (szigetelés romlása – csökken a szigetelési ellenállás, rövidzárak)
  - Elektronikus rendszerek – elvben az elemek meghibásodása korlátozza

HW csere

- Majdnem problémamentes, árban nem igényes – standard elemek

SW csere

- A szoftver fizikailag nem használódik el
- A szoftver kompatibilis lesz az új HW-rel (gyors technológiai váltás az elektronikus elemeknél)

Összefoglalás

- **A biztosítóberendezési rendszert az EN 50129 szabvány értelmében folyamatos üzemű rendszernek kell tekinteni, és ezért nemcsak a biztonságintegritási, hanem a készenléti követelményeket is teljesítenie kell.**
- **Az a kockázat, aminek az utas ki van téve, nem lehet nagyobb, mint az általánosan tolerálható kockázat, és nem függhet az alkalmazott műszaki eszközöktől.**
- **A biztosítóberendezés egész hasznos élettartama alatt kell, hogy teljesítse azokat a feltételeket, amelyek alapján fejlesztették és amelyeket figyelembe vettek a berendezés biztonságának értékelésénél.**

Köszönöm a figyelmet!