

Automatika - Közlekedésautomatika 4.

**Logisztikai mérnök MSc szak
Közlekedési mérnök MSc szak**

Biztonsági kérdések

Biztonság fogalma

- *Köznapi értelmezésben* veszélymentességet jelent, a biztonság az ember fontos pszichológiai igénye
- *Műszaki értelmezésben* ez is valószínűségi jellegű számszerű jellemző
- Biztonság különböző értelmezési módjai
 - „safety” értelmében véve,
 - „security” értelmében véve

Biztonság, mint pszichológiai igény (Maslow)



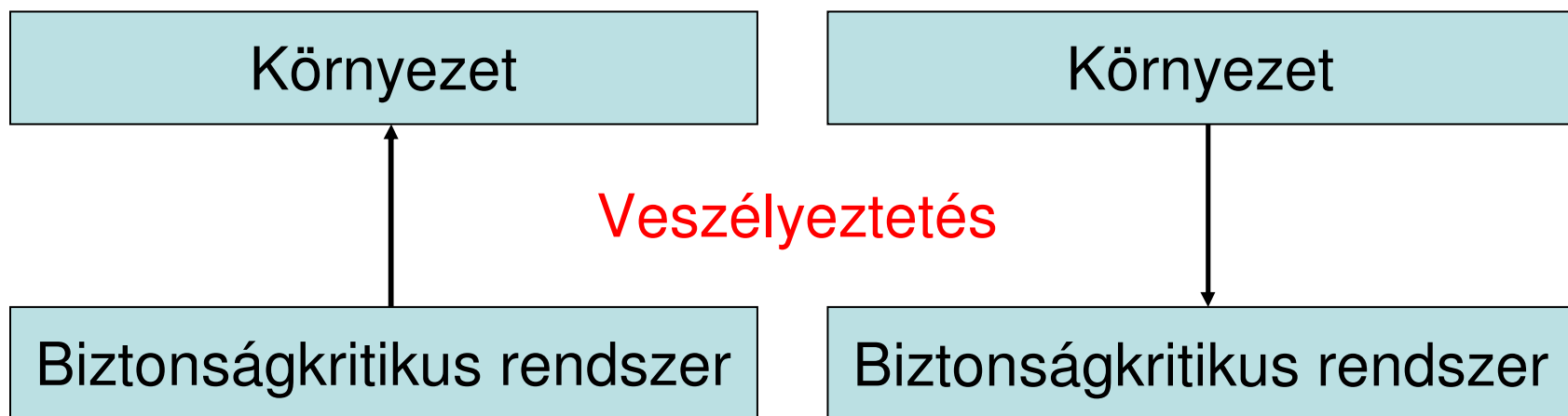
Biztonság értelmezési módjai (1)

(Biztonság safety ill. security értelmében)

- „safety” értelmében vett biztonság: a műszaki rendszerből származóan ne érje veszélyeztetés a környezetet, és az ott lévő embereket
- „security” értelmében vett biztonság: a műszaki rendszert ne érje veszélyeztetés a környezet ill. az ott lévő emberek felől

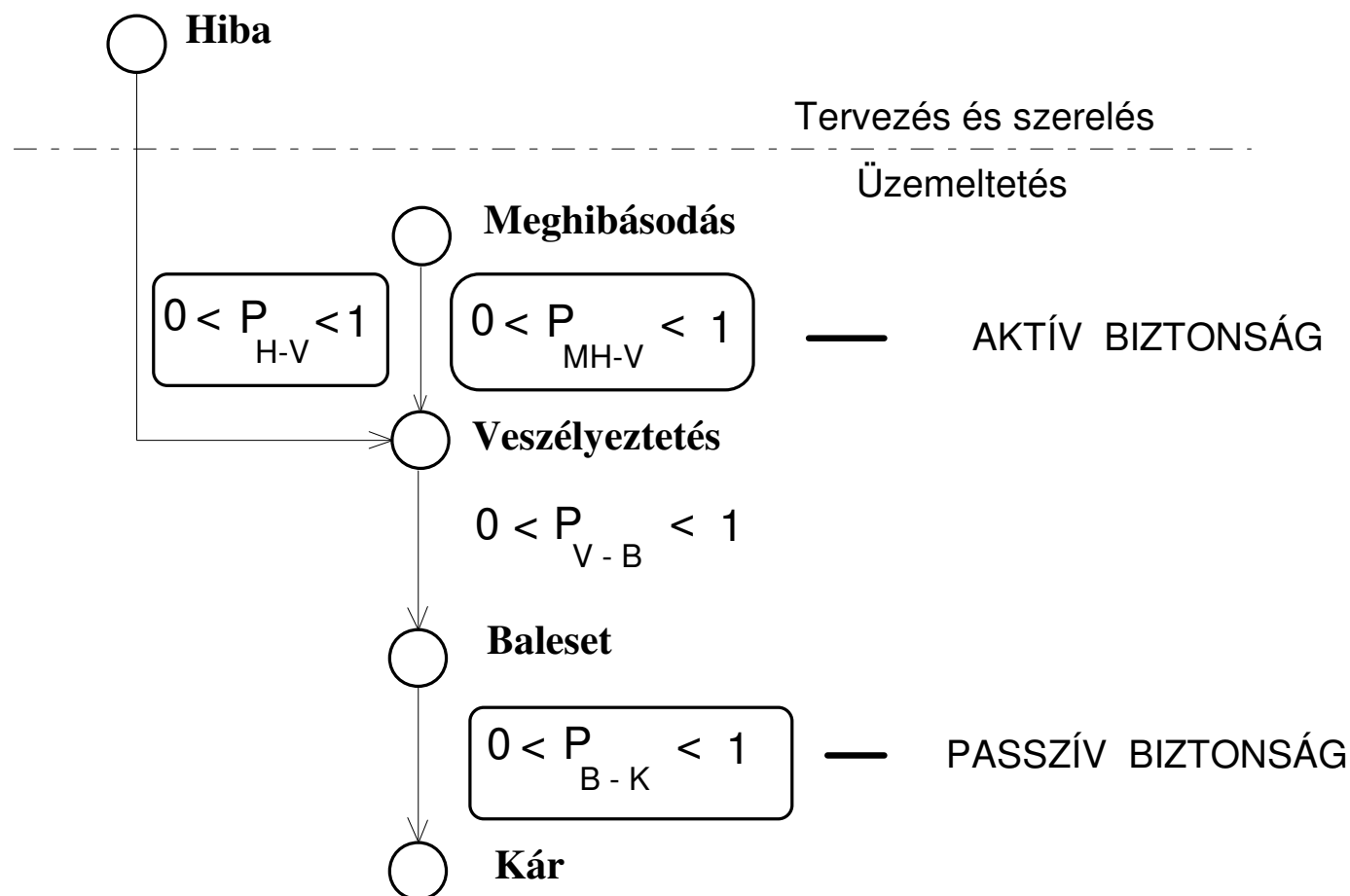
Biztonság értelmezési módjai (2)

(Biztonság safety ill. security értelmében)



Biztonság értelmezési módjai (3)

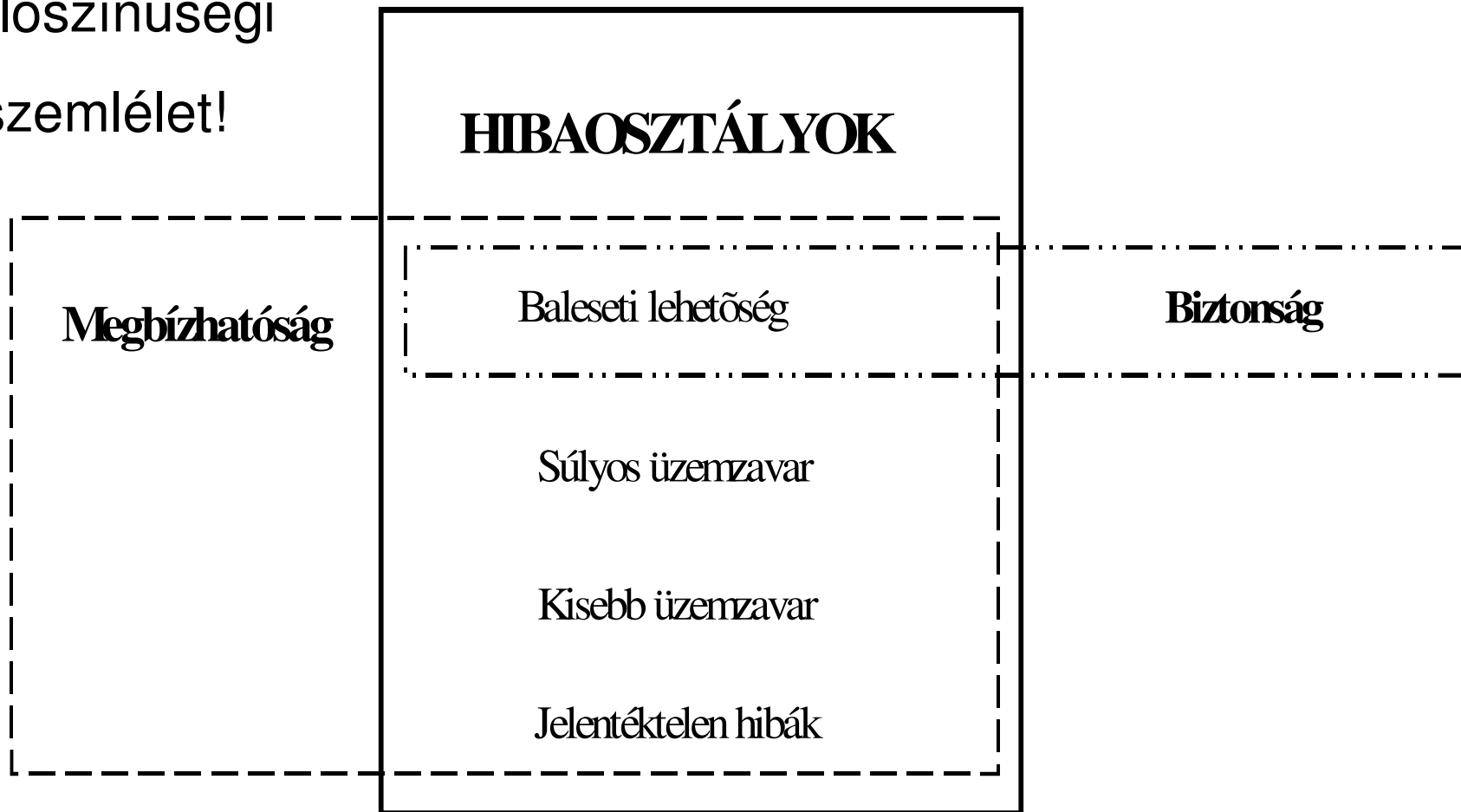
(Aktív és passzív biztonság)



A biztonság és a megbízhatóság fogalmának	
Hasonlósága:	Különbözősége:
Mindkét fogalom hibákkal, meghibásodásokkal kapcsolatos	Megbízhatóság vizsgálatánál valamennyi hibát (akadályozó/veszélyes) figyelembe kell venni
Mindkét fogalom az adott időpontbeli hibátlan állapot valószínűségét jelenti	Biztonság vizsgálatnál csak a veszélyes hibát kell figyelembe venni

A biztonsági és a megbízhatósági vizsgálatok hibaszemlélete

Valószínűségi
szemlélet!



Biztonság valószínűségi jellemzői (1)

- A biztonság számjellemzőinek meghatározása során a meghibásodásoknak csak egy (veszélyeztetést okozó) részét vesszük figyelembe
- Ezek részaránya legyen az i -ik alkatrészre α_i , ennek segítségével tudjuk meghatározni a veszélyes meghibásodásokra vonatkozó λ_{iv} értéket
ahol

$$\lambda_{iv} = \alpha_i \cdot \lambda_i$$

$$0 \leq \alpha_i \leq 1 \quad \text{és} \quad 0 \leq \lambda_{iv} \leq \lambda_i$$

Biztonság valószínűségi jellemzői (2)

- Ezzel a feltételezéssel („hibaredukcióval”) vesszük figyelembe, hogy nem minden meghibásodás okoz veszélyeztetést
- Ennek segítségével a biztonsági rendszereket is állandó meghibásodási rátájú soros rendszereként modellezzük
- A különböző sztochasztikus jellemzőket a megbízhatósági számjellemzőkhöz hasonló módon definiáljuk

Megbízhatósági jellemző		Biztonsági jellemző	
Megbízhatósági függvény	R(t)	Biztonsági függvény	S(t)
Meghibásodási valószínűség	F(t)	Veszélyeztetési valószínűség	G(t)
Meghibásodás sűrűség fgv.e	f(t)	Veszélyeztetés sűrűség fgv.e	g(t)
Meghibásodási ráta	$\lambda(t)$	Veszélyeztetési ráta	$\rho(t)$
Javítási ráta	$\mu(t)$	Biztonság helyreállítási ráta	v(t)
Üzemkésztség	D(t)	Védelem jósága	$V_s(t)$

A biztonsági számjellelmezők és összefüggései (1)

$$S(t) = e^{-\int_0^t \rho(\tau) d\tau}$$

$$G(t) = 1 - S(t) = 1 - e^{-\int_0^t \rho(\tau) d\tau}$$

$$g(t) = \rho(t) \cdot e^{-\int_0^t \rho(\tau) d\tau} = -\frac{dS}{dt} = \frac{dG}{dt}$$

A biztonsági számjellemzők és összefüggéseik (2)

$$\rho(t) = \frac{g(t)}{\int_t^{\infty} g(\tau) d\tau} = -\frac{1}{S(t)} \cdot \frac{ds}{dt} = \frac{1}{1-G(t)} \cdot \frac{dG}{dt}$$

$$V_s(t) = \sum_i P_i(t) = 1 - P\{x_v(t) = 1\}$$

$$V_s(t \rightarrow \infty) = \frac{v}{\rho + v} = \frac{MTBD}{MTBD + MTTSR}$$

A biztonsági számjellemzők és összefüggéseik (3)

- Ez utóbbi képletben az élettartam paraméterek elnevezése:
 - MTBD = Mean Time Between Danger
 - MTTSR = Mean Time To Safety Repair
- Az összefüggések teljesen azonos módon alakulnak, mint a megbízhatóságnál láttuk
- Itt is igaz, hogy a négy alapjellemzőből egy ismeretében az összes többi meghatározható

A biztonság kockázatalapú meghatározása

- Kockázat = „rizikó” $\Rightarrow$ „rhiza” (görög szó: „zátony”, a görög hajósok kockázata!)
- Kockázat fogalma: a nyereség vagy veszteség lehetőségét tartalmazza
- Valamely műszaki folyamattal vagy állapottal összefüggő kockázat szintén valószínűségi kijelentéssel írható le

Kockázati tényezők (1)

- A kockázattal kapcsolatos valószínűségi tényezők:
 - a kárhoz vezető esemény fellépésének **várható gyakorisága**,
 - és az esemény fellépésekor bekövetkező **kár nagysága**.

Kockázati tényezők (2)

- Mai civilizáció kockázati tényezői:
 - géntechnika,
 - atomerőművek,
 - közlekedés,
 - rák stb.
- Technika kettős szerepe:
 - segít kizárni a veszélyeztetéseket,
 - maga is veszélyforrást jelent.

Kockázat értelmezési módjai (1)

- Kockázat, mint biztosítási kifejezés:
kiváltó esemény és vele kapcsolatos kár valószínűsége
- Kockázat, mint műszaki kifejezés:
annak a várakozásnak a mértéke, hogy emberi vagy műszaki hibából kár következhet be

Kockázat értelmezési módjai (2)

- Egyéni kockázat: annak a valószínűsége, hogy egy személy meghatározott esemény miatt előre meghatározott károsodást szenved (pl. gépkocsivezető halálos balesete)
- Kollektív kockázat: fenti valószínűség személyek meghatározott csoportjára

Kockázat számszerűsítése (1)

$$R = p_E \cdot K$$

ahol: K - a kár nagysága

p_E - a kár bekövetkezésének
valószínűsége (gyakorisága)

- Az összefüggés alapján szokás kockázati hiperboláról beszélni, amely az azonos R kockázatot jelentő pontokat köti össze egy K - p_E diagramban

Kockázat számszerűsítése (2)

- A számszerű meghatározás ellenére itt azért csupán minőségi definícióról van szó: általában nem adható meg, hogy milyen függvénykapcsolatban van a két befolyásoló paraméter
- Pontos mennyiségi meghatározás helyett általában csak a két paraméterre vonatkozó kategóriákban adható meg az összefüggés:
- Adott kockázat adódhat (kockázati „izo-görbe”):
 - nagyon ritkán bekövetkező nagyon nagy kár,
 - „gyakran” bekövetkező „csekély” kár és
 - nagyon gyakran bekövetkező nagyon kis kár esetén

Kockázat értékelésének módja

- Értékelés a kár nagyságának és bekövetkezési valószínűségének (gyakoriságának) kategorizálásával történhet
- Kár elszenvedésének valószínűsége függ a veszélyeztetésnek való kitétel mértékétől
- Lehetséges kockázati kategóriák:
 - R1 - elhanyagolható kockázat
 - R2 - elfogadható kockázat
 - R3 - nem kívánatos kockázat
 - R4 - elfogadhatatlan kockázat

Kár nagyságának meghatározása (1)

- A kár értékelése a különböző területeken eltérő lehet
 - a gazdasági világban az anyagi kárt,
 - nagy technológiák, munkavédelem területén az emberéletben esett kárt,
 - informatikában az adatokban bekövetkezett kárt jelentheti.
- A kár nagyságát általában valamilyen természetes mértékegységben adják meg:

Kár nagyságának meghatározása (2)

- Anyagi kár esetén: pénzben fejezhető ki a kár nagysága
- Ember életben okozott kár esetén:
 - halálesetek száma,
 - súlyos sérülések száma,
 - könnyű sérülések száma;
- Adatokban esett kár esetén az adatállomány mérete (pl. MByte)

Kár nagyságának meghatározása (3)

- Az ember életben okozott kár esetében szokás az egyszerűség érdekében ún. ekvivalens kárnagysággal számolni
 - 10 (vagy 20) könnyű sérülés ekvivalens lehet 1 súlyos sérüléssel,
 - 10 súlyos sérülés ekvivalens lehet 1 halálesettel
- Fentiek alapján átszámolva a károkat szokás csak halálesetekkel megadni a kockázat nagyságát

Emberéletben esett kár nagyságának kategóriái

Kár		Kockázati kategória	
jellege	nagysága	neve	jele
haláleset	több	katasztrofális	K4
	egy	kritikus	K3
súlyos sérülés	több		
	egy	csekély	K2
könnyű sérülés	több		
	egy	jelentéktelen	K1

Gyakorisági szint kategóriái (p_E)

Gyakorisági szint			
<i>jele</i>	<i>neve</i>	<i>leírása</i>	<i>nagyság</i> $\left[\frac{1}{6}\right]$
A	gyakori	állandó veszélyeztetés	$> 10^{-3}$
B	valószínű	gyakori veszélyeztetés	$10^{-3} \dots 10^{-4}$
C	esetleges	többszöri veszélyeztetés	$10^{-4} \dots 10^{-5}$
D	csekély	legalább egyszeri veszélyeztetés	$10^{-5} \dots 10^{-7}$
E	valószínűtlen	veszélyeztetés kivételes esetben	$10^{-7} \dots 10^{-9}$
F	hihetetlen	veszélyeztetés nem várható	$< 10^{-9}$

A lehetséges kockázati kategóriák (ún. kockázati mátrix)

Valószínűségi szint	Kárkihatási kategóriák			
	Jelentéktelen	Csekély	Kritikus	Katasztrofális
Gyakori	nem kívánatos	elfogadhatatlan	elfogadhatatlan	elfogadhatatlan
Valószínű	elfogadható	nem kívánatos	elfogadhatatlan	elfogadhatatlan
Esetleges	elfogadható	nem kívánatos	nem kívánatos	elfogadhatatlan
Csekély	elhanyagolható	elfogadható	nem kívánatos	nem kívánatos
Valószínűtlen	elhanyagolható	elhanyagolható	elfogadható	elfogadható
Hihetetlen	elhanyagolható	elhanyagolható	elhanyagolható	elhanyagolható

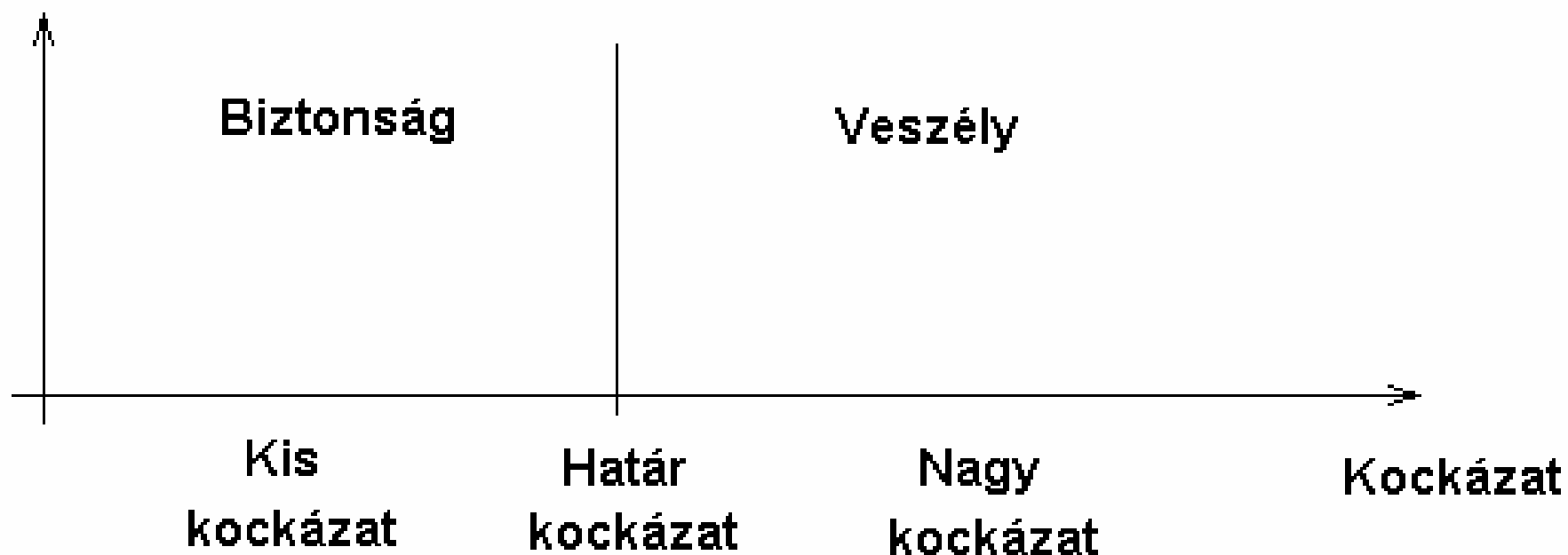
Kockázati mátrix

- A kockázati mátrix jó lehetőség a potenciális kár nagyság és bekövetkezési gyakoriság grafikus ábrázolására
- Felépítése a vizsgált szakterületektől függően változhat (fenti 4/6/4 mellett 3/5/5 ill. 3/4/4 elrendezésű mátrix alkalmazása is előfordul)
(A jelölésben szereplő számok az R, p_E és K nagyságára vonatkozó kategóriák számát jelenti)

Kockázatalapú biztonság (1)

- Kockázat fogalom alapján meghatározható egy ún. **határkockázat**, ami alatt valamely műszaki folyamattal vagy állapottal kapcsolatos még elviselhető maximális kockázatot értjük
- Biztonság teljesül, ha a kockázat a határkockázat alatt van, egyébként veszélyeztetés áll fenn (l. ábra)

Kockázatalapú biztonság (2)



A biztonság definíciójából következő tények

- abszolút (100%-os) biztonság nem érhető el!
(=teljesen kockázatmentes állapot)
- valamely műszaki rendszernél a szükséges biztonsági szint függ az emberek kockázattűrésétől,
- a megfelelő biztonsági szint mindig csak meghatározott környezeti feltételek között érhető el:
 - hőmérséklet,
 - nedvességtartalom,
 - mechanikus rezgés,
 - elektromágneses mezők, stb.

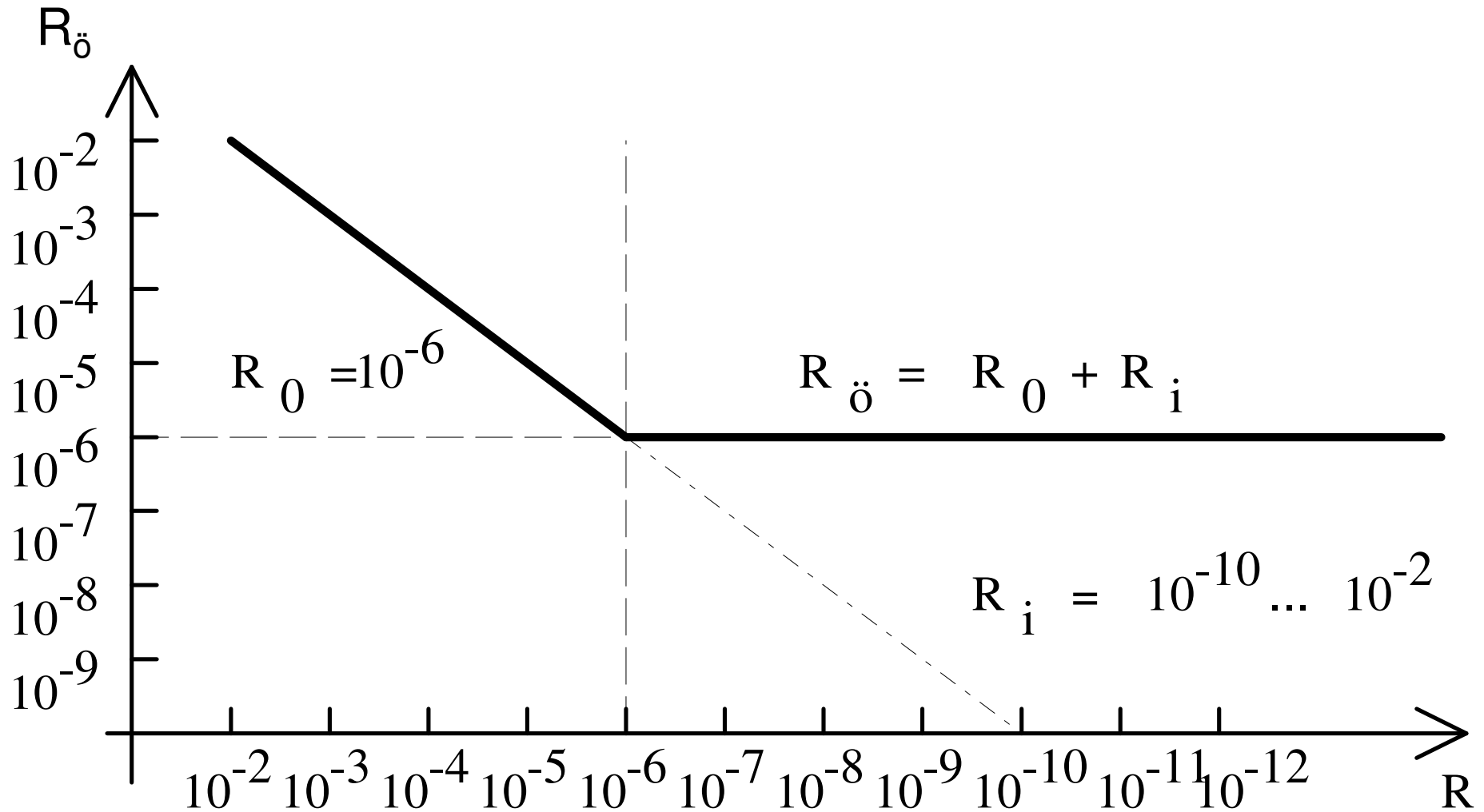
Az éleettel kapcsolatos kockázat

- Az élet teljes kockázata $R_{\ddot{o}} = R_0 + R_i$
- A pótlólagos kockázatok származhatnak
 - foglalkozásból,
 - közlekedésből,
 - közvetlen és tágabb környezetből, stb.
- Az R_0 alapkockázat az, ami nem változtatható, és mindenképpen jelentkezik az összkockázatban - ez a domináns tényező!

Az éleettel kapcsolatos kockázat (folyt.)

- A pótlólagos kockázat a statisztikák szerint
 - az alapkockázat értékétől felfelé és lefelé egyaránt nagy mértékben eltérhet,
 - ha nagyobb az alapkockázatnál, akkor általában ez a domináns
 - esetenként lehet az élet alapkockázatánál lényegesen kisebb értékű is $\Rightarrow$ de ez nem javítja észrevehetően az összkockázat szintjét
- Az új műszaki megoldásoknál nincs értelme a pótlólagos kockázat értékét jelentősen az alapkockázati szint alá vinni

Az élet alapkövázata



A kockázattűrés meghatározása

- A kockázattűrés nagysága társadalom-pszichológiai tényezőktől függ
- Tapasztalatok szerint nincs szoros összefüggésben az adott folyamat objektív veszélyességével
- A korábban megismert veszélypotenciálsor megítélése nagy mértékben függ szubjektív tényezőktől is

Veszélypotenciál szubjektív megítélése

Férfi alkalmazottak			
Női alkalmazottak			
Statisztika			
Élvezeti szerek	→ 1	3	1
Egyéni közlekedés	→ 2	2	2
Tömegközlekedés	→ 3	4	4
Atomerőmű	→ 4	1	3

A kockázattűrés jelentősége

- A kockázattűrés társadalmilag elfogadott mértéke nem marad csupán kötetlen formában megadott számérték, hanem a törvényadó testületeken keresztül minőségi és mennyiségi **biztonsági előírásokban** ölt testet (atomerőművekre vonatkozó törvény, CENELEC szabványok a vasúti közlekedés biztonságára vonatkozóan, stb.)

A kockázattűrés szokásos értékei (1)

- Az élet alapkockázata statisztikák szerint:

$$w_A = 10^{-6} \left[\frac{\text{haláleset}}{\text{fő} \cdot \text{óra}} \right]$$

- Kockázattűrés saját felelősség esetén:

$$w_{\text{saját}} = 10^2 \cdot w_A = 10^{-4} \left[\frac{\text{haláleset}}{\text{fő} \cdot \text{óra}} \right]$$

A kockázattűrés szokásos értékei (2)

- Kockázattűrés túlnyomóan saját felelősség esetén:

$$w_{\text{saját/idegen}} = w_A = 10^{-6} \left[\frac{\text{haláleset}}{\text{fő} \cdot \text{óra}} \right]$$

- Kockázattűrés túlnyomóan idegen felelősség esetén:

$$w_{\text{idegen/saját}} = 10^{-1} \cdot w_A = 10^{-7} \left[\frac{\text{haláleset}}{\text{fő} \cdot \text{óra}} \right]$$

A kockázattűrés szokásos értékei (3)

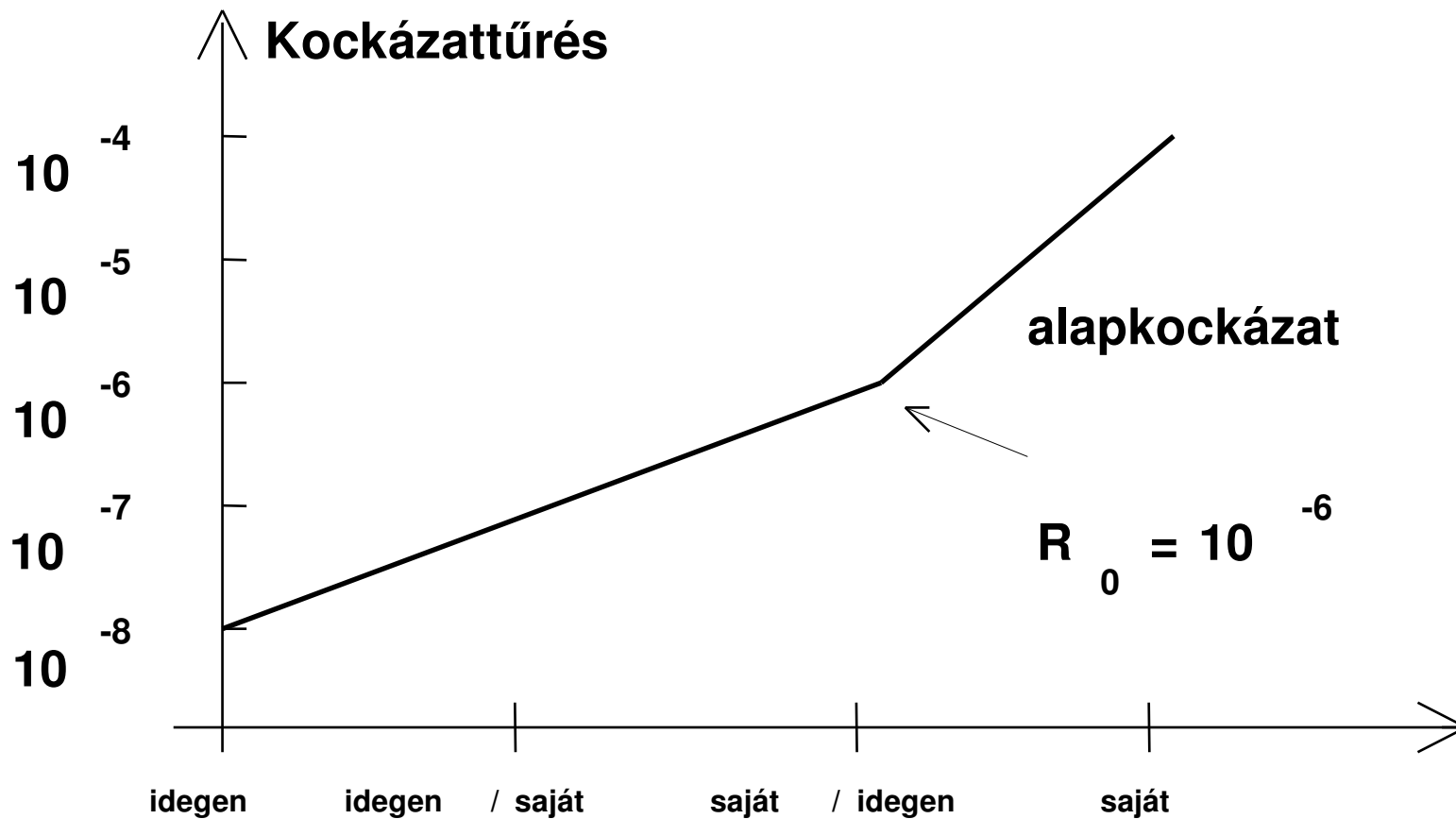
- Kockázattűrés kizárólag idegen felelősség esetén:

$$w_{\text{idegen}} = 10^{-2} \cdot w_A = 10^{-8} \left[\frac{\text{halott}}{\text{fő} \cdot \text{óra}} \right]$$

- Figyelemre méltó, hogy
a kockázattűrés teljes tartománya 4
nagyságrendet fog át $10^{-4} \dots 10^{-8}$ között!

NB.: A számértékek csak durva közelítő
értékeknek tekinthetők

A kockázattűrési nagysága



A kockázattűrés nagyságát befolyásoló tényezők

- A kockázatnak kitett csoport nagyságával fordított az összefüggés - kisebb érintett csoport esetén nagyobb a megtűrt kockázati szint
- A kockázatvállalás gazdasági haszna is befolyásolja az elfogadható szintet:
 - a haszon nagysága,
 - a haszon jelentkezésének időpontja (közvetlen vagy későbbi időpontban)

Az automatizálható folyamat jellemzői (1)

- a folyamat **veszélyessége**: baleseti statisztikák alapján különböző ipari és közlekedési területekre (ún. veszélypotenciál sor, megítélése gyakran szubjektív!)

Az automatizálható folyamat jellemzői (2)

- Veszélypotenciál sor – baleseti statisztikai adatok alapján rangsorolva közli a különböző biztonságkritikus rendszereket:
 - Háztartási berendezések
 - Gépi működtetésű kapuk
 - Nagyfeszültségű kapcsolók
 - Gépjármű
 - Orvosi készülékek
 - Emelő szerkezetek
 - Mozdólépcsők

- Veszélypotenciál sor (folytatás)
 - Tüzelő berendezések
 - Daruk
 - Drótkötélpálya
 - Közúti jelzőlámpák
 - Felvonók
 - gőzkazánok
 - Vasúti biztosítóberendezések
 - Olajfúró szigetek
 - Repülőgépek
 - Kémiai reaktorok
 - Atomreaktorok
 - Stb.

Az automatizálendő folyamat jellemzői (3)

- a folyamatban lehetséges **biztonságos állapotok száma** – az üzemszerű állapot jól megtervezett rendszernél mindig biztonságos, fontos kérdés, hogy meghibásodás esetére **van-e biztonságos tartalékállapot?**
- az **ember szerepe** a folyamatban (ember elválasztható-e a veszélyforrástól?).

Biztonsági automatika rendszerek (1)

- A folyamat automatizálásának biztonságfilozófiáját alapvetően a folyamat fenti biztonsági jegyei határozzák meg.
- Ha a rendszernek nincs biztonságos tartalék-állapota (safe life technológia), akkor a meghibásodásokat nagy valószínűséggel ki kell zárni

Biztonsági automatika rendszerek (2)

- Ha a rendszernek van biztonságosan elérhető tartalékállapota (ún. fail-safe technológia), akkor a meghibásodás esetén törekedni kell e tartalék állapot elérésére

Biztonsági automatika rendszerek (3)

Az automatikák biztonságos kialakítását eldöntő kérdések:

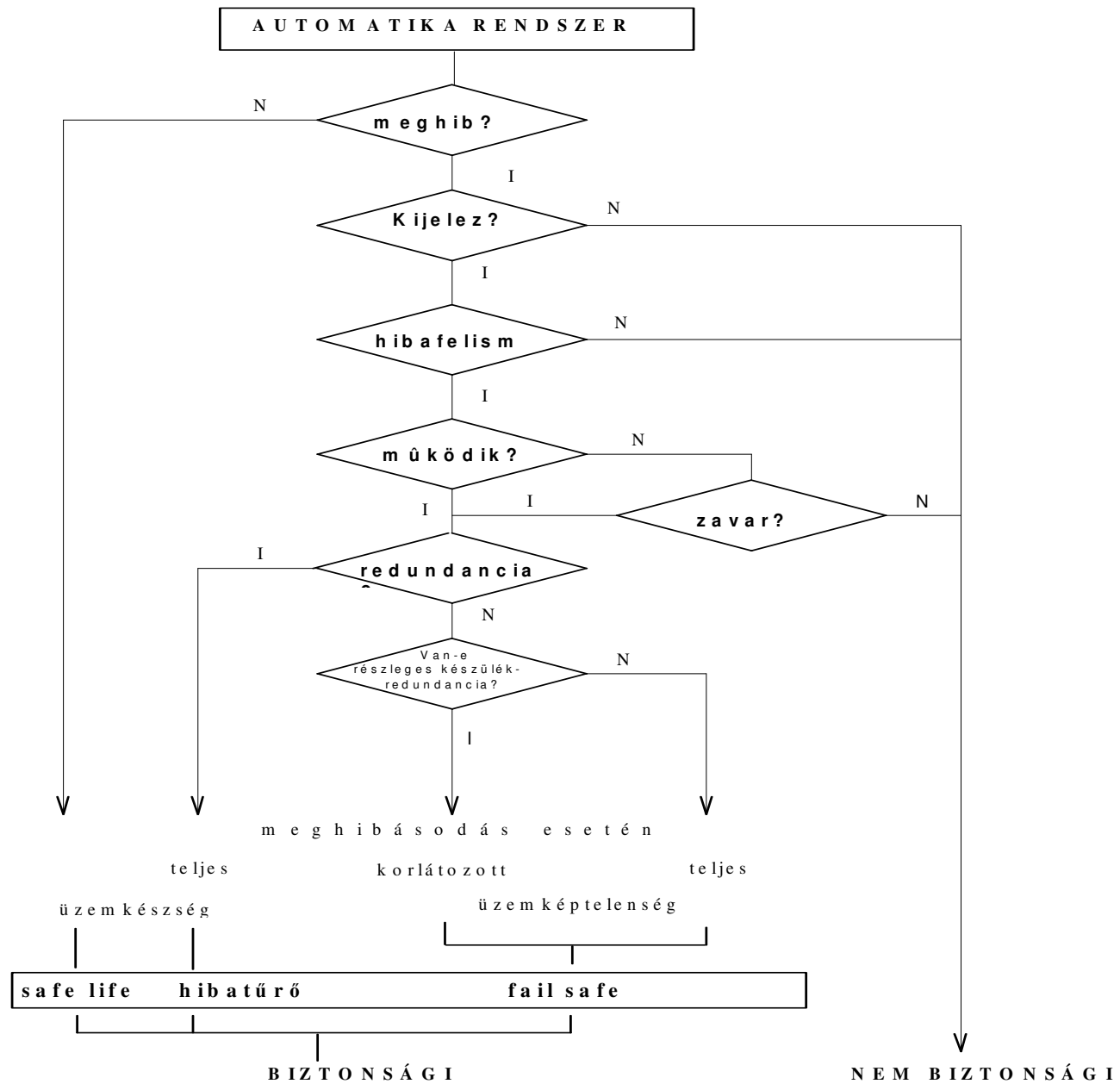
- Kell-e a rendszerelemek **meghibásodásával** számolni?
- Hiba esetén van-e megfelelő **hibafelismerési mechanizmus** a hibák érzékelésére?
- Ha igen, az **kijelzi-e** a fellépett hibákat (azok legalább zavarként jelentkeznek-e?)
- Van-e a meghibásodok esetére **redundancia** a rendszerben?

Biztonsági automatika rendszerek (4)

- Fenti kérdésekre adott különböző válaszok alapján megkülönböztethető biztonsági automatika rendszerek:
safe life, fault tolerant és a fail-safe rendszer!
- Definíciók:
 - **safe life** (=„*hibamentes*”) **rendszer** - az engedélyezett üzemidőn belül nem kell meghibásodással számolni (rendszeres felülvizsgálatot igényel),

Biztonsági automatika rendszerek (5)

- **fault tolerant** (=„*hibatűrő*”) **rendszer** - kell számolni meghibásodással, azt a hibafelismerő mechanizmus felismeri, vagy zavarként kijelzi, teljes készülék-redundancia meghibásodás esetére is teljes üzemkésztséget garantál
- **fail safe** (=„*hibabiztos*”) **rendszer** - mint előbb, de nincs, vagy csak részleges készülék-redundancia van, emiatt meghibásodás esetén részleges vagy teljes üzemképtelenséggel kell számolni



Au

Műszaki

54

RAM(S) fogalma

- A megbízhatóság tágabb értelemben felöleli a
 - Megbízhatóság (**R**eliability)
 - Üzemkésztség (**A**vailability)
 - Karbantarthatóság (**M**aintainability)
 - Biztonság (**S**afety)területét (utóbbi általában csak biztonságkritikus rendszerek esetén)

A megbízhatóság értelmezése

- Megbízhatóság minőségi szempontból is értelmezhető
- Műszaki rendszerek megítéléséhez szükséges a mennyiségi számjellemzők ismerete
- Megbízhatóság szűkebb értelemben a működőképességet jelenti
- Tágabb értelemben a teljes RAM(S) teljesítmény

Megbízhatósági számjellemezők

- A legfontosabb megbízhatósági jellemzők
 - Megbízhatósági függvény $R(t)$
 - Meghibásodási függvény $F(t)$
 - Meghibásodási tényező $\lambda(t)$
 - Várható élettartam MTTF
- Elektronikus alkatrészekenél a meghibásodási tényező általában állandó értékű, meghibásodási rátaaként értelmezhető

Meghibásodási ráta

- A $\lambda(t) = \lambda$ feltétel teljesülésének okai
 - Korai meghibásodások szakaszát a gyártó cég minőségbiztosítási rendszere garantálja
 - Öregedési fázist a elektronikus rendszerek általában nem érik el (nem tartalmaznak mozgó alkatrészt)
- A biztonságkritikus rendszereknél szükséges redundáns architektúrák esetén ez elektronikus alkatrészek esetén sem teljesül

Karbantarthatóság (M)

- Nem az üzembe helyezés valószínűségét, hanem inkább a peremfeltételek teljeskörű figyelembevételét jelenti
- Ezek a feltételek:
 - Fenntartó személyzet szakértelem,
 - Szükséges szerszámok, eszközök,
 - Tartalék alkatrészek meghatározása, ellátás

Üzemkésztség (A)

- Ez is valószínűség-jellegű mennyiség, a függvény hosszabb idő után egy stacioner értékhez tart (K – tartós üzemkésztség)
- A K érték egyszerű javítható rendszer esetén az ismert módon:

$$K = \frac{MTBF}{MTBF + MTTR}$$

A RAM területek kapcsolata

- Az üzemkésztség tekinthető a megbízhatóság és karbantartás közötti összekötő fogalomnak
- A fenti képletben szereplő idő-jellemzők
 - MTBF – a hibák közötti jó működés ideje
 - MTTR – a javításhoz szükséges idő, szokták helyette az
 - MDT (Mean Down Time) értéket is használni

Megbízhatóság-menedzsment szükségessége (1)

- Gazdaságos eredmények megkövetelik a megfelelő megbízhatóságot
- A biztonságkritikus automatikák területén a szükségesség eltérően jelentkezik

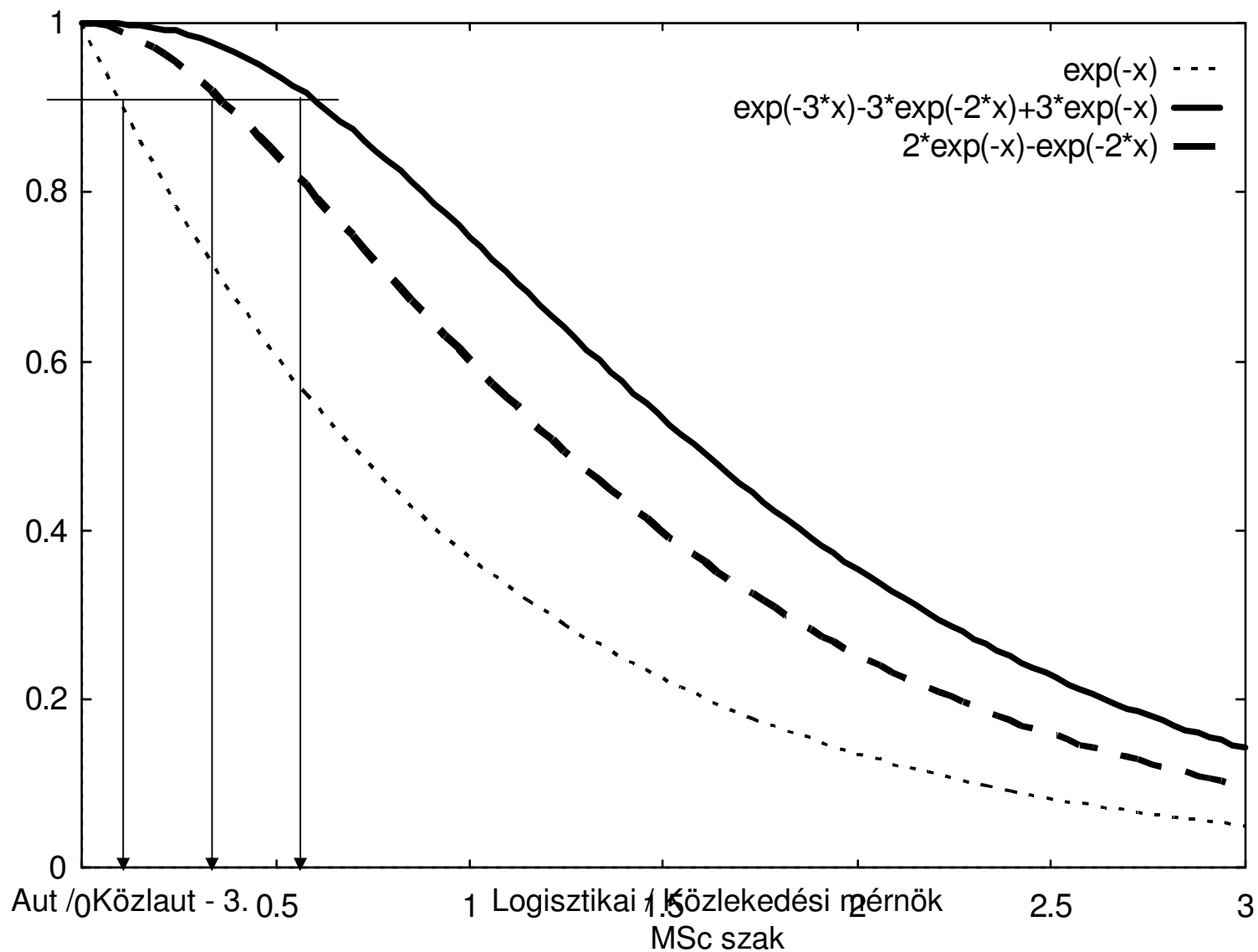
Megbízhatóság-menedzsment szükségessége (2)

- Safe-life rendszereknél már régen alkalmazzák – a megengedett kockázati szinthez kellett a megbízhatóságot illeszteni
- Fail-safe rendszereknél csak az elektronikus rendszerek megjelenésével vált szükségessé

Hibamentesség értelmezése safe-life rendszereknél (1)

- A maximális kockázathoz (hibavalószínűséghez) meghatározható a megengedett minimális megbízhatóság
- A minimális megbízhatóság megszabja az alkalmazható maximális üzemidőt - ezen belül nem kell meghibásodással számolni
- A következő ábra egyetlen elemre, ill. kétszeres és háromszoros redundanciára mutatja a megfelelő időértékeket

Hibamentesség értelmezése safe-life rendszereknél (2)



A biztonsági folyamat feladatai

- Felhasználó alapvető feladata a ***kockázatelemzés***
- Gyártó feladata a ***veszélyeztetés elemzés***
- Mindkét elemzés feltétlfüzetek formájában jelenik meg - amit a felügyeleti hatóságnak jóvá kell hagyni

A kockázatelemzés részfeladatai (1)

- A kockázatok felmérése - a rendszerrel kapcsolatos funkcionális követelmények meghatározása (műszaki megoldástól függetlenül)
 - Technológiai kérdések tisztázása
 - Üzemi paraméterek meghatározása
 - A rendszer határainak definíciója
- A rendszerrel kapcsolatos alapvető kockázatok (veszélyeztetések) azonosítása (esetleg katalógusba foglalása)

A kockázatelemzés részfeladatai (2)

- Az azonosított veszélyeztetések értékelése, veszélyeztetési ráták becslése
- A veszélyeztetések következményeinek elemzése (baleset, „majdnem baleset”, biztonságos állapot felvétele)
- Az adódó kockázat elfogadhatóságának igazolása (a megfelelő kockázattűrési kritériumok alapján)
- Intézkedési terv összeállítása a kockázatok csökkentésére (kockázatredukció)

A kockázatelemzés részfeladatai (3)

- A kockázatok csökkentésére vonatkozó intézkedések végrehajtása
- Elfogadható veszélyeztetési ráták meghatározása (THR = Tolerable Hazard Rate)
- A kockázatok folyamatos újraszámítása

A kockázat elviselhető mértéke

- az elfogadható kockázat szintjét a CENELEC nem szabja meg - ez inkább a nemzeti vagy európai törvényi előírásoktól függ
- Kockázattűrés mértékének javasolt meghatározási módjai (EN 50126 szerint)
 - ALARP (= As Low As Reasonably Practicable) - Anglia
 - GAMAB (= Globalement Au Moins Aussi Bon) - Franciao.
 - MEM (= Minimum Endogenous Mortality) – Németo.

ALARP (1)

- Alapgondolata a megfizethető biztonság: eljárása a biztonságnövelő ráfordítások és hatások elemzése.
- Az ALARP módszer két szélsőséges kockázati szintet határoz meg
 - tűrhetetlen nagy - amit vagy
 - = csökkenteni kell, vagy
 - = a rendszer nem üzemeltethető.
 - elhanyagolhatóan kis kockázat - nem igényel további intézkedést

ALARP (2)

- A két szélső tartomány közt van az ún. ALARP tartomány: itt a kockázatot az ésszerűen megvalósítható legalacsonyabb szintre kell csökkenteni
 - be kell mutatni, hogy a jelenlegi legjobb szabványokat ill. gyakorlati módszereket alkalmazzák,
 - ha az új szabványok alkalmazása kétséges, akkor ún. költség-haszon elemzés, ill. az „életérték” elv alkalmazható

ALARP (3)

- A kockázat szintje csak akkor fogadható el, ha
 - a kockázat csökkentése megvalósíthatatlan, vagy
 - a kockázat csökkentés költségei aránytalanul nagyobbak a kockázatcsökkentéssel járó haszonnál

Elfogadhatatlan
sáv

"ALARP" - sáv
tűrhetőségi sáv

(Kockázatvállalás
csak a kívánt haszon
elérése esetén)

Messzemenően
elfogadható sáv
(Nincs szükség
tevékenységre az ALARP
bizonyításához)

ALARP (4)

Az ALARP kockázati mátrix

(3 kockázati kategóriával)

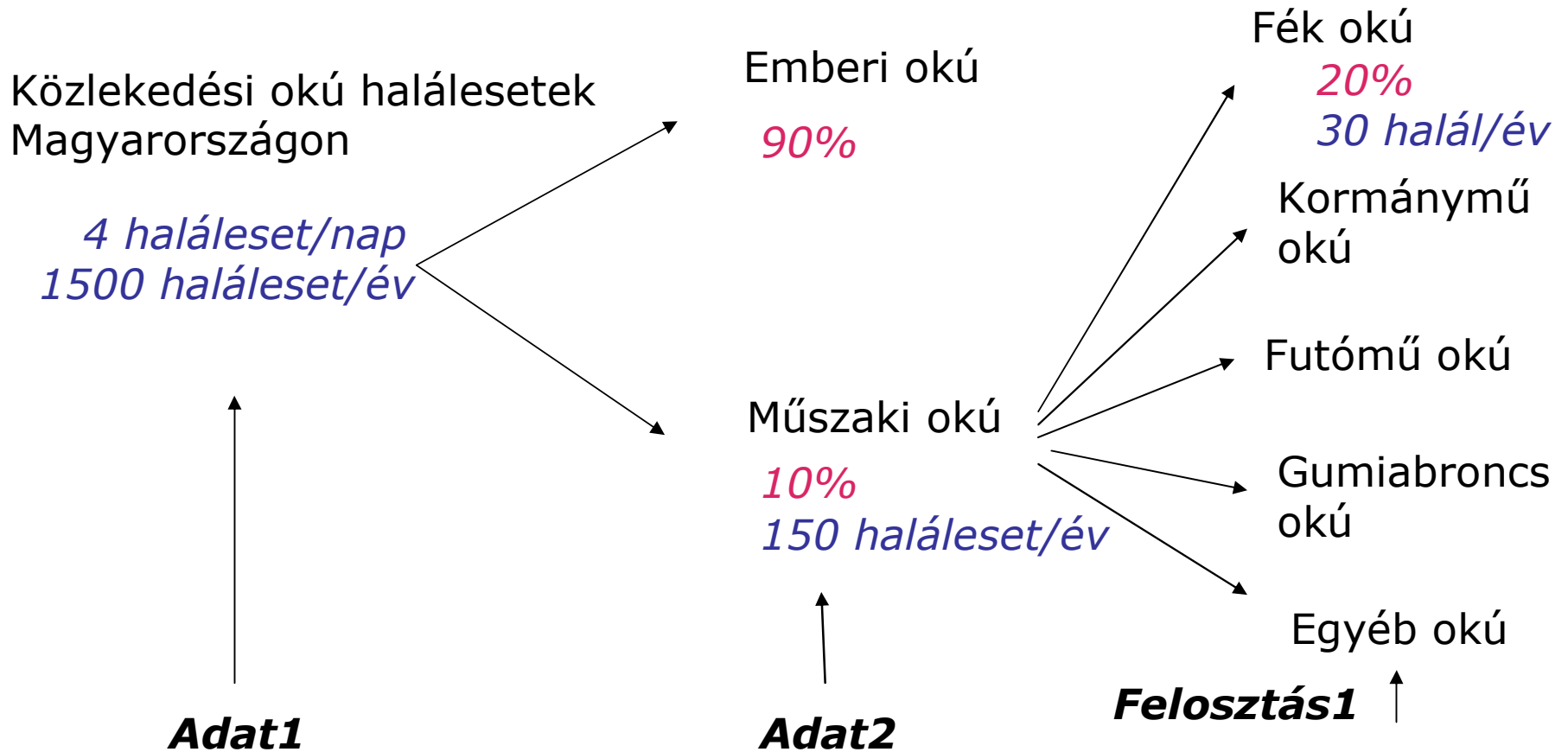
Valószínűségi szint	Kárkihatási kategóriák			
	Jelentéktelen	Csekély	Kritikus	Katasztrofális
Gyakori			Elfogadhatatlan	
Valószínű				
Esetleges			ALARP	
Csekély				
Valószínűtlen	Elfogadható			
Hihetetlen				

GAMAB (= Globalement Au Moins Aussi Bon)

- Minden új rendszernek legalább a meglévő egyenértékű rendszerrel azonos biztonsági szintet kell nyújtania
- Minőségi megfogalmazásként nem mérlegeli a konkrét kockázatot
- Mennyiségi megközelítésben a meglévő rendszer biztonságát egy τ_{cref} hányadossal jellemezhetjük: ez a halálesetek relatív száma, ami meglévő rendszerek statisztikai adataiból határozható meg!

Példa a GAMAB alkalmazására (1)

(BME Szabó Géza példája)



Példa a GAMAB alkalmazására (2)

- A fenti adatok alapján bizonyos feltételezésekkel tudjuk meghatározni a THR értéket
- A halálos áldozatok száma kisebb, mint a baleseteké (Kb. 0,5 haláleset/baleset esetén 60 baleset/év adódik)
- Nem minden fékhiba vezet balesethez - ha kb. minden negyedik fékhiba vezet balesethez, akkor 240 hibaeset/év adódik

Példa a GAMAB alkalmazására (3)

- A gépkocsik napi 2 (évi 730) órás futásteljesítményét feltételezve $\sim 0,33$ hibaeset/üzemóra adódik
- Magyarországon kb. 2 millió személygépkocsit feltételezve fenti adatokkal

$$\text{THR} = 1,65 \cdot 10^{-7} \text{ [hibaeset/üzemóra]}$$

adódik, ami a szabványi besorolás szerint SIL3 biztonsági szintet igényel

MEM - Minimális endogén halálozás elve (1)

- Endogén halálozás azt az R kockázat jelenti, hogy valamely egyén halálát ún. „technológiai körülmények” okozzák:
 - szórakozás, sport, házi tevékenység,
 - munkagépek használata, közlekedés
(betegség, vele született fogyatékoság nem tartozik ide!)
- E kockázat fejlett országokban 5 és 15 év között a legkisebb, ez a minimális érték:

$$R_m = 2 \cdot 10^{-4} \left[\frac{\text{halálos kimenetelű baleset}}{\text{személy} \cdot \text{év}} \right]$$

MEM - Minimális endogén halálozás elve (2)

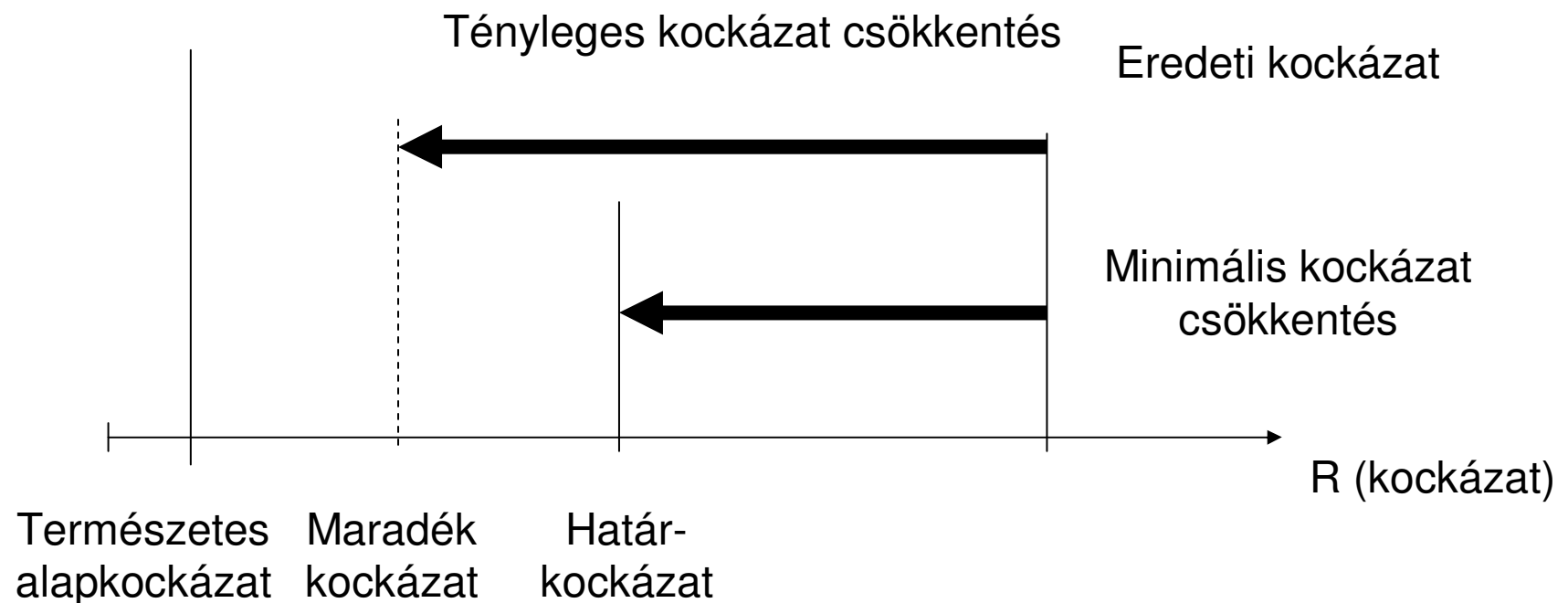
- A MEM által megfogalmazott alapszabály: új rendszer alkalmazásából származó veszélyeztetések nem növelhetik számottevően R_m értékét
- Gyakorlatban használt értékek:
 - $R_1 = 10^{-5}$ [halálos baleset/személy/év]
 - $R_2 = 10^{-4}$ [komoly sérülés/személy/év]
 - $R_3 = 10^{-3}$ [könnyű sérülés/személy/év]
- Nagyszámú halálesetet okozó rendszerek esetén ún. DRA értéket kell meghatározni meg (= Differential Risk Aversion)

A kockázatértékelés módszerei

- kockázati mátrix alkalmazása
- kockázati prioritások alkalmazása (autóiparban, szoftver tervezés területén) az FMEA - FMECA
- kockázati gráfok alkalmazása
- a „Sárga könyv”-ben közölt módszer - az Angliában alkalmazott biztonságmenedzsment eljárása
- ASCAP - a GAMAB amerikai változatának igazolására
- az egyéni kockázat értékelése az EN 50129 szerint

Intézkedések a kockázatok csökkentésére (1)

- A biztonsági szabványokban alkalmazott kockázatfogalmak



Intézkedések a kockázatok csökkentésére (2)

- A kockázat csökkentésére két lehetőség:
 - a kár bekövetkezési valószínűségének csökkentése
 - a bekövetkezett kár nagyságának csökkentése

A veszélyeztetés-elemzés lépései (1)

- rendszerdefiníció
- veszélyeztetések azonosítása
- következmények, veszteségek elemzése
- kockázatértékelés
 - az egyéni kockázat explicit meghatározása,
 - implicit megoldási feltételezések
 - további megoldási feltételezések

A veszélyeztetés-elemzés lépései (2)

- veszélyeztetési okok elemzése
 - a funkció részesedése a veszélyeztetésben - adódik e funkcióra a THR értékek listája,
 - az egyes részrendszerek által realizált funkciók meghatározása - adódik a részrendszerek számára a THR értékek listája
- a közös okra visszavezethető meghibásodások (CCF = Common Cause Failure) elemzése
- a biztonsági követelmény-szintek hozzárendelése (SIL_i)

SIL szintek hozzárendelése

- SIL fokozat: egyensúly a hibák és meghibásodások elleni intézkedések között

THR [1/óra*funkció]	SIL fokozat
$10^{-9} \leq \text{THR} \leq 10^{-8}$	4
$10^{-8} \leq \text{THR} \leq 10^{-7}$	3
$10^{-7} \leq \text{THR} \leq 10^{-6}$	2
$10^{-6} \leq \text{THR} \leq 10^{-5}$	1

Az automatikák kialakításának gazdasági vonatkozása

- Biztonságkritikus rendszerek biztonsági szintjének meghatározásakor nem lehet gazdasági optimumra törekedni,
- Tökéletes biztonság nem érhető el, a rendelkezésre álló anyagi lehetőségek végesek
- Az elegendő biztonsági szint meghatározásához az élet alapkockázata jelentheti az objektív alapot

A biztonságelemzés célkitűzése (1)

- A biztonságelemzés célja annak igazolása, hogy a biztonsági rendszer és az üzemi folyamat esetén a maradék kockázati szint a megengedhető érték alatt marad.
- Az igazolás analitikus módszerrel történik, biztonságkritikus vizsgálatok, tesztek nem tartoznak a biztonságelemzés körébe
- Az elemzés a biztonsági rendszerek által elkerülendő általános kockázatokra vonatkozik

A biztonságelemzés célkitűzése (2)

- A kockázatok felmérése a fejlesztésben részes szakértők bevonásával, ez alapján
 - esetleges biztonsági hiányosságok felfedezhetők, és
 - az ezzel kapcsolatos szakértői döntések meghozhatók
- A fő cél nem az összes kockázat abszolút meghatározása, hanem a biztonsági ráfordítások lehető koncentrálásával megfelelő biztonság elérése

A biztonságázelemzés módszere

- Klasszikus megoldás a megbízhatósági blokkdiagramra alapozott módszer (különböző területeken számos módszert alkalmaznak)
- A megbízhatóság-technika különböző módszerei alkalmazhatók, de azokat a konkrét alkalmazási esethez kell illeszteni