BIZTONSÁGKRITIKUS SZÁMÍTÓGÉP RENDSZEREK

Kritikus rendszer: valamely jellemzőjével szemben a szokásosnál nagyobbak a követelmények

1. Bevezetés

- Számítógépek alkalmazása kritikus területeken
- A biztonság
- Biztonsági rendszerek fejlesztése
- Költség-haszon

SZÁMÍTÓGÉPEK ALKALMAZÁSA KRITIKUS TERÜLETEKEN (1)

- Mikroprocesszor 1970-es évek eleje
- Folyamatos árcsökkenés a számítógép-bázisú technológiánál
- A számítógép-használat drámai növekedése (több gép, mint ember)
- A processzorokat túlnyomórészt nem asztali vagy más hagyományos számítógép formában használják:

  beágyazott rendszerek (embedded systems)
- Spektrum: mosógéptől a korszerű, bonyolult repülőgép-irányításig, az ABS-től a nukleáris erőművek védelmi rendszeréig
- Milliós darabszámban: autóipar, háztartási gépek
- Ipari, közlekedési folyamatirányító rendszerek

SZÁMÍTÓGÉPEK ALKALMAZÁSA KRITIKUS TERÜLETEKEN (2)

- Különbség az általános célú és a beágyazott rendszerek között:
  - a hibás működés várható következményei
- A beágyazott rendszerek hibás működése közvetlen sérülés, környezetkárosodás okozója lehet:
  - atomerőmű
  - repülőgép
  - autó motor- vagy fékvezérlés
  - vasúti közlekedés
- Az ipar módszereket fejlesztett ki a kockázatok megfelelő kezelésére (ezekkel foglalkozunk a későbbiekben)
- Számos esetben (pl. háztartási gépek) a beágyazott rendszer hibájából adódó veszélyeztetés nem annyira nyilvánvaló
- Gyakorlatilag bármely rendszer, amely energiát irányít, képes károkozásra (pl. hiba folytán bekapcsolódva marad egy mosógép vagy kenyérpirító fűtése - tűzeset - halálozás)

A biztonság fogalma

- Egy lehetséges definíció:

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

  A **biztonsági rendszer** olyan rendszer, amelynek révén egy rendszer vagy berendezés biztonsága elérhető

  Safety-related system= safety-critical system
- Terjedelem: mikrokapcsolótól az erőművi védelmi rendszerig
- Feladat lehet:
  - Kifejezetten biztonsági
  - Egyéb feladatok mellett biztonsági is (pl. robotpilóta vagy vasúti bizt. ber.)
- Abszolút biztonság helyett az **alkalmazásnak megfelelő biztonság** elérése
- A megfelelőség megítélése gyakran szubjektív (pl. repüléstől való félelem - az autózás veszélyesebb)

A biztonság - Integritási szintek

- A biztonság megfelelőségének megítélését számos technika segíti
- A hibás működés következményei az egyes alkalmazási területeken rendkívül különbözőek lehetnek
- Az **integritási szintek** tükrözik a helyes működés fontosságát
- Egy projekthez rendelt **biztonsági integritási szint** meghatározza az alkalmazandó fejlesztési, tervezési, gyártási, üzemeltetési módszereket
- Minden rendszerfejlesztéskor meg kell állapítani a biztonsági vonatkozásokat
  - veszélyelemzés
  - kockázatelemzés
- Az előbbiek alapján meg kell határozni az integritási szintet

A biztonság terjedelme

- A biztonsági vonatkozások a rendszer életének valamennyi fázisát érintik, a koncepciótól az üzemen kívül helyezésig
- A HW és a SW integrált szerepe a biztonság elérésében
- Érzékelők, beavatkozók, kábelezés, csatlakozók, tápellátás
- Kezelő és karbantartó személyzet szerepe a biztonságban

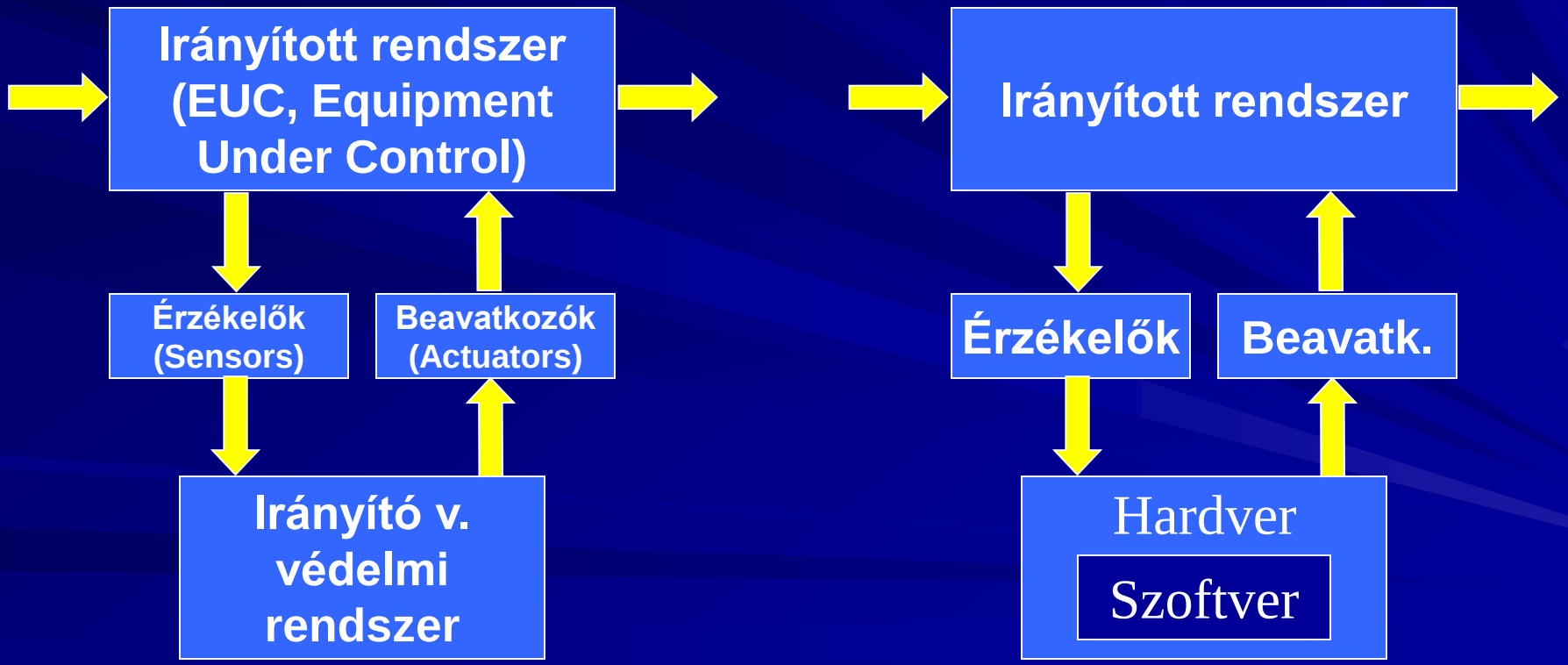
- A biztonság eléréséhez kevés a jó tervezés:
  - Gyártási, szerelési, kezelési, üzemeltetési hibák
- A biztonság és **minőség-menedzsment** kapcsolata
- A biztonsági kérdések érintettjei:
  - A megrendelő, az esetleges független szakértő és a hatóság
  - A tervező és a gyártó
  - A szerelő, a kezelő és a karbantartó (üzemeltető)
  - A lakosság mint egy káresemény elszenvedője

Számítógépek biztonsági vonatkozásai

- A rendszerek **elsődleges biztonsága** (a HW által okozott közvetlen veszélyeztetés, pl. villamos áramütés, tűz)
- **Funkcionális biztonság** (HW és SW korrekt működése a folyamatirányításban) - ezzel foglalkozunk
- **Indirekt biztonság** (pl. számítógép-hiba közvetett hatása egy biztonsági információs rendszerre)
- A fejlesztéshez használt HW és SW eszközök (tool-ok) helyes működésének fontossága a biztonság szempontjából

Biztonsági rendszerek fajtái

- Irányító rendszerek (control systems) - Védelmi rendszerek (protection system
- PES - Programmable Electronic System
- PLC - Programmable Logic Controller
- Nem mindenhez kell számítógép - elég lehet egy termosztát



Számítógépek a biztonsági rendszerekben (1)

- A számítógépes rendszerek előnyei
  - Nagy teljesítmény (sok be-/kimenet kezelése, gyors számítás), kis fogyasztás, kis helyigény
    - olyan komplex feladatok is megoldhatók, amelyek hagyományosan nem
  - Extrém megbízhatóság (nagy integráltság, kevés alkatrész, kevés összeköttetés)
  - Flexibilitás (SW változtatás, HW marad)
    - Viszonylag olcsó módosítás
  - A legtöbb esetben alacsonyabb létesítési költség, mint a hagyományosnál - különösen igaz nagy komplexitásnál (kis volumenű projekteknél a fejlesztési, különösen a SW költségek dominálnak!)
  - A nagy teljesítmény lehetővé teszi bonyolult stratégiák alkalmazását is
    - Öndiagnosztikai rutinok futtatása
    - Feltételek meglétének, tartományok határainak figyelése, ellenőrzése
    - Összetett, komplikált függőségek megvalósítása.

Számítógépek a biztonsági rendszerekben (2)

- A számítógépes rendszerek hátrányai
  - A legfontosabb éppen a lényegéből adódó nagy **komplexitás**
    - VLSI - elemek százezrei, rendkívül komplex viselkedés
    - A szoftver nem kevésbé komplex - még egy viszonylag egyszerű programnak is lehet több ezer végrehajtási útvonala
    - A komplex rendszereket nehezebb tervezni, valószínűbb a tervezési hiba
    - Nehezebb tesztelni is, valószínűleg több detektálatlan hiba marad bennük
    - Nehezebben áttekinthetők és érthetők, ezért könnyebb elkövetni installációs vagy üzemeltetési hibát
  - Lehetséges **meghibásodási módjainak száma** (VLSI) rendkívül nagy (praktikusan végtelen)
    - Kimerítő tesztelés és teljes körű hibadetektálás lehetetlen (v.ö. diszkrét elemek)
    - A SW tesztelhetősége legalább annyira problematikus (v.ö. A SW egyre nagyobb szerepével a biztonsági rendszerekben)

Hibaok, hiba, rendszer-meghibásodás

- **Hibaok** - fault
  - valamilyen hiányosság a rendszerben (HW - SW, tervezés)
  - **Véletlenszerű** (csak HW) - rendszerviselkedés megjóslása
  - **Szisztematikus** (HW: specifikációs, fejlesztési stb., az összes SW)
    - Nem véletlenszerű - a rendszerviselkedés nehezen jósolható
  - **Tartós**
  - **Átmeneti** - hatása lehet tartós
- **Hiba** - error
  - A hibaok aktiválódik, **megjelenik** (HW - SW)
  - A rendszer vagy egy alrendszer kívánt működéstől való eltérése
- **Rendszer-meghibásodás** – system failure
  - A rendszer nem hajtja végre a megkövetelt funkciókat
  - **Biztonságkritikus rendszerek**: a hiba lehetőleg ne okozzon rendszer-meghibásodást
- **Hibamentes rendszerek**
  - Tökéletes fejlesztés nem érhető el
  - A rendszer HW-elemei működés közben meghibásodhatnak

Biztonságkritikus rendszerek - hiba-menedzselés

- Nem-kritikus rendszerek - a jó teljesítményhez általában elegendő:
  - Jó fejlesztés/tervezés
  - Jó minőségű elemek
- Kritikus rendszerek - kiegészítő intézkedések szükségesek a hibák uralásához
  - A hibaokok **elkerülése** - megelőzés a fejlesztésben
  - A hibaokok **eltávolítása** - HW és SW tesztelési technikák, üzembe helyezés előtt
  - A hibák **detektálása** - üzem közben, a hibák hatásának mérséklésére
  - **Hibatűrés** - a rendszert úgy alakítják ki, hogy a benne jelenlévő hiba ellenére is megfelelően működjön
- Hibamenedzselési technikák kombinációja
  - Önmagában egyik technika sem tökéletesen hatékony
  - A rendszer-meghibásodások kívánt/elfogadható szintjének elérése

Költség - Haszon (1)

- A biztonság drága
- Kompromisszumot kell találni a biztonság és a költségek között
- Tapasztalat:
  - A megfelelő biztonság elérését célzó szisztematikus eljárások költsége alacsonyabb, mint a bekövetkezett baleset következményeinek helyreállítása
- Mennyi az emberi élet vagy a szenvedés pénzbeli értéke?
- Sebességcsökkentés - balesetcsökkenés
  - Készek vagyunk elfogadni a nagyobb eljutási időt és az utak zsúfoltságának növelését emberéletek megmentéséért?
- A biztonság növelésének árát megfizetik-e a felhasználók?
- A biztonság mekkora foka fogadható el?

Költség - Haszon (2)

- Mekkora biztonsági ráfordítások fogadhatók el?
  - Gyártó/üzemeltető
  - Vevő/utas
- Bizonyos kockázatok speciális esetekben elfogadhatók az emberiség egészének vagy egy ország népének érdekében
- Hol a határ? Mekkora kockázat fogadható el? Mekkora haszonnal kell hogy ez járjon?
- Ki viseli a kockázatot és kié a haszon?
  - Befolyásolja az elfogadható kockázati szintet (pl. nagy sebesség versenypályán vagy országúton)
- Válasz: Veszély- és kockázatelemzés

Jogi vonatkozások

- A gyártó, illetve az üzemeltető felelős az okozott kárért
- A biztonság növelhető, de nem lehet abszolút
  - viszont számos olyan technika van, amellyel növelhetjük bizalmunkat a rendszer biztonságában
- A felelősség megállapításának anyagi következményei igen nagyok lehetnek
- A gyártónak védenie kell magát
  - Megfelelő gondossággal kell eljárni a termék kialakításakor
  - Megfelelő figyelmeztetésekkel a felelősséget a használóra lehet hárítani (részben)
  - Biztosítás - igen költséges lehet
- A rendszer olyan biztonságos, amennyire az ésszerűen elvárható - „state of the art”
  - Demonstrálni kell az alkalmazott fejlesztési, tervezési technikákat
  - A szabványoknak, irányelveknek való megfelelőség
  - Eltérés esetén igen nehéz a helyesség bizonyítása
- A tervező kötelezettsége
  - A tervező, a vállalat többi dolgozójával együtt felelős az általa fejlesztett/tervezett termékért (szakmai, társadalmi, morális stb. felelősség)

2. Biztonsági kritériumok

- Bevezetés
- Rendszer követelmények
- Biztonsági követelmények
- Biztonságigazolás

Bevezetés

- Követelményrendszer
  - A megrendelő követelményeinek egyértelmű megfogalmazása
  - Funkcionális követelmények
  - Nem-funkcionális követelmények (méret, karbantarthatóság, költségek stb.)
- Biztonsági rendszernél: biztonsági követelmények rendszere
  - Mit követelünk a rendszertől a megfelelő biztonság érdekében
  - Részben funkcionális követelmények:
    - Mit kell tenni (pl. a veszélyforrás aktivitásakor a biztonsági kapu zárva legyen)
    - Mit nem szabad tenni (pl. nyitott biztonsági kapunál a veszélyforrást ne lehessen aktiválni)
  - Egyéb fontos követelmények (általános rendszerjellemzők), pl.:
    - Megbízhatóság (működőképesség, rendelkezésreállás, karbantarthatóság)
    - Fail-safe működés
    - Rendszerintegritás, adatintegritás
    - A rendszer helyreállíthatósága

Rendszer követelmények (1)

- Az egyes követelmények fontossága alkalmazásfüggő
- Megbízhatóság - Dependability: RAMS
  - a rendszernek az a tulajdonsága, amely lehetővé teszi a rendszer szolgáltatása iránti bizalmat
- Működőképesség (túlélési valószínűség) - Reliability
  - annak a valószínűsége, hogy egy rendszer meghibásodása csak az adott időpont után következik be - a megelőző időszakra vonatkozik
    - A rendszer a megfigyelési időpont elején működőképes volt
    - Az adott időpontban is specifikációjának megfelelően működik
    - Közben sem hajtottak végre rajta javítást
  - Igen fontos a tervezett működési időtartam - alkalmazásfüggő
    - Ha a javítás igen költséges vagy lehetetlen - hosszú működési idő
      - Kommunikációs műholdak
      - Űrrobotok
      - Pacemaker-ek
    - Speciális, „küldetéses” katonai alkalmazásoknál elegendő lehet néhány perc/óra is
  - Különleges jelentőségű a működőképesség olyan alkalmazásoknál, ahol a biztonság alapvetően a működőképességen alapul, pl.
    - Repülés-kritikus rendszerek

Rendszer követelmények (2)

- Rendelkezésreállás - Availability
  - annak a valószínűsége, hogy egy rendszer az adott időpontban működőképes - szintén időfüggő, de időpontra vonatkozik
  - Időszakra vonatkoztatott értéke átlagérték (MTBF, MTTR)
  - A magas rendelkezésreállás általános célkitűzés, nemcsak biztonsági rendszereknél, pl. az inaktív idő bevételkiesést jelent
    - Időosztásos számítógép rendszerek
    - Banki rendszerek
    - Telefonközpontok
  - Ilyen rendszereknél ez még fontosabb lehet, mint a nagy túlélési valószínűség, ha **gyorsan javíthatóak**
  - Biztonságkritikus rendszereknél egyértelműen nagy a jelentősége
    - Értéke közel 100% kell legyen
    - Ezért gyakran inkább a **rendelkezésre nem állás** értékét adják meg
    - Különösen a **nem folyamatos üzeműeknél**, pl. atomerőmű védelmi rendszerénél nagy a jelentősége, inkább, mint a túlélési valószínűségé

Rendszer követelmények (3)

- Karbantarthatóság - Maintainability
  - annak a valószínűsége, hogy egy meghibásodott rendszert az adott időpontra ismét üzembe helyeznek
  - Megelőző karbantartás: megtartja a rendszer tervezett működési feltételeit
  - Javító karbantartás: visszaállítja a rendszer tervezett működési feltételeit
  - MTTR igen fontos biztonságkritikus rendszereknél
  - A karbantartás módja alkalmazásfüggő
    - Működés közben (pl. 2x(2v2) vagy más tartalékolt rendszernél)
    - Rövididejű leállással (kártyacsere nem tartalékolt rendszernél)
    - Üzemszünetben (pl. repülőgép, más járművek szervizben)
  - A **karbantartással indukált** hibák
    - Nem minden javítás sikeres (SW is!!!)
    - Új, az előbbitől független hiba kerül a rendszerbe (SW is!!!)

Rendszer követelmények (4)

- Fail-safe működés
  - Biztonságos kimeneti állapottal rendelkező rendszerek hiba esetén ebbe az állapotukba kerülnek, és ezt maguktól nem (csak megfelelő javítás, újbóli indítás után) hagyhatják el
  - Pl. vasúti biztosítóberendezés: minden jelző vörös lesz, a váltók korábbi állapotukban rögzítve maradnak, a vonatok megállnak.
  - Sok rendszer nem rendelkezik ilyen biztonsági állapottal
    - Pl. fly-by-wire rendszer számítógépének nincs biztonságos kimeneti állapota - a repülőgép számára ilyen csak a földön van!
- Rendszerintegritás (eredeti, a jelenleg alkalmazottól eltérő jelentés!)
  - A rendszer képessége arra, hogy működése közben detektálja a hibákat, és értesítse erről a kezelőt (pl. autopilot meghibásodás)
  - E vonatkozásban a hibadetektálás fontosabb, mint a hibatűrés
  - Különösen fontos a fail-safe rendszereknél
- Az integritás tágabb értelmezései - közel a „dependability”-hez
  - Nagy integritású rendszerek
  - Biztonsági integritási szint

Rendszer követelmények (5)

- Adatintegritás - a rendszer képessége
  - Adatbázisa sérülésének megelőzésére
  - A fellépő hibák detektálására, lehetőleg javítására
  - Nem biztonsági rendszernél is fontos lehet (banki, biztosítási rendszer, ahol az adat sokba kerül, értékes)
- A rendszer helyreállíthatósága
  - A hibatűrésre való tervezés ellenére felléphetnek rendszerhibák, leállások
  - Tranziens jelenségek is okozhatják, pl.
    - közeli villámlás
    - Áramellátási „tüske”
  - Gyors, automatikus újraindítás
    - különösen fontos, ha nincs fail-safe állapot
  - Alkalmazásfüggően szükséges lehet
    - A rendszer aktuális állapotának meghatározása
    - Megfelelő újraindítási eljárás végrehajtása, inicializálás
    - A biztonság fenntartása

A rendszer követelmények konfliktusa

- Hagyományos követelmény-konfliktusok
  - Nagy teljesítmény - alacsony ár
  - Méret - funkcionalitás
- Követelmény-konfliktusok fail-safe biztonsági rendszernél
  - Biztonság - működőképesség
  - Biztonság - rendelkezésreállás
- A konfliktus feloldása
  - Kompromisszum a biztonság és a funkcionalitás között (alkalmazásfüggő)
  - Mind a biztonság, mind a funkcionalitás szükséges mértékét a veszély- és kockázatelemzés alapján kell meghatározni

3. Veszélyelemzés

- Bevezetés
- Elemzési módszerek
- Hibamód és -hatás elemzés
- Veszély- és működőképesség elemzés
- Hibafa elemzés
- Veszélyelemzés a fejlesztési életciklusban

Biztonsági követelmények meghatározása (1)

1. A rendszerhez kapcsolódó potenciális veszélyeztetések meghatározása
   - Milyen módon tud ártani a rendszer?
2. Az előbbi veszélyeztetések osztályozása - Kockázat
   - A veszélyeztetésből adódó baleset következményeinek súlyossága
   - A veszélyeztetés fellépésének gyakorisága
3. A veszélyeztetések kezelésének (menedzselésének meghatározása)
4. A megfelelő biztonsági követelmények hozzárendelése
   - megbízhatóság, rendelkezésre állás, fail-safe működés stb.
5. A biztonságintegritási szint meghatározása (SIL)
6. A SIL-hez tartozó fejlesztési módszerek specifikálása

Biztonsági követelmények meghatározása (2)

- A veszélyeztetések meghatározása
  - A rendszerek kimenetük révén tudnak kárt okozni
  - Minden potenciálisan veszélyeztető kimenethez meg kell határozni, milyen módon árthat a rendszer
  - Azt, hogy egy rendszer milyen módon árthat környezetének, veszélyeztetésnek nevezzük.
    - a veszélyeztetés súlyossága: milyen súlyos sérülés lehet a következménye
    - a veszélyeztetés természete: fontos ahhoz, hogy kezeljük

Biztonsági követelmények meghatározása (2a)

- A veszélyeztetés természetének kérdései
  - A veszélyeztetés gyakran teljesen a rendszer közvetlen hatása
    - pl. lézerfény ki/bekapcsolás
  - A veszélyeztetés néha abból adódik, hogy az irányított jellemző csak késéssel követi az irányító jelet
    - pl. energiatárolós esetek - feltöltött kondenzátor, jármű mozgási energiája stb.

    → függőségek!!!
  - Lehet, hogy a veszélyforrásra az irányító rendszernek nincs közvetlen hatása
    - pl. közúti csomópont jelzőlámpáinak a járművek és a gyalogosok viselkedésére)

    → figyelmeztető rendszerek az emberek távoltartására, amíg a veszély el nem múlik (pl. gyalogoslámpa, gázérzékelő/-kijelző)
  - Az irányítórendszer meghibásodásából adódó veszélyeztetés - különösen, ha fail-safe állapot nem lehetséges (pl. repülés) - csak a működőképesség megtartásával előzhető meg – követelmények
- A veszélyeztetések kockázatának elemzése
  - ld. később

Elemzési módszerek

Egyes módszerek ágazat-specifikusak, mások teljesen általánosan használatosak. A **leggyakoribb** veszélyelemző módszerek:

- Hibamód és -hatás elemzés - failure modes and effects analysis (FMEA)
- Hibamód, -hatás és kritikusság elemzés - failure modes, effects and criticality analysis (FMECA)
- Veszély- és működőképesség elemzés - Hazard and operability studies (HAZOP)
- Eseményfa elemzés - event tree analysis (ETA)
- Hibafa elemzés - fault tree analysis (FTA)

Hibamód és -hatás elemzés (FMEA)

- Az elemzés végrehajtható
  - Hardver elemekre vagy
  - Funkciókra vonatkoztatva
- Feltevésekkel él az elemek/funkciók lehetséges hibamódjairól, majd meghatározza ezek hatását
  - az adott egységre és
  - a teljes rendszerre
- Ennek során figyelembe veszi a rendszer valamennyi elemének/funkciójának valamennyi lehetséges hibamódját
- Esetenként javaslatot tesz a talált problémák orvoslására.

Hibamód és -hatás elemzés (FMEA)

Potential
Failure Mode and Effects Analysis
(Design FMEA)

___System
___Subsystem
_X_Component: Connector System
Model Year/Vehicle(s): / 42 VOLT SYS
Core Team: Refer to workgroup list

Design Responsibility: Workgroup
Key Date: October 2000

Item / Function	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s)/ Mechanism(s) Failure	Occur	Current Design Controls	Detec	R.P.N.
- handles rated electrical current with maximum voltage drop of (50mV), for up to xxx sec. over and ambient temperature range of -40C to 80C. Voltage drop spec. referenced to end-of-conditioning status, including Meet stds.for underhood environment (corrosion resistance) Must withstand SAEJ537 spec.for vibration Must satisfy thermal cycling spec.	Excessive voltage drop	Overheating Reduced voltage to loads	8		decreased normal force		end-of-line check test		
					partially backed-out connector				
					partially backed-out terminal				
					loss of asparities(terminal interface)				
					Environmental conditions				
					material properties				
	system not electrically connected	open circuit	7		excessive mating force				
					broken connector latch				
					inadequate connector latch				
	terminal not connected	open circuit	7		terminal partially seated				
					damaged terminal				
					improper terminal orientation				
					excessive mating force				
maintains mechanical integrity	doesn't support cable load	open, short, or intermittent circuit, or overheating			inadequate material selection(housing or terminal)				
					inadequate strain relief				
	unmated connectors	Open circuit overheating Reduced voltage to loads			partially backed-out connector				
					partially backed-out terminal				

Printed on: 2000_03_01 12:47:35

Design FMEA

Revision 6.0 2/11/98

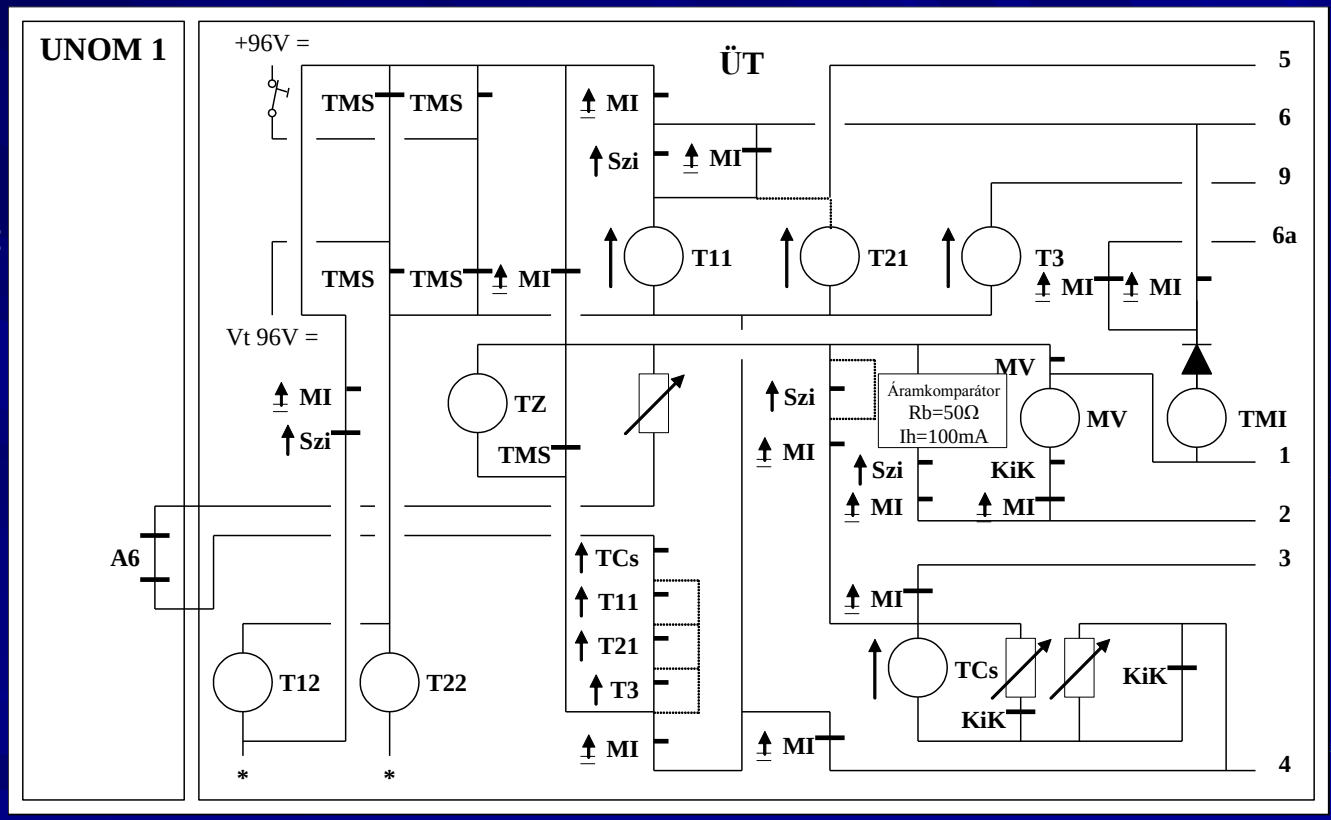
☐ System ☐ Subsystem ☑ Component	**Customer** Chrysler Motors Corporation		**Customer Part No.** DC-77323-XYZ	**Org. Date** 2/11/98	**Page** 1 of 2
	Supplier Any Company, Inc.	**Code** ACI-001	**Supplier Part No.** A-9514	**Dwg. Rev.** 8	**Key Date** 2/11/98	**FMEA No.** DFMEA-001
Part Name Filter			**Design Responsibility** Brad Anderson	**Application/Model Year** Sedan / 1998		
Core Team Brad Anderson,Jerry Benware,Lisa Brown,Ken Caracci,Bill Cox,Fred Jordan,Ken Kratz			**Prepared By** Brad A. Anderson		**Date** 2/11/98	

Item / Function	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s) / Mechanisms of Failure	Occur	Current Design Controls	Detec	R.P.N.	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	Sev	Occ	Det	R.P.N.
Filter for assembly with B44 to firewall	Insufficient wax coverage over specified surface	Deteriorated life of door leading to: Unsatisfactory appearance due to rust through paint over time, Impaired function of interior door hardware	4	◇	Insufficient wax thickness specified	4	Supplier certification	1	16	None	N/A 2/11/98					
					Inappropriate wax specified	5	set up set up	4	80							
							Five piece setup, in-process, end of run study	2	40	None	N/A 2/11/98					
	Corroded interior lower door panels	Improper oxide coating	6	⛉	Entrapped air prevents wax from entering corner/edge access	6	Test spray pattern at startup and after idle periods, and ...	5	180	Add team evaluation using production spray equipment and specified wax	Engineering and Assembly Operations 2/18/98	Based on test reults (Test #9989) spray head modified to ...	6	2	5	60
				⛉	Spray heads clogged: Viscosity too high, Temperature too low, Pressure too low	4	Incomming audit per 200-16 certification, SPC Lot/Qtr	2	48							
							Laboratory test using "worst case" wax and application hole size	3	72	Add laboratory accelerated corrosion testing	ABC Labs 2/27/98	Test results show specified ...	6	3	3	54
										Conduct DOE on wax thickness	Engineering Associates 2/18/98	DOE shows 25% variation in specified thickness is acceptable	6	2	2	24
					Feeder not properly or	3										

	Approved By Brad A. Anderson	**Date** 2/11/98

FMEA - biztonságigazoláshoz

- jelfogók:
  - érintkező nemzárása,
  - jelfogó el nem ejtése,
  - jelfogó meg nem húzása,
- diódák:
  - rövidzár,
  - szakadás,
- ellenállások, potenciométerek:
  - szakadás,
  - ellenállásnövekedés,
  - rövidzár (csak fémrétegnél),
- kondenzátorok:
  - rövidzár,
  - szakadás,
  - kapacitáscsökkenés,
- kismegszakítók:
  - szakadás,
- belsőtéri rendszerkábelek:
  - érszakadás,
- szekrény belső huzalozás:
  - szakadás,
- vezetőpálya a NYÁK-lapon (kártya vagy backpanel):
  - szakadás.



FMEA bizt. ig.

Jelfogó neve	**Kártya**
Térközjelzők Megállj! segédjelfogó (TMS)	ÜT1-S

Érintkező	**Nemzárás következménye**
II.5/6	a térközjelzők Megállj!-ra kapcsolt állapotában antivalenciahiba a SIMIS-IS bemenetén, zavarjelzés a kezelőfelületen
I.5/6	a Térközjelzők Megállj! kezelés hatástalan
II.3/4	a vonali hurok áramkör nem épül fel, a Térközjelzők Megállj! kezelés hatástalan
I.3/4	a vonali hurok áramkör nem épül fel, a Térközjelzők Megállj! kezelés hatástalan
II.1/2	a vonali hurok áramkör nem épül fel, hamisfoglaltság-visszajelentések a térközből, vonat nem indítható, menetirány nem fordítható
I.1/2	a vonali hurok áramkör nem épül fel, hamisfoglaltság-visszajelentések a térközből, vonat nem indítható, menetirány nem fordítható

El nem ejtés következménye	kijárat esetén a térközjelzők szándékolatlanul Megállj! állásban maradnak
Meg nem húzás következménye	a Térközjelzők Megállj! kezelés hatástalan

Az FMEA alkalmazása

- A fejlesztési folyamat legkülönbözőbb fázisaiban alkalmazható
- Az életciklus korai fázisában, funkciókra alkalmazva, a SIL meghatározásában játszhat szerepet
- A rendszer kialakításának jóval későbbi fázisaiban már hardver elemekre is alkalmazható → biztonságigazolás
- Kiválóan alkalmas az egyes szinteken az elemzés finomítására
  - Motorhiba hatása a repülőgépre
  - Üzemanyag-szivattyú hibájának hatása a motorra
  - szelephiba hatása az üzemanyag-szivattyúra
- Az analízis kiegészíthető valószínűségi információval is
- Gyakran „szállít” bemenő adatokat az FTA számára

Az FMEA értékelése

- Mivel a módszer minden lehetséges hibát figyelembe vesz, különösen alkalmas az **egyszeres hibák detektálási feltételeinek** meghatározására
- Ugyanakkor **nem** veszi figyelembe a többszörös hibákat
- Mivel minden hibát figyelembe vesz, igen sok ráfordítást igényelnek azok a hibák, amelyek nem okoznak veszélyeztetést
- Nagy, komplex rendszerek esetén rendkívül ráfordítás-igényes
- Ezért sok esetben csak a fejlesztési folyamat végső fázisaiban, és csak a kritikus területek vizsgálatára alkalmazzák

Hibamód, -hatás és kritikusság elemzés (FMECA)

- A FMEA kiterjesztése
- Figyelembe veszi az elemek meghibásodásainak fontosságát is:
  - az egyes hibák következményeit és
  - fellépésének gyakoriságát vagy valószínűségét
- Ezzel meghatározza a rendszer azon részeit, amelyekben a hibák a leginkább kritikusak
- Ezáltal lehetővé teszi, hogy az erőfeszítéseket arra a területre irányítsák, ahol azokra a legnagyobb szükség van

Veszély- és működőképesség elemzés (HAZOP)

- Eredetileg vegyipari, ma már széleskörű alkalmazás
- „Guide words” - „Mi történik, ha …” típusú kérdésekre adott válaszokkal igyekszik meghatározni a normál működési feltételektől való eltérések hatásait, pl.:
  - Mi történik, ha megnő a hőmérséklet?
  - Mi történik, ha csökken a nyomás?
- Különösen alkalmas a paraméterváltozások és az előírt tartományokból való kilépések (out-of-range) biztonságra gyakorolt hatásának vizsgálatára
- Elemző team - jártasság
  - A fejlesztési módszerekben
  - Az adott alkalmazási területen
  - A HAZOP és más veszélyelemzési technikák területén
- Rendkívül munka- és időigényes

Vezérszavak (guide words)

Vezérszó (guide word)		JELENTÉS
ANGOL	**MAGYAR**	
NO	Nincs	Tervezési célok teljes elmaradása
LESS	Kevesebb, kisebb	Mennyiségi csökkenés
MORE	Több, nagyobb	Mennyiségi növekedés
PART OF	Részben	Minőségi csökkenés
AS WELL AS	Még	Minőségi növekedés
REVERSE	Fordított	Tervezési célok fordítottja
OTHER THAN	Más mint	Teljes helyettesítés
LATER THAN	Később	Szakaszos folyamatban később
SOONER THAN	Előbb	… előbb
TOO QUICKLY	Túl gyorsan	…előírtnál gyorsabban
TOO SLOWLY	Túl lassan	… előírtnál lasabban

HAZOP példa

Process Unit: DAP Production

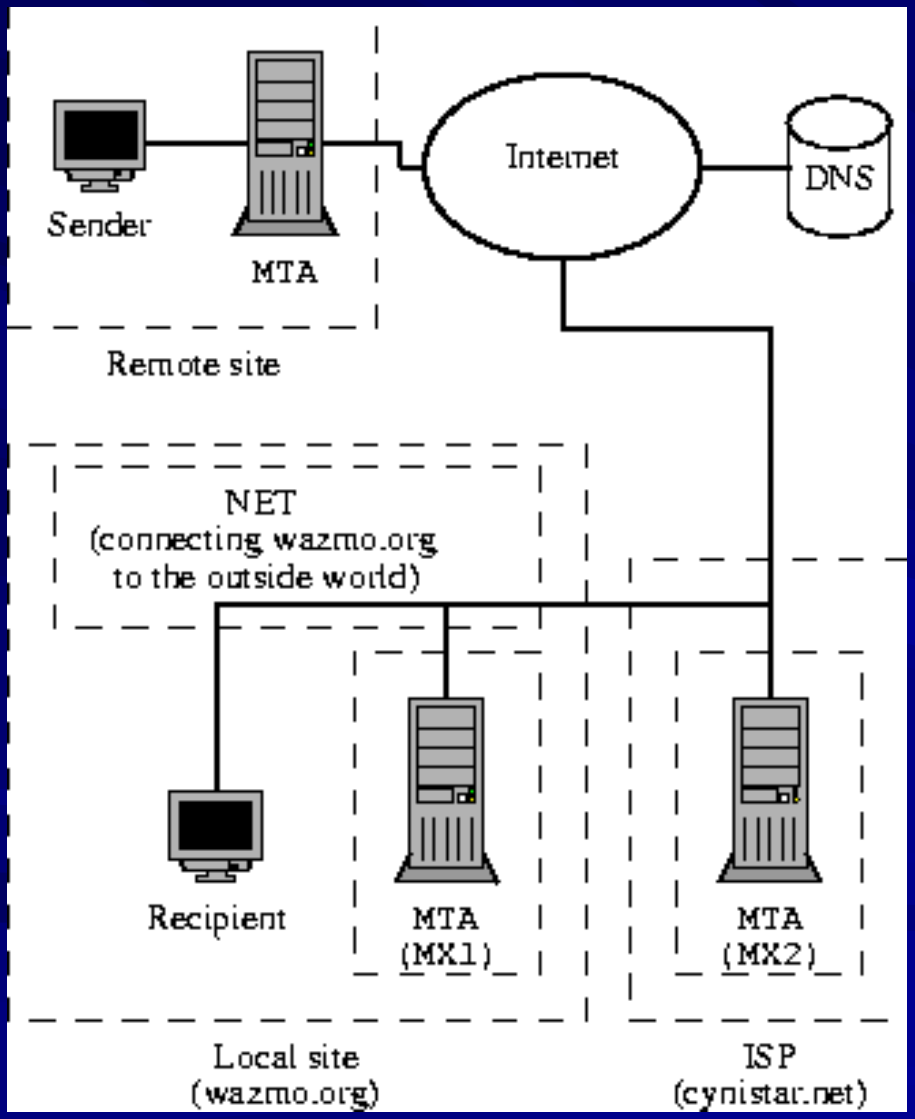
Node: 1 Process Parameter: Flow

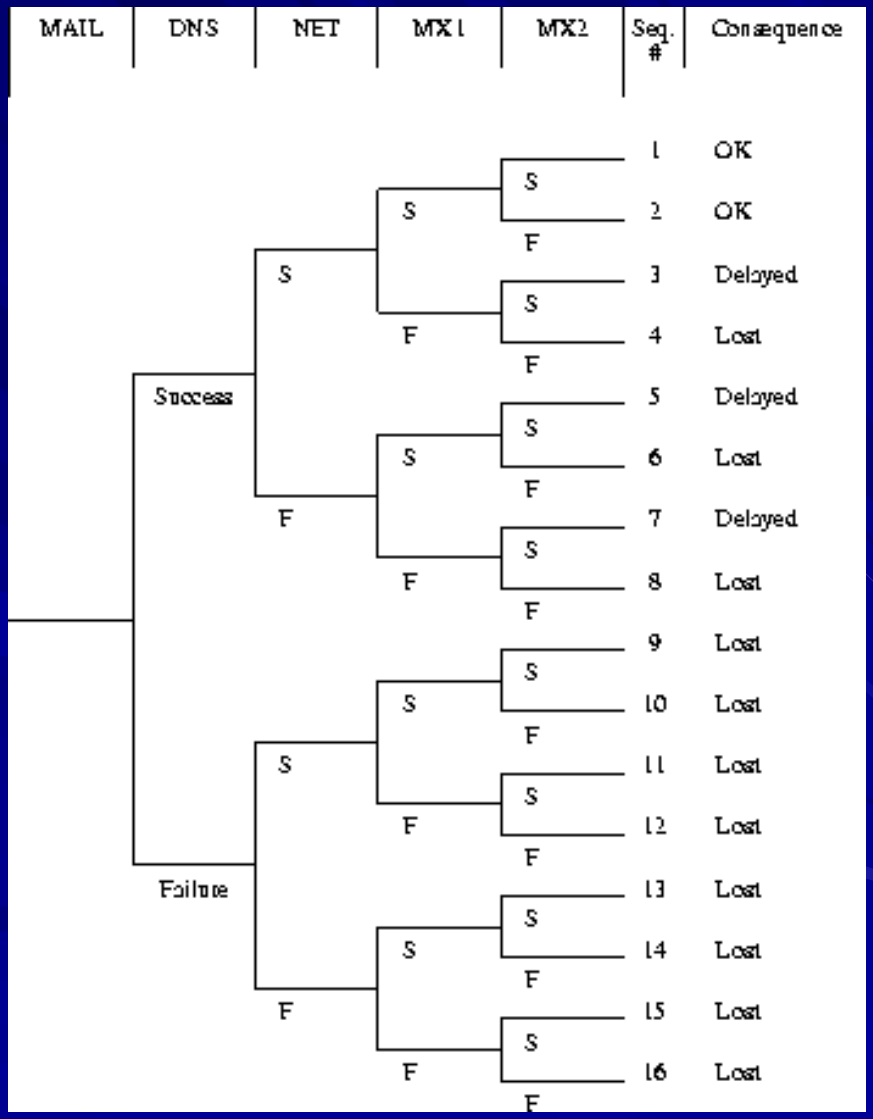
GUIDE WORD	DEVIATION	CONSEQUENCES	CAUSES	SUGGESTED ACTION
No	No Flow	Excess ammonia in reactor. Release to work area.	(1) Valve A fails closed	Automatic closure of valve B on loss of flow from phosphoric acid supply
			(2) Phosphoric acid supply exhausted	
			(3) Plug in pipe; pipe ruptures	
Less	Less Flow	Excess ammonia in reactor. Release to work area, with amount released related to quantitative reduction in supply. Team member to calculate toxicity vs. flow reduction.	(1) Valve A partially closed	Automatic closure of valve B on reduced flow from phosphoric acid supply. Set point determined by toxicity vs. flow calculation
			(2) Partial plug or leak in pipe	
More	More Flow	Excess phosphoric acid degrades product. No hazard to work area.	--	--
Part of	Normal flow of decreased concentration of phosphoric acid	Excess ammonia in reactor. Release to work area, with amount released related to quantitative reduction in supply.	(1) Vendor delivers wrong material or concentration	Check phosphoric acid supply tank concentration after charging
			(2) Error in charging phosphoric acid supply tank	

Eseményfa elemzés (ETA)

- A kiindulópont egy olyan esemény, amely hatással lehet a rendszerre (de önmagában nem feltétlenül veszélyeztető)
- A kiinduló esemény hatását rendre kombináljuk minden további, számbajövő esemény hatásával
- A hatást
  - mind normál,
  - mind hibás működésre vizsgálják
- Fa-struktúra szerű szétágazás - „n” esemény: 2^n ág
- Igazi haszna komplexebb esetekben van, amikor az eredmény nem annyira nyilvánvaló

ETA példa


Sender
MTA
Internet
DNS
Remote site
NET
(connecting wazmo.org
to the outside world)
Recipient
MTA
(MX1)
MTA
(MX2)
Local site
(wazmo.org)
ISP
(cynistar.net)


MAIL
DNS
NET
MX1
MX2
Seq. #
Consequence
Success
Failure
S
F
1 OK
2 OK
3 Delayed
4 Lost
5 Delayed
6 Lost
7 Delayed
8 Lost
9 Lost
10 Lost
11 Lost
12 Lost
13 Lost
14 Lost
15 Lost
16 Lost

Hibafa elemzés (FTA)

- Az elemzés fordított irányban halad, mint az ETA-nál:
  - Egy már - esetleg FMEA vagy HAZOP révén - azonosított, veszélyeztető hatású, ún. **csúcseseményből** kiindulva
  - visszafelé haladva határozzuk meg a csúcseseményt kiváltó ún. **elemi eseményeket**
- A hatások kombinálásánál logikai (Boole) operátorokat használunk
- A hibafában csak azok az események szerepelnek, amelyek veszélyeztető hatásúak, így az FTA-struktúra jóval egyszerűbb lehet, mint az ETA-struktúra

4. Kockázatelemzés

- Bevezetés
- A hibás működés következményei - súlyosság
- A hibás működés valószínűsége - gyakoriság
- Kockázatosztályozás
- Az elfogadható kockázat
- Integritási szintek
- Társadalmi, etikai szempontok

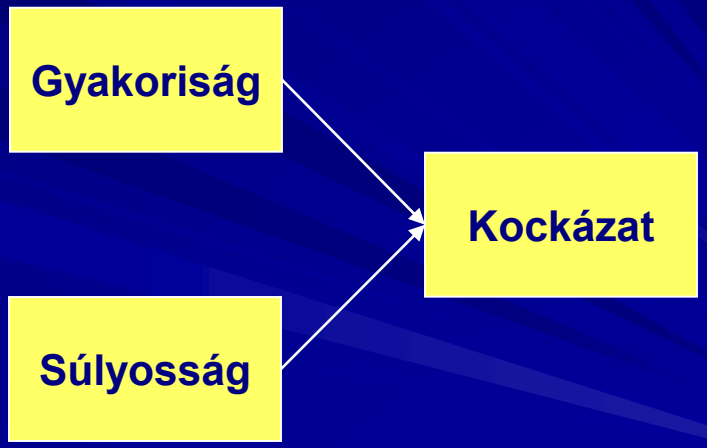
Biztonsági kockázat

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

Biztonsági kockázat:

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

kombinációja.



A kockázat **meghatározható**

- mennyiségileg
- minőségileg (kockázatosztályozás)

Példa a kockázat számszerű kifejezésére (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)

Globális kockázat és individuális kockázat

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

Mekkora a villámcsapásból adódó halálozás kockázata?

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

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

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

A kockázat minőségi meghatározása

- Alap paraméterek
  - súlyosság
  - gyakoriság
- Kiegészítő paraméterek
  - veszélyzónában való tartózkodás
  - baleset elkerülésének lehetősége

Kárkihatási kategóriák (súlyosság) a polgári repülésben (példa

Figyelembe veszi

- a repülőgépre gyakorolt hatást
- a személyzetre gyakorolt hatást
- az utasok biztonságára várhatóan gyakorolt hatást

Kategória	Definíció
Katasztrofális (Catastrophic)	megakadályozza a biztonságos továbbrepülést, és a leszállást
Veszélyes (Hazardous)	…
Lényeges (Major)	…
Nem lényeges (Minor)	nem csökkenti érdemben a repülés biztonságát, kisebb funkcionális visszaesés, szükséges lehet a személyzet beavatkozása, de túlterhelést még nem jelent számukra
Hatástalan (No effect)	…

Katonai számítógépes bizt. krit. rendszerek kárkihatási kategóriái

Interim Defence Standard 00-56 (UK, 1995)	
Kategória	Definíció
Katasztrofális	Több haláleset
Kritikus	Egy haláleset és/vagy súlyos sérülés vagy betegség
Marginális	Egy súlyos sérülés vagy betegség és/vagy több könnyebb sérülés vagy betegség
Elhanyagolható	Legfeljebb kisebb sérülés vagy betegség

Kockázatosztályozás - Kárkihatási kategóriák (példa)

(IEC 61508)

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

Súlyosság ISO26262 Abbreviated Injury Scale

- 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

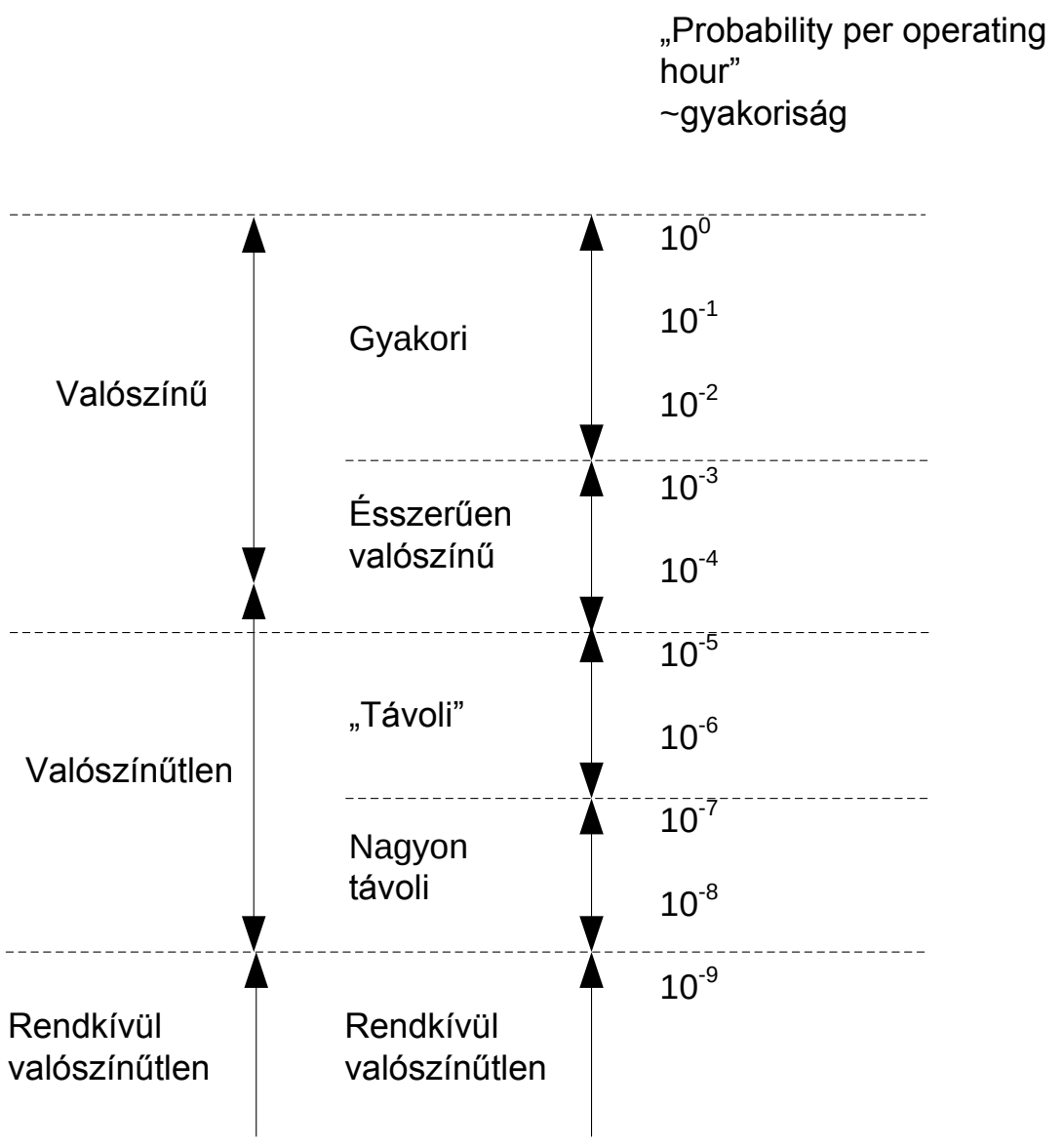
Példák súlyossági kategóriákra Vezetési szcenáriók alapján

- 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/valószínűség

- Megadása
  - a veszélyeztetés valószínűsége, gyakorisága *(nem konzekvensek a szabványok!)*
  - esemény / üzemóra, üzemév
  - élettartam alatt várható események száma
  - védelmi (on-demand) rendszerek: elvárt működéshez viszonyítva

Gyakoriságok – polgári repülés



Gyakoriságok – katonai rendszerek (UK)

Gyakoriság	**Előfordulás az összes ilyen rendszer üzemideje alatt**
Gyakori	Folyamatosan tapasztalható
Valószínű	Gyakran megtörténik
Esetenként	Néhányszor megtörténik
Távoli	Párszor megtörténik
Valószínűtlen	Nem valószínű, de kivételesen előfordulhat
Hihetetlen	Kifejezetten valószínűtlen, hogy egyáltalán megtörténik

Kockázatosztályozás - Veszélybekövetkezési gyakoriság (példa)

CENELEC 50126 (vasúti szabvány)

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	valószínűtlen	Valószínűtlen; azzal lehet számolni, hogy a veszély csak kivételesen lép fel	$10^{-7} \ldots 10^{-9}$
F	rendkívül valószínűtlen	Rendkívül valószínűtlen bekövetkezés; azzal lehet számolni, hogy a veszély nem lép fel	$<10^{-9}$

Gyakoriság ISO 26262

- 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
  - Fellépési gyakoriság és a hibafelfedési idő szorzata ($\sigma \times T$) on-demand jellegű rendszereknél (pl. légzsák)

Gyakoriság ISO 26262

- 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

Kockázat osztályozás

- A gyakoriság és a súlyosság kombinációja
- Mátrixos formában

- Gyakran már a kockázat elfogadási kritériumokat is tartalmazza

Kockázatosztályozás Katonai rendszerek (UK)

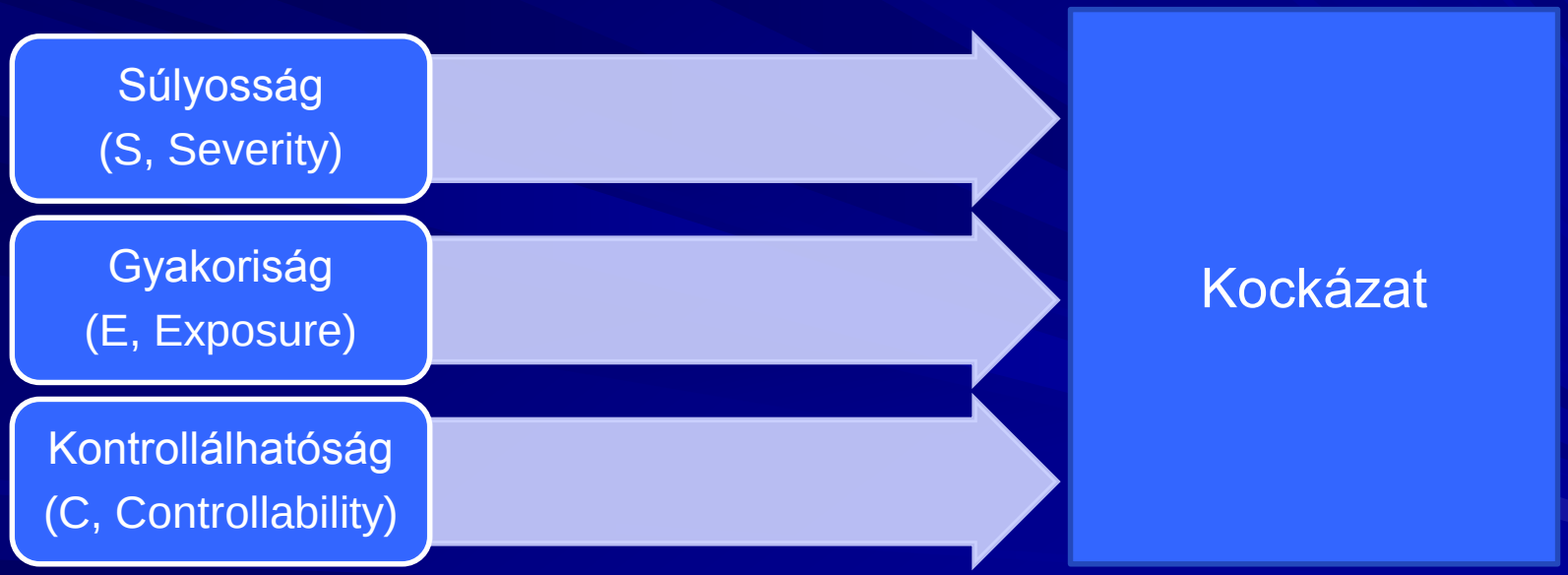
	Következmény			
Gyakoriság	Katasztrofális	Kritikus	Marginális	Elhanyagolható
Gyakori	**A**	**A**	**A**	**B**
Valószínű	**A**	**A**	**B**	**C**
Esetenként	**A**	**B**	**C**	**C**
Távoli	**B**	**C**	**C**	**D**
Valószínűtlen	**C**	**C**	**D**	**D**
Hihetetlen	**D**	**D**	**D**	**D**

Kockázati osztályok (példa)

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

ISO 26262 Veszélyelemzés és kockázatértékelés

- A veszélyeztetések osztályozása (kockázat meghatározása)



Kockázatértékelés ISO26262

- Kockázat: $R = F(f, C, S)$
  - f: gyakoriság (frequency of occurence)
  - C: kontrollálhatóság (elkerülhetőség, menekülési lehetőség)
  - S: súlyosság (severity)
- Gyakoriság: $f = E \times \lambda$
  - E: a veszélyeztetés fellépésének gyakorisága/valószínűsége, mennyi ideig vannak az egyes személyek a potenciálisan veszélyeztető helyzetben
    - ISO 26262: az adott vezetési szcenárió fellépésének valószínűsége
  - λ : az egység meghibásodási gyakorisága (szisztematikus és véletlenszerű), amely a veszélyes szituációhoz vezet
    - ezt nem ismerjük a fejlesztés kezdetén, ezért nem vesszük figyelembe, illetve éppen a megfelelő mérték elérésére törekszünk

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

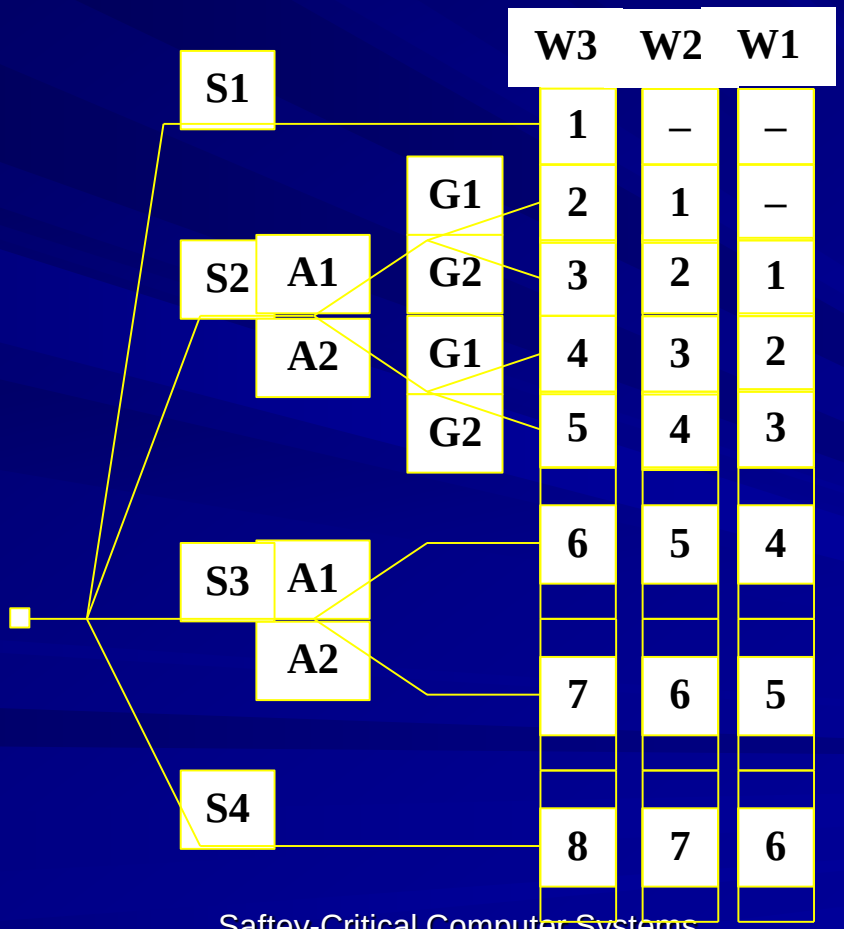
- C0 (mindenki): a rádió hangerő váratlan felerősödése, figyelemelterelő jelzések
- C1 (99%+): a vezetőülés pozíciójának helytelen állítása (lefékezés, megállás), kormány blokkolása induláskor
- C2 (90%+): ABS hiba vészfékezésnél, lámpák kikapcsolása sötét úton
- C3 (90%-): fékhiba, hibás légzsák nyitás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

ASIL meghatározás

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 gráf - Követelményosztályok (DIN 19250)

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



KOCKÁZATCSÖKKENTÉS KOCKÁZATTŰRÉS

Kockázatmentesség, kockázatcsökkentés

Társadalmi igény:

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

Kockázattűrési megközelítések

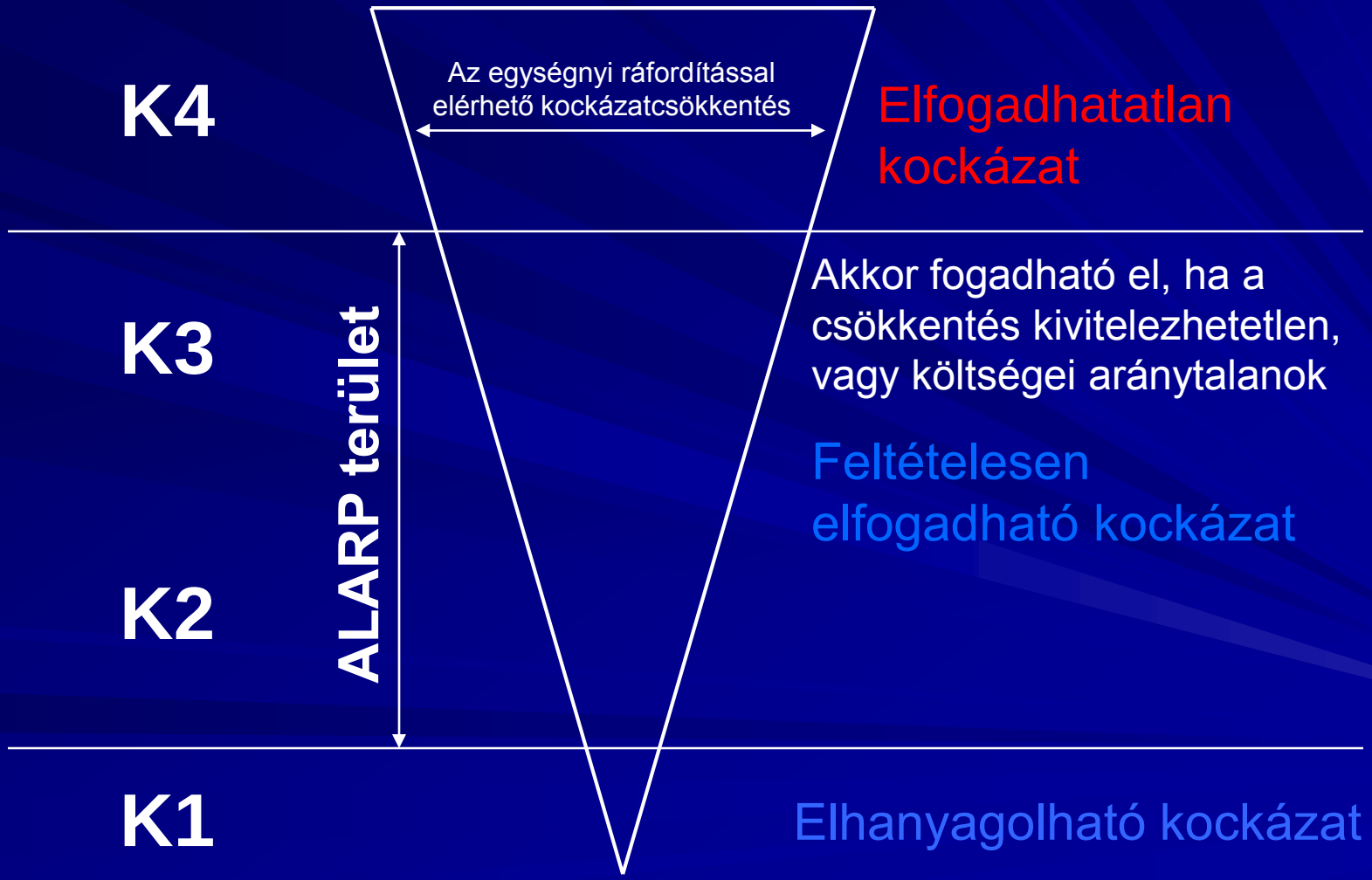
- MEM
  - Minumum endogeneous mortality
  - minimális „halandóság”
  - 5-15 év között az értéke 2×10^{-4} haláleset/fő/év
  - Feltételezése szerint egyidejűleg max. 20 műszaki rendszer veszélyeztethet egy egyént
  - egy rendszerre 10^{-5} haláleset/fő/év jut
  - azaz 10^{-9} haláleset/fő/óra

Kockázattűrési megközelítések

- GAME / GAMAB
  - Globalement Au Moins Equivalent
  - Egy új rendszer nem lehet rosszabb, mint a régiek
  - Mi van új rendszer esetén?

Kockázatcsökkentés – Az ALARP elv

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



Kockázatosztályozás Katonai rendszerek (UK)

	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**

Kockázat elfogadás Katonai rendszerek (UK)

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

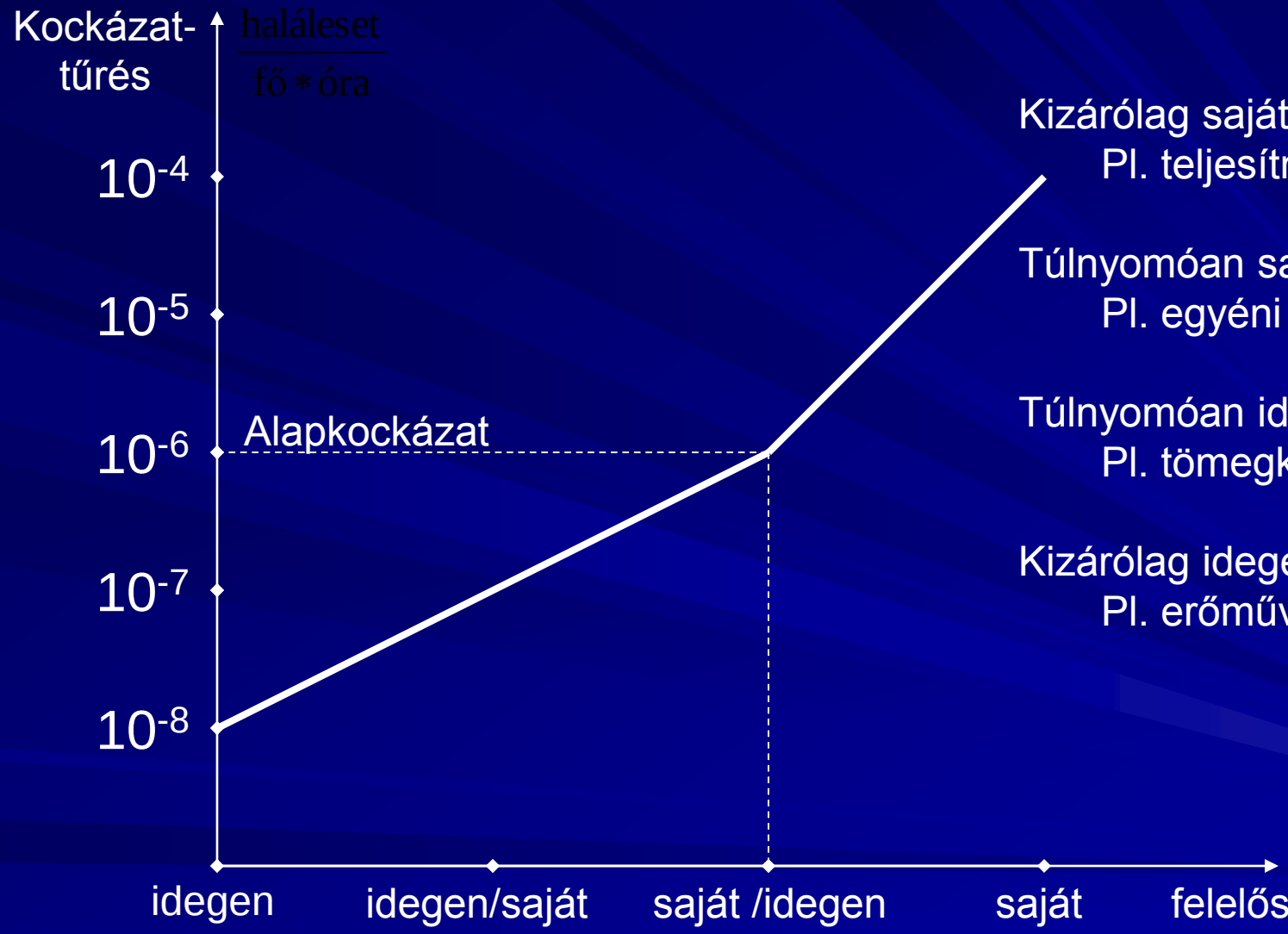
Kockázati osztályok (példa)

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

Kockázat elfogadás

- 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**

A kockázattűrés függése a felelősségtől



Kizárólag saját felelősség
Pl. teljesítménysportok

Túlnyomóan saját felelősség
Pl. egyéni közlekedés

Túlnyomóan idegen felelősség
Pl. tömegközlekedés

Kizárólag idegen felelősség
Pl. erőművek közelében

Társadalmi, etikai szempontok (1)

- Az integritási szint, a biztonság növeléséért teendő erőfeszítések meghatározása nemcsak mérnöki feladat - társadalmi vonatkozásai is vannak - közvetve az emberi élet, a sérülések pénzben vagy másként kifejezett értékéről is szó van
- Az áldozat „értékének” megítélése különböző (csecsemő, kenyérkereső, idős ember - pl. becsült keresetkiesés)
- Az élet megőrzésének költségei eltérő körülmények között igen különbözőek lehetnek
  - Minimum: amennyit költenénk rá
  - Maximum: amennyit már nem költenénk rá
- Különböző példákból az arány akár 1:1000 is lehet

Társadalmi, etikai szempontok (2)

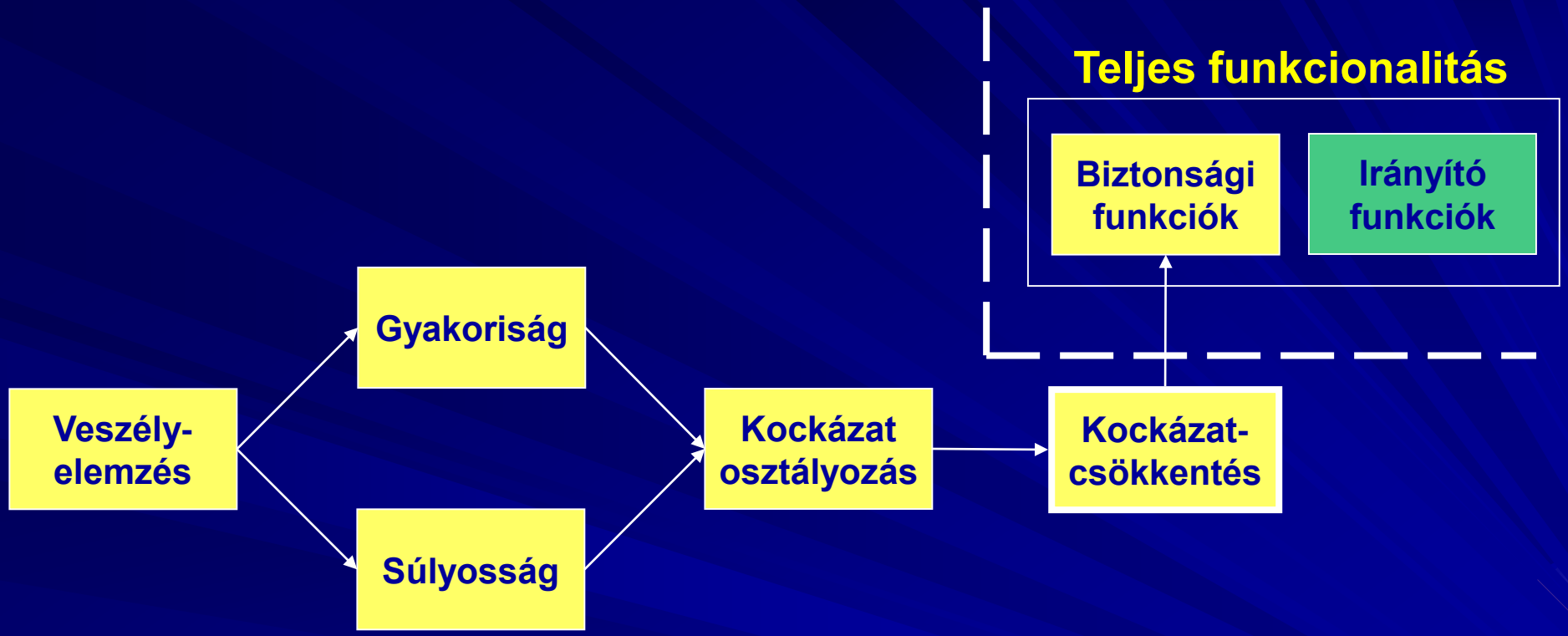
- A kockázat társadalmi megítélése nagymértékben függ a kockázat jellegétől
  - A tömegbalesetet súlyosabbnak ítélik meg, mintha ugyanannyi ember hal meg egyenként (vasút, repülő - közút)
- Erősen befolyásolja a megítélést, hogy mennyire van befolyásunk az eseményekre
  - Atomerőművi katasztrófa - nem tudjuk megvédeni magunkat
  - Autó elgázol - sajnos nem mindig befolyásolható, csak gondoljuk
- Érzelmi tényező
  - Egy űrhajó meghibásodása kevesebb életet kockáztat, mint egy utasszállító gépé, elvesztését mégis nemzeti katasztrófaként élik meg
- Irányelvek, amelyek a kockázat megítélésének nemcsak a műszaki, hanem a társadalmi vonatkozásait is figyelembe veszik

Társadalmi, etikai szempontok (3)

- Abszolút biztonság nincs
  - Ilyen követelménnyel nem lehetne semmilyen műszaki berendezést létesíteni, üzemeltetni
- Célunk **megfelelő biztonságú** rendszerek létesítése, üzemeltetése
- A szabványok minimális integritási szinteket írnak elő - a hatóságok ezt követelik meg
- A mérnök számára ez alapozza meg a döntést a fejlesztendő rendszer biztonsági megfelelősségével kapcsolatban
- Emellett azonban a mérnök szakmai és morális felelősséget visel azért, hogy

a rendszer olyan biztonságos legyen, amennyire csak lehet

Biztonsági funkciók



IRÁNYÍTANDÓ FOLYAMAT

IRÁNYÍTÓ RENDSZER

Kockázatcsökkentés – Kockázatmenedzselés