Biztonságkritikus rendszerek

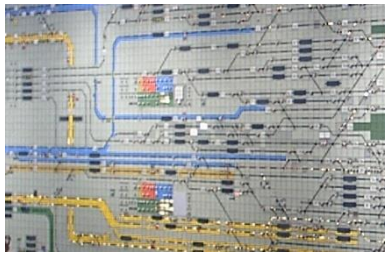
Rendszertervezés és -integráció

dr. Majzik István

Méréstechnika és Információs Rendszerek Tanszék

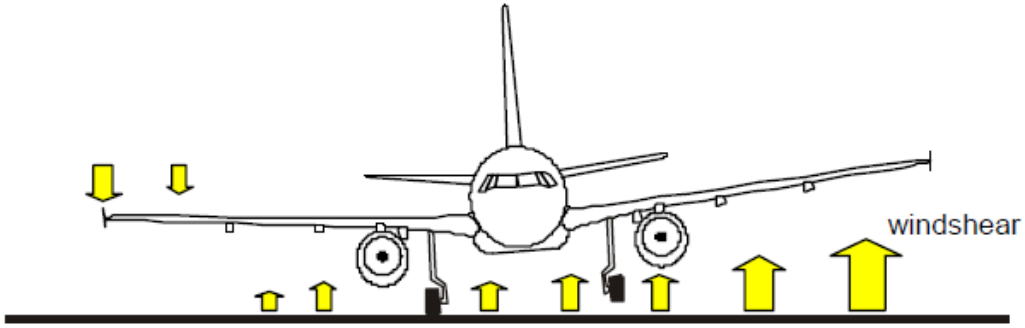
Mik azok a biztonságkritikus rendszerek?

- A hibázás, azaz a specifikáció nem teljesítése balesethez, környezeti kárhoz vezethet
- Miért kell velük külön foglalkozni?
  - Speciális analízis és követelmények
    - Mely funkciók, hibák vezethetnek balesethez?
    - Milyen biztonsággal teljesíthetők a követelmények?
  - Speciális fejlesztési megoldások szükségesek
    - Redundáns architektúra, hibatűrés
    - Kockázatcsökkentési módszerek
    - Biztonságigazolás, szisztematikus tesztelés, ...
  - Szabványok, előírások vonatkoznak a fejlesztésre
    - IEC 61508: Programozható elektronikai rendszerek
    - DO 178B: Repülőgép-fedélzeti beágyazott rendszerek
    - EN 5012x: Vasúti jelzőrendszerek
    - ISO 26262: Gépjármű elektronikai rendszerek biztonsága



Baleseti példák

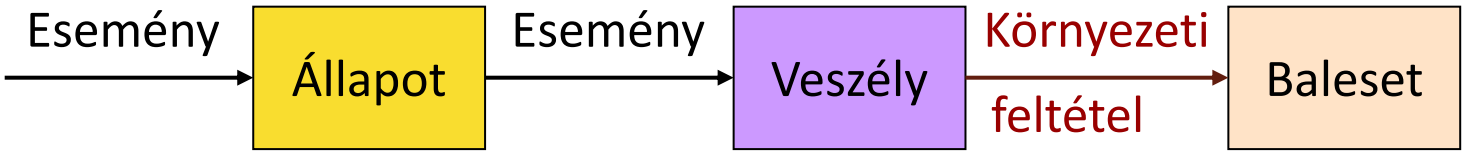
- A320-211 balesete Varsóban (1993. szept. 14.)
  - Oldalszél: A bal kerék 9 másodperccel később ért földet, mint a jobb
  - Intelligens fékezés vezérlés: Kerekek terhelésének és forgásának figyelése
  - Késői fékezés → túlfutás → ütközés



- Toyota gépkocsi balesete San Diegóban, 2009. aug.
  - Szőnyeg (+ szoftverhiba) miatt beragadt gázpedál → „padlógáz”
  - Miért nem volt elég hatásos
    - a fékezés?
    - a sebességváltó üresbe állítása (D → N)?
    - a motor lekapcsolása?

Tapasztalatok balesetek elemzése alapján

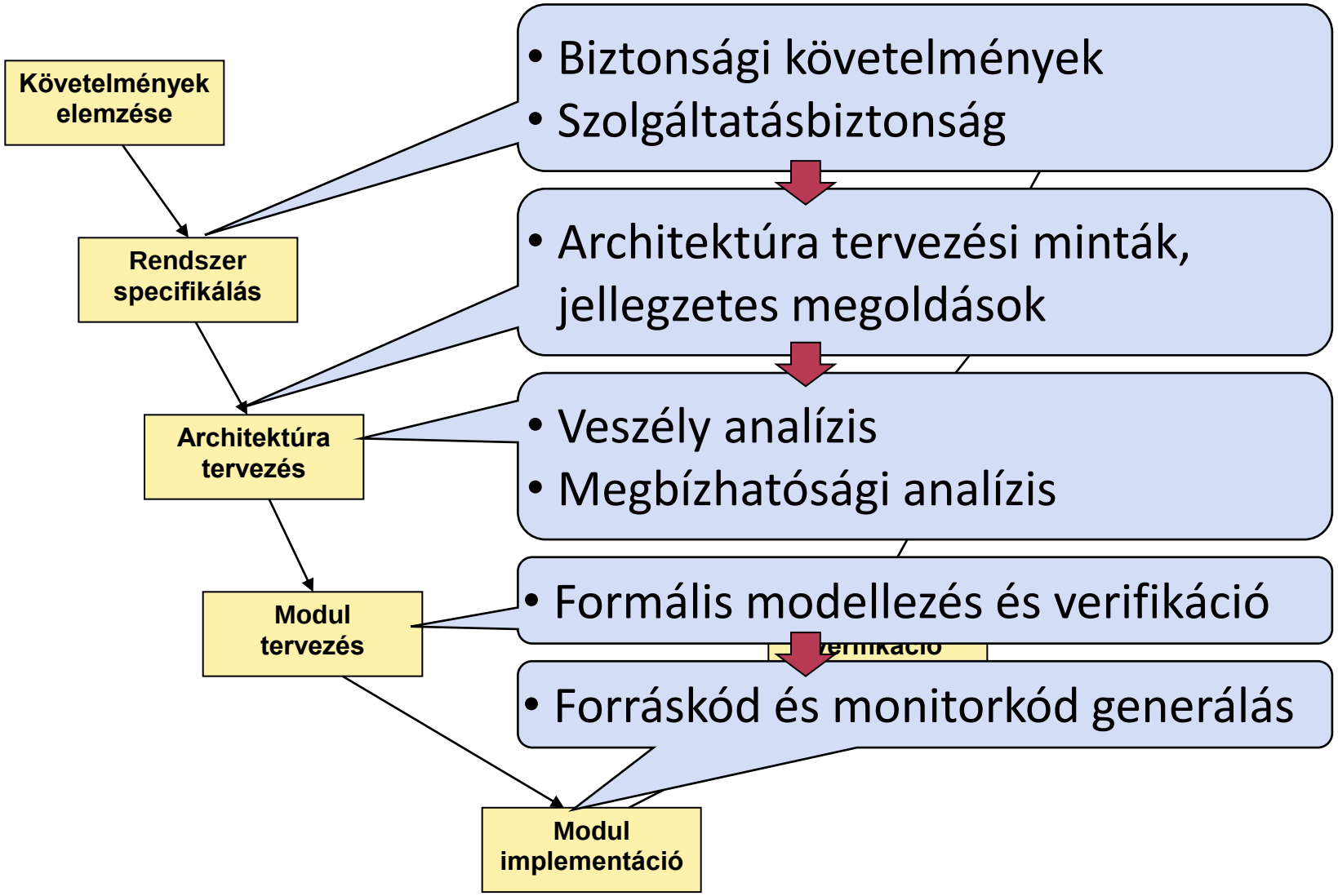
- A baleset tipikusan összetett esemény-szekvencia
  - Tervezési fázisban előre kellene látni



- Veszély ≠ meghibásodás
  - A detektálatlan hiba tipikusan veszélyt jelent
  - De előfordulhat veszély hibátlan működés esetén is

- Jellegzetességek a tervezési folyamatban
  - Kockázat analízis: A veszélyt okozó szituációk elemzése
  - Biztonsági funkciók hozzárendelése:
    a veszély és baleset kialakulásának elkerülésére
  - Extra-funkcionális biztonsági követelmények specifikálása

Mivel foglalkozunk majd?

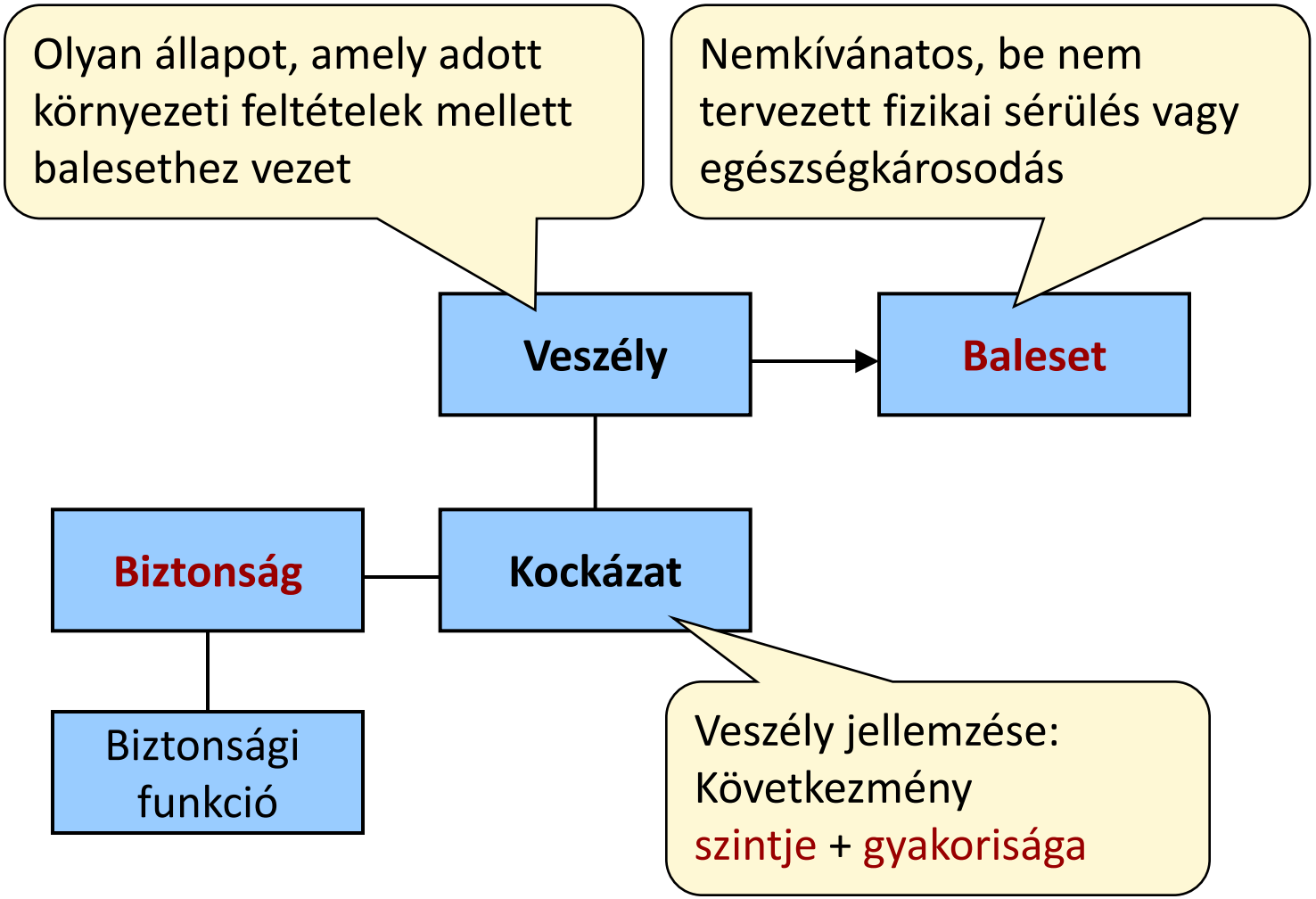


Biztonsági követelmények

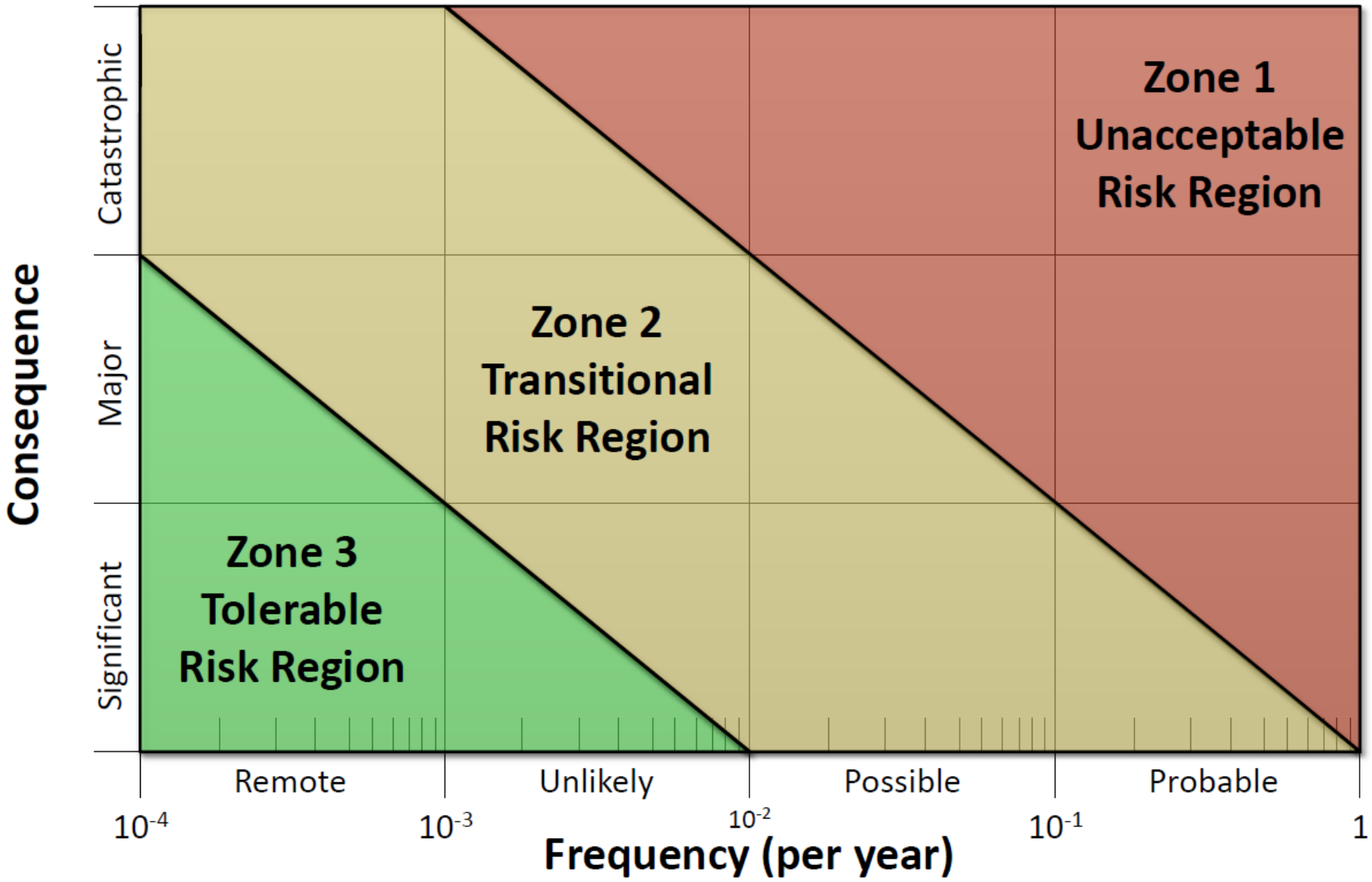
Terminológia

- Baleset (*accident*):
  Nemkívánatos, be nem tervezett sérülés, veszteség
- Veszély (*hazard*), veszélyes állapot:
  Olyan állapot, amely adott környezeti feltételek mellett balesethez vezet
- Kockázat (*risk*):
  Veszély jellemzése: következmény szintje + gyakorisága
- Biztonság(osság) (*safety*):
  Balesetektől való mentesség (ideális eset!)
  → Elfogadhatatlan kockázattól való mentesség
- Biztonsági funkció (→ rendszer, szoftver is):
  Veszélyes állapotokkal kapcsolatba hozható a hibás vagy hiányzó végrehajtása

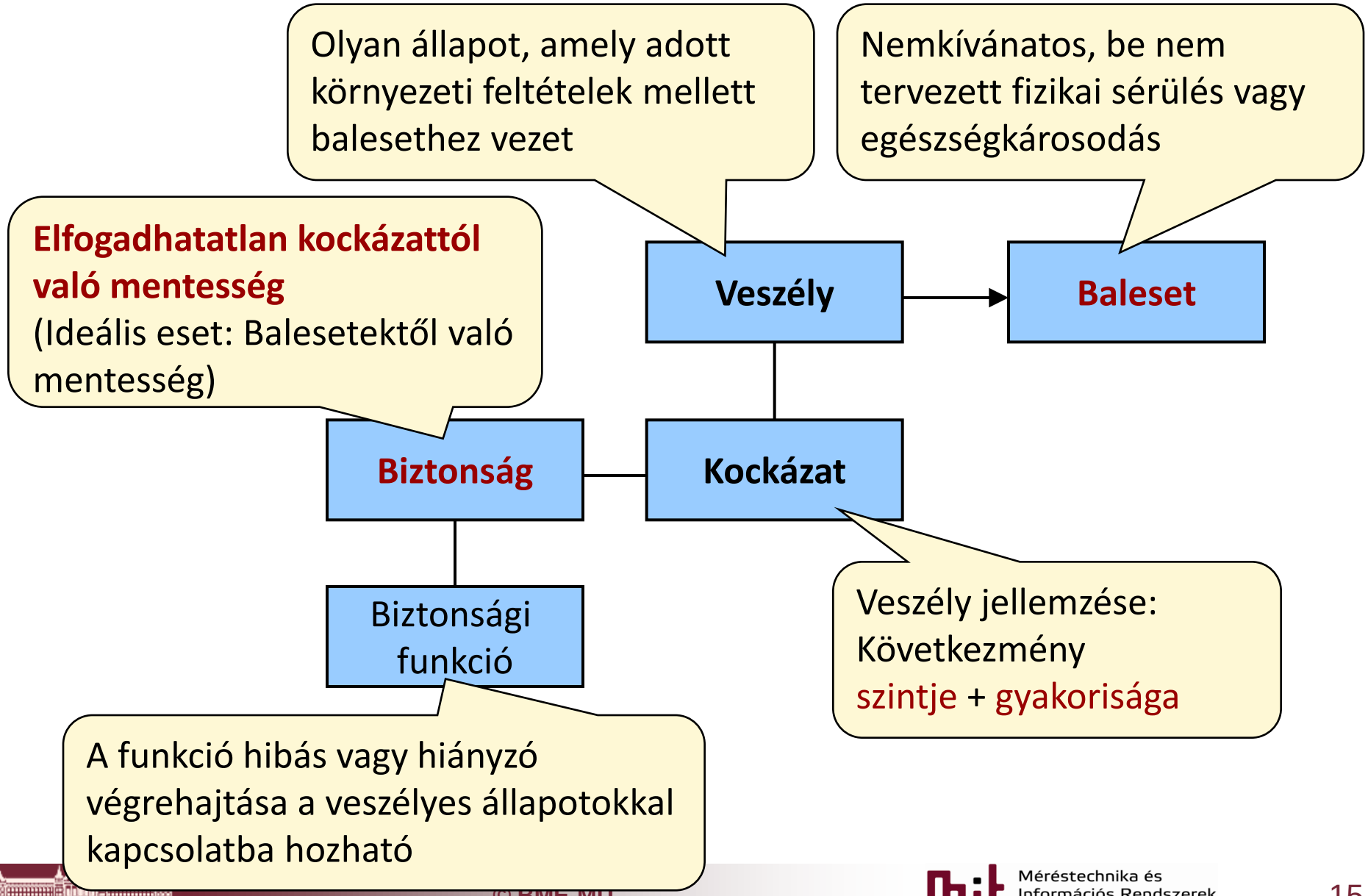
Terminológia



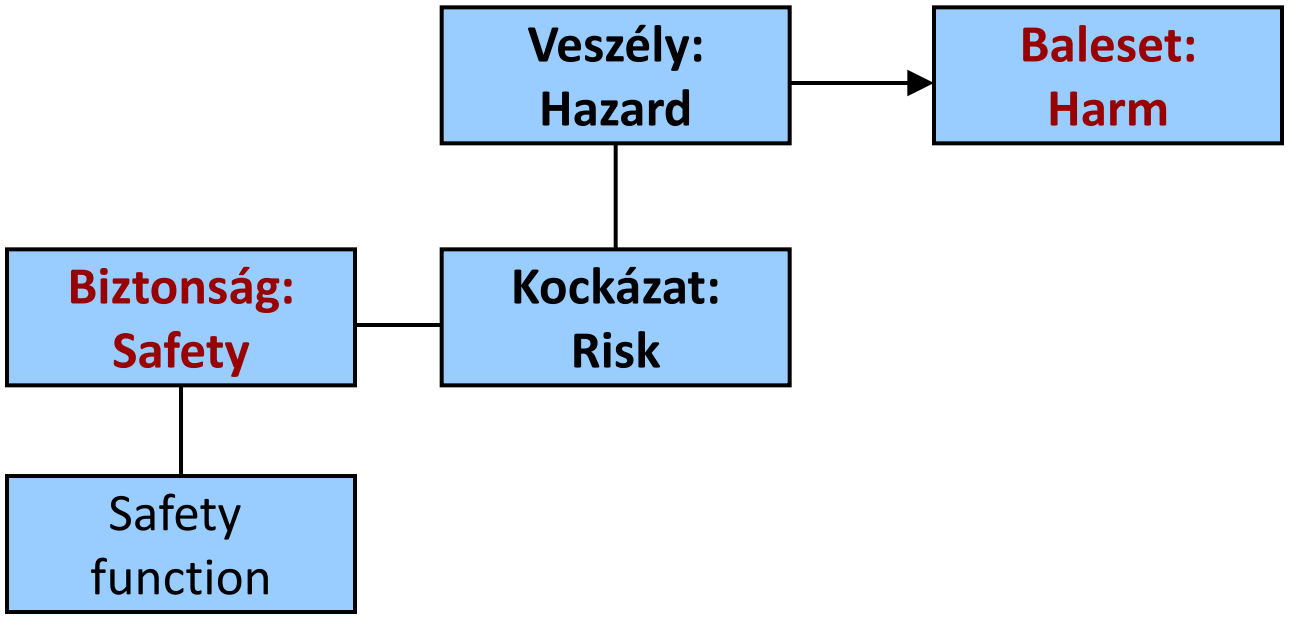
Kockázati kategóriák



Terminológia

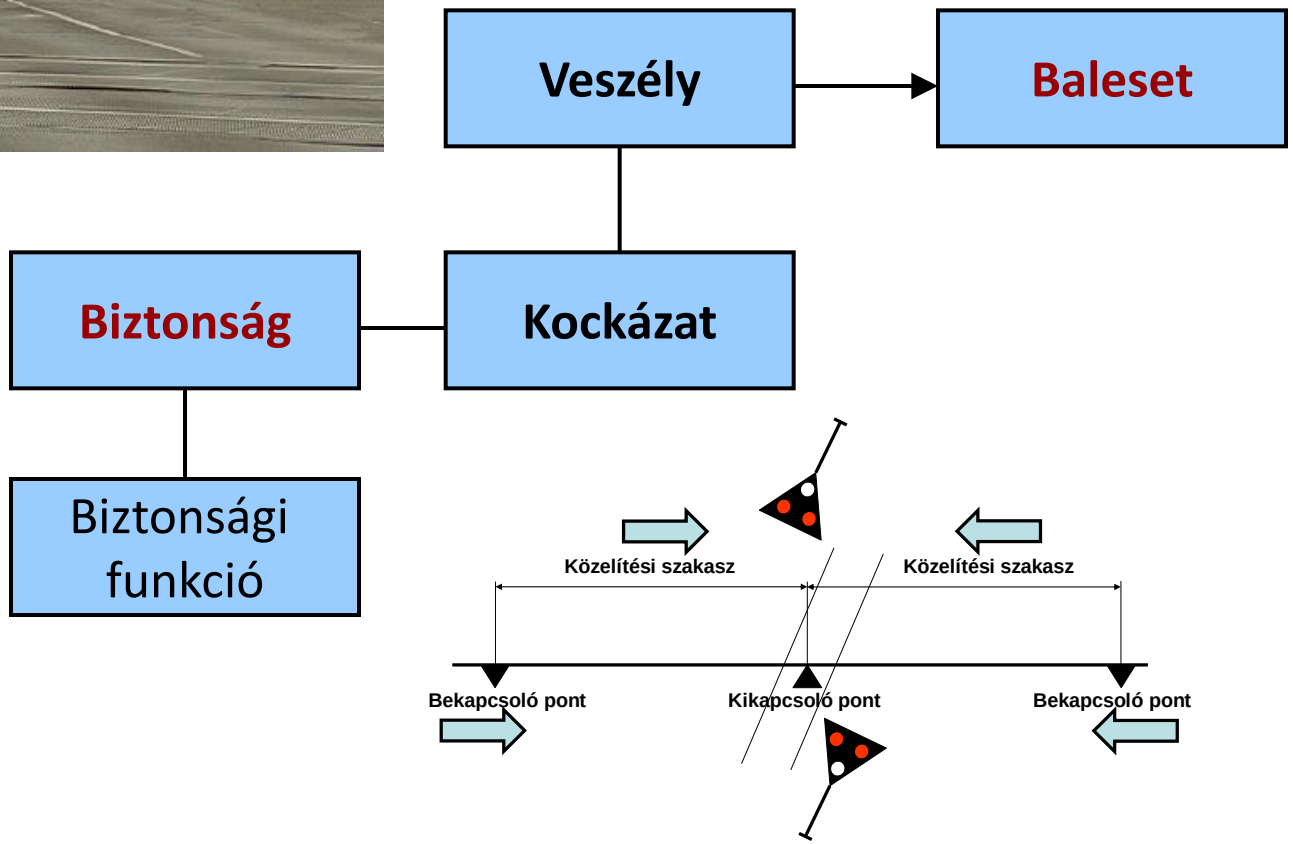


Angol nyelvű terminológia



Példa: A terminológia alkalmazása

Vonat által vezérelt önműködő útátjáró-fedező berendezés nyíltvonalon



Mi szerepeljen a specifikációban?

- Funkcionális biztonsági követelmények
  - Mi az a funkció, ami a biztonságot eléri illetve megtartja (mit kell megvalósítania a rendszernek)
  - A funkcionális specifikációhoz tartozik
- Biztonságintegritási követelmények
  - Mi annak a bizonyossági foka, hogy a biztonságkritikus rendszer a biztonsági funkciót kielégítően megvalósítja adott feltételek és időtartam mellett
  - A biztonság valószínűségi alapú kezelése
    - Példa 1: Házak méretezése 50 év alatt >10% valószínűséggel előforduló földrengésre
    - Példa 2: Gátak méretezése a 100 évente tipikusan előforduló legmagasabb vízállásra

Biztonságintegritási követelmények

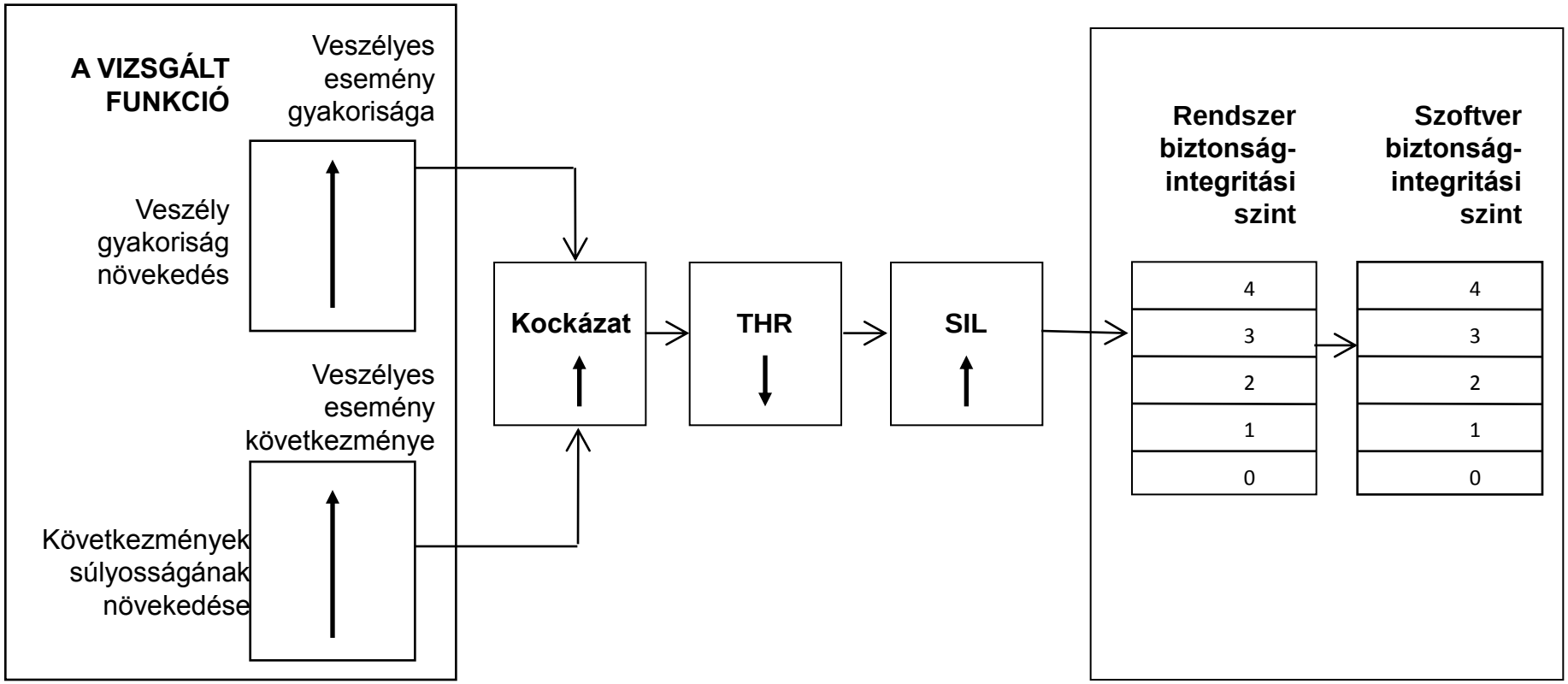
- Előírások a biztonsági funkció kockázatelemzése alapján
  - Nem folytonos (eseti) üzemmód: A funkció meghívása esetén a veszélyt okozó hibajelenség valószínűségére
    - PFD: Probability of Failure on Demand
  - Folytonos üzemmód: Veszélyt okozó hibajelenség gyakoriságára
    - PFH: Probability of Failure per Hour
    - THR: Tolerable Hazard Rate – elviselhető hibagyakoriság
- Kategóriák: Biztonságintegritási szint
  - SIL: Safety Integrity Level

Ha 15 év az élettartam, akkor ez alatt kb. 750 berendezésből 1-ben lesz hiba

SIL	Biztonságkritikus funkció hibája / óra
1	$10^{-6} \leq THR < 10^{-5}$
2	$10^{-7} \leq THR < 10^{-6}$
3	$10^{-8} \leq THR < 10^{-7}$
4	$10^{-9} \leq THR < 10^{-8}$

Hiba nélküli működés >11.000 év??

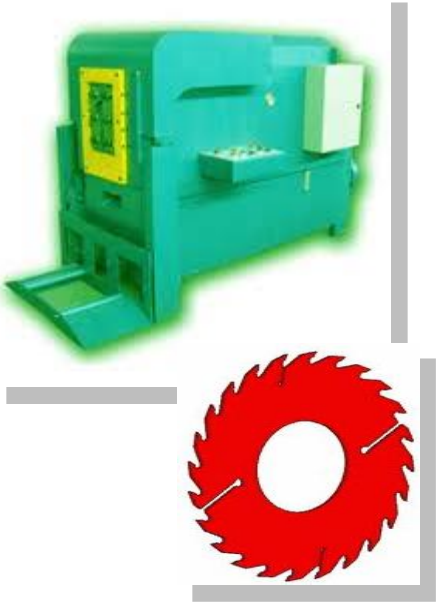
SIL meghatározás alapelve



Kockázatelemzés –> Funkció THR –> Funkció SIL –> (Al)rendszer SIL

Példa biztonsági követelményre

- Fűrészgép, a forgó korong előtt védőráccsal
  - Tisztításhoz a védőrácsot fel kell húzni
- Veszély analízis: Kezelőt baleset érheti tisztításkor, ha a korong nincs leállítva
  - Veszély: Ha a védőrácsot 50 mm-nél jobban felhúzzák, és a motor 3 másodperc alatt nem áll le
  - 20 gép van, 500-szor kell tisztítást végezni az élettartam alatt; ez alatt legfeljebb 1-szer elviselhető, hogy a leállítás ne működjön

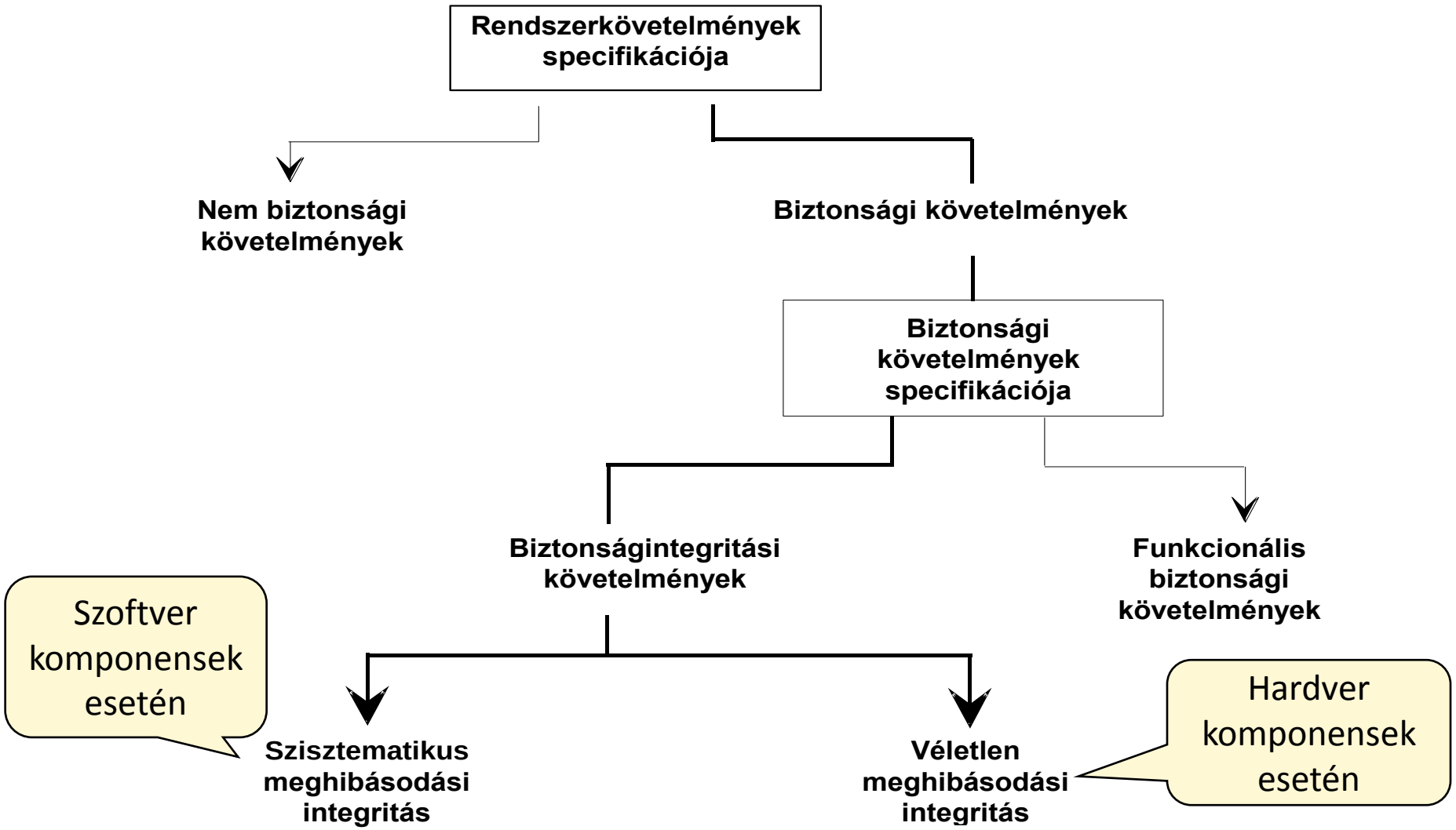


- Funkcionális biztonsági követelmény
  - Biztonsági funkció: Védőkapcsolás a motorhoz
  - Ha a védőrácsot 25 mm-re felhúzzák, a motort 2,5 s alatt leállítja
- Biztonságintegritási követelmény:
  - A védőkapcsolás hibájának valószínűsége legyen kisebb, mint 10^{-4} (maximum 1 hiba 10.000 művelet esetén)

A biztonsági követelmények teljesítése

- A biztonságot befolyásoló hibák alapján
  - Véletlen (hardver) hibák: Környezeti vagy belső hatás miatt működés közben véletlenszerű előfordulás
    - Számításokkal ellenőrizhető gyakoriság/valószínűség
  - Szisztematikus (szoftver) hibák: Tervezési, megvalósítási hibák miatt determinisztikus előfordulás
    - Számításokkal nem ellenőrizhető valószínűség
    - Módszer- és eszközkészlet előírt a fejlesztés során
    - Fejlesztési szabványok tartalmazzák

Biztonsági követelmények felépítése



A szolgáltatásra vonatkozó további minőségi követelmények

(A biztonság önmagában nem elég)

A szolgáltatás használhatóságának jellemzése

- Jellegzetes követelmények
  - Megbízhatóság, rendelkezésre állás, adatintegritás, ...
  - Befolyásolja: Előállítási folyamat jó minősége + használat közben előforduló hibák
- Összetett jellemző: Szolgáltatásbiztonság
  - Angol megnevezés: *Dependability*
  - Definíció: Képesség olyan szolgáltatás nyújtására, amiben igazoltan bízni lehet
    - Igazoltan: elemzésen, méréseken alapul
    - Bizalom: szolgáltatás az igényeket kielégíti

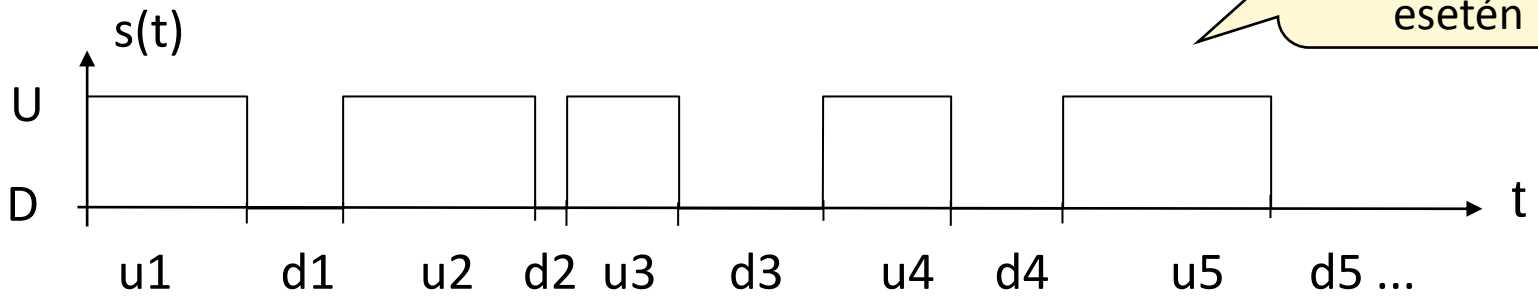
A szolgáltatásbiztonság alapjellemzői

Alapjellemző	Definíció
Rendelkezésre állás (availability)	Helyes szolgáltatás valószínűsége (közben hiba esetén javítás végezhető)
Megbízhatóság (reliability)	Folyamatosan helyes szolgáltatás valószínűsége (az első hibáig megbízható)
Biztonság (safety)	Elfogadhatatlan kockázattól való mentesség
Integritás (integrity)	Hibás változás, változtatás elkerülésének lehetősége
Karbantarthatóság (maintainability)	Javítás és fejlesztés lehetősége

Definíciók: Várható értékek

- Állapot particionálás s(t) rendszerállapotra
  - Hibamentes (Up) illetve Hibás (Down) állapotpartíció

Javított rendszer esetén



- Várható értékek:
  - Első hiba bekövetkezése: MTFF = E{u1}
    (Mean Time to First Failure)
  - Hibamentes működési idő: MUT = MTTF = E{ui}
    (Mean Up Time, Mean Time To Failure)
  - Hibás működési idő: MDT = MTTR = E{di}
    (Mean Down Time, Mean Time To Repair)
  - Hibák közötti idő: MTBF = MUT + MDT
    (Mean Time Between Failures)

Definíciók: Valószínűség időfüggvények

- Rendelkezésre állás:

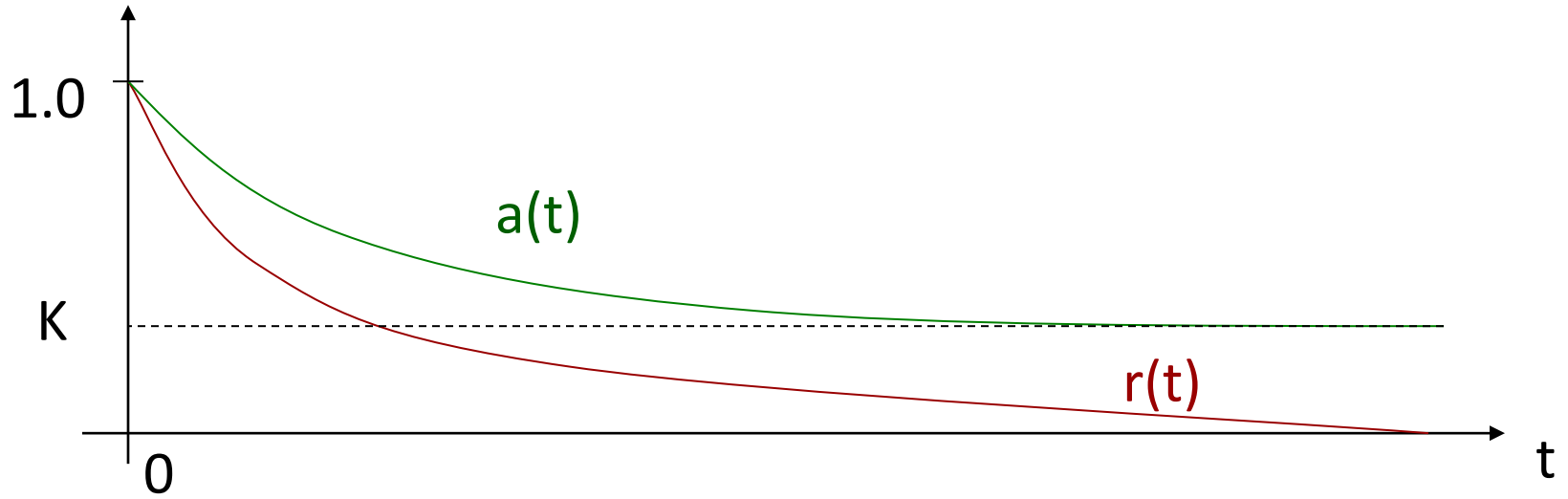
  $a(t) = P\{ s(t) \in U \}$ (közben meghibásodhat)

- Készenlét: $K = \lim_{t \to \infty} a(t)$ (ha rendszeresen javított)

  Jelölhető A-val is: $A = K = MTTF / (MTTF + MTTR)$

- Megbízhatóság:

  $r(t) = P\{ s(t') \in U, \ \forall t' < t \}$ (t-ig nem hibásodhat meg)



Készenlét tipikus követelményei

Készenlét	Max. kiesés egy év alatt
99%	~ 3,5 nap
99,9%	~ 9 óra
99,99% („4 kilences”)	~ 1 óra
99,999% („5 kilences”)	~ 5 perc
99,9999% („6 kilences”)	~ 32 másodperc
99,99999%	~ 3 másodperc

Komponensekből felépített rendszer készenléte, ahol egy komponens készenléte 95%:

- 2 komponensből álló rendszer: 90%
- 5 komponensből álló rendszer: 77%
- 10 komponensből álló rendszer: 60%

Komponens jellemző

- Meghibásodási gyakoriság (~ tényező): $\lambda(t)$
  - $\lambda(t)\Delta t$ adja meg: a komponens mekkora valószínűséggel fog t időpont Δt környezetében elromlani, ha t-ig jól működött

$$\lambda(t)\Delta t = P\{ s(t+\Delta t) \in D \mid s(t) \in U \}, \quad \text{miközben } \Delta t \to 0$$

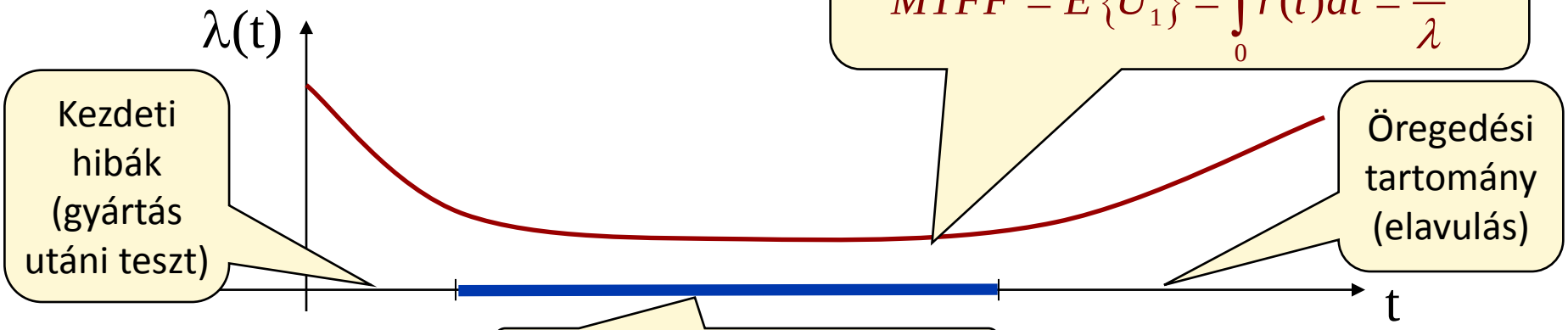
  - Megbízhatóság kifejezhető ez alapján:

$$\lambda(t) = -\frac{1}{r(t)}\frac{dr(t)}{dt}, \quad \text{így} \quad r(t) = e^{-\int_0^t \lambda(t)dt}$$

  - Elektronikai alkatrészekre:

Itt $r(t) = e^{-\lambda t}$

$$MTFF = E\{U_1\} = \int_0^\infty r(t)dt = \frac{1}{\lambda}$$



Példa: Egy DMI fejlesztése: Célkitűzés

Mozdonyvezető

DMI

EVC

EVC: European Vital Computer (fedélzeti)

Karbantartó központ

Jellegzetességek:

- Biztonságkritikus működés
  - Információ megjelenítése
  - Vezetői parancsok feldolgozása
  - Adatátvitel az EVC-hez
- Biztonságos vezeték nélküli kommunikáció
  - Konfiguráció
  - Diagnosztika
  - Szoftver frissítés

Példa: Egy DMI fejlesztése: Prototípus

Példa: Egy DMI fejlesztése: Követelmények

- Biztonság:
  - Biztonsági funkció elviselhető hibája óránként (Tolerable Hazard Rate): $10^{-7} <= THR < 10^{-6}$
  - Biztonságintegritási szint: SIL 2
- Megbízhatóság:
  - Mean Time To Failure: MTTF > 5000 óra (5000 óra: ~ 7 hónap)
- Rendelkezésre állás (készenlét):
  - A = MTTF / (MTTF+MTTR), A > 0.9952
    - Hibás állapot: évenként kevesebb, mint 42 óra
    - Teljesíthető a fenti MTTF esetén, ha MTTR < 24 óra

A szolgáltatásbiztonság befolyásoló tényezői

Fejlesztési folyamat → **Működő termék**

- Tervezési hibák
- Implementációs hibák

- Hardver hibák
- Konfigurációs hibák
- Kezelői hibák

Hibahatások

Fejlesztési folyamat → **Működő termék**

- Tervezési hibák
- Implementációs hibák

- Hardver hibák
- Konfigurációs hibák
- Kezelői hibák

Fejlesztési folyamat jellemzői:

- Jobb minőségbiztosítás, jobb módszertanok
- De növekvő bonyolultság, nehezebb ellenőrzés

Szokásos becsült értékek 1000 kódsorra:

- Jó kézi fejlesztés és tesztelés: <10 hiba marad
- Automatizált fejlesztés: ~1-2 hiba marad
- Formális módszerek használata: <1 hiba marad

Hibahatások

Fejlesztési folyamat → **Működő termék**

- Tervezési hibák
- Implementációs hibák

- Hardver hibák
- Konfigurációs hibák
- Kezelői hibák

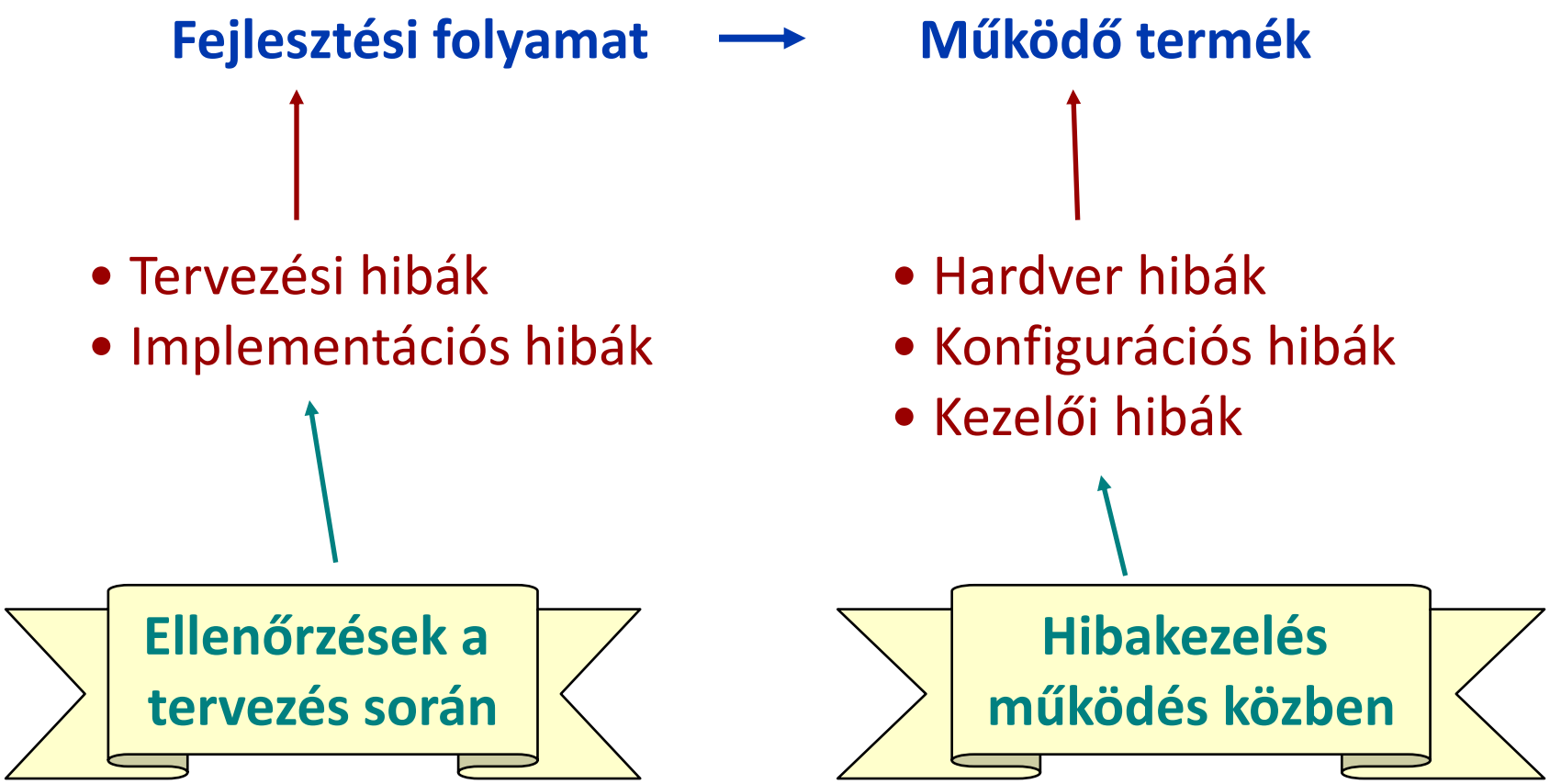
Technológia korlátai:

- Jobb minőségbiztosítás, jobb anyagok
- De növekvő érzékenység

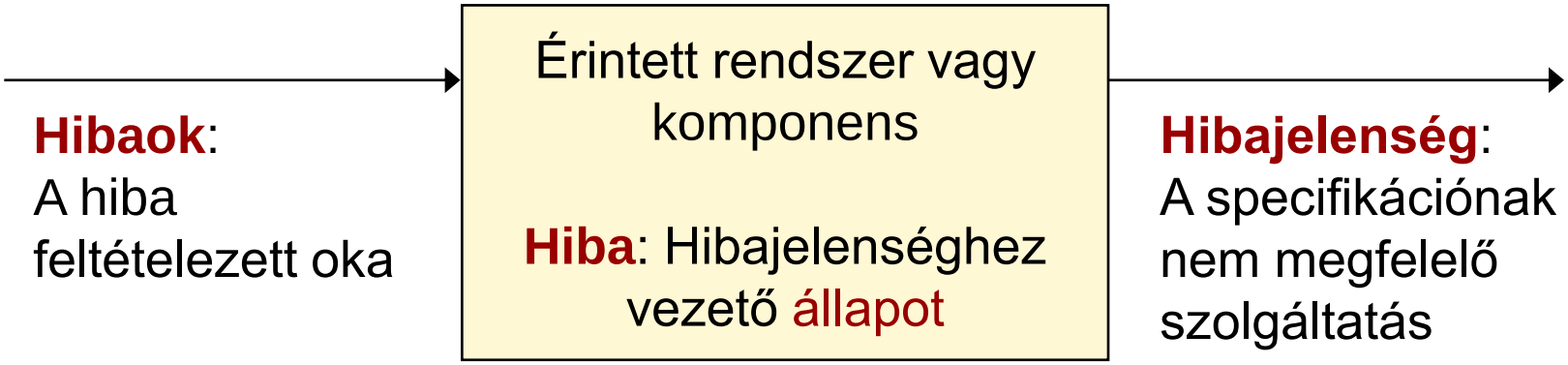
Szokásos becsült értékek:

- CPU: 10^{-5}…10^{-6} hiba/óra
- RAM: 10^{-4}…10^{-5} hiba/óra
- LCD: ~ 3…5 év élettartam

Hibahatások kiküszöbölése



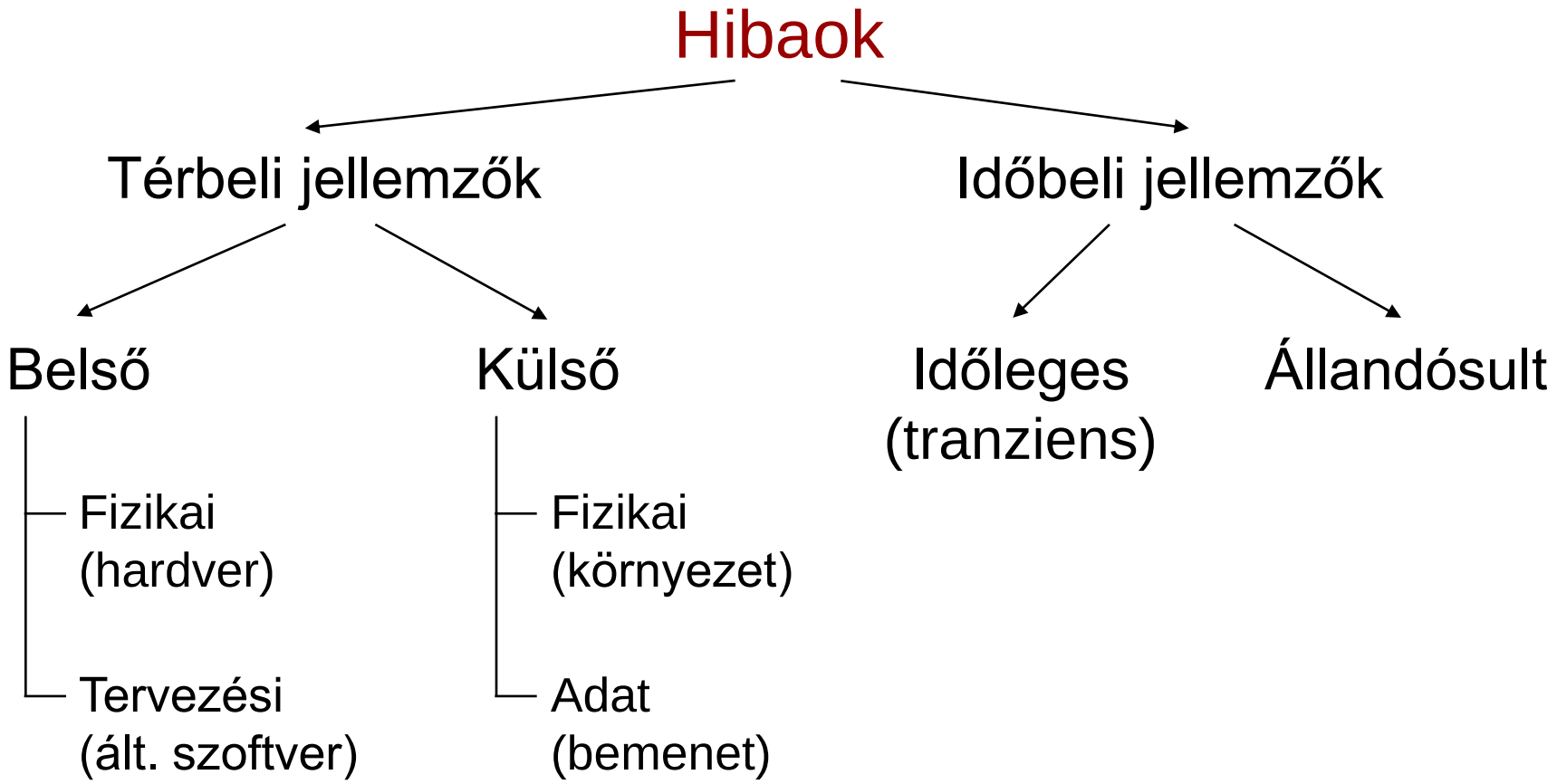
A hibaok hatáslánc



Hibaok → Hiba → Hibajelenség hatáslánc példák:

Hibaok	→ Hiba	→ Hibajelenség
Kozmikus sugárzás egy bitet átbillent a memóriában	Hibás memóriacella olvasása	Robotkar a falnak ütközik
Programozó csökkentés helyett növel egy változót	Vezérlés ráfut, a változó értéke hibás lesz	A számítás végeredménye rossz

A hibaok jellemzői



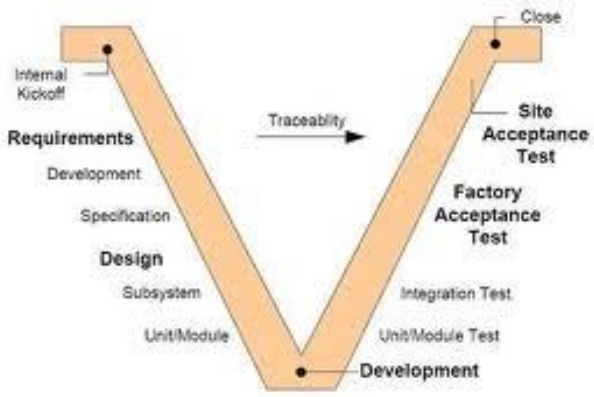
Szoftver hiba:

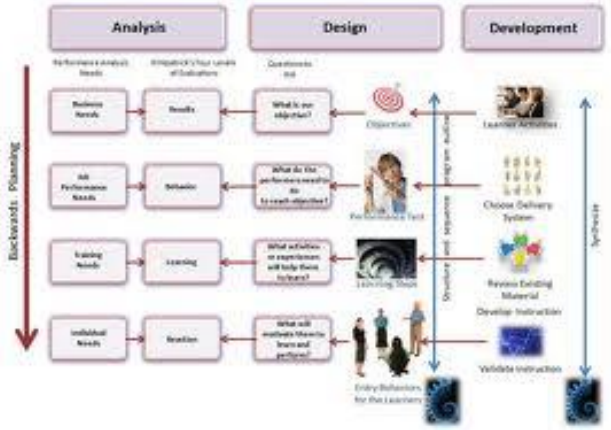
- Állandósult, tervezési hiba (szisztematikus meghibásodás)
- Hiba aktiválás a működési profil (bemenetek) függvénye

Eszközök a szolgáltatásbiztonság növelésére

- Hiba megelőzés: Hibaok megakadályozása
  - Fizikai hibák: Jó minőségű alkatrészek, árnyékolás,...
  - Tervezési hibák: Jó fejlesztési módszerek
- Hiba megszüntetés:
  - Tervezési fázis: Ellenőrzések (verifikáció, validáció)
  - Gyártási fázis: Tesztelés, diagnosztika, javítás
- Hibatűrés: Szolgáltatást nyújtani hiba esetén is
  - Működés közben: Hibakezelés, redundancia aktiválás
- Hiba előrejelzés: Hibák és hatásuk becslése
  - Mérés és „jóslás”, ez alapján megelőző karbantartás

Biztonságkritikus rendszerek fejlesztése





Ismétlés: Biztonsági követelmények

- Funkcionális és biztonságintegritási követelmények
  - Meghatározás: Kockázatelemzés alapján
  - Biztonságintegritási szint: SIL 1, 2, 3, 4
    - Folyamatos működés: Veszélyt okozó hibajelenség gyakorisága
    - Nem folyamatos: Veszélyt okozó hibajelenség valószínűsége
- A SIL követelmény teljesítésének ellenőrzése
  - Véletlen meghibásodásokra:
    - Számításokkal ellenőrizhető gyakoriság/valószínűség
  - Szisztematikus meghibásodásokra (pl. szoftver):
    - Számításokkal nem ellenőrizhető valószínűség
    - Módszer- és eszközkészlet előírt a fejlesztés során

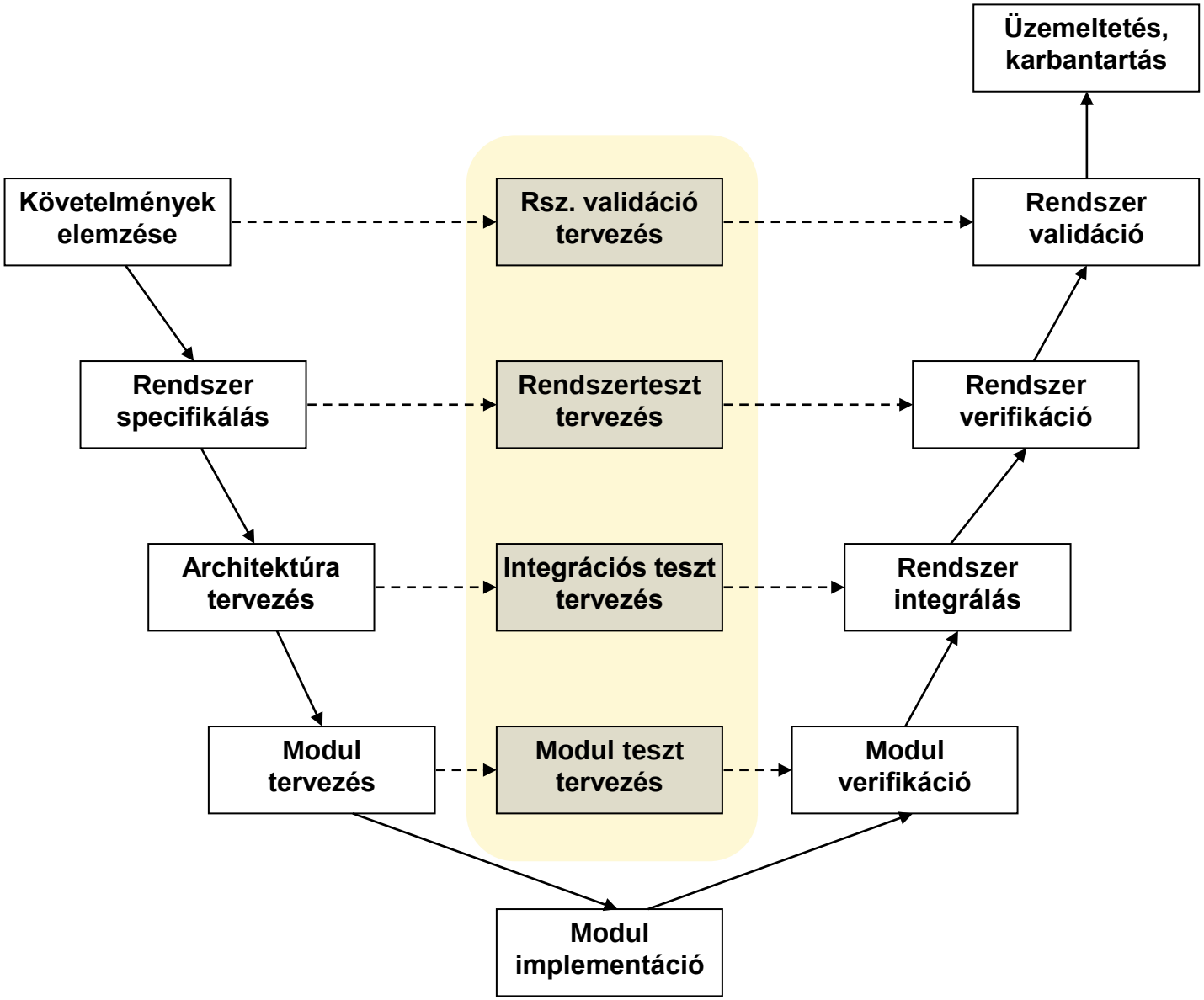
A szabványok szerepe

- Elismeri: Teljes hibamentesség nem garantálható komplex rendszer (pl. szoftver) esetén
  - Cél: Bennmaradó hibák számának csökkentése
- Szisztematikus meghibásodásokra: Komplex „megoldás-csomag” az egyes biztonságintegritási szintekhez
  1. Fejlesztési folyamat (életciklus modell)
  2. Előírt technikák és intézkedések (megoldás-csomag)
     - Egy-egy szabványban 50-100 módszer (+kombinációjuk)
  3. Előírt dokumentáció
  4. Szervezeti rend (felelősségek)

1. A fejlesztési folyamat

- Általában jól definiált fázisokat tartalmaz
  - Előre definiált fejlesztési lépések
  - Jól meghatározott specifikáció, ismert környezet
- Szigorú feltételekhez kötött előrelépés:
  Hangsúlyos a fejlesztési lépések ellenőrzése
  - Hibák kockázata nagy (felelősség)
  - Üzembehelyezés utáni javítás költsége nagy
  - Biztonság demonstrálása kell (hatósági engedélyezés)
- Szabványokban ajánlott fejlesztési folyamat
  - Jellegzetes az ún. V modell

Ellenőrzések tervezése a V-modellben

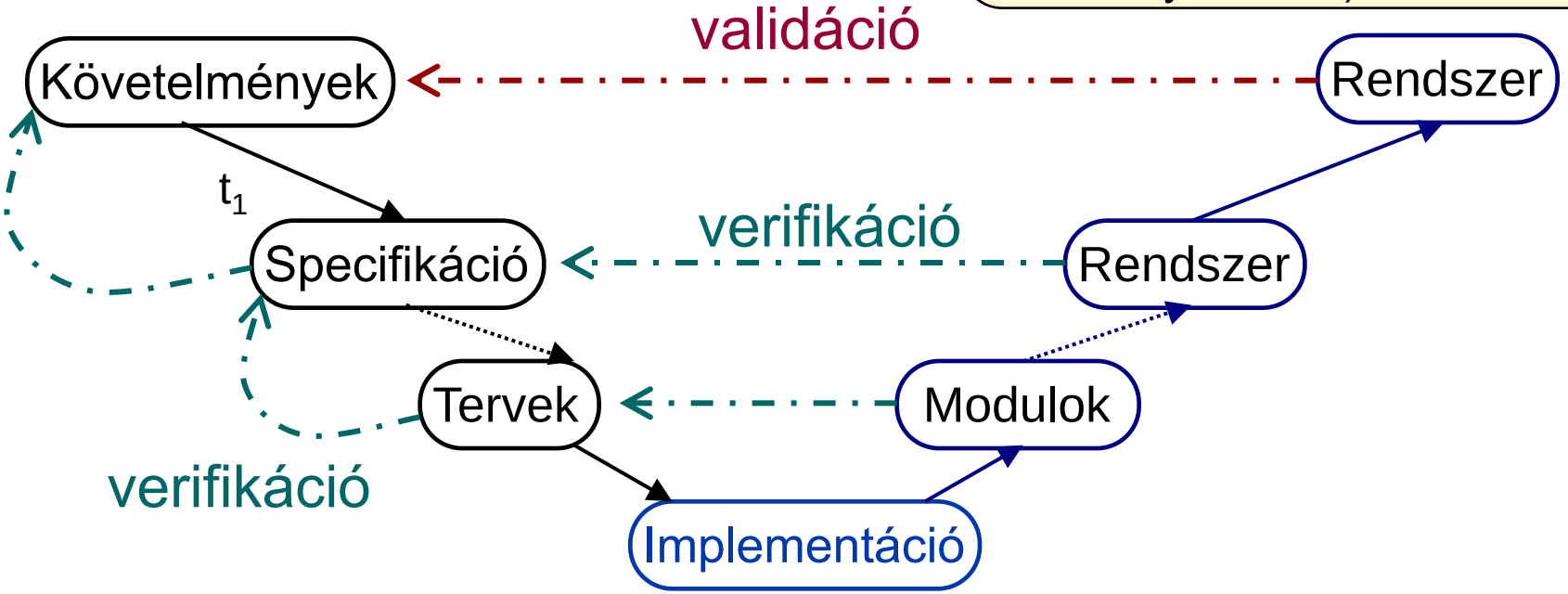


A verifikáció és validáció szerepe

- **Verifikáció** (igazolás):
  - Jól fejlesztem-e a rendszert?
- **Validáció** (érvényesítés):
  - Jó rendszert fejlesztettem-e?

Egy fejlesztési lépés eredménye megfelelő-e:
Tervek (formális) ellenőrzése, szimuláció, tesztelés

A rendszer megfelel-e a felhasználói elvárásoknak:
Tesztelés (használati környezetben), mérések



2. Módszerek és intézkedések megadása

Tesztelés

MÓDSZER / INTÉZKEDÉS	Említés helye	SW-SIL0	SW-SIL1	SW-SIL2	SW-SIL3	SW-SIL4
1. Valószínűségi tesztelés	B47	-	R	R	HR	HR
2. Teljesítmény tesztelés	D6	-	HR	HR	M	M
3. Funkcionális és “fekete doboz” tesztelés	D3	HR	HR	HR	M	M
4. Modellezés	D5	-	R	R	R	R
Követelmény: 1. Az 1, 2, 3 és 4 szoftver-biztonságintegritási szintek esetén a 2. és 3. módszer kombinációja jóváhagyottnak tekintendő.						

- Előírások:
  - M Kötelező
  - HR Nyomatékosan ajánlott (elhagyása indoklást igényel)
  - R Ajánlott (kombinációból kihagyható)
  - – Nincs javaslat vagy ellenérv
  - NR Ellenjavallt (használata indoklást igényel)
- Módszerkombinációk választhatók

Példa: A technikák további finomítása

- Funkcionális és fekete doboz tesztelés (D3):

1.	Test Case Execution from Cause Consequence Diagrams	B.6	-	-	-	R	R
2.	Prototyping/Animation	B.49	-	-	-	R	R
3.	Boundary Value Analysis	B.4	R	HR	HR	HR	HR
4.	Equivalence Classes and Input Partition Testing	B.19	R	HR	HR	HR	HR
5.	Process Simulation	B.48	R	R	R	R	R

- Teljesítmény tesztelés (D6):

TECHNIQUE/MEASURE		Ref	SWS ILO	SWS IL1	SWS IL2	SWS IL3	SWS IL4
1.	Avalanche/Stress Testing	B.3	-	R	R	HR	HR
2.	Response Timing and Memory Constraints	B.52	-	HR	HR	HR	HR
3.	Performance Requirements	B.46	-	HR	HR	HR	HR

Példa: Módszerek és intézkedések megadása

- IEC 61508:
  Functional safety in electrical / electronic / programmable electronic safety-related systems
- Példa:
  Szoftver architektúra tervezés

Table A.2 – Software design and development: software architecture design (see 7.4.3)

	Technique/Measure*	Ref	SIL1	SIL2	SIL3	SIL4
1	Fault detection and diagnosis	C.3.1	---	R	HR	HR
2	Error detecting and correcting codes	C.3.2	R	R	R	HR
3a	Failure assertion programming	C.3.3	R	R	R	HR
3b	Safety bag techniques	C.3.4	---	R	R	R
3c	Diverse programming	C.3.5	R	R	R	HR
3d	Recovery block	C.3.6	R	R	R	R
3e	Backward recovery	C.3.7	R	R	R	R
3f	Forward recovery	C.3.8	R	R	R	R
3g	Re-try fault recovery mechanisms	C.3.9	R	R	R	HR
3h	Memorising executed cases	C.3.10	---	R	R	HR
4	Graceful degradation	C.3.11	R	R	HR	HR
5	Artificial intelligence - fault correction	C.3.12	---	NR	NR	NR
6	Dynamic reconfiguration	C.3.13	---	NR	NR	NR
7a	Structured methods including for example, JSD, MASCOT, SADT and Yourdon.	C.2.1	HR	HR	HR	HR
7b	Semi-formal methods	Table B.7	R	R	HR	HR
7c	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	---	R	R	HR
8	Computer-aided specification tools	B.2.4	R	R	HR	HR

NOTE – The measures in this table concerning fault tolerance (control of failures) should be considered with the requirements for architecture and control of failures for the hardware of the programmable electronics in IEC 61508-2.

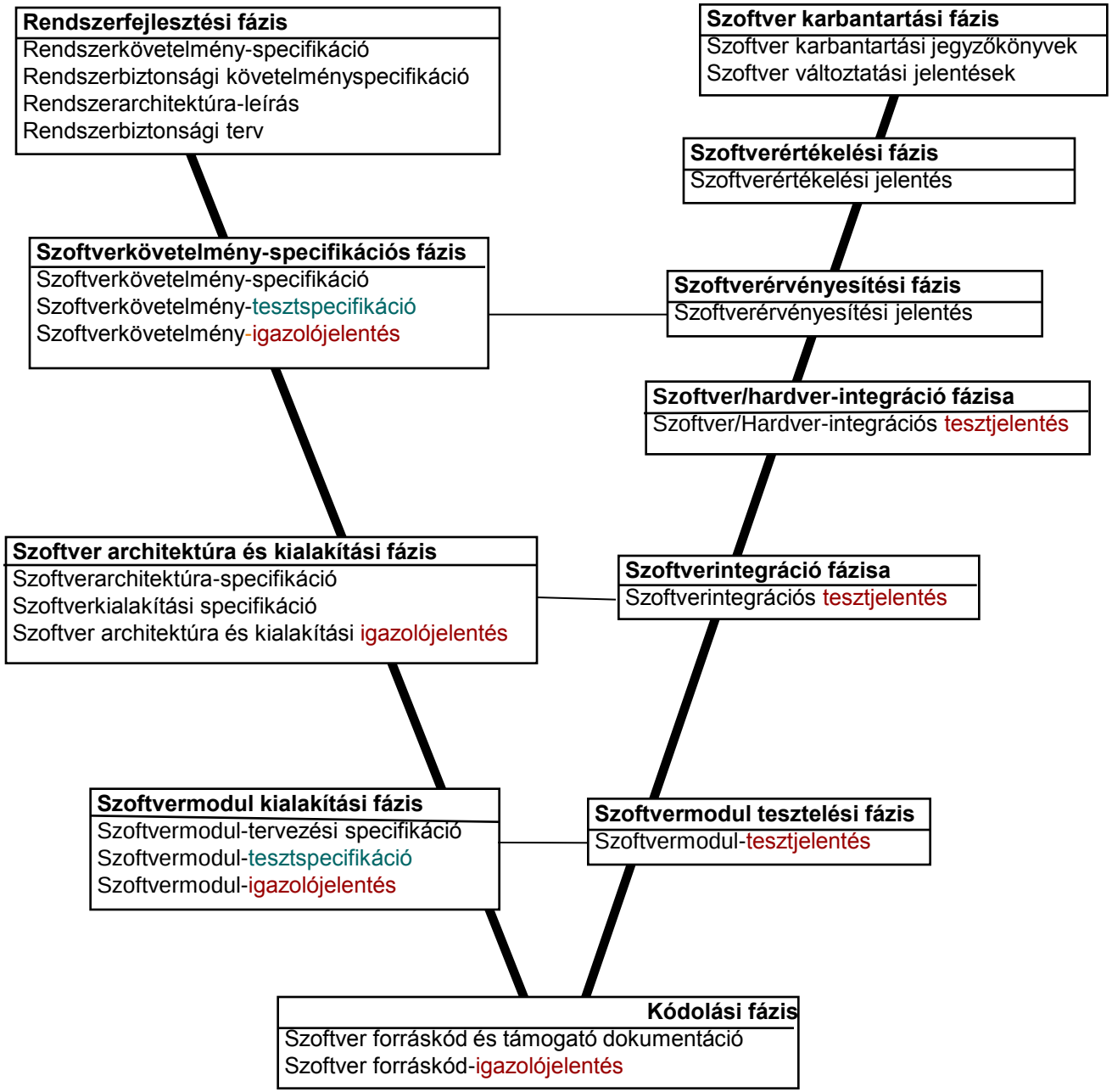
* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measures has to be satisfied.

3. A dokumentáció követelményei

- Dokumentáció típusa
  - Átfogó (pl. fejlesztési terv, verifikációs terv)
  - Életciklus fázishoz kötődő (pl. teszt jelentés)
- Dokumentum kereszt-referencia táblázat
  - Melyik életciklus fázishoz milyen dokumentáció
  - Dokumentumok egymásra épülése
- Dokumentumok követhetősége szükséges
  - Ugyanazon terminológia, rövidítések, elnevezések
- Dokumentumok összevonhatók
  - Részlet nem veszhet el
  - De független szereplők dokumentumai nem vonhatók össze

Példa: Előírt dokumentáció (EN50128)

Szoftvertervezési fázis
Szoftverfejlesztési terv
Szoftver-minőségbiztosítási terv
Szoftverkonfiguráció menedzselési terv
Szoftverigazolási terv
Szoftverintegrációs teszterv
Szoftver/hardver-integrációs teszterv
Szoftverérvényesítési terv
Szoftver-karbantartási terv

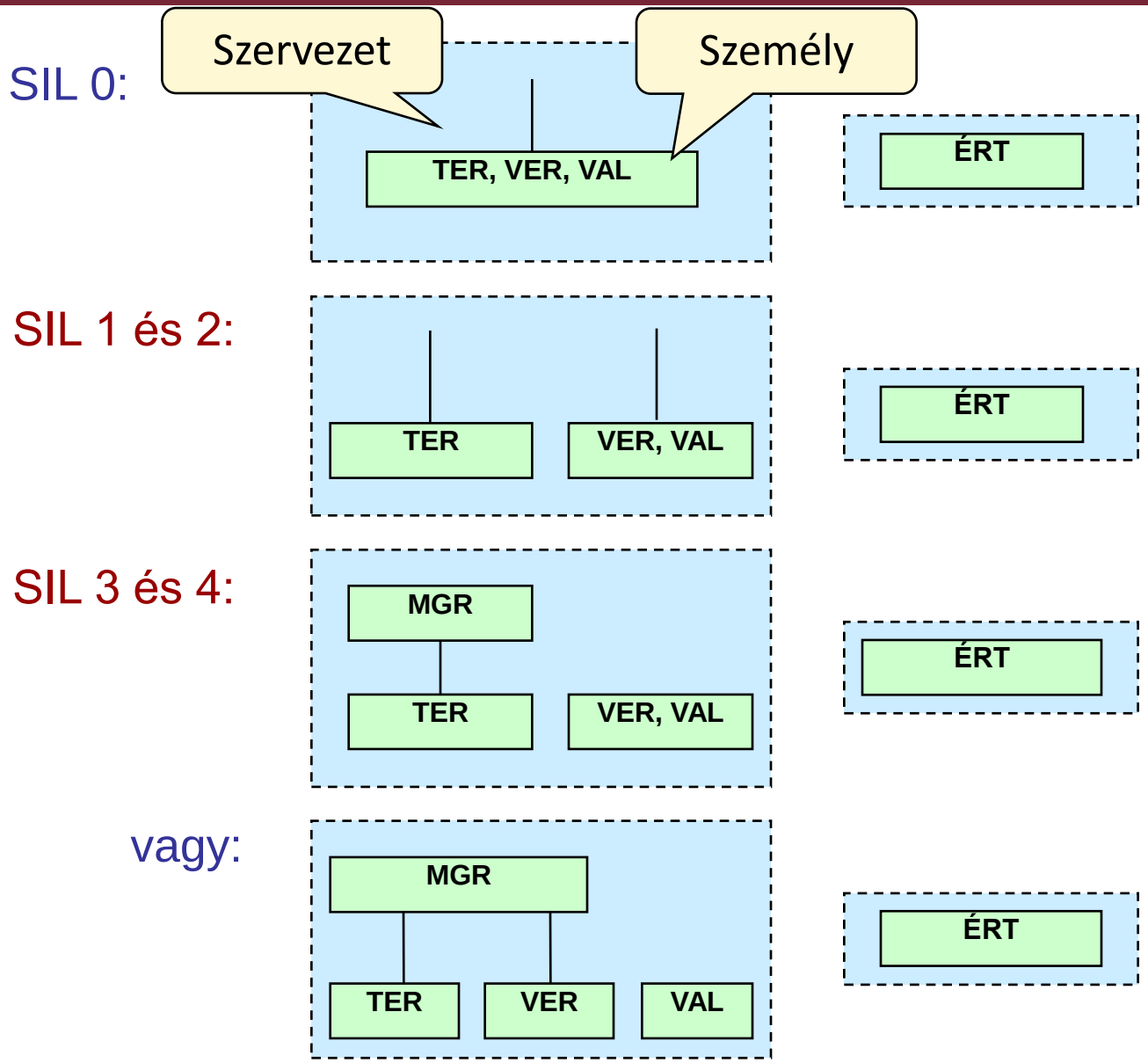


EN 50128:
kb. 30 dokumentum!

4. Szervezeti rend

- Minőségi illetve biztonsági szervezet létrehozása – a biztonságmenedzselés bizonyítása
  - ISO 9001 vonatkozó részeinek alkalmazása
  - Konfigurációmenedzselés
- Képzettség (alkalmasság) igazolása
- Szerepkörök:
  - TER: Tervező (elemző, tervező, kódoló, unit tesztelő)
  - VER: Verifikátor (igazoló)
  - VAL: Validátor (érvényesítő)
  - ÉRT: Értékelő (független felülvizsgáló)
  - MGR: Projekt menedzser
  - MIN: Minőségbiztosítási felelős

Példa: Minimális függetlenség követelményei



Összefoglalás

- Biztonságkritikus rendszerek alapfogalmai
  - Veszély, kockázat
  - THR és biztonságintegritási szintek
- Szolgáltatásbiztonság
  - Jellemzők
  - Hibaok −> hiba −> hibajelenség hatáslánc
  - Eszközök a szolgáltatásbiztonság növelésére
- Fejlesztési folyamat specialitásai
  - Módszerek és technikák
  - Életciklus és dokumentáció: Jól meghatározott fázisok
  - Szervezeti rend