Közlekedési automatika

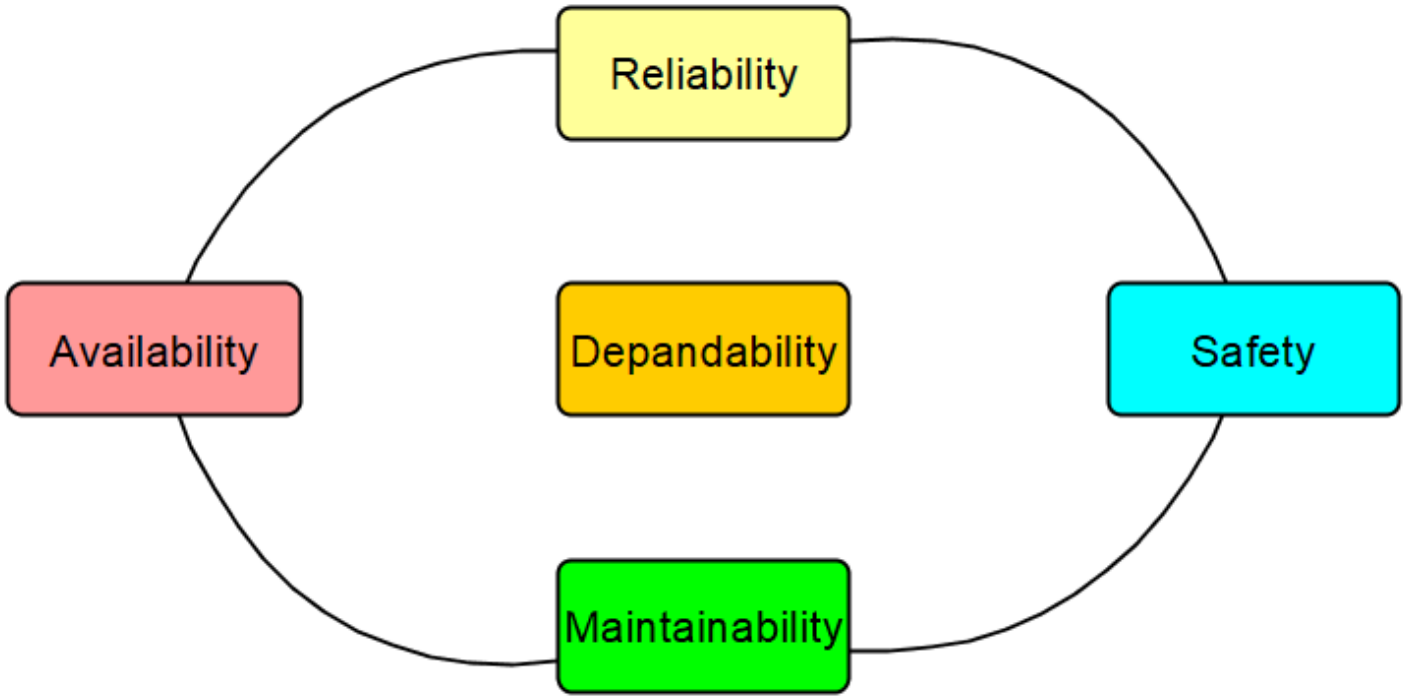
Biztonságintegritás, életciklus modellek

Dr. Sághi Balázs diasora alapján
összeállította, kiegészítette: Lövétei István Ferenc

BME Közlekedés- és Járműirányítási Tanszék
2019

Tartalomjegyzék

Bevezetés – Biztonság, RAMS



- Depandability:
  - a rendszer azon tulajdonsága, mely lehetővé teszi a szolgáltatása iránti bizalmat,
- Reliability – működőképesség:
  - R(t) – λ – T,
  - elemek, soros és párhuzamos rendszerek ,
  - lásd korábbi gyakorlati órák,
- Maintainability – karbantarthatóság:
  - M(t) – ha a rendszer karbantartható,
  - javítások, javítható rendszerek,
  - lásd gyakorlati órák,
- Availability – rendelkezésre állás:
  - A(t), A_{ss} - ha a rendszer javítható, (és ha nem?)
  - lásd gyakorlati órák,
- Safety - biztonság ???????

Bevezetés - Biztonság

a célunk az, hogy olyan rendszereket hozzunk létre, amelyek a **saját feladatukat** a **megfelelő* biztonsággal** hajtsák végre….

*megfelelő: társadalmilag elviselhető kockázati szinten

Bevezetés - Biztonság

- **Safety – Biztonság (def.):** egy rendszer azon tulajdonsága, hogy nem veszélyezteti az emberi életet és a környezetét. – *általánosan*
  - az **elfogadhatatlan kockázatoktól** való mentesség – pl: vasútbiztonsági szabványok, MSZ EN 50126, villamos/elektronikus/programozható elektronikus biztonsági rendszerek IEC 61508,
  - az **ésszerűtlen kockázatok** hiánya – járműipari szabvány, ISO 26262,
  - az **elfogadhatatlan károk kockázatától** való mentesség – EUROCONTROL,
  - az az állapot, amikor a repüléssel összefüggő kockázatok amelyek közvetve vagy közvetlenül a repülőgépek üzemeltetéséhez kapcsolódnak, **elfogadható szintre** vannak csökkentve, és ott **kontrollálva** vannak – ICAO (International Civil Aviation Organization).

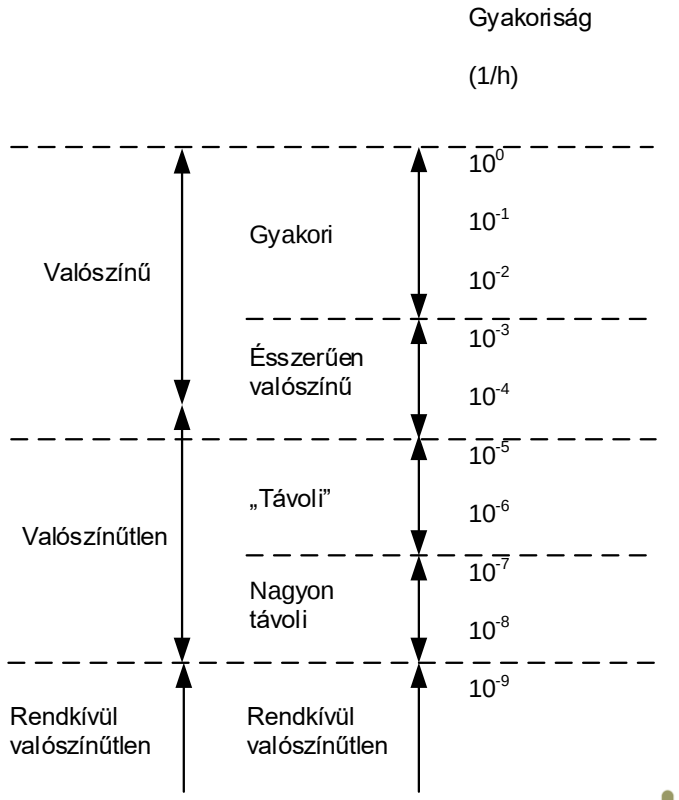
- **Safety – related (or critical) system – Biztonságkritikus rendszer:** olyan rendszer, amely egy berendezés vagy üzem biztonságát biztosítja.
  - olyan rendszer, amely meghibásodása vagy hibás működése emberek halálát/sérülését, a környezet/berendezések károsodását okozhatja.

Bevezetés - Kockázatosztályozás

Valószínűségi szint		Kárkihatási kategóriák			
		Katasztrofális 4	Kritikus 3	Csekély 2	Elhanyagolható 1
gyakori	A	K4			
valószínű	B				
néha	C		K3		
alig	D			K2	
valószínűtlen	E				
rendkívül valószínűtlen	F				K1

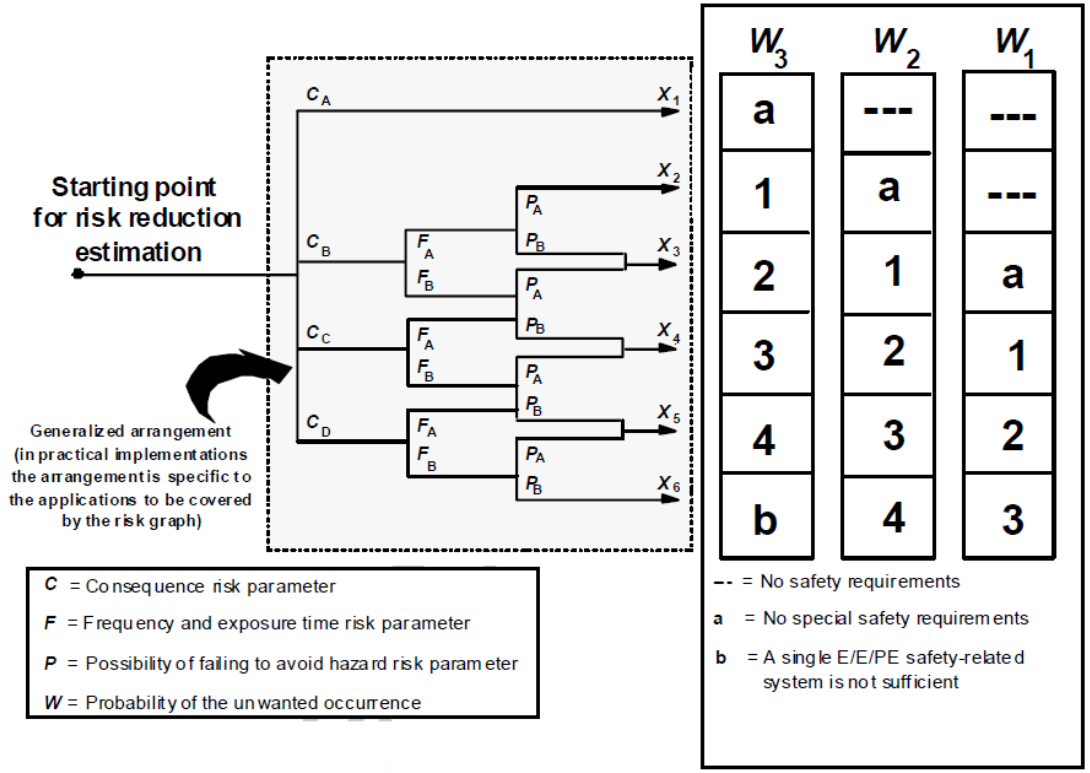
Risk probability		Risk severity				
		Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E

Figure 2-13. Safety risk assessment matrix



Bevezetés - Kockázatosztályozás

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



Közúti közlekedés - Kockázatcsökkentés

- **Gépi úton ellenőrzött utasítások jelzések révén.**
  - **Ellenőrző mechanizmusok biztosítják, hogy ne jelenhessen meg olyan jelzés, amelynek következtében veszélyes forgalmi szituáció alakulhat ki (kizáró mátrix),**
  - **még meghibásodás esetén se.**
- Az utasítások betartása humán döntésen alapul.
  - Szabályozott rendszerhozzáférés,
  - Újabban: támogató és beavatkozó rendszerek a járműveken.

Légi közlekedés - Kockázatcsökkentés

- Utasítások adása humán döntés.
- Utasítások betartása humán döntés.
- Alapja:
  - **támogató eszközök – légiforgalmi irányítás,**
  - magas szintű képzés,
  - folyamatos tréning.
- Műszaki biztonsági irányítói rendszerek:
  - **ütközéselkerülő rendszerek,**
  - **radarok, szenzorok, stb…**
  - **autopilóta.**

Vasúti közlekedés - Kockázatcsökkentés

- Jelzésadás – menetengedély:
  - gépi úton ellenőrzött,
  - biztosítóberendezések
- Jelzések betartása:,
  - korán megjelenik a gépi úton való kikényszerítés,
  - vonatmegállító, vonatbefolyásoló berendezések,
  - automata vonatvezérlő rendszerek.

RATP, Paris, IRJ

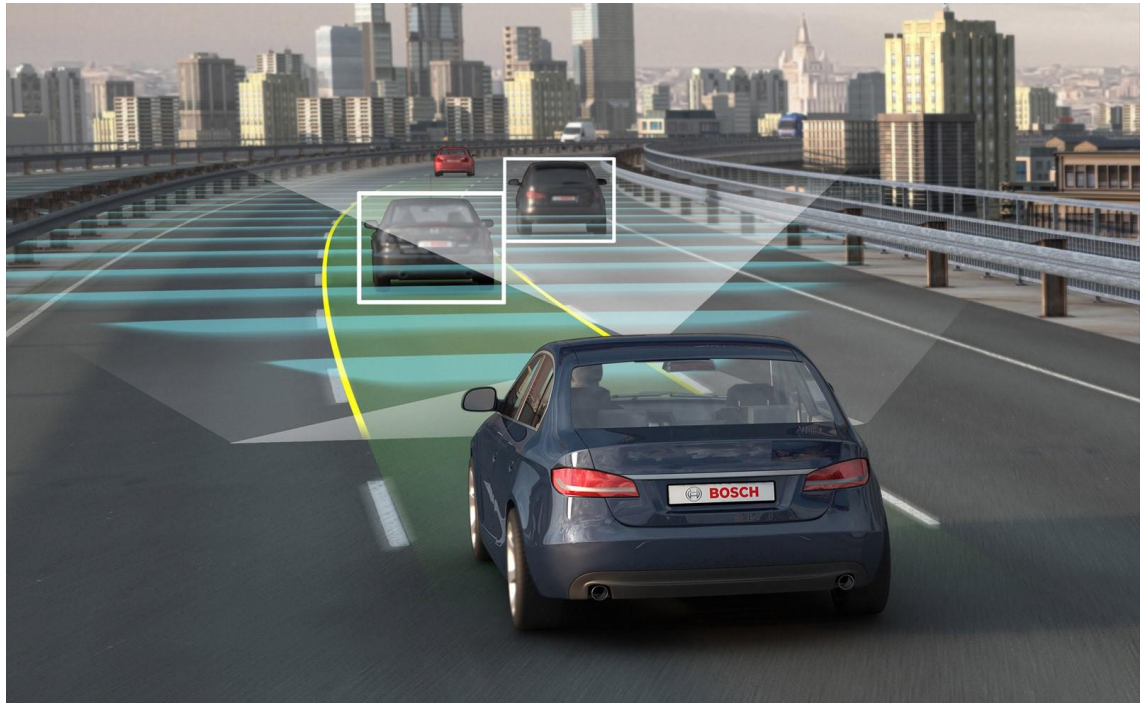
Vizi közlekedés - Kockázatcsökkentés

- Vizi közlekedési szabályok:
  - nemzetközi jelzési rendszer,
  - humán képesítés,
- Kikötői közlekedés:
  - dedikált, képzett pilóták – Rotterdam, Panama-csatorna,
- Automatizálási rendszerek:
  - **Automata dokkolás – kikötői irányítói rendszerek,**
    - kikötői kapacitások növelése,
    - ütközések elkerülése.

Autodocking Technology

Járműirányítás - Kockázatcsökkentés

- Autonóm funkciók:
  - az ember szerepének csökkentése,
- Járművek irányítási feladatai:
  - **szenzorok, aktuátorok,**
  - **irányítási algoritmusok implementációja,**
- Járművek és infrastruktúra közötti kommunikáció:
  - hálózatok, hálózati irányítási algoritmusok.

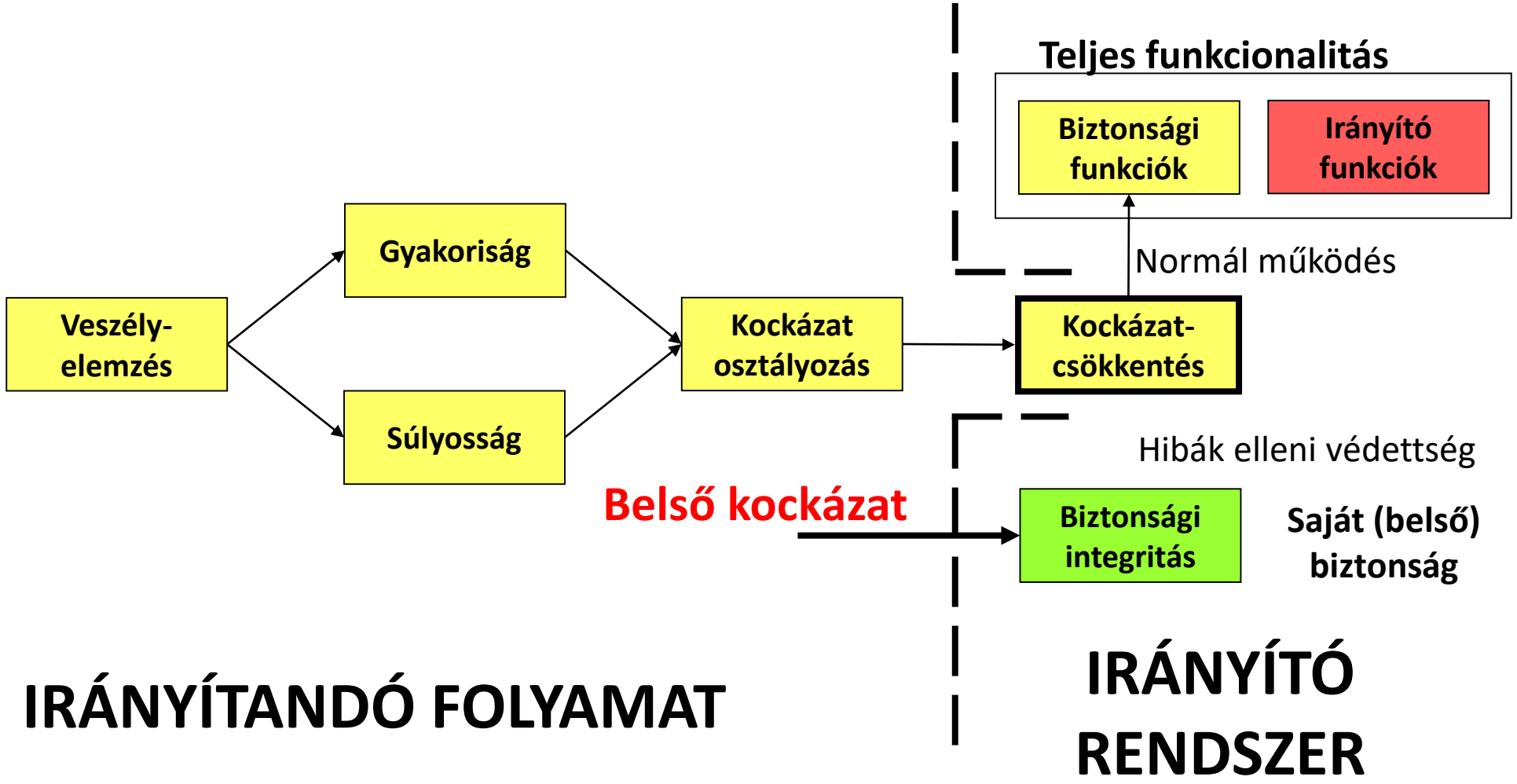


The Road Ahead

Gépi eszközök az irányítási rendszerben

- A kockázatcsökkentést megvalósító eszközök a közlekedésben:
  - folyamatirányító rendszerek – **biztonsági rendszerek.**
- Milyen tulajdonságokat kell támasztani az irányító rendszerrel szemben?
- Hogyan kell megvalósítani az elvárt viselkedést?
- Kell-e szabályokat alkalmazni a rendszer (komponens) fejlesztése során?
- Milyen biztonsági funkciót - funkciókat kell megvalósítani?

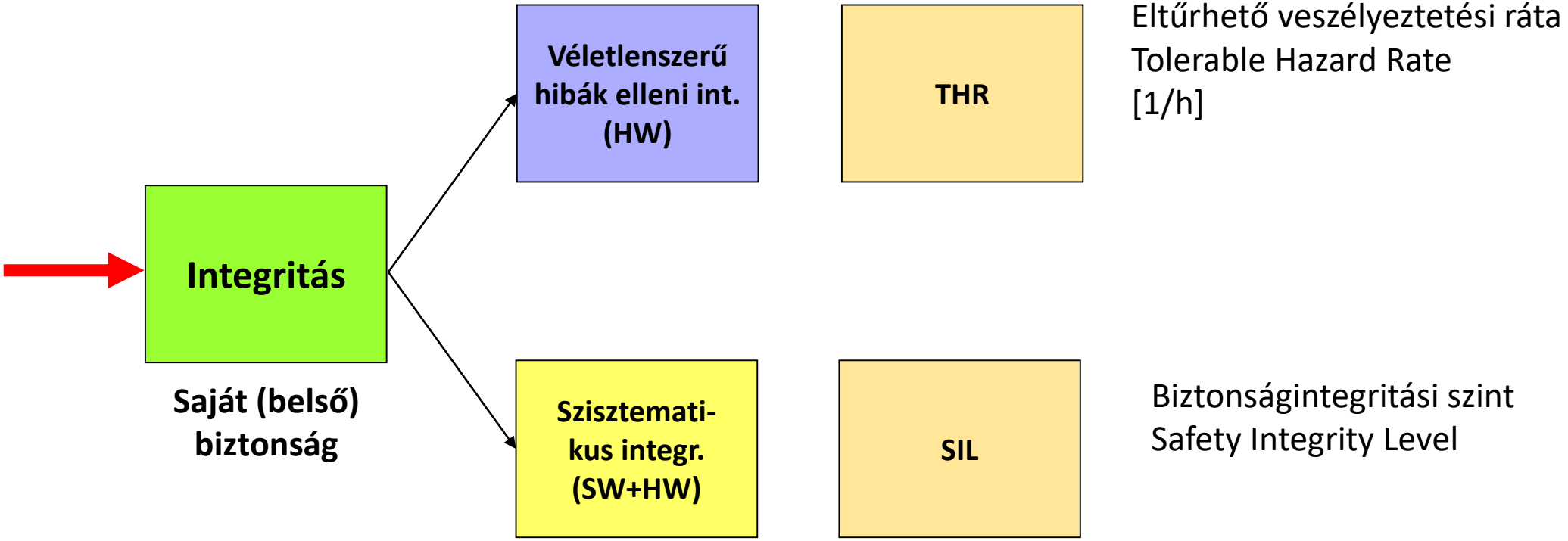
Biztonsági funkciók - Biztonságintegritás



A biztonsági rendszerek belső veszélyforrásai

- Szisztematikus hibák:
  - A rendszer **létrehozása során** elkövetett emberi hibák, amelyek
  - a rendszer üzemelése során helytelen működést okoznak.
  - Specifikációs hibák, tervezési hibák, gyártási hibák, szoftverhibák stb.
  - Fellépési gyakoriság nem adható meg.
- Véletlenszerű meghibásodások hibák:
  - A rendszer **üzemelése során** fellépő meghibásodások.
  - Fellépési gyakoriságuk megadható.
  - A fellépési gyakoriságot befolyásolja az üzemmód, környezeti hatások, túlterhelés stb.

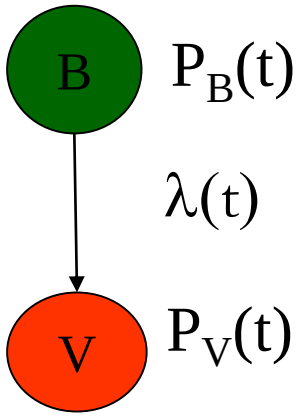
Biztonságintegritási szintek és hibakezelés



Biztonságintegritás – általános megközelítés

- **biztonságintegritás (def):** annak a valószínűsége, hogy egy biztonsági irányítórendszer az előírt biztonsági funkciókat egy adott időszakban **meghatározott körülmények** között megfelelően végrehajtja, azaz nem lép fel **veszélyeztető meghibásodás.**

véletlenszerű meghibásodásokra:



a biztonság kívánt foka:

$$P_B(t) \geq P_{Bmin} \leftrightarrow P_V(t) \leq P_{Vmax}$$

Biztonságintegritási szintek – iparági megközelítés, példák

- Safety Integrity Level – vasúti szabványok, MSZ EN 50126:
  - egy olyan diszkrét érték, amely specifikálja a biztonságintegritási követelményeket egy biztonságkritikus rendszer **biztonsági funkcióival** szemben,
- Automotive Safety Integrity Level – közúti járművek funkcionális biztonsága, ISO 26262:
  - egy a négy szint közül, amelyek specifikálják egy elem vagy rendszer ISO 26262 szerinti követelményeit, és amelyek specifikálják azokat a **módszereket**, amelyekkel elkerülhető az **ésszerűtlen maradék kockázat**, a „D” a legszigorúbb, az „A” a legkevésbé szigorú szintet jelenti.

Biztonságintegritási szintek – iparági megközelítés, példák

- Safety Integrity Level - villamos/elektronikus/programozható elektronikus biztonsági rendszerek IEC 61508:
  - egy diszkrét szint (egy a négy lehetséges közül) amely egy biztonságintegritási értéknek felel meg, ahol a „4”-es a legmagasabb, az „1”-es a legalacsonyabb szintet jelenti.
- Design Assurrance Level – légijárművek, DO-178B, csak SW!
  - öt szintet állapít meg az alapján, hogy egy hiba milyen lehetséges **következménnyel** járhat, a legalacsonyabb szint a DAL E, a legmagasabb a DAL A (olyan hibák, amelyek több ember halálát és a légijármű súlyos károsodását okozhatják).

A biztonságintegritási szintek száma és értelmezése, példák

Biztonsági integritási szintek **SIL**	Az **irányító** rendszer veszélyes meghibásodásának valószínűsége [h^{-1}]	A **védelmi** rendszer elmaradt működéseinek aránya az összes kívánt működéshez képest
4	10^{-9} … 10^{-8}	10^{-5} … 10^{-4}
3	10^{-8} … 10^{-7}	10^{-4} … 10^{-3}
2	10^{-7} … 10^{-6}	10^{-3} … 10^{-2}
1	10^{-6} … 10^{-5}	10^{-2} … 10^{-1}
0	---	---

A biztonságintegritási szintek száma és értelmezése, példák

TFFR [h^{-1}]	SIL attribution	SIL qualitative measures
$10^{-9} \leq TFFR < 10^{-8}$	4	Defined in sector-specific standards
$10^{-8} \leq TFFR < 10^{-7}$	3	
$10^{-7} \leq TFFR < 10^{-6}$	2	
$10^{-6} \leq TFFR < 10^{-5}$	1	

- TFFR: Tolerable Functional Failure Rate:
  - egy funkció eltűrhető veszélyes meghibásodási rátája,
  - új megközelítés.

A biztonságintegritási szintek száma és értelmezése, példák

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

A biztonságintegritási szintek száma és értelmezése, példák

ASIL	Random hardware failure target values
D	$<10^{-8}\ h^{-1}$
C	$<10^{-7}\ h^{-1}$
B	$<10^{-7}\ h^{-1}$

NOTE The quantitative target values described in this table can be tailored as specified in 4.1 to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car).

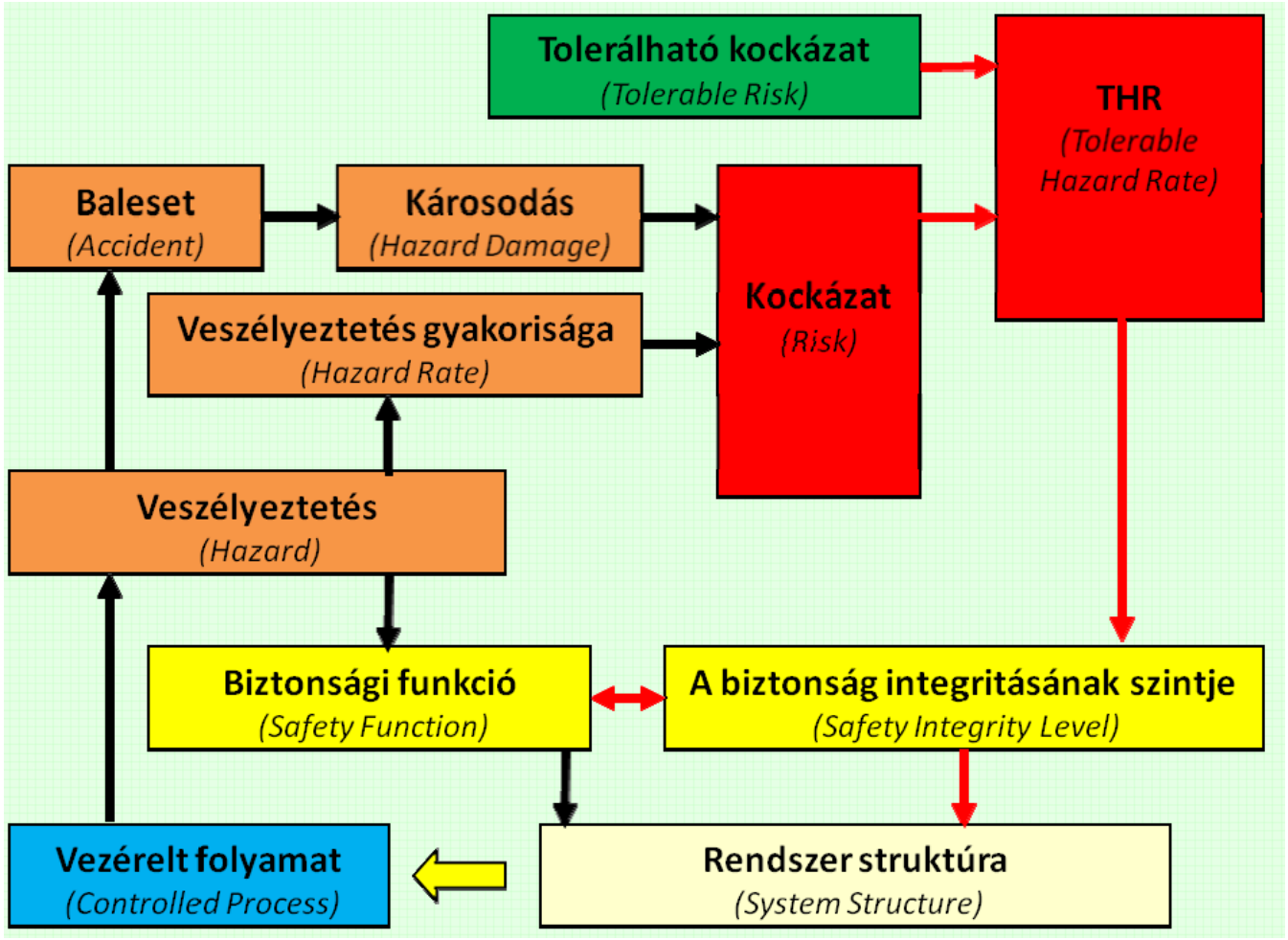
A biztonságintegritási szintek száma és értelmezése, példák

Hazard Classification	Development Assurance Level	Maximum Probability per Flight Hour
Catastrophic	A	10^{-9}
Hazardous	B	10^{-7}
Major	C	10^{-5}
Minor	D	--
No Effect	E	--

A biztonságintegritási szintek összehasonlítás

Domain	Domain-Specific Safety Levels				
Automotive (ISO 26262)	QM	ASIL-A	ASIL-B/C	ASIL-D	-
General (IEC-61508)	-	SIL-1	SIL-2	SIL-3	SIL-4
Aviation (DO-178/254)	DAL-E	DAL-D	DAL-C	DAL-B	DAL-A
Railway (CENELEC 50126/128/129)	-	SIL-1	SIL-2	SIL-3	SIL-4

SIL meghatározás biztonsági funkciók számára, példa

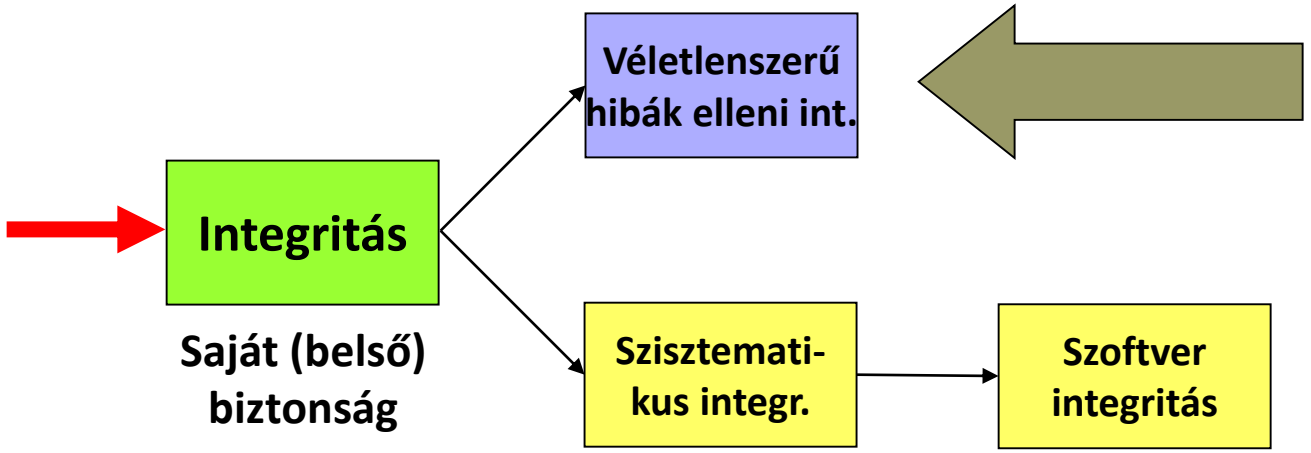


- *A kockázatelemzés, illetve a szabványok azt deklarálják, hogy lesz egy adott mértékű maradék kockázat, vagyis* ***a rendszerünkbe beépítjük a veszteség lehetőségét!***

az ábra forrása: prof. Ing. Karol Rástocny, PhD; doc. Ing. Izabela Krbilová, PhD; Biztosítóberendezések biztonságának értékelése, egyetemi előadás, Budapest, 2011, link

Biztonságintegritási szintek és hibakezelés

Véletlen hardver hibák elleni védelem:
- A biztonsági szintnek megfelelő megbízhatóság elérése, biztonsági stratégiák



Hibadetektálás
Hibatűrés
Biztonsági állapot

A hibák
- **elkerülése**
- **eltávolítása**

Diverz kialakítás

Szisztematikus hibák elleni védelem:

- **Minőségbiztosítás a teljes életciklusban (szervezett folyamat)**
- **A biztonsági szintnek megfelelő fejlesztési módszerek alkalmazása**

A szisztematikus hibák elleni védelem

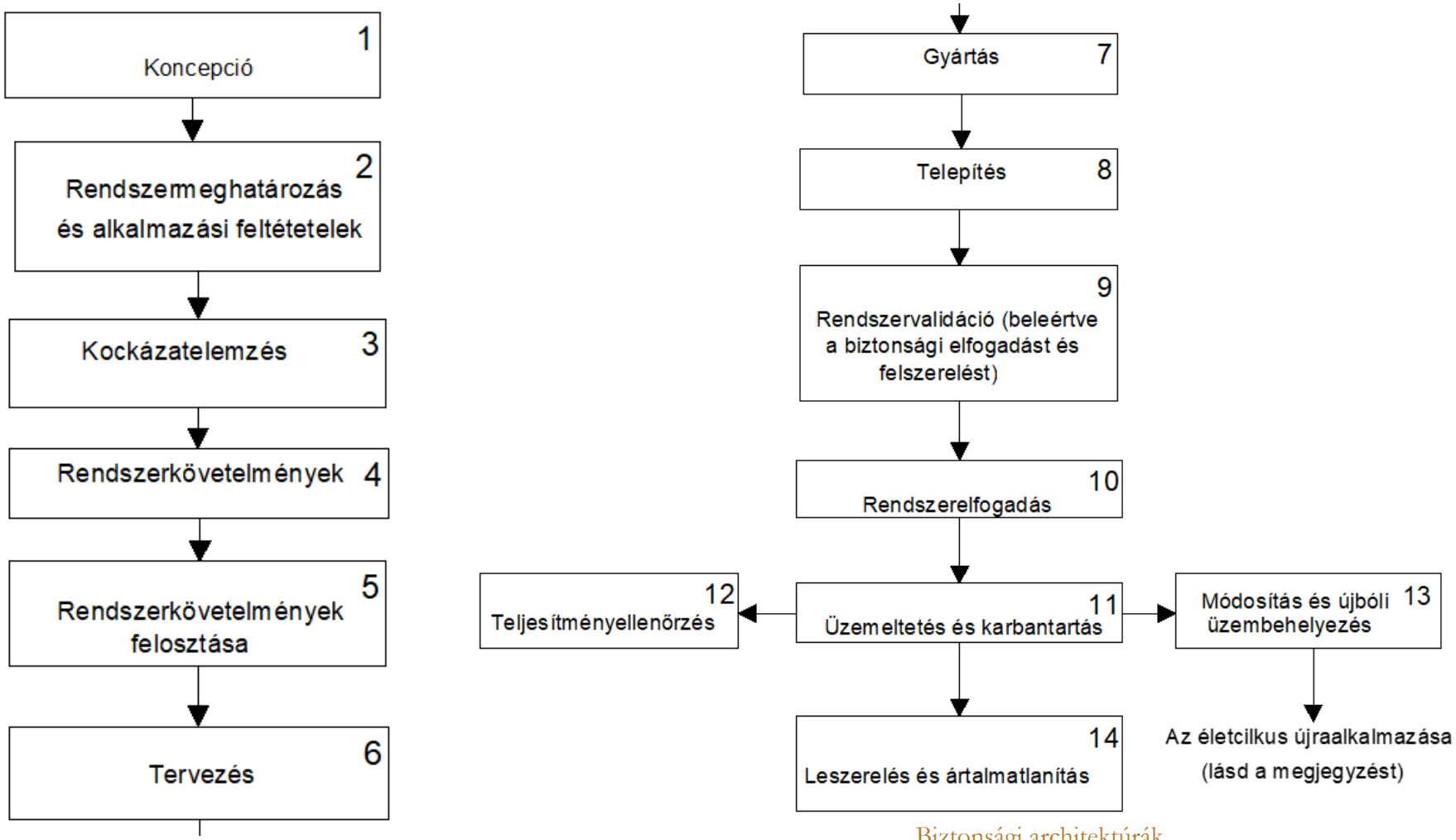
- A fejlesztési/tervezési/gyártási folyamat szabályozása → életciklus modellek
  - **(követelmény~) követhetőség, ellenőrizhetőség, áttekinthetőség,**
- Személyi függetlenségek:
  - ellenőrizhetőség,
- Megfelelő módszerek alkalmazása:
  - hibaelkerülés.

Életciklus modellek - meghatározás

- Biztonsági életciklus modell:
  - olyan **szükséges cselekvések összessége** a biztonságkritikus rendszerek megvalósítása során, amely a koncepciónál kezdődik és akkor fejeződik be, amikor a villamos/elektronikus/programozható elektronikus biztonságkritikus rendszerek és más kapcsolódó kockázatcsökkentő intézkedések* tovább nem kerülnek felhasználásra – IEC 51608,
  - olyan **azonosított szakaszok sorozatának összessége**, amely során egy termék áthalad a koncepciótól kezdve az ártalmatlanításáig – vasúti szabványok,
  - azon **fázisok teljessége**, amelyek egy termék koncepciójától a leszereléséig tartanak – ISO 26262.

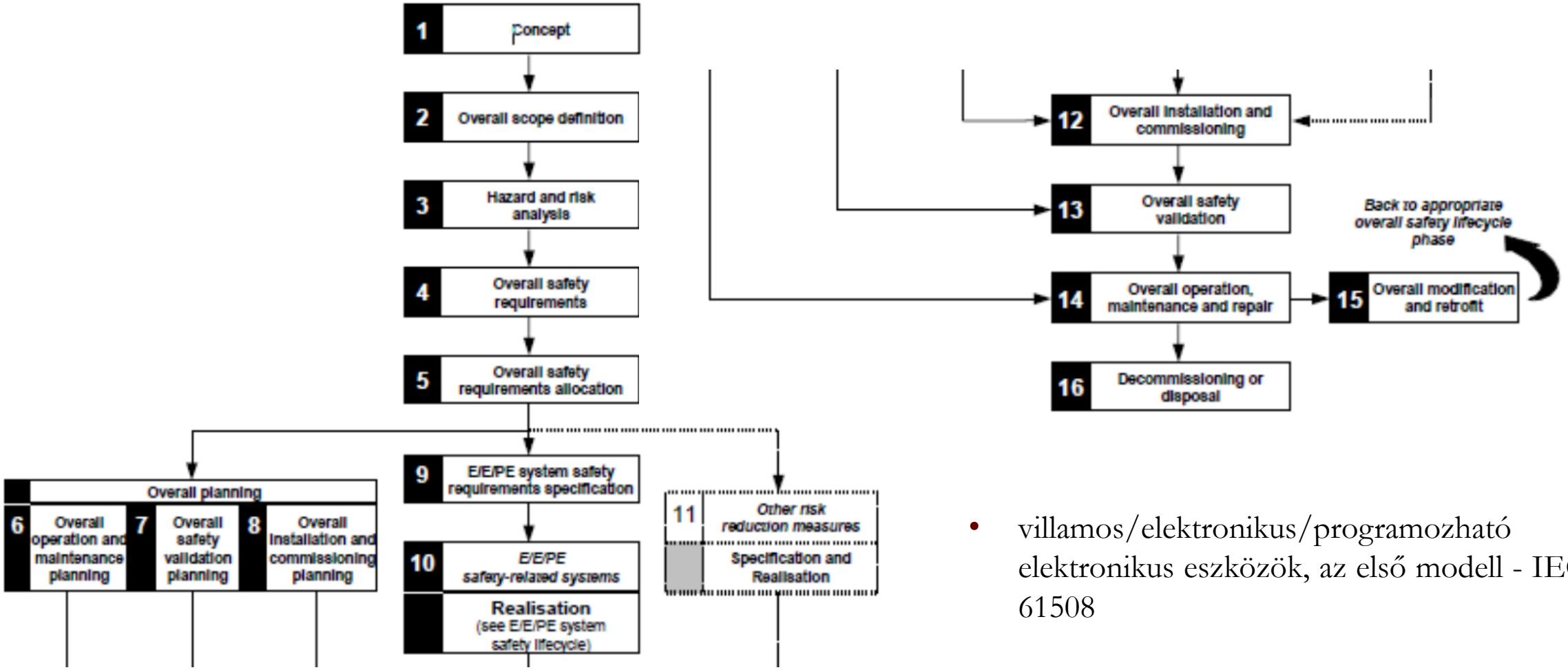
*például egy mechanikus szelep egy ilyen rendszerben

Életciklus modellek – példa



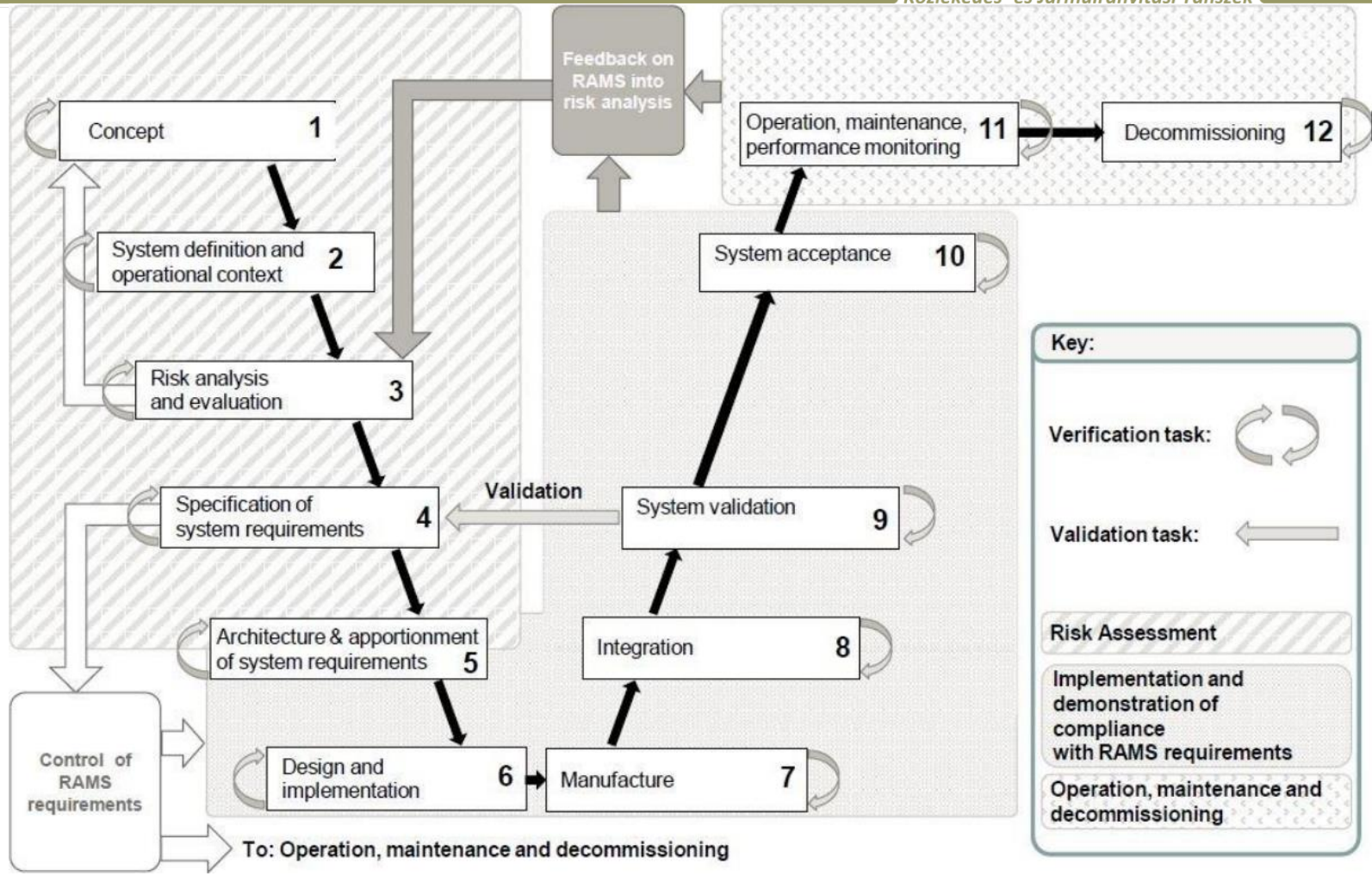
- Megjegyzés: Az a fázis, amelynél a módosítás a rendszer életciklusába belép, függ a módosítandó rendszertől és a szóban forgó módosítás jellegétől

Életciklus modellek - példa



- villamos/elektronikus/programozható elektronikus eszközök, az első modell - IEC 61508

Életciklus modellek – példa, V – vízesés modell



- Vasútbiztonsági szabványokban definiált biztonsági életciklus modell - MSZ EN 50126

Verifikáció & Validáció

- Verifikáció:
  - annak az objektív bizonyítása, hogy a meghatározott követelmények teljesülnek:
    - a fázis bemenő követelményei a fázis kimenetén teljesítésre kerülnek,
    - tesztek, elemzések,
- Validáció:
  - annak az objektív bizonyítása, hogy egy meghatározott célú alkalmazás követelményei teljesülnek,
    - a rendszerkövetelményeknek való megfelelőség,
- Sikeres verifikációs lépések ≠sikeres validáció!

Verifikáció & Validáció

My Definition of Validation

VERIFICATION

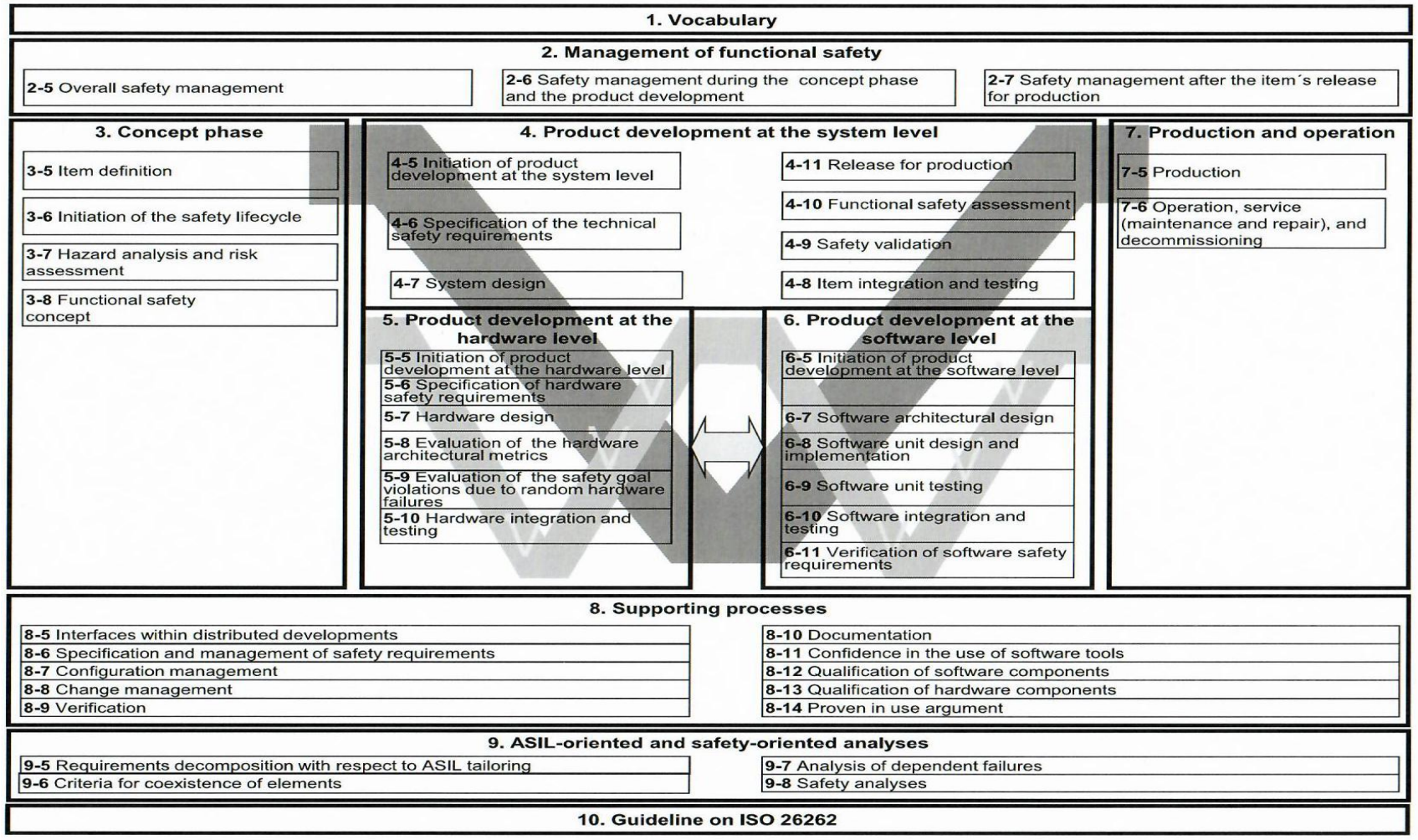
- 2 sleeves?
- Is it size L?
- Is it blue?
- Are any buttons missing?

VALIDATION

- Does it fit?
- Is it comfortable to drive in?
- Does the colour match my eyes?
- Can I afford it?
- Is it good quality?
- Will my date like it?

V&V

Életciklus modellek - példa



Menedzsment - keretrendszer

Fejlesztés

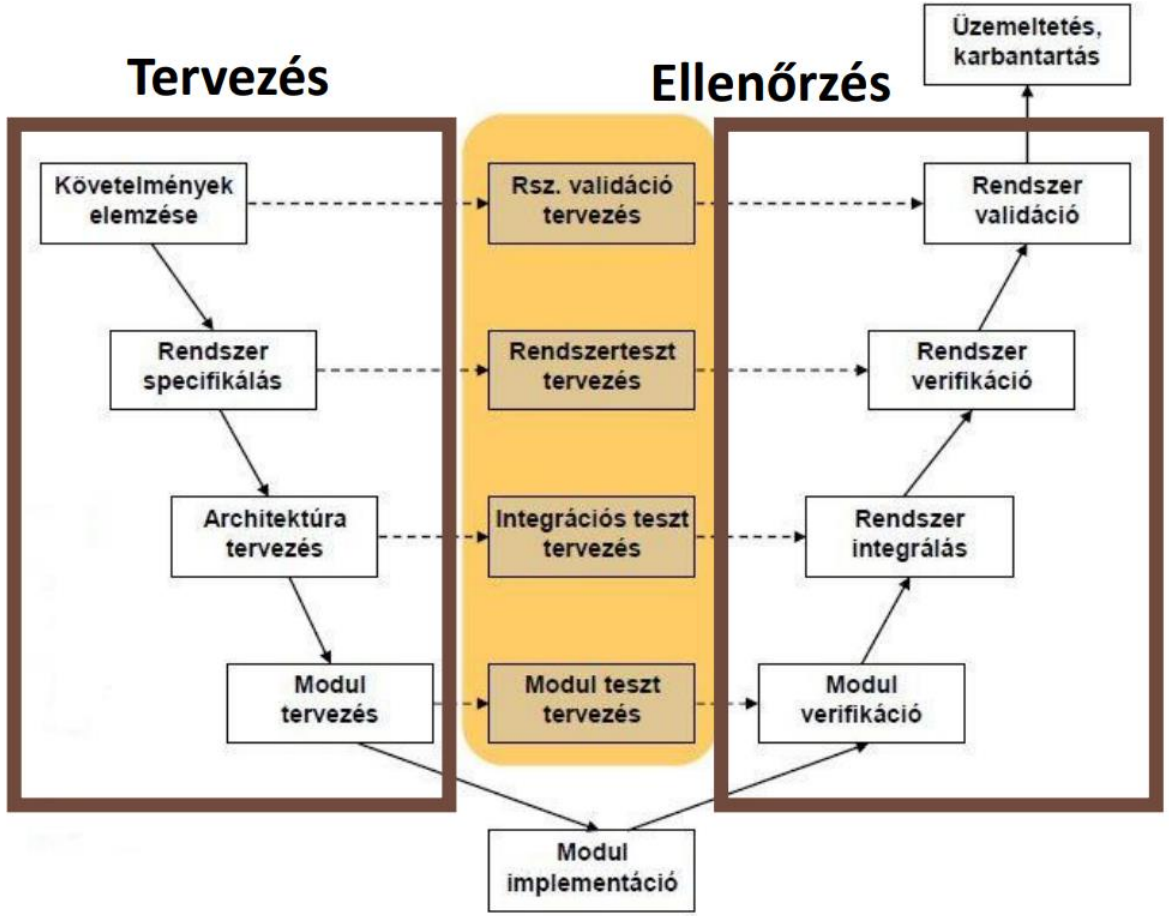
Támogató folyamatok

Biztonsági analízis

Iránymutatás

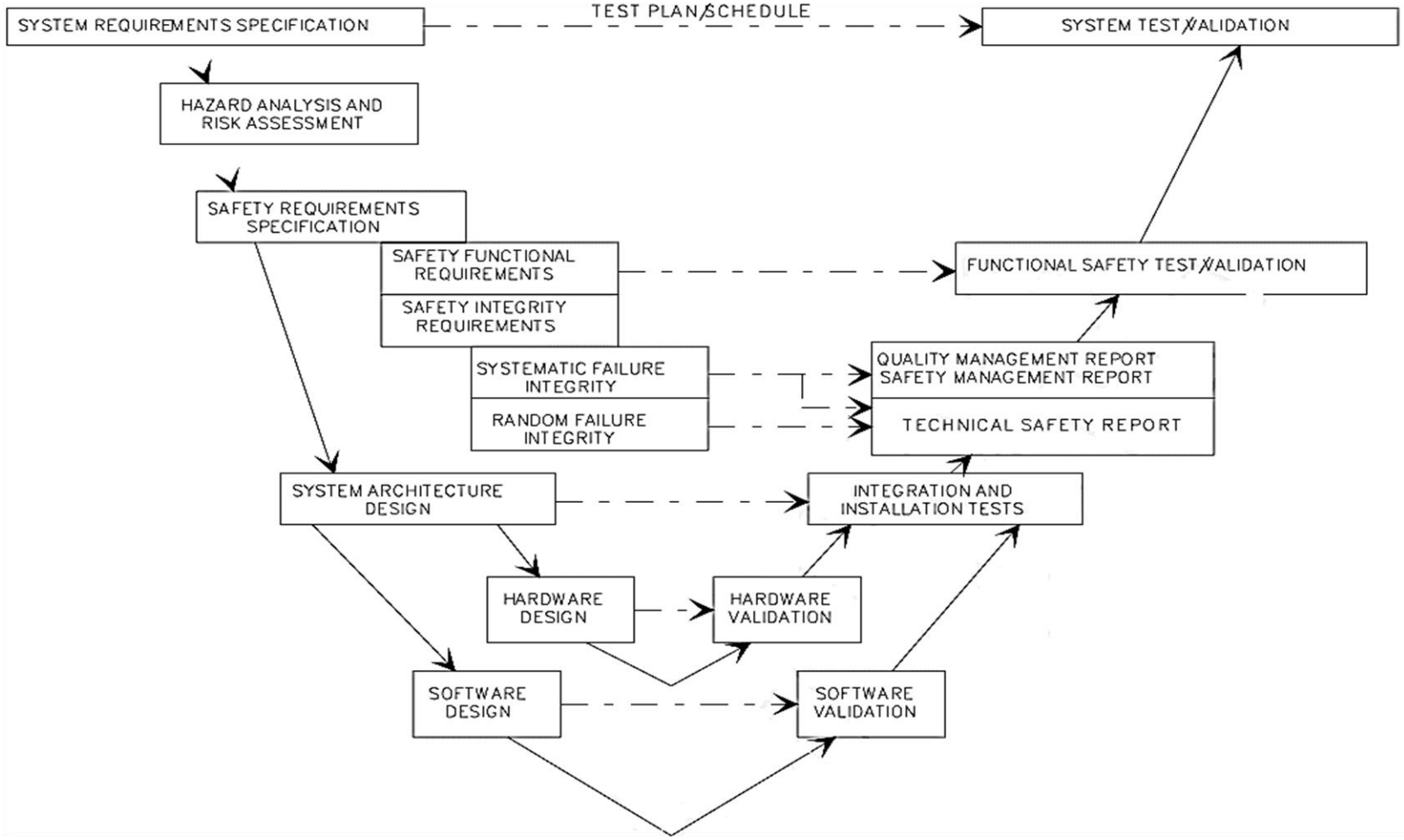
- Autóipari szabvány - ISO 26262

Életciklus modellek - példa



- SW életciklus modell

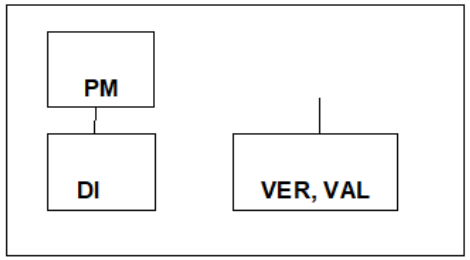
Életciklus modellek - példa

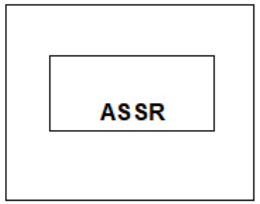


- Biztonsági életciklus modell - MSZ EN 50129

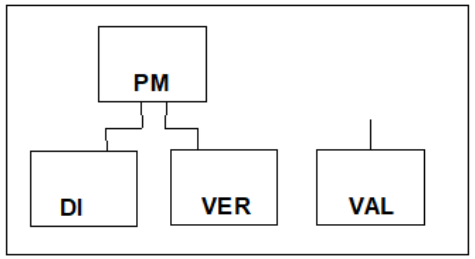
Személyi függetlenség - példa

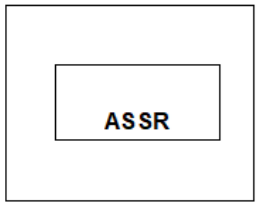
SIL 3 ÉS 4



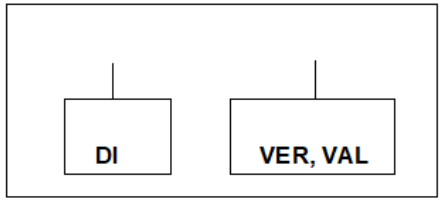


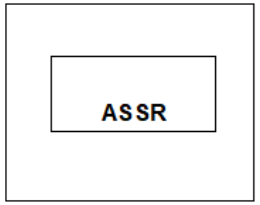
OR



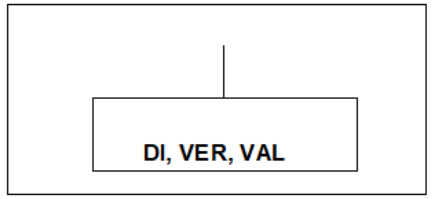


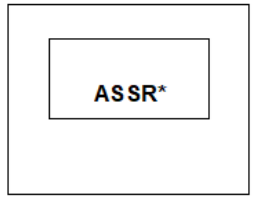
SIL 1 ÉS 2





SIL 0





Magy.:
PM = Project Manager
DI = Tervező, megvalósító
VER = Verifikáló
VAL = Validáló
ASSR = Asszesszor

= lehet egyazon személy

=lehet egyazon szervezet

* =SIL0-ra csak akkor kell asszesszor, egy átfogó rendszer biztonságára lehet hatással

SIL fejlesztési módszerek, intézkedések, technikák - példa

Technikák/Intézkedések	SIL 1	SIL 2	SIL 3	SIL 4
1. A biztonsági szervezet tagjainak képzése	HR: Kezdeti képzés minden biztonságorientált tevékenységnél		HR: Minden biztonságorientált tevékenységgel kapcsolatban ismétlődő képzés vagy a tevékenység rendszeres teljesítése	
2. A résztvevők személyi függetlensége	lásd a 6. ábrát: a függetlenség megszervezése (előző dia)			
3. A biztonsági szervezet személyzetének képesítése (lásd az 1. sz. megjegyzést) 4. (lásd a megjegyzést)	HR: műszaki oktatás vagy elegendő tapasztalat		HR: magasabb szintű műszaki oktatás vagy szélesebb körű tapasztalat	

- Vasútbiztonsági szabványokban definiált biztonsági életciklus modell - MSZ EN 50129

SIL fejlesztési módszerek, intézkedések, technikák - példa

Technikák/Intézkedések	SIL 1	SIL 2	SIL 3	SIL 4
1. A biztonságorientált és nem biztonságorientált rendszerek szétválasztása	R: jól meghatározott interfészek a biztonságorientált és nem biztonságorientált rendszerek között		HR: jól meghatározott interfészek a biztonságorientált és nem biztonságorientált rendszerek között és interfész-elemzés	
2. Grafikus leírás beleértve pl. blokkdiagramokat	HR		HR	
3. Strukturált specifikáció	HR: manuális, hierarchikus szétválasztás alfeladatokra, interfészleírások		HR: hierarchikus szétválasztás formális módszerek alkalmazásával, automatikus konzisztencia-ellenőrzés, finomítás a funkcionális szintig	
4. Formális vagy félformális módszerek			R: számítógéppel támogatott	
5. Számítógéppel támogatott specifikációs eszközök		R: eszközök kiválasztása bármely konkrét tervezési módszer előnyben részesítése nélkül	R: modellorientált eljárások hierarchikus felosztással, minden objektum, kapcsolatainak, közös adatbázisának, automatikus konzisztencia-ellenőrzésének leírása	
6. Ellenőrzőlisták	R: előkészített ellenőrzőlisták minden biztonsági életciklus-fázisra		R: előkészített részletes ellenőrzőlisták minden biztonságorientált életciklus-fázisra	
7. Veszélynapló	HR: A Veszélynaplót fel kell fektetni és karban kell tartani a rendszer teljes életciklusa során			

- Vasútbiztonsági szabványokban definiált biztonsági életciklus modell - MSZ EN 50129

SIL fejlesztési módszerek, intézkedések, technikák - példa

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

MEGJEGYZÉS: Minden, szürke mezőben feltüntetett technika alternatívát jelent, azaz az „R” azt jelenti, hogy ezen technikák közül legalább egy választása ajánlott.

- Vasútbiztonsági szabványokban definiált biztonsági életciklus modell - MSZ EN 50129
- *lásd részletesen a 10.-11. héten

SIL fejlesztési módszerek, intézkedések, technikák - példa

	Properties	ASIL			
		A	B	C	D
1	Hierarchical design	+	+	++	++
2	Precisely defined interfaces	+	+	+	+
3	Avoidance of unnecessary complexity of hardware components and software components	+	+	+	+
4	Avoidance of unnecessary complexity of interfaces	+	+	+	+
5	Maintainability during service	+	+	+	+
6	Testability during development and operation	+	+	++	++

- Autóipari szabványban definiált biztonsági életciklus modell - ISO 26262

SIL fejlesztési módszerek, intézkedések, technikák - példa

Methods		ASIL			
		A	B	C	D
1a	Analysis of requirements	++	++	++	++
1b	Analysis of external and internal interfaces	+	++	++	++
1c	Generation and analysis of equivalence classes for hardware-software integration	+	+	++	++
1d	Analysis of boundary values	+	+	++	++
1e	Error guessing based on knowledge or experience	+	+	++	++
1f	Analysis of functional dependencies	+	+	++	++
1g	Analysis of common limit conditions, sequences, and sources of dependent failures	+	+	++	++
1h	Analysis of environmental conditions and operational use cases	+	++	++	++
1i	Analysis of field experience	+	++	++	++

- Autóipari szabványban definiált biztonsági életciklus modell - ISO 26262

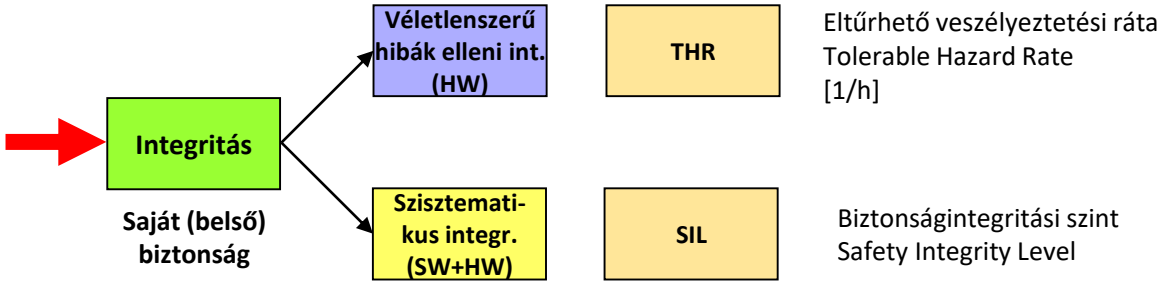
SIL fejlesztési módszerek, intézkedések, technikák - példa

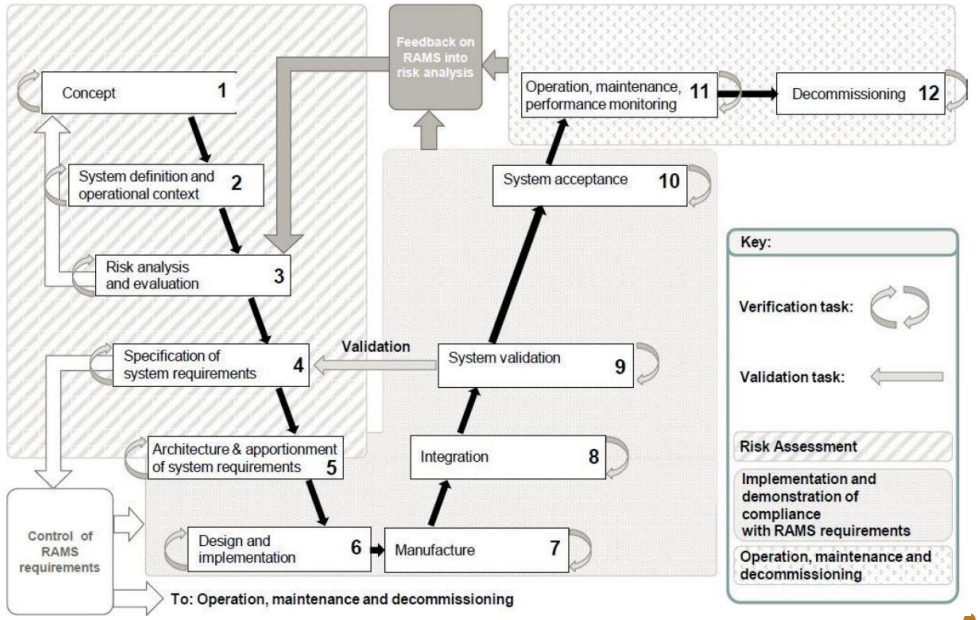
Methods		ASIL			
		A	B	C	D
1a	Environmental testing with basic functional verification[a]	++	++	++	++
1b	Expanded functional test[b]	o	+	+	++
1c	Statistical test[c]	o	o	+	++
1d	Worst case test[d]	o	o	o	+
1e	Over limit test[e]	+	+	+	+
1f	Mechanical test[f]	++	++	++	++
1g	Accelerated life test[g]	+	+	++	++
1h	Mechanical Endurance test[h]	++	++	++	++
1i	EMC and ESD test[i]	++	++	++	++
1j	Chemical test [j]	++	++	++	++

- Autóipari szabványban definiált biztonsági életciklus modell - ISO 26262

Összefoglalás

- THR/TFFR:
  - védelem a véletlenszerű meghibásodásokkal szemben: rendszerfelépítés, a RAM követelményeknek való megfelelőség,
- SIL/ASIL/DAL:
  - fejlesztési módszerek, életciklus modellek mind SW, mind HW komponensekre,
  - iparági szabályozások, módszertanok,
- maradék kockázat mindig lesz! – kérdés annak a mértéke.





Köszönöm a figyelmet!

Biztonságintegritás, életciklus modellek

Lövétei István Ferenc
(lovetei.istvan@mail.bme.hu)
Dr. Sághi Balázs