A fejlesztési szabványok szerepe a szoftverellenőrzésben

Majzik István
majzik@mit.bme.hu

http://www.inf.mit.bme.hu/

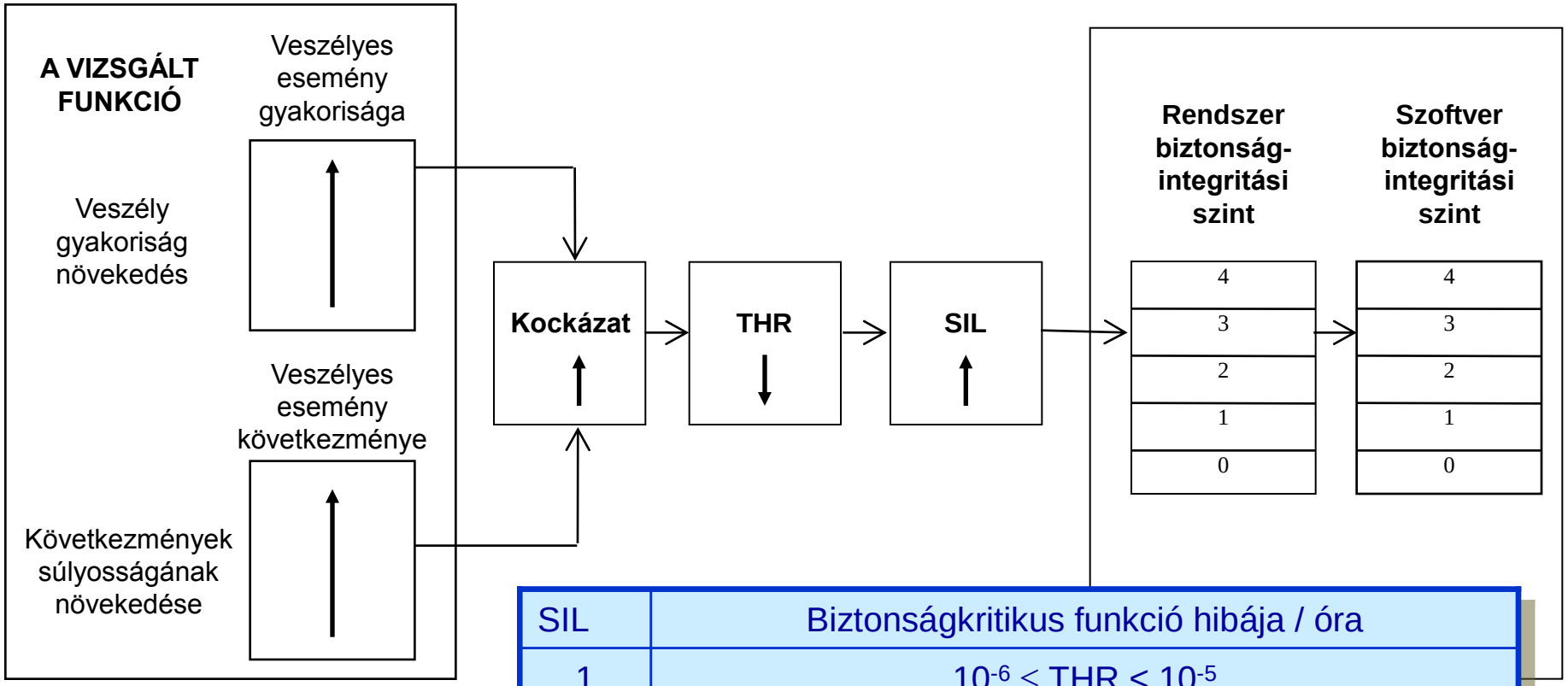
Tartalomjegyzék

- Biztonságkritikus rendszerek
  - A biztonságintegritási szint
  - Az ellenőrzés szerepe
- Hogyan határozzák meg a fejlesztési szabványok a szisztematikus ellenőrzést?
  1. A fejlesztési folyamat általános előírásai
  2. Módszerek és intézkedések megadása
  3. A dokumentáció követelményei
  4. A szervezeti rend követelményei

Jellegzetes példa: Biztonságkritikus rendszerek

- Széles körben használt szabványok
  - IEC 61508: Functional safety in electrical / electronic / programmable electronic safety-related systems
  - EN 50128: Vasúti irányítástechnika szoftverek
  - ISO 26262: Biztonsági funkciók gépjárművekben
  - DO 178B: Repülőgép fedélzeti rendszerek
- Biztonsági funkciók
  - Célja a biztonságos állapot elérése vagy fenntartása
  - Biztonságintegritás: Milyen gyakorisággal viselhető el adott szintű hatások mellett a biztonsági funkció hibája?
- Biztonságintegritási szint (Safety Integrity Level, SIL)
  - Meghatározása: Kockázatelemzés alapján
  - „Elviselhető veszélygyakoriság” – Tolerable Hazard Rate (THR)
    - Folytonos: Veszélyt okozó hibajelenség gyakorisága
    - Nem folytonos: Veszélyt okozó hibajelenség valószínűsége
  - THR tartományok szerinti kategóriák: SIL 1, 2, 3, 4

SIL meghatározás alapelve



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	$10^{-9} \leq THR < 10^{-8}$

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

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

A SIL követelmények betartásának ellenőrzése

- Véletlen meghibásodásokra (pl. hardver):
  - A SIL tartományok betartása számításokkal ellenőrizhető
    - Kvantitatív analízis, megbízhatósági modellezés
- Szisztematikus meghibásodásokra (pl. szoftver):
  - Számításokkal nem ellenőrizhető valószínűség
  - Módszer- és eszközkészlet adható az elkerülésre és kezelésre
  - Komplex „intézkedés-csomag” az egyes SIL szintekhez:
    1. Fejlesztési folyamat
    2. Előírt módszerek és technikák
    3. Előírt dokumentáció
    4. Szervezeti rend (felelősségek)

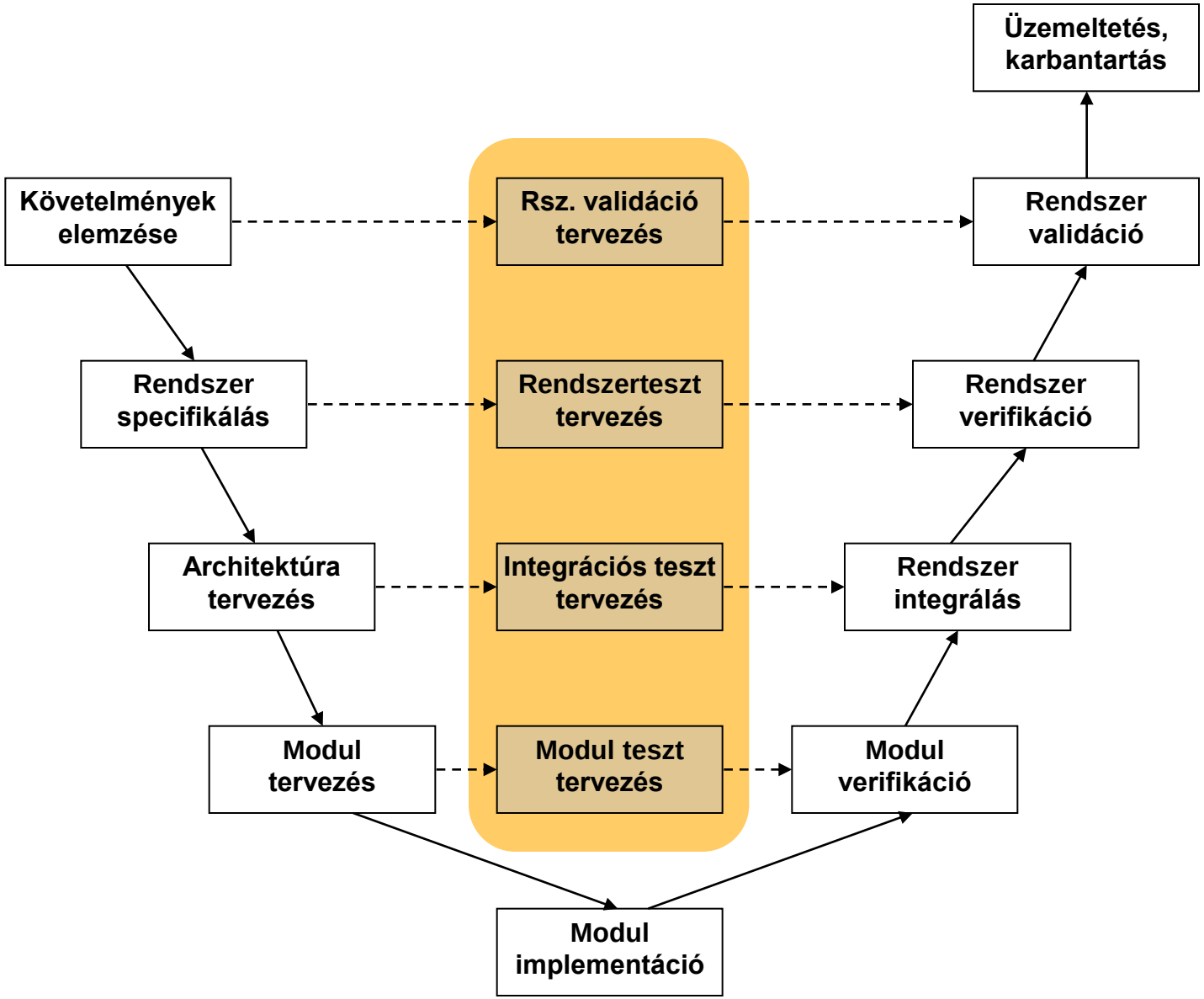
Tartalomjegyzék

- Biztonságkritikus rendszerek
  - A biztonságintegritási szint
  - Az ellenőrzés szerepe
- Hogyan határozzák meg a fejlesztési szabványok a szisztematikus ellenőrzést?
  1. A fejlesztési folyamat általános előírásai
  2. Módszerek és intézkedések megadása
  3. A dokumentáció követelményei
  4. A szervezeti rend követelményei

1. A fejlesztési folyamat általános előírásai

- Jól definiált fázisokat tartalmaz
  - Általában jól meghatározott specifikáció, ismert környezet
  - Meghatározott fejlesztési lépések (pl. V-modell)
- Szigorú feltételekhez kötött előrelépés: Hangsúlyos a fejlesztési lépések ellenőrzése
  - Hibák kockázata nagy (felelősség)
  - Üzembe helyezés utáni javítás költsége nagy
- További jellegzetességek:
  - Biztonságigazolás: „Biztonsági ügy” elkészítése (safety case)
  - Független értékelés (assessment)
  - Tanúsítás (certification)
  - Hatósági felügyelet

V-modell: Jól meghatározott ellenőrzések



2. Módszerek és intézkedések megadása

- Példa: Szoftver tesztelés (EN 50128)

MÓDSZER / INTÉZKEDÉS	Említés helye	SW-SIL0	SW-SIL1	SW-SIL2	SW-SIL3	SW-SIL4
1. Valószínűségi tesztelés	B47	-	R	R	HR	HR
2. Teljesítéstesztelés	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: EN 50128 módszerek és intézkedések

- Software design and implementation:

TECHNIQUE/MEASURE		Ref	SWS IL0	SWS IL1	SWS IL2	SWS IL3	SWS IL4
14.	Functional/ Black-box Testing	D.3	HR	HR	HR	M	M
15.	Performance Testing	D.6	-	HR	HR	HR	HR
16.	Interface Testing	B.37	HR	HR	HR	HR	HR

- Functional/black box testing (D3):

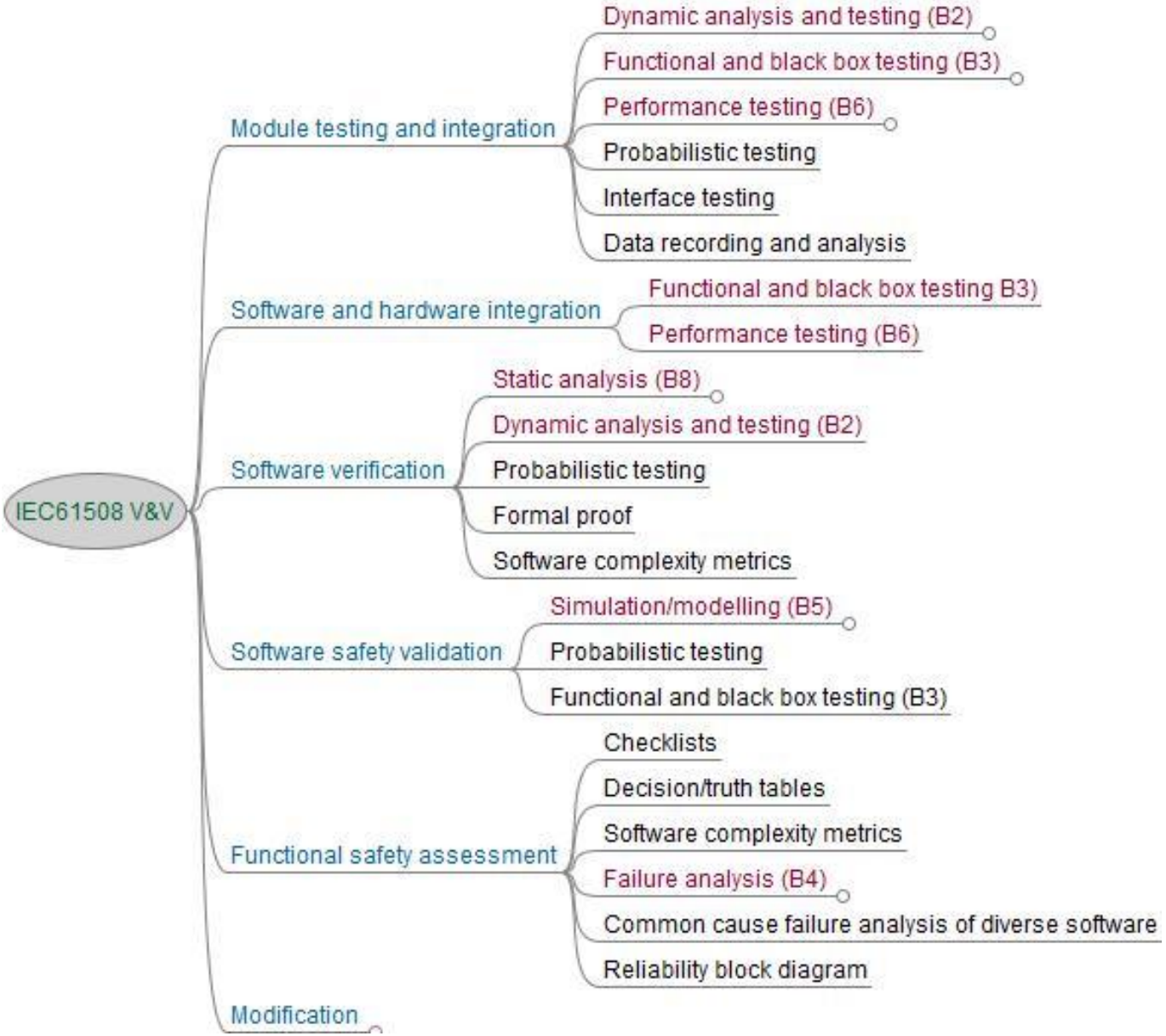
1.	Test Case Execution from Cause Consequence Diagrams	B.6	-	-	-	R	R
2.	Prototyping/Animation	B.49	-	-	-	R	R
3.	Boundary Value Analysis	B.4	R	HR	HR	HR	HR
4.	Equivalence Classes and Input Partition Testing	B.19	R	HR	HR	HR	HR
5.	Process Simulation	B.48	R	R	R	R	R

Példa: EN 50128 módszerek és intézkedések

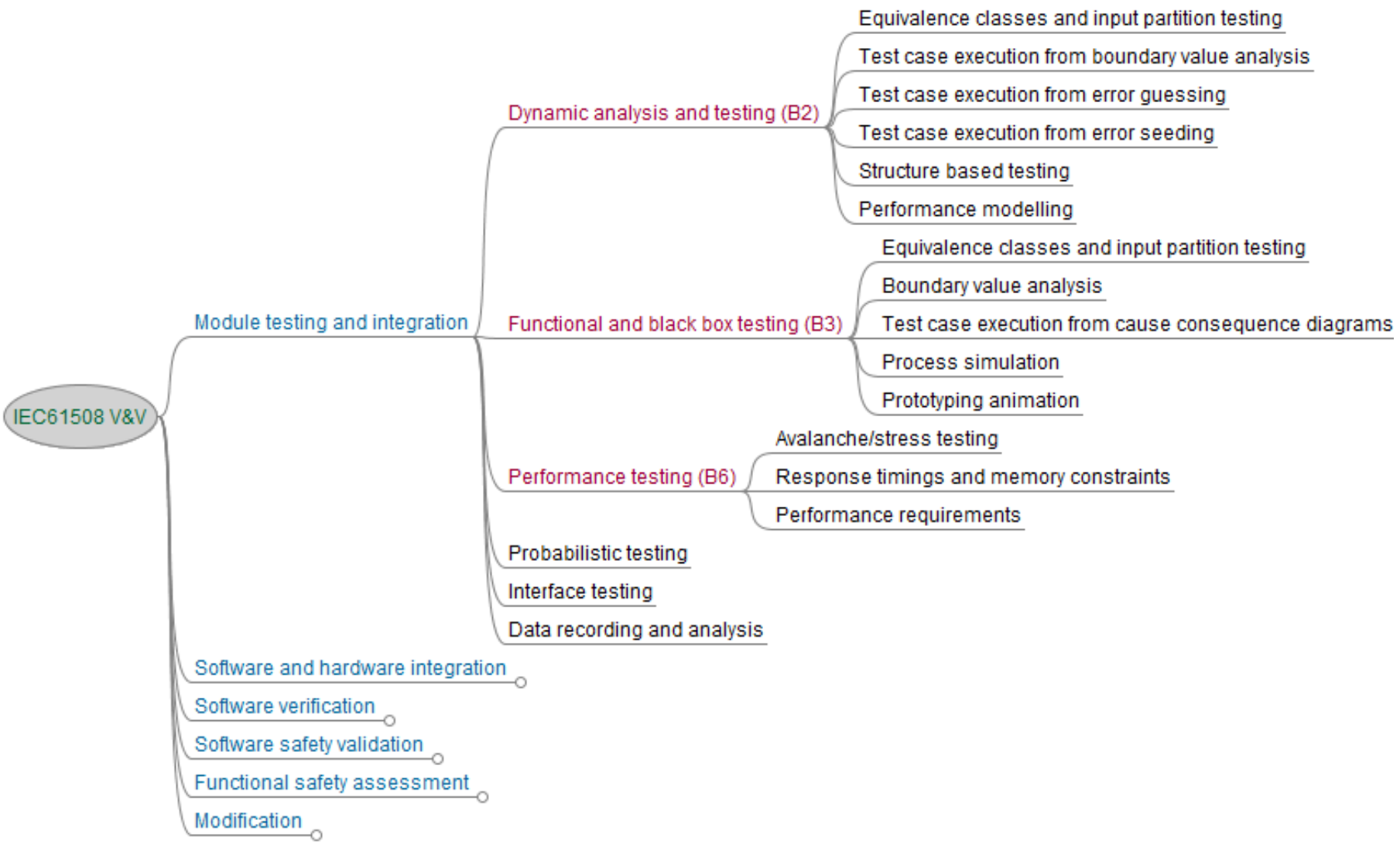
- Performance testing (D6):

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

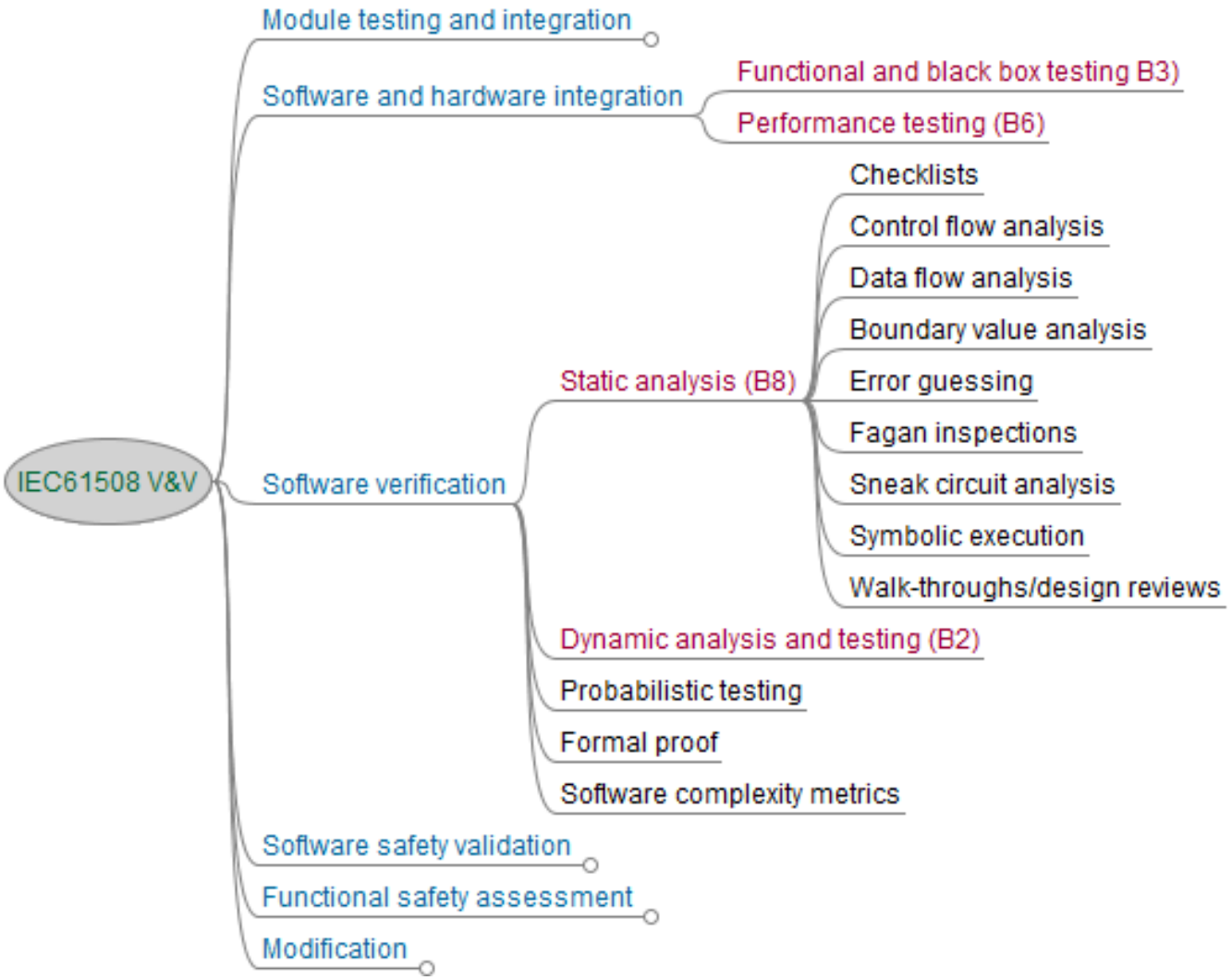
Példa: IEC 61508 V&V módszerek



Példa: IEC 61508 V&V módszerek – Tesztelés



Példa: IEC 61508 V&V módszerek – Statikus analízis



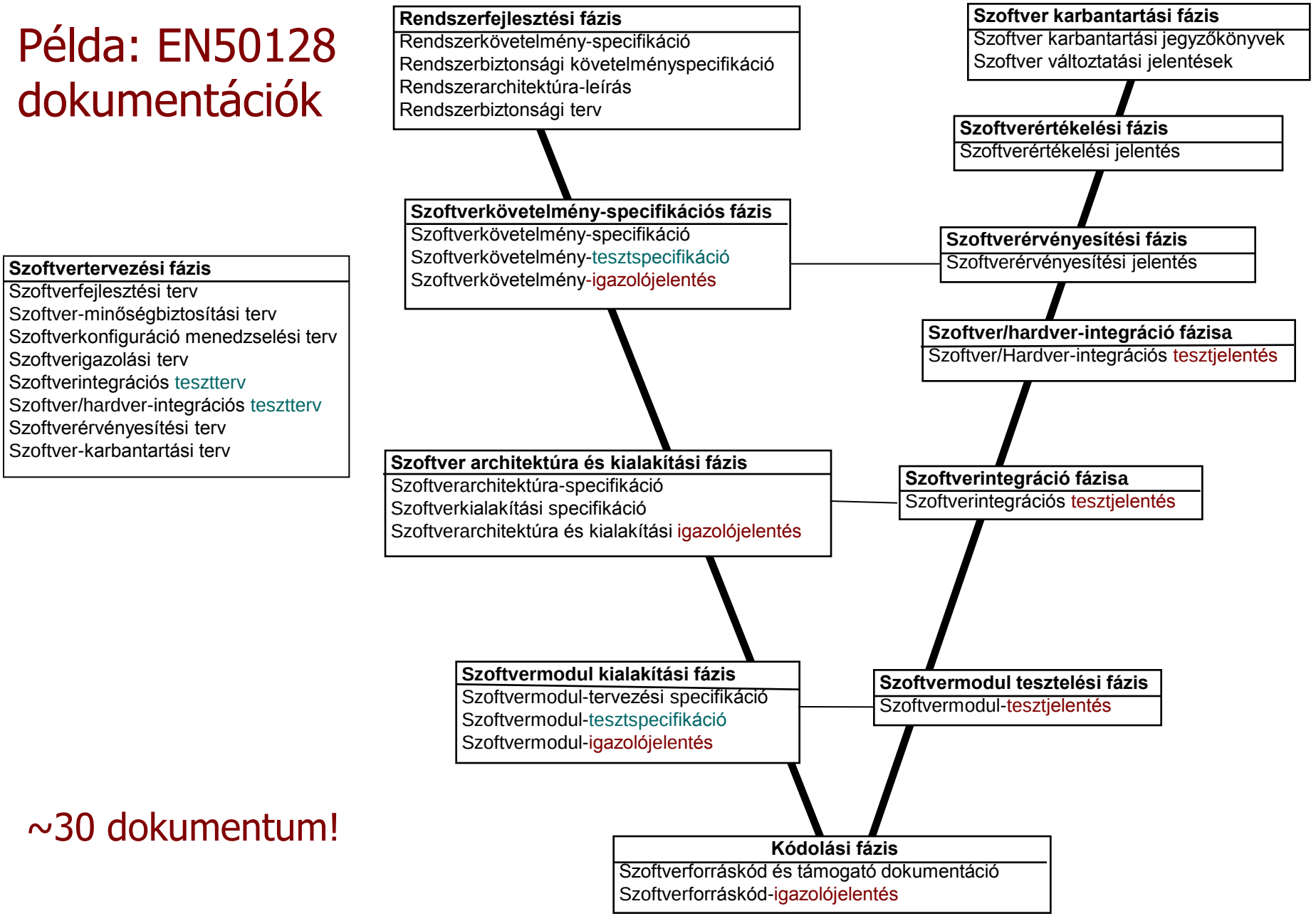
Példa: IEC 61508 kevésbé ismert V&V technikái

- Probabilistic testing
  - Valószínűségi jellemzők származtatása a szoftver komponens megbízhatóságáról az (automatikus) tesztelés eredményei alapján
    - Környezet szimulációja a gyakori trajektóriák meghatározására
- Test case execution from error seeding
  - Hibák beillesztése annak érdekében, hogy a tesztelés után bennmaradó hibák számát megbecsülhessük a beillesztett és detektált hibák számából
- Fagan inspections
  - Hibák felderítése a dokumentumok és tervek szisztematikus felülvizsgálatával (audit)
- Sneak circuit analysis
  - Nem várt (nem szándékos) kapcsolatok illetve hatások detektálása, amelyek hibához vezetnek

3. A dokumentáció követelményei

- Dokumentáció típusa
  - Átfogó
    - Pl. fejlesztési terv, verifikációs terv
  - Életciklus fázishoz kötődő
    - Pl. modul teszt jelentés, modul verifikációs jelentés
- Dokumentum keresztreferencia táblázat
  - Melyik életciklus fázishoz milyen dokumentáció készül
  - Melyik dokumentum melyik másikra épül
- Dokumentumok követhetősége szükséges
  - Ugyanazon terminológia, rövidítések, elnevezések
- Dokumentumok összevonhatók
  - Eredmény nem veszhet el
  - Független szereplők dokumentumai nem vonhatók össze

Példa: EN50128 dokumentációk



~30 dokumentum!

Példa: EN50128 dokumentum kereszt-referencia táblázat

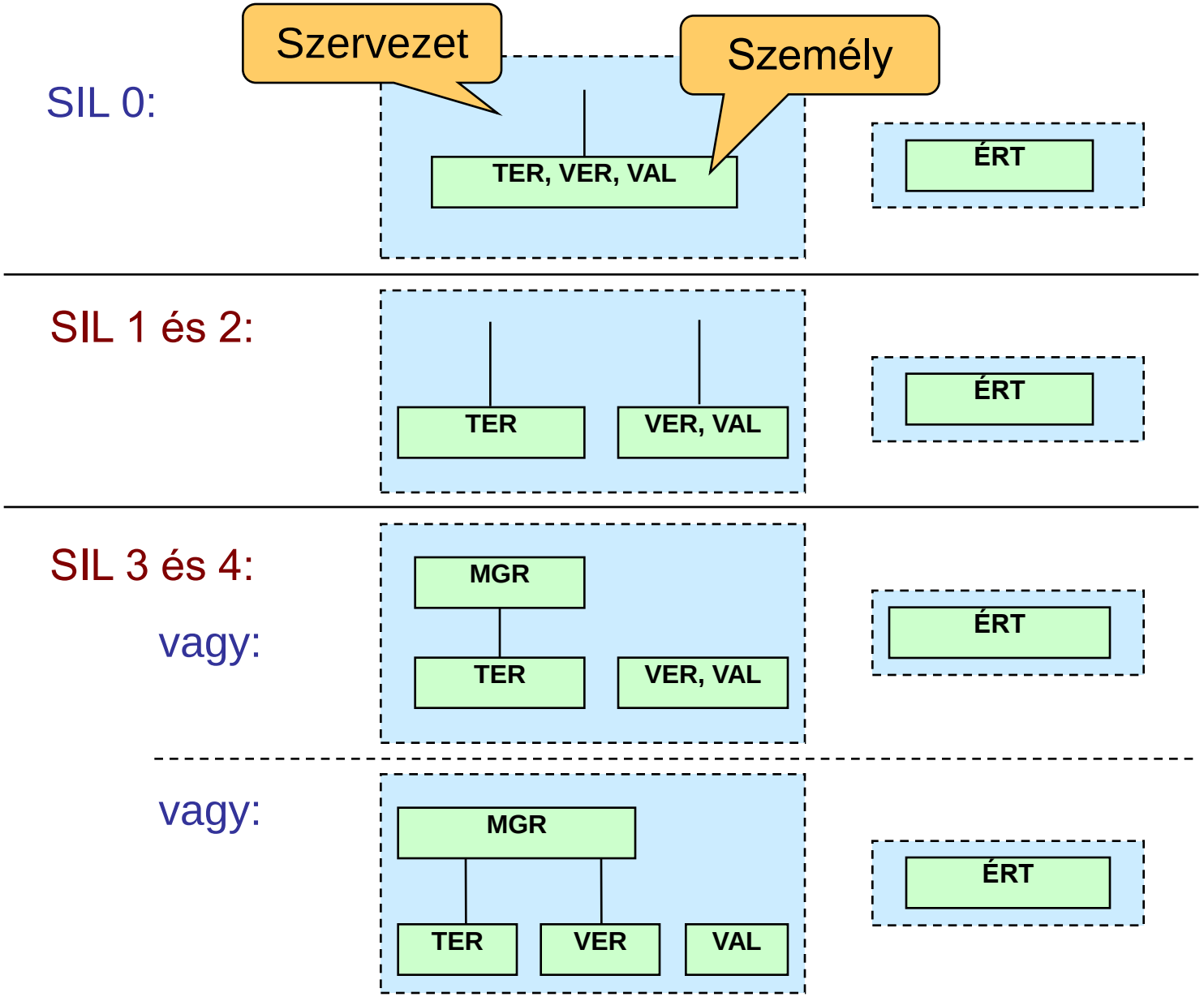
- ■ Dokumentum létrehozás
- ◆ Dokumentum felhasználása egy-egy fázisban

cím	SRS	SA	SDD	SVer	S/H	SVal	Ass	Q	MA	
FÁZISOK (*) = más fázisokkal párhuzamosan										**DOKUMENTUMOK**
SW KÖVETELMÉNYEK	■	◆	◆	◆	◆	◆	◆			Sw Követelményspecifikáció
										Alkalmazási Követelmények Specifikációja
	■			◆	◆	◆	◆			Sw Követelmény Teszt Specifikáció
				■						Sw Követelmények Verifikációs Jelentése
SW KONSTRUKCIÓ KIALAKÍTÁS		■	◆	◆	◆	◆	◆			Sw Architektúra Specifikáció
			■	◆	◆	◆	◆			Sw Konstrukció specifikáció
				■						Sw Architektúra és Konstrukció Verifikációs Jelentés
SW MODUL KONSTRUKCIÓ KIALAKÍTÁS			■	◆	◆	◆	◆			Sw Modul Konstrukció Specifikáció
			■	◆	◆	◆	◆			Sw Modul Teszt Specifikáció
				■						Sw Modul Verifikációs Jelentés
KÓDOLÁS			■	◆	◆	◆	◆			Sw Forráskód
				■		◆	◆			Sw Forráskód Verifikációs Jelentés
MODUL TESZTELÉS			■	◆						Sw Modul Teszt Jelentés
SW INTERGRÁCIÓ				■						Sw Integráció Teszt Jelentés
										Adatteszt Jelentés
SW/HW INTEGRÁCIÓ					■					Sw/Hw Integráció Teszt Jelentés
VALIDÁCIÓ (*)						■				Sw Validációs Jelentés

4. Szervezeti rend

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

Példa: EN50128 minimális függetlenségi követelményei



Miről volt szó?

- Motiváció
  - Milyen minőségi igények vannak a szoftverrel szemben, és mit tud ma a szoftveripar?
  - Miért olyan nagy a szoftver ellenőrzési technikák jelentősége?
- A verifikáció és validáció technikái (áttekintés)
  - Milyen tipikus technikák vannak?
- Fejlesztési életciklus modellek
  - Milyen szerepet kapnak a tipikus technikák az egyes fejlesztési folyamatokban?
- Fejlesztési szabványok szerepe
  - Hogyan valósul meg a szisztematikus ellenőrzés?