Fejlesztés kockázati alapokon 2.

Az IEC61508 és az IEC61511

Szabó Géza
Szabo.geza@mail.bme.hu

A blokk célja

- Áttekintő kép a 61508-ról és a 61511-ről,
- A filozófia megismertetése,
- Nem cél a követelmények szó szerinti meghivatkozása.

- A szabvány eredetijében érvényes!
  - IEC….. MSZ-EN

A 61508 – Funkcionális biztonság

- Általános célú szabvány,
- A funkcionális biztonság fogalma,
- Kockázati (kockázatcsökkentési) alapon specifikálja a biztonságintegritást,
- Biztonságintegritás: THR, SIL

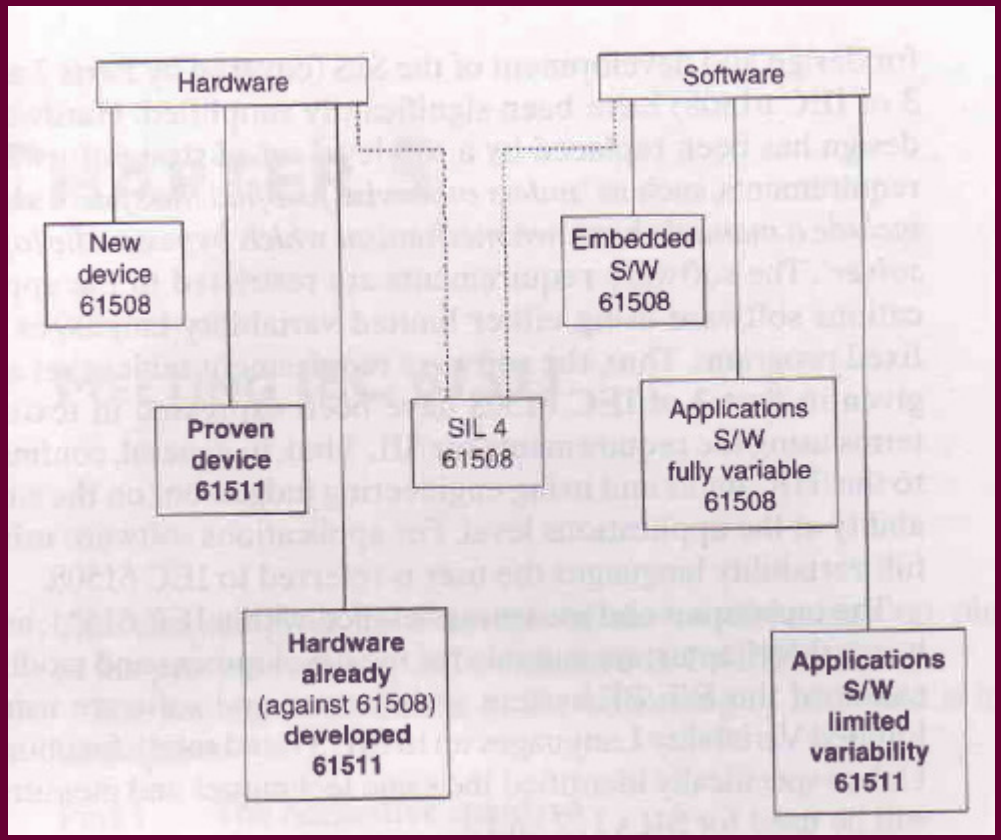
A 61508 – Funkcionális biztonság

- **THR teljesítése**
  - Architektúra,
  - Redundancia,
  - Egyedi elem megbízhatóságok.
- **SIL teljesítése**
  - Életciklus,
  - Kompetencia,
  - Függetlenség,
  - Dokumentáltság (információáramlás),
  - Módszerek és eljárások

A 61508 – Funkcionális biztonság

- **Biztonságértékelés**

IEC61508 – folyamatirányítási szektor



Célok:
Egyszerűsítés,
meglévő HW integrálhatósága

Különválik a berendezés
és a rendszerszint

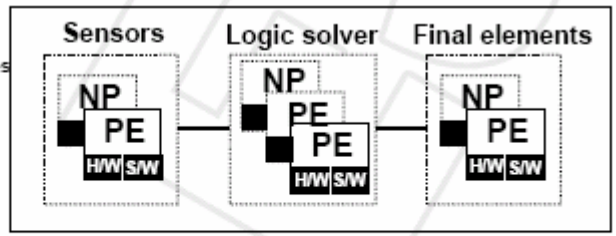
!

IEC61508 – 61511 fogalmi kapcsolatok

IEC 61508-4	IEC 61511-1
E/E/PE safety related system	SIS
PES	SIS
Process control system	Basic process control system
EUC	Process
Safety function	Safety instrumented function (SIF)

IEC 61508	IEC 61511
Part 1	Part 1
Part 2	Part 1
Part 3	Part 1
Part 4	Part 1
Part 5	Part 3
Part 6	Part 2
Part 7	All parts

SIS architecture and safety instrumented function example with different devices shown



IEC 3246/02

Figure 7 – Example of SIS architecture

61511 - biztonságmenedzsment

- Cél: A funkcionális biztonsági cél eléréséhez szükséges menedzsment tevékenységek azonosítása.
- Felelős szervezetek (fázis elvégzés vagy ellenőrzés) meghatározása, értesítése.
- Kompetencia biztosítása
  - Folyamatirányítási gyakorlat,
  - Technológiai gyakorlat,
  - Szenzorok és beavatkozók ismerete,
  - Jogi szabályozási környezet ismerete,
  - Menedzsment és vezetői ismeretek (ha szükséges),
  - Események következményeinek ismerete,
  - SIS SIL.

61511 – biztonságmenedzsment (2)

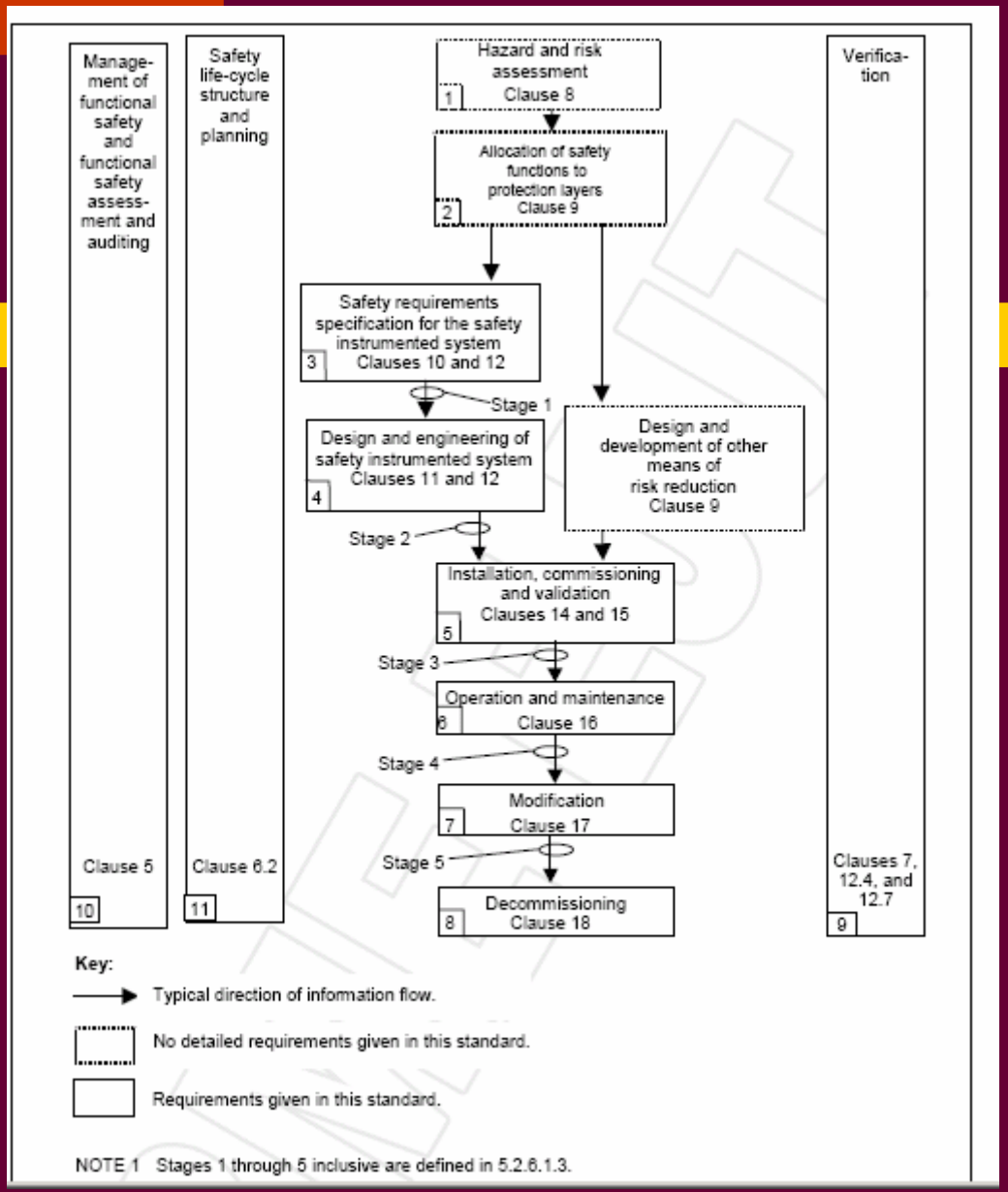
- Kockázatértékelés és kockázat menedzsment,
- Tervezés
  - A minőségbiztosítási terv részeként,
  - Önálló biztonsági tervként,
  - Több önálló dokumentumként.
- Javaslatok figyelembevételének megtervezése:
  - Veszélyelemzés és kockázatértékelés
  - Biztonságértékelések és auditok,
  - Verifikáció, validáció,
  - Eseményeket követő cselekvések.

61511 – biztonságmenedzsment (3)

- Szállítók felelőssége (ha egy vagy több fázisért közvetlenül felelősek): teljesíteni kell a felelős szervezet biztonsági tervében foglaltakat.
- SIS teljesítési szint kiértékelése:
  - Lehetséges szisztematikus hibák,
  - SIS veszélyes meghibásodási ráta,
  - Igény gyakoriság.

61511 – biztonságmenedzsment (4) Biztonságértékelés

- Cél az értékelés („megfelel” – „nem felel meg” a biztonsági követelményeknek),
- Az eljárásokat definiálni kell,
- Az értékelő csapatnak egy, a kivitelezésben nem érintett vezető szakértőt is tartalmaznia kell,
- Az értékelések helyét az életciklusban definiálni kell. !
- A biztonságértékelések száma és terjedelme függ:
  - A projekt méretétől,
  - A komplexitástól,
  - A biztonságintegritástól,
  - A tervezési tulajdonságok szabványosságától,
  - A biztonsági szabályozás követelményeitől,
  - Korábbi tapasztalatok mennyiségétől stb.


Manage-ment of functional safety and functional safety assess-ment and auditing
Safety life-cycle structure and planning
Hazard and risk assessment
1
Clause 8
Allocation of safety functions to protection layers
2
Clause 9
Safety requirements specification for the safety instrumented system
3
Clauses 10 and 12
Stage 1
Design and engineering of safety instrumented system
4
Clauses 11 and 12
Design and development of other means of risk reduction
Clause 9
Stage 2
Installation, commissioning and validation
5
Clauses 14 and 15
Stage 3
Operation and maintenance
8
Clause 16
Stage 4
Modification
7
Clause 17
Stage 5
Decommissioning
8
Clause 18
Verifica-tion
Clauses 7, 12.4, and 12.7
9
Clause 5
10
Clause 6.2
11
Key:
Typical direction of information flow.
No detailed requirements given in this standard.
Requirements given in this standard.
NOTE 1 Stages 1 through 5 inclusive are defined in 5.2.6.1.3.

61511 – biztonságmenedzsment (5) Biztonságértékelés

- Legalább egyet csinálni kell! (3. állapot – a veszély fellépése előtt),
- Ha fejlesztő és gyártóeszközök kerülnek alkalmazásra, azok is tárgyai a biztonságértéklésnek
  - Biztonságra gyakorolt hatásuk alapján
- Auditok
- Függetlenség (definiálni kell)

61511 – biztonságmenedzsment (6)

- SIS konfigurációmenedzsment (HW, SW)
  - A formális konfigurációellenőrzés helyei az életciklusban,
  - Az azonosítás módja,
  - Nem megengedett eszközök bekerülésének megakadályozása.

61511 – Biztonsági életciklus

- Cél:
  - fázisok definiálása és a követelmények meghatározása;
  - a technikai cselekmények szervezése;
  - annak biztosítása, hogy létezik (vagy ki lesz dolgozva) olyan terv, ami biztosítja, hogy a SIS meg fog felelni a biztonsági követelményeknek
- Minden fázisra definiálni kell:
  - A fázis elfogadásának kritériumát,
  - Az alkalmazandó technikákat, eljárásokat.

Safety life-cycle phase or activity		Objectives	Require-ments	Inputs	Outputs
Figure 8 box number	Title		Clause or subclause		
1	Hazard and risk assessment	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	8	Process design, layout, manning arrangements, safety targets	A description of the hazards, of the required safety function(s) and of the associated risk reduction
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each safety instrumented function, the associated safety integrity level	9	A description of the required safety instrumented function(s) and associated safety integrity requirements	Description of allocation of safety requirements (see Clause 9)
3	SIS safety requirements specification	To specify the requirements for each SIS, in terms of the required safety instrumented functions and their associated safety integrity, in order to achieve the required functional safety	10	Description of allocation of safety requirements (see clause 9)	SIS safety requirements; software safety requirements

4	SIS design and engineering	To design the SIS to meet the requirements for safety instrumented functions and safety integrity	11 and 12.4	SIS safety requirements Software safety requirements	Design of the SIS in conformance with the SIS safety requirements; planning for the SIS integration test
5	SIS installation commissioning and validation	To integrate and test the SIS To validate that the SIS meets in all respects the requirements for safety in terms of the required safety instrumented functions and the required safety integrity	12.3, 14, 15	SIS design SIS integration test plan SIS safety requirements Plan for the safety validation of the SIS	Fully functioning SIS in conformance with the SIS design results of SIS integration tests Results of the installation, com-missioning and validation activities
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	16	SIS requirements SIS design Plan for SIS operation and maintenance	Results of the operation and maintenance activities

7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained	17	Revised SIS safety requirements	Results of SIS modification
8	Decommission-ing	To ensure proper review, sector organization, and ensure SIF remain appropriate	18	As built safety requirements and process information	SIF placed out of service
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	7, 12.7	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase
10	SIS functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the SIS	5	Planning for SIS functional safety assessment SIS safety requirement	Results of SIS functional safety assessment

61511 – Verifikálás

- Cél: egy fázis megfelelőségének igazolása
  - Review (mérnöki ítélet), elemzés, teszt
- Verifikációs tervet kell készíteni
  - Verifikációs tevékenységek,
  - Verifikációs eljárások, technikák,
  - Résztvevők,
  - A verifikálandó dolgok,
  - A nem-megfelelés kezelése,
  - Eszközök és támogató elemzési eljárások
- A verifikációk eredményeinek rendelkezésre kell állniuk

61511 – Veszély és kockázatértékelés

- A folyamatra, és a hozzá tartozó (nem biztonsági) szabályzásokra (Basic Process Control System – BPCS),
- Eredmény:
  - Veszélyes állapotok listája,
  - Következmény súlyosságok és valószínűségek,
  - Az üzemállapot, amelyben fellép (normál, indulási, leállási, karbantartási, vészleállás stb.)
  - A kockázatcsökkentés módjai,
  - Az értékelésnél alkalmazott feltételezések (pl. emberi beavatkozások, meghibásodási ráták, indítási gyakoriságok)
  - A biztonsági funkciók védelmi rétegekre történő allokációja, a SIS funkciók azonosítása
  - A BPCS veszélyes meghibásodási rátája, ami védelmi beavatkozást kíván, nem lehet jobb 1e-5 1/h-nál.

!

61511 – Biztonsági funkciók allokációja

- A biztonsági funkciók szétosztása, a SIS biztonsági funkcióinak meghatározása
- A SIS biztonsági szintjét a leosztott kockázatcsökkentési értékből kell meghatározni.

Table 3 – Safety integrity levels: probability of failure on demand

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	**Target average probability of failure on demand**	**Target risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	>10 000 to ≤100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1 000 to ≤10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 to ≤1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 to ≤100

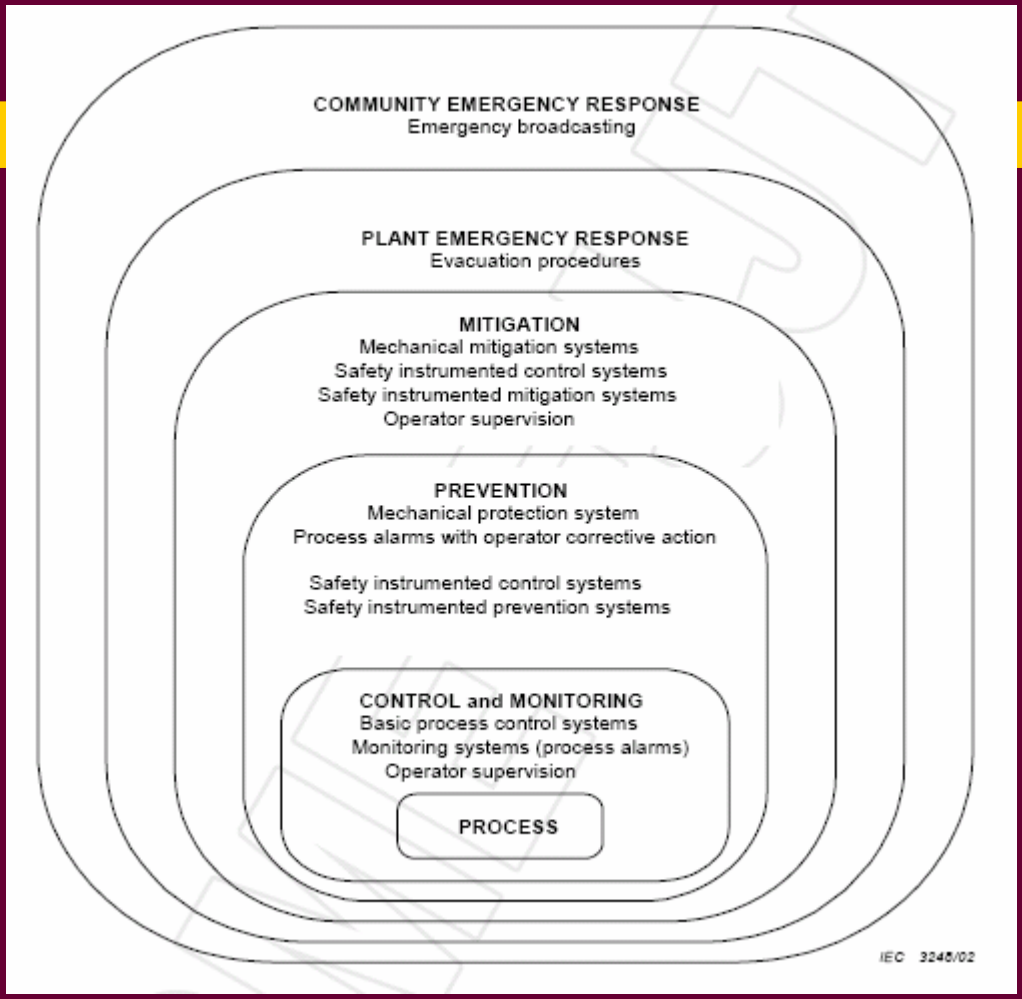
61511 – Biztonsági funkciók allokációja

- Igény szerinti mód: Bármelyik a két táblázat közül.
- Folyamatos mód: csak a 4. táblázat.

CONTINUOUS MODE OF OPERATION	
Safety integrity level (SIL)	**Target frequency of dangerous failures to perform the safety instrumented function (per hour)**
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

61511 – Biztonsági funkciók allokációja

- SIL4:
  - SIL4-nél magasabb szint nem lehet
  - SIL4 nagyon magas szintű kompetenciát igényel. Meg kell fontolni:
    - További védelmi szint beiktatását,
    - A veszélyes folyamat átalakítását.
  - SIL4 akkor lehet, ha:
    - Explicit módon kimutatható elemzéssel és tesztekkel, hogy a biztonságintegritási követelmények teljesülnek, VAGY
    - A komponensekre nagy mennyiségű felhasználói tapasztalat áll rendelkezésre, ÉS elégséges meghibásodási adat is van.



- A BPCS is lehet védelmi szint
- Ha nem felel meg a 61508 vagy 61511-nek, akkor a védelem <10.
- Figyelembe kell venni, hogy a BPCS lehet indító is.
- Védelmi szintek közötti függések (CCS kizárása)

61511 – SIS biztonsági követelmények specifikációja

- A biztonsági funkciók allokációjából kell származnia,
- Elégségesnek kell lennie a SIS létrehozásához:
  - Funkciók leírása,
  - CCF kezelés,
  - A folyamat biztonsági állapota minden biztonsági funkcióra,
  - Biztonsági állapotok egyidejű fellépéseinek kockázatai,
  - Igények forrásai és gyakoriságuk,
  - Ellenőrzési intervallumok,
  - Válaszidő követelmények (min…max),
  - SIL és mód minden funkcióra,
  - Mérések és beavatkozási szintjeik,
  - Kézi leállítások,
  - Indítási feltételek
  - Bénítási feltételek,
  - MTTR
  - Környezeti feltételek, határok

61511 – SIS biztonsági követelmények specifikációja

- A szoftver biztonsági követelményeknek a biztonsági követelményspecifikációból kell származniuk a választott architektúra figyelembe vételével.

61511 – SIS tervezés

- Biztonsági és nem biztonsági részek kezelése,
- Különböző SIL szintű funkciók megvalósítása,
- BPCS-től való függetlenség, ha az nem felel meg a 61511-nek,
- Követelmények az üzemeltetésre, a karbantartásra és a tesztelésekre.
- Emberi képességek és korlátok figyelembe vétele, HMI,
- Biztonsági állapot elérése és megtartása,
- Általában kézi beavatkozás lehetősége is szükséges,
- BPCS-SIS függőség.

61511 – SIS tervezés

- Hibadetektálás redundáns rendszerben
  - Vagy biztonsági állapot, vagy további biztonságos működés a javítási időn belül (MTTR túllépését kezelni)
- Hibadetektálás nem redundáns rendszerben, igény szerinti módnál
  - Vagy biztonsági állapot, vagy javítás a javítási időn belül (MTTR túllépését kezelni)
- Mindkét esetben a valószínűségi elemzések a mérvadóak.
- Hibadetektálás nem redundáns rendszerben, folyamatos módnál
  - Hibareakció

61511 – SIS tervezés - hibatűrés

- Kötelező hibatűrési szint – programozható logika

Table 5 – Minimum hardware fault tolerance of PE logic solvers

SIL	Minimum hardware fault tolerance		
	SFF < 60 %	SFF 60 % to 90 %	SFF > 90 %
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

61511 – SIS tervezés - hibatűrés

- Kötelező hibatűrési szint – szenzor, aktuátor, nem programozható logika
  - Domináns meghibásodási mód biztonságos (tervezés!), vagy a veszélyes állapot detektálásra kerül.

SIL	Minimum hardware fault tolerance (see 11.4.3 and 11.4.4)
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

  - Ha a feltételek nem igazak: hibatűrés + 1

61511 – SIS tervezés - hibatűrés

- Kötelező hibatűrési szint – szenzor, aktuátor, nem programozható logika
  - Hibatűrés -1, ha:
    - A komponens korábbi tapasztalattal rendelkezik,
    - Csak folyamatfüggő paraméter beállítása lehetséges,
    - A folyamatfüggő paraméterhez való hozzáférés védett,
    - SIL4 alatt
- Választás szerint használható a 61508 is.

61511 – SIS tervezés - komponensválasztás

- Vagy 61508 szerint minősített,
- vagy SIL1-SIL3 között lehet korábbi tapasztalaton alapuló.
- Az eszköz-megfelelőség megállapításánál a gyártó HW és SW dokumentációit is figyelembe kell venni.

!

61511 – SIS tervezés – komponensválasztás korábbi tapasztalat alapján

- Bizonyítani kell tudni a megfelelést:
  - A komponensek megfelelő azonosítása
  - A gyártó minőség-, menedzsment- és konfigurációmenedzsment rendszereinek figyelembe vétele
  - Hasonló alkalmazásból szerzett tapasztalatok (esetleg nem biztonsági)
  - A tapasztalatok mennyisége

61511 – SIS tervezés – komponensválasztás korábbi tapasztalat alapján

- FPL alrendszerek
  - A nem használt tulajdonságokat azonosítani kell, valamint bizonyítani, hogy nem befolyásolnak biztonsági funkciót.
  - SIL3: bizonyítani kell, hogy
    - A tapasztalatok alapján kellően kicsi a valószínűség a funkció nemteljesülésre
    - Képes a funkció teljesítésére,
    - Vagy már használatban volt, vagy tesztelték hasonló profilú alkalmazásban.

61511 – SIS tervezés – komponensválasztás korábbi tapasztalat alapján

- LVL programozható alrendszerek
  - SIL1-SIL2-re, az FPL feltételek alapján
    - Ha a korábbi alkalmazások és a tervezett alkalmazás között különbség van, azt azonosítani és hatásait vizsgálni kell,
    - Ismerni kell a nem biztonságos meghibásodási módokat,
    - Firmware-ek nagy alkalmazási idővel rendelkeznek és megfelelőek,
    - Biztosított a nem megengedett módosításokkal szemben.

61511 – SIS tervezés – komponensválasztás korábbi tapasztalat alapján

- LVL programozható alrendszerek
  - SIL2-nél plusz: Programvégrehajtási hibák detektálása
    - Programszekvencia monitorozás,
    - Kódvédelem módosítás ellen,
    - Változók tartomány és hihetőség ellenőrzése,
    - Hibakizárás vagy diverz programozás,
    - Moduláris megközelítés,
    - Kódolási szabályok alkalmazása ,
    - Dinamikus elemzések és tesztek elvégzése,
    - Mesterséges intelligencia és dinamikus rekonfigurálás mellőzése,
  - SIL2-nél a berendezésnek biztonsági kézikönyvvel is kell rendelkeznie

61511 – SIS tervezés – komponensválasztás korábbi tapasztalat alapján

- FVL programozható alrendszerek

  Csak IEC61508 alapján minősített eszköz alkalmazható.

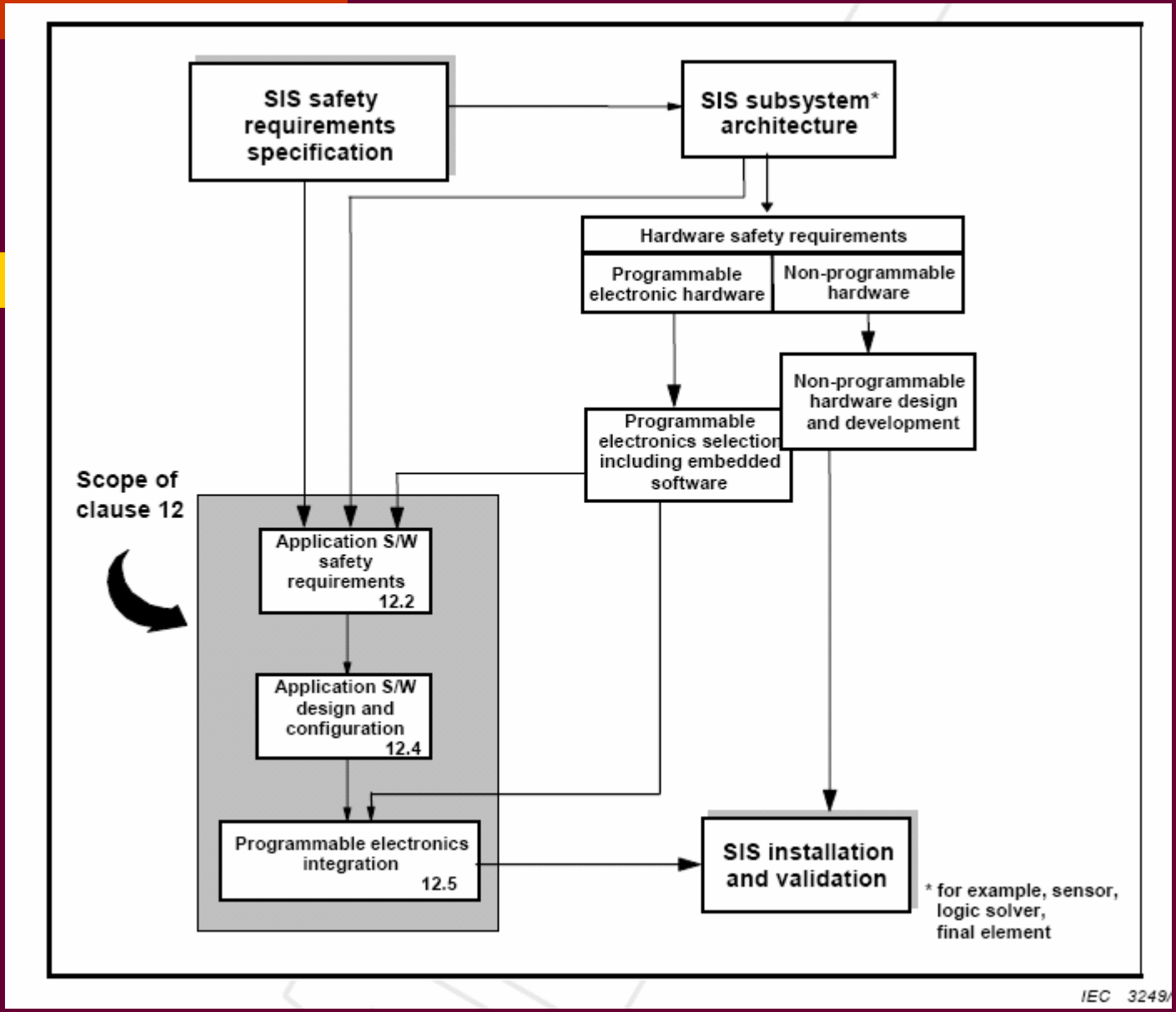
61511 – SIS tervezés – HMI

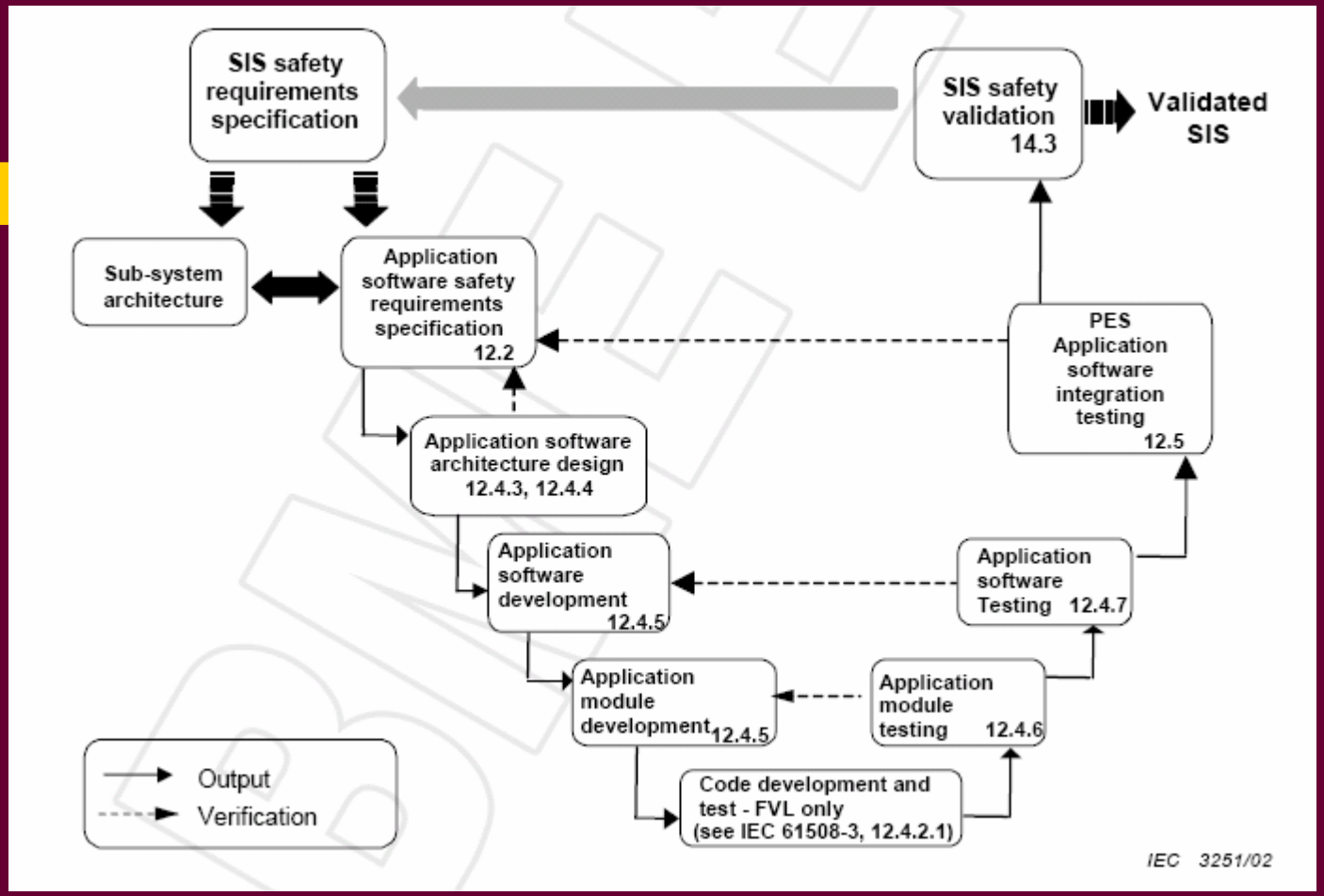
- Lehet közös a BPCS HMI-vel, de elemzéseket igényel.
- Minimális operátori opcióválasztást igényeljen
- Bypass kapcsolások védelme kulccsal vagy jelszóval,
- A biztonságintegritási szint fenntartásához szükséges SIS állapotinformációt meg kell jeleníteni

61511 – felhasználói szoftver

- SW Típusok:
  - Felhasználói szoftver,
  - Szoftver tool-ok,
  - Embedded SW.
- Szoftverfejlesztő nyelvek:
  - FPL – Fixed Program Languages
  - LVL – Limited Variability Languages
  - FVL – Full Variability Languages
- 61511: SW: SIL1…SIL3, FPL vagy LVL
- SIL1, SIL2 és SIL3 között szoftver szempontból nincs különbség

!


SIS safety requirements specification
SIS subsystem* architecture
Hardware safety requirements
Programmable electronic hardware
Non-programmable hardware
Non-programmable hardware design and development
Programmable electronics selection including embedded software
Scope of clause 12
Application S/W safety requirements 12.2
Application S/W design and configuration 12.4
Programmable electronics integration 12.5
SIS installation and validation
* for example, sensor, logic solver, final element
IEC 3249/


SIS safety requirements specification
SIS safety validation 14.3
Validated SIS
Sub-system architecture
Application software safety requirements specification 12.2
PES Application software integration testing 12.5
Application software architecture design 12.4.3, 12.4.4
Application software development 12.4.5
Application software Testing 12.4.7
Application module development 12.4.5
Application module testing 12.4.6
Code development and test - FVL only (see IEC 61508-3, 12.4.2.1)
Output
Verification
IEC 3251/02

61511 – SW életciklus

Safety life-cycle phase		Objectives	Require-ments clause	Information required	Required results
Figure 11 box number	Title				
12.2	Application software safety requirements specification	To specify the requirements for the software safety instrumented functions for each SIS function necessary to implement the required safety instrumented functions To specify the requirements for software safety integrity for each safety instrumented function allocated to that SIS	12.2.2	SIS safety requirements specification Safety manuals of the selected SIS SIS architecture	SIS application software safety requirements specification Verification information
12.3	Application software safety validation planning	To develop a plan for validating the application software	12.3.2	SIS application software safety requirements specification	SIS application software safety validation plan Verification information

12.4	Application software design and development	Architecture To create a software architecture that fulfils the specified requirements for software safety To review and evaluate the requirements placed on the software by the hardware architecture of the SIS	12.4.3	SIS application software safety requirements specification SIS hardware architecture design manuals	Description of the architecture design, for example, segregation of application S/W into related process sub-system and SIL(s), for example, recognition of common application S/W modules such as pump or valve sequences Application software architecture and sub-system integration test specification Verification information
	Application software design, and development	Support tools and programming languages To identify a suitable set of configuration, library, management, and simulation and test tools, over the whole safety life cycle of the software (utility software) To specify the procedures for development of the application software	12.4.4	SIS application software safety requirements specification Description of the architecture design Manuals of the SIS Safety manual of the selected SIS logic solver	List of procedures for use of utility software Verification information

12.4	Application software design, and development	Application software development and application module development To implement the application software that fulfils the specified requirements for application safety	12.4.5	Description of the architecture design List of manuals and procedures of the selected PES for use of utility software	1) Application software program (for example, function block diagrams, ladder logic) 2) Application program simulation and integration test 3) Special purpose application software safety requirements specification 4) Verification information
12.4	Application program development using full variability languages	Program development and test – FVL only To implement full variability language that fulfils the specified requirements for software safety	12.4.6 and 12.4.7	Special purpose application software safety requirements specification	Refer to IEC 61508-3
12.4	Application software design and development	Application software testing 1) To verify that the requirements for software safety have been achieved 2) To show that all appli-cation program subsystems and systems interact correctly to perform their intended functions and do not perform unintended functions Can be merged with the next phase (12.5) subject to satisfactory test coverage	12.4.6, 12.4.7, 12.7	Application program simulation and integration test specification (structure based testing) Software architecture integration test specification	1) Software test results 2) Verified and tested software system 3) Verification information

61511 – SW életciklus (4)

12.5	Program-mable elec-tronics integration (hardware and soft-ware)	To integrate the software onto the target programmable electronic hardware	12.5.2	Software and hardware integration test specification	Software and hardware integration test results Verified software and hardware
12.3	SIS safety validation	Validate that the SIS, including the safety application software, meets the safety requirements	12.3	Software and SIS safety validation plans	Software and SIS validation results

61511 – SW megvalósítás

- Olyan módszert és nyelvet kell választani, ami biztosítja, hogy:
  - A szoftverben nem marad nemdeterminált eset,
  - A követelmények sorba rendezését,
  - Az információáramlást a modulok között,
  - A funkcionalitást (logikai leírásként vagy algoritmikus funkciókként),
  - Az időkorlátok betartását

61511 – SW architektúra

- Leírás is kell!
  - Belső struktúra a felhasznált komponensek specifikációja,
  - A SIF célokra nem használt szoftver modulok,
  - A logikai feldolgozás folyamata, sorrendje,

61511 – SW tool-ok

61511 – egyebek

- FAT (informatív)
- SIS installálás
- Biztonsági validálás
- Üzemeltetés és karbantartás
  - Normás és speciális tevékenységek,
  - Tesztelések,
  - Üzemeltetési és karbantartási eljárások,
  - Az üzemeltetés és karbantartás verifikációja,
  - Felelősségek és kompetencia

És ami hiányzik a 61511-ből

- Módszerek és eljárások részletes megadása