Fejlesztés kockázati alapokon

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.

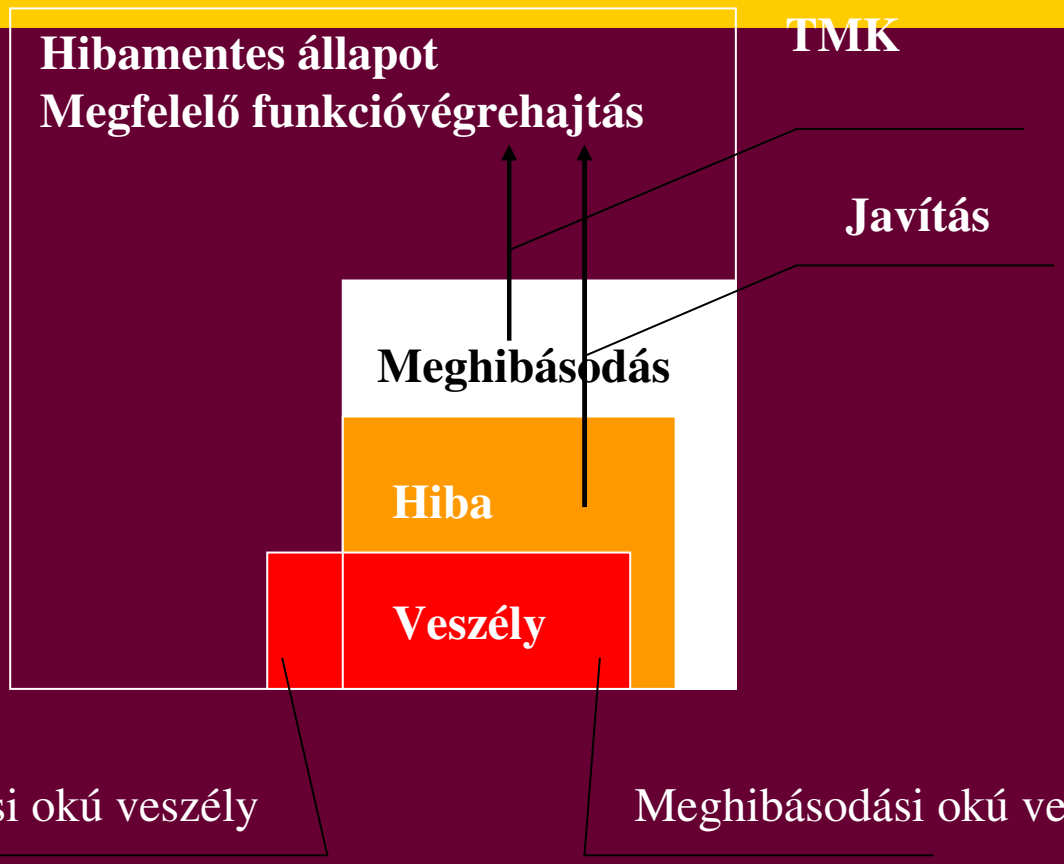
- A szabvány eredetijében érvényes!
  - IEC….. MSZ-EN

- Cégeknél: Az ilyen tanfolyam is lehet része egy biztonsági életciklusnak – ennek megfelelő dokumentálás.

Bevezetés

- Kockázati alapú megközelítések bevezetése
  - Abszolút biztonság nem létezik,
  - A teljes kitesztelés egyre inkább lehetetlen (bizalom kell)
  - Védekezés a véletlen meghibásodások és a szisztematikus hibák ellen,
  - Védekezés mértéke a kockázat, illetve az elvárt kockázatcsökkentés függvénye.
- THR és SIL
  - Véletlen hibák ellen: THR (Tolerable Hazard Rate)
  - Szisztematikus hibák ellen: SIL (Safety Integrity Level)

Bevezetés (2)


Hibamentes állapot
Megfelelő funkcióvégrehajtás
TMK
Javítás
Meghibásodás
Hiba
Veszély
Tervezési okú veszély
Meghibásodási okú veszély

Bevezetés (3a)

- THR és SIL kapcsolata: arányosság elve
  - (igény szerinti üzemmód)

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

Bevezetés (3b)

- THR és SIL kapcsolata: arányosság elve
  - (folyamatos üzemmód)

Table 4 – Safety integrity levels: frequency of dangerous failures of the SIF

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 $< 10^{-5}$

Bevezetés (4)

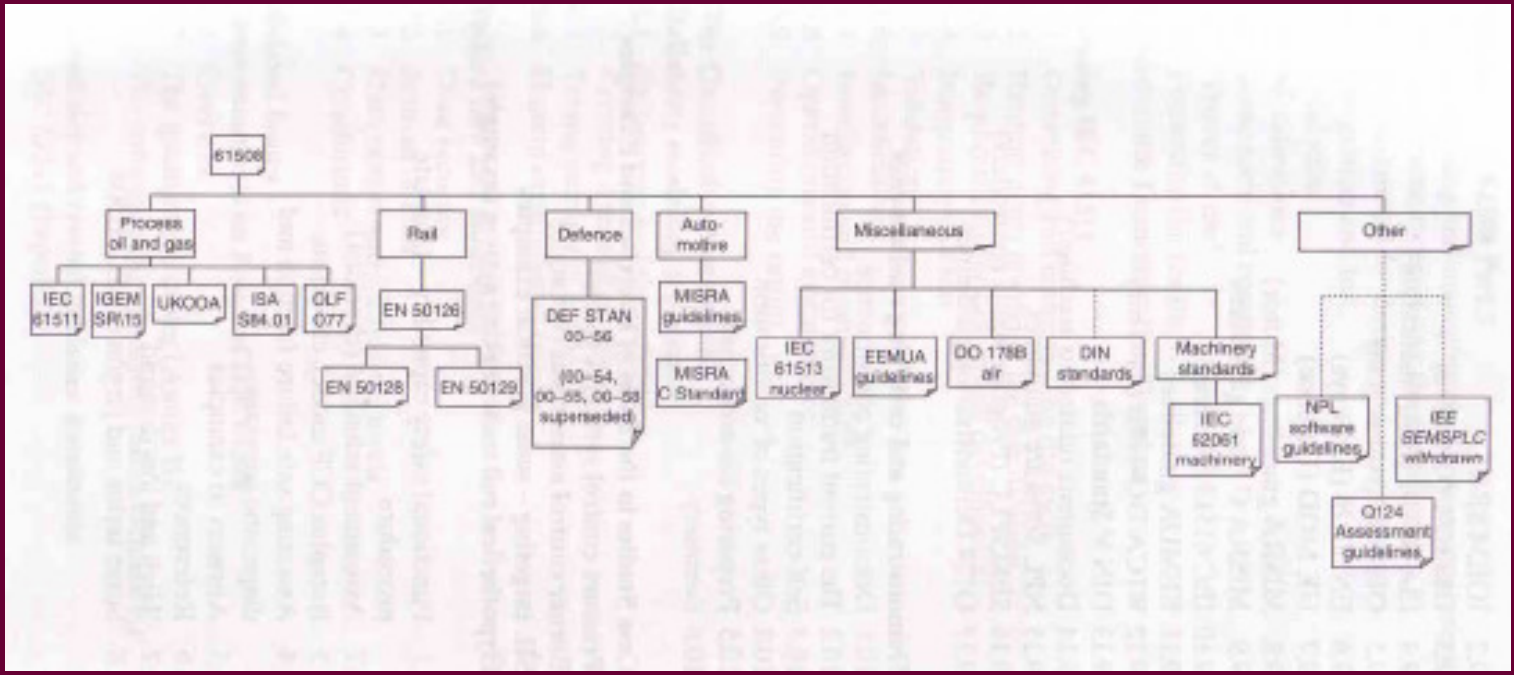
- **THR teljesítése**
  - Architektúra,
  - Redundancia,
  - Egyedi elem -megbízhatóságok.
- **SIL teljesítése**
  - Életciklus,
  - Kompetencia,
  - Függetlenség,
  - Dokumentáltság (információáramlás),
  - Módszerek és eljárások
- Best Practice…

Bevezetés (5)

- A SIL követelmények teljesítése életciklus-szerű
  - Utólag nem pótolható (vagy csak revízióval…),
  - Utólag nehezen igazolható.

Bevezetés (6)

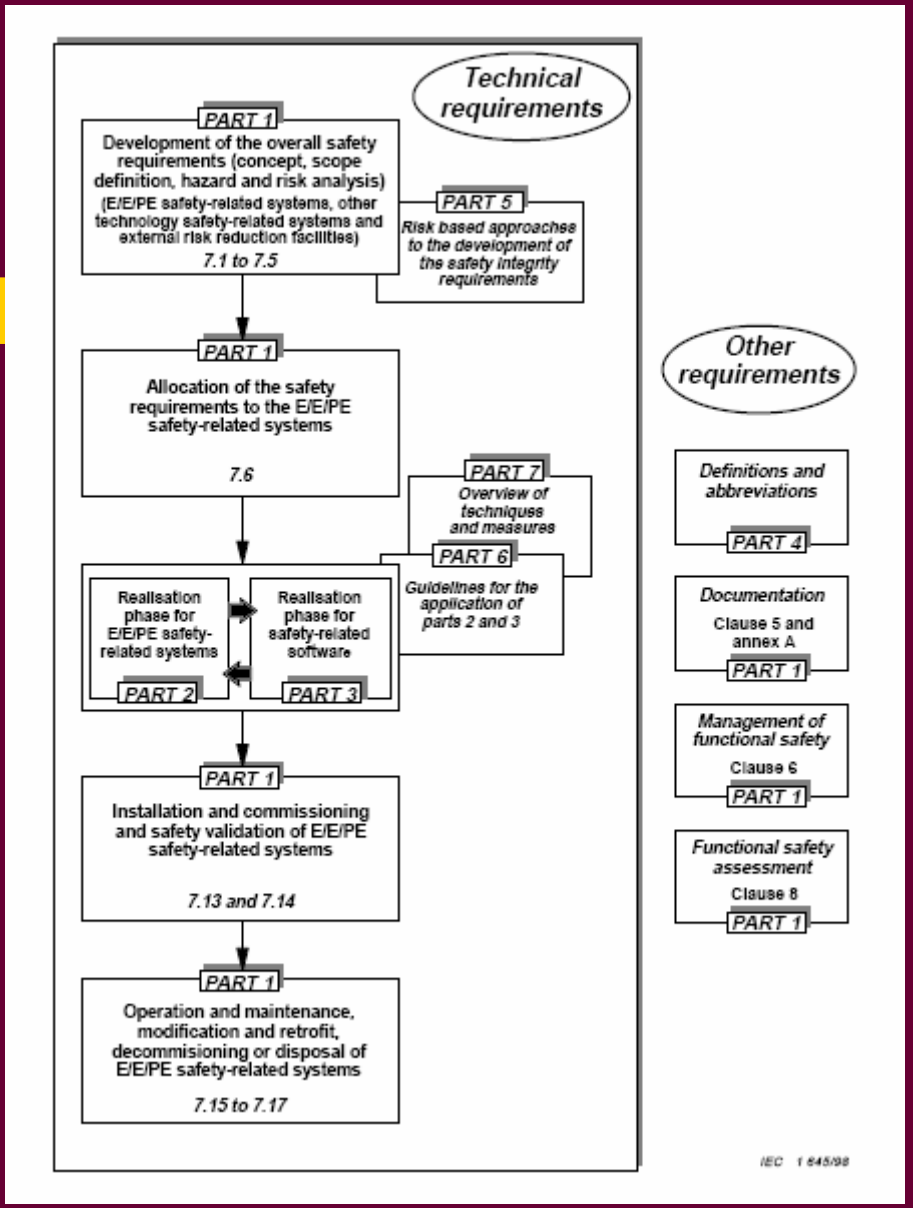
- Szabványok viszonyai



IEC61508 – Funkcionális biztonság

- A funkcionális biztonság fogalma
- E / E / PE
- EUC – Equipment Under Control
- Felépítése:
  - 1. rész: általános követelmények
  - 2. rész: hardver követelmények
  - 3. rész: szoftver követelmények
  - 4. rész: definíciók és rövidítések
  - 5. rész: példák a biztonságintegritás meghatározására
  - 6. rész: irányelvek a 2. és a 3. rész alkalmazásához,
  - 7. rész: a javasolt eljárások áttekintése

IEC61508


Technical requirements
PART 1
Development of the overall safety requirements (concept, scope definition, hazard and risk analysis)
(E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities)
7.1 to 7.5
PART 5
Risk based approaches to the development of the safety integrity requirements
PART 1
Allocation of the safety requirements to the E/E/PE safety-related systems
7.6
PART 7
Overview of techniques and measures
PART 6
Guidelines for the application of parts 2 and 3
Realisation phase for E/E/PE safety-related systems
PART 2
Realisation phase for safety-related software
PART 3
PART 1
Installation and commissioning and safety validation of E/E/PE safety-related systems
7.13 and 7.14
PART 1
Operation and maintenance, modification and retrofit, decommisioning or disposal of E/E/PE safety-related systems
7.15 to 7.17
Other requirements
Definitions and abbreviations
PART 4
Documentation
Clause 5 and annex A
PART 1
Management of functional safety
Clause 6
PART 1
Functional safety assessment
Clause 8
PART 1
IEC 1 645/98

61508 – Kockázatok értelmezése

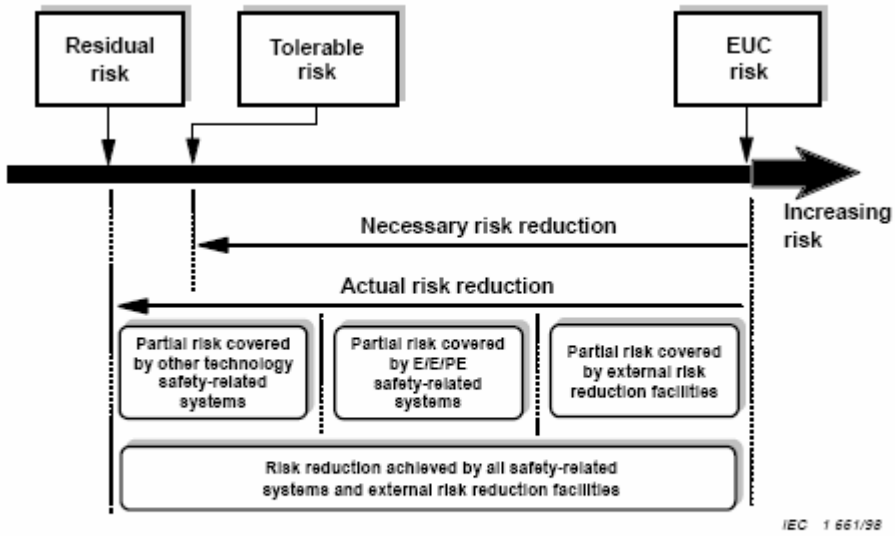


Figure A.1 – Risk reduction: general concepts

Igény szerinti üzem:
A kockázatcsökkentés valószínűségi

Folyamatos üzem:
A kockázatcsökkentés gyakorisági
(ECU risk = 1)

61508 – Kockázatok értelmezése

- Kockázat = f(veszély, gyakoriság)

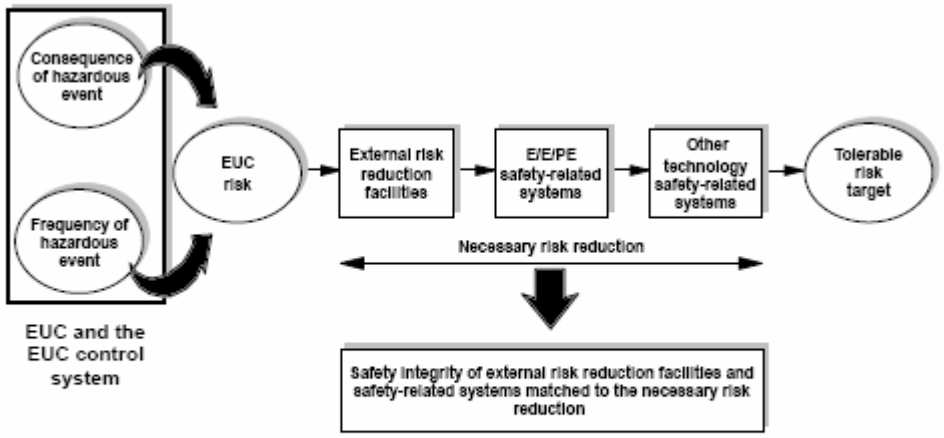


Figure A.2 – Risk and safety integrity concepts

61508 - Kockázatelemzés

- Cél az eltűrhető kockázat meghatározása
  - Nem egyéni vélemény, szakmai, de inkább társadalmi elfogadottság szükséges
- Veszélyes szituációk meghatározása: funkciók alapján (pl. HAZOP)
- Veszélyes szituációkhoz tartozó lehetséges kár meghatározása (emberi veszteség, anyagi veszteség, természeti veszteség)
- Eltűrhető kockázatból adódik a megengedett gyakoriság

61508 – Kockázatelemzés (2)

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

- Kockázatelemzésre az életciklus több pontján van szükség!

61508 – Kockázatelemzési módszerek

- A módszerek csak ajánlottak!
- Kvantitatív – számszerű eredményt szolgáltatóak
  - GAMAB
  - MEM
  - ALARP
- Kvalitatív – SIL szint meghatározására irányulóak
  - RiskGraph (DIN V 19250)

Példa 1: Vasúti fénysorompó

- Funkció azonosítása,
- Veszélyes állapotok (esetleges akadályozó állapotok),
- Eltűrhető kockázat meghatározása (GAMAB)
  - környezet figyelembe vétele
- Egyéb kockázatcsökkentő lehetőségek figyelembe vétele

Példa 1: Vasúti fénysorompó (2)

Ismert és sajnos mindenki által elfogadott tény, hogy a közúti közlekedésben naponta négy ember hal meg. Tételezzük fel, hogy a közút-vasút kereszteződések (amelyek köztudottan a közlekedés egyik legveszélyesebb részét képezi) a napi halálozási rátának csak a 0,01 szeresét, 1%-át adják, vagyis Magyarországon útátjáró balesetben naponta 0,04 személy vesztheti életét. Tételezzük fel, hogy 2000 biztosított útátjáró létezik, ezek biztosítási szintje ugyan eltérő (az igazán veszélyesek minden esetben csapórúddal is biztosítottak), de számításunkban ettől eltekintünk. Ez alapján egy útátjáróban naponta $0,04/2000=2*10^{-5}$ személy halhat meg.

Az útátjáró balesetek egy részét a jól működő útátjáró mellett a közúti járművek vezetőinek felelőtlen magatartása okozza, ezért a berendezés hibájaként csak $1*10^{-5}$ személy halálát engedjük meg naponta, óránként ez kb. $4*10^{-7}$ érték. Tételezzük fel, hogy a járművezetők magatartása felelős (a felelőtlen magatartást már korábban figyelembe vettük), ezért csak minden ötödik veszélyes szituáció jár balesettel, viszont egy balesetben egynél több személy is meghalhat, a számítási egyszerűség kedvéért az egy balesetben elhunytak átlagos számát tekintsük ötnek, így $4*10^{-7}$ 1/óra adódik a veszélyes meghibásodás gyakoriságára.

Veszélyes az a szituáció, amikor a vörös jelzés szükséges lenne, és az nem jelenik meg. Ez lehetséges a vezérlő biztosítóberendezés meghibásodása miatt (pl. foglaltság-érzékelés hibája stb.). Mivel a biztosítóberendezés magas biztonsági szintű, alapvetően SIL4 szintre tervezett, ezért az ilyen hibákra csak 10^{-8} -10^{-9} hiba/óra gyakoriságot engedünk meg, ekkor az optika hibára (jó közelítéssel) továbbra is marad a $4*10^{-7}$ 1/óra érték. Itt a továbbiakban figyelembe vesszük, hogy a vörös jelzés adása két, egymástól független optikával történik, amelyek együttes meghibásodása jelent csak a szempontunkból veszélyes állapotot. Az együttes meghibásodás számításához tételezzük fel, hogy az egyedi optika meghibásodási rátája y 1/óra, így egy év alatt $365*24*y$ meghibásodással számolhatunk. Tételezzünk fel 24 órás maximális javítási időt az egyedi optika vonatkozásában (ehhez a veszélyes meghibásodásnak detektáltnak kell lennie, ez később teljesítendő), így egy év alatt $24*(365*24*y)$ hibás állapotban töltött idővel számolhatunk (feltételezve, hogy ez az idő nem lehet hosszabb egy évnél), a hibás állapot valószínűsége:

$24*(365*24*y)/(365*24)= 24*y=P$

A két optika együttes meghibásodásának gyakorisága:

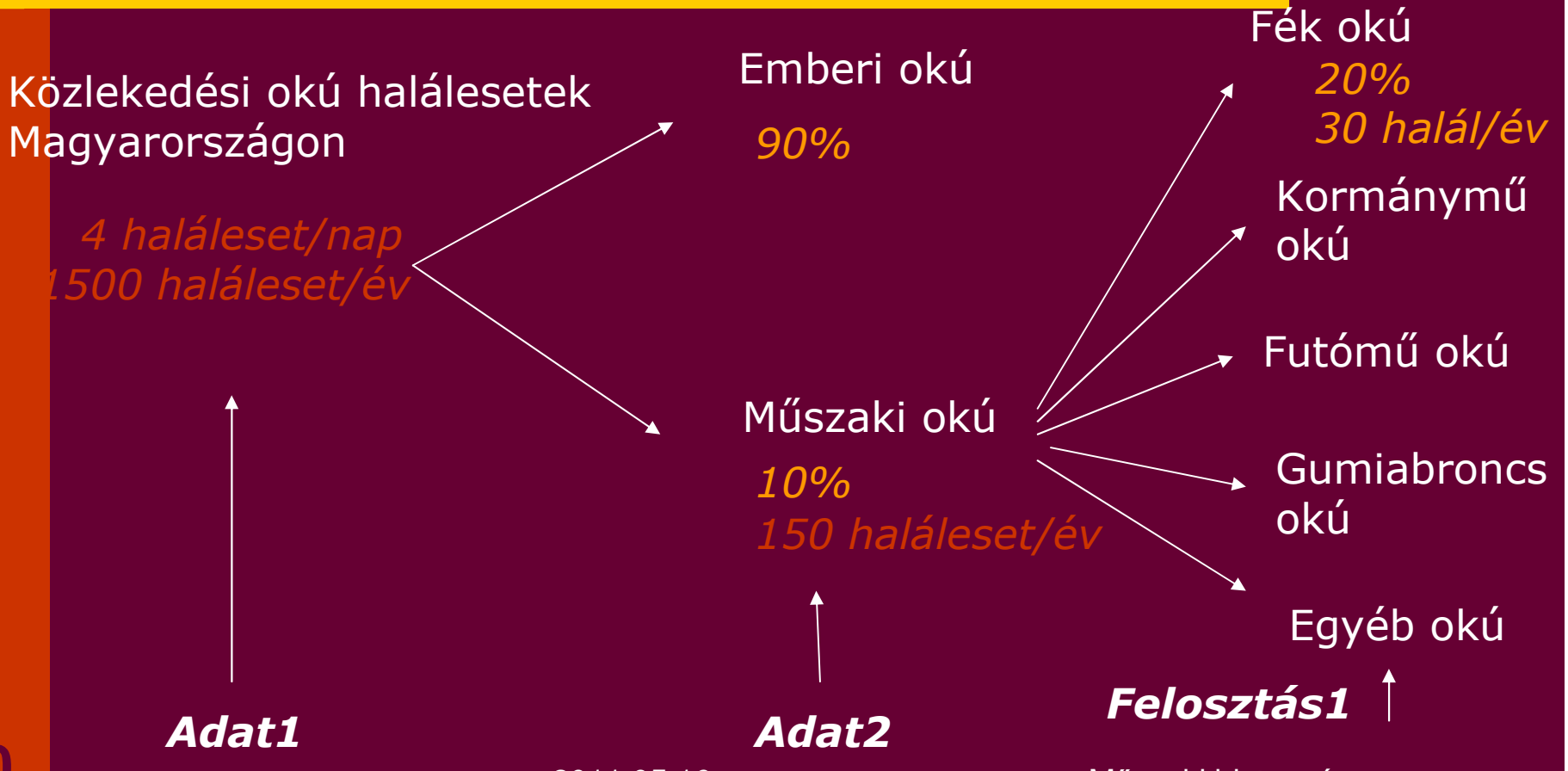
$P*y+P*y$, feltételezve a két optika azonosságát, ennek az értéknek kell kisebbnek lennie, mint $4*10^{-7}$ 1/óra. Ebből y=**$9,12*10^{-5}$ 1/óra**.

Ez az érték a SIL1 Biztonságintegritási szintnek felelne meg. Vegyünk figyelembe azonban egy 10-es biztonsági faktort, az optika vonatkozásában írjunk elő **$9,12*10^{-6}$ 1/óra** veszélyes meghibásodási gyakoriságot. **Ez az optika vonatkozásában SIL2 értéket jelent.**

Példa 2: gépjármű fékberendezés

- Funkció azonosítása,
- Veszélyes állapotok (esetleges akadályozó állapotok),
- Eltűrhető kockázat meghatározása (GAMAB)
  - környezet figyelembe vétele
- Egyéb kockázatcsökkentő lehetőségek figyelembe vétele

Példa 2: gépjármű fékberendezés

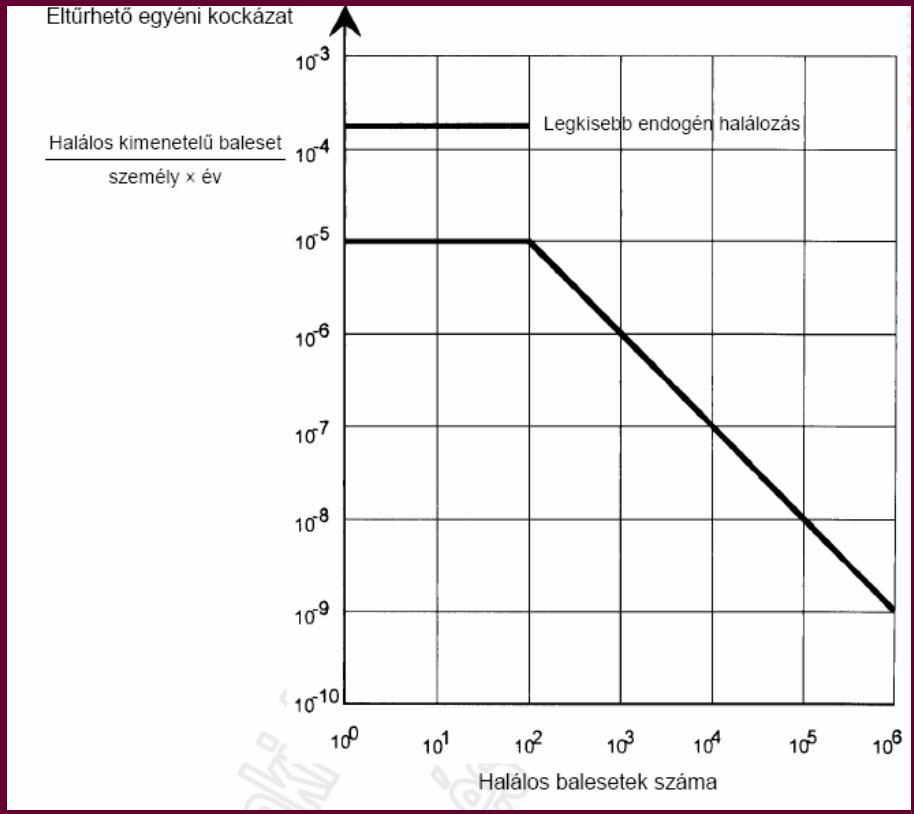


Példa 2: gépjármű fékberendezés

Példa 2: gépjármű fékberendezés

61508 – Kockázatelemzési módszerek

- MEM módszer

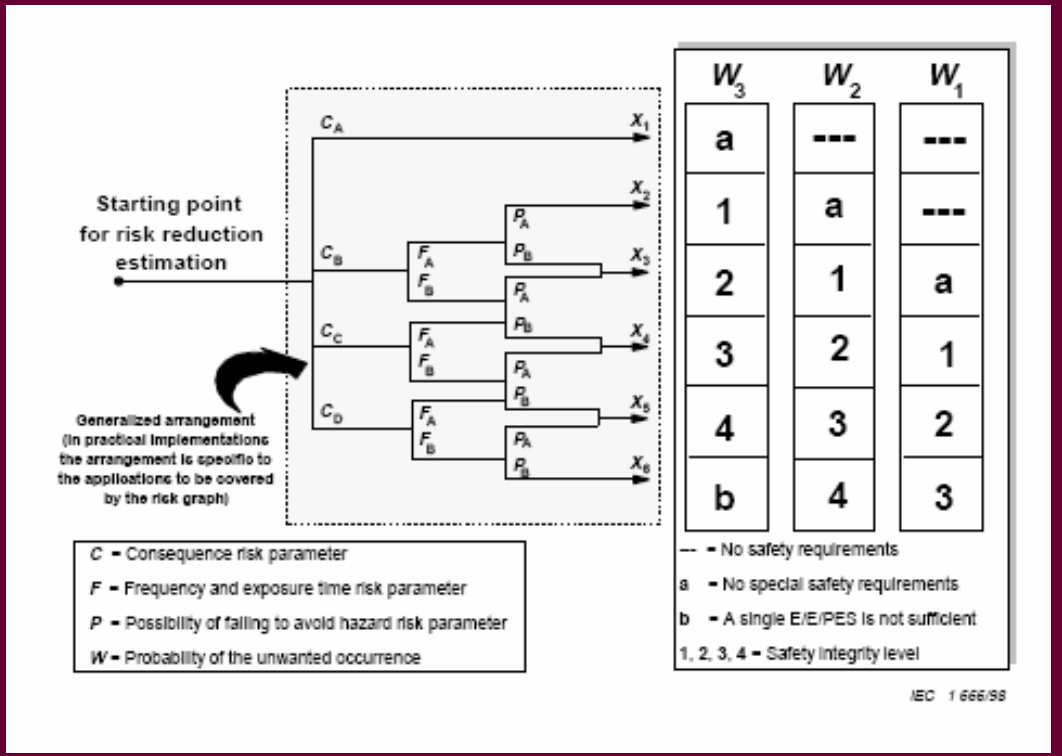


A gyakorlatban a következő adatok használatosak:

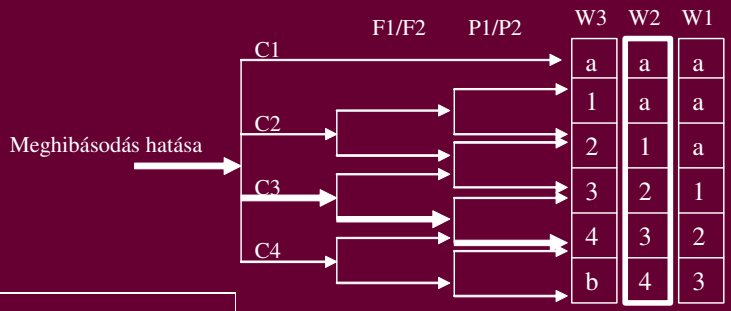
- $R_1 \leq 10^{-5}$ halálos kimenetelű baleset/személy × év
- $R_2 \leq 10^{-4}$ komoly sérülések/személy × év
- $R_3 \leq 10^{-3}$ könnyű sérülések/személy × év

61508 – Kockázatelemzési módszerek

- RiskGraph módszer

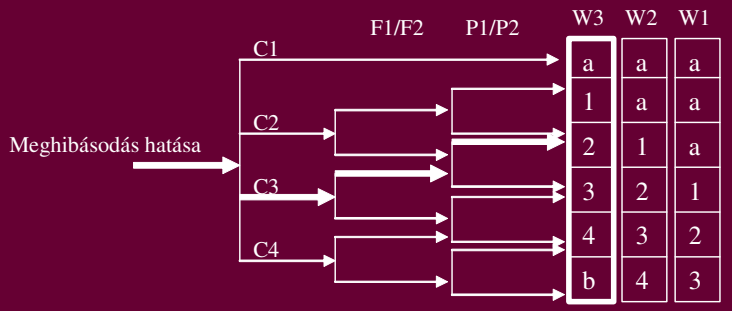


Elemzési példák (1)
fék alapfunkció



Kockázati paraméter		*Értelmezés*
Következmény	C1	Kisebb sérülés
	C2	Súlyosabb sérülés egy vagy több személynél, vagy egy személy halála
	C3	***Több személy halála. Az elsődleges fékfunkció hiánya olyan balesethez vezethet (különösen haszonjárművek esetén), amelynél több személy halálával is számolni kell.***
	C4	Nagyon sok személy halála, katasztrófa
A veszélyes zónában tartózkodás	F1	Ritkától átlagos gyakoriságig
	F2	***Gyakori tartózkodástól állandó tartózkodásig. A fékfunkció igen gyakran kerül felhasználásra egy átlagos felhasználásban. (Ugyanakkor nagy távolságú utakat, valamint városokat elkerülő útvonalat feltételezve F1 paraméter is elképzelhető lenne).***
A veszély elkerülésének lehetősége	P1	Lehetséges bizonyos körülmények között
	P2	***Majdnem lehetetlen. A veszélyes szituáció sem kormánymozgással, sem figyelmeztető jelzések adásával nem kerülhető el hatékonyan. (Megjegyzendő, hogy megfelelő kijelzés mellett P1 paraméter alkalmazása is elfogadható)***
A nem kívánt esemény gyakorisága	W1	Nagyon kis valószínűség
	W2	***Kis valószínűség. A további kockázatcsökkentési lehetőségek között vettük figyelembe a kézifék alkalmazási lehetőségét.***
	W3	Nagy valószínűség

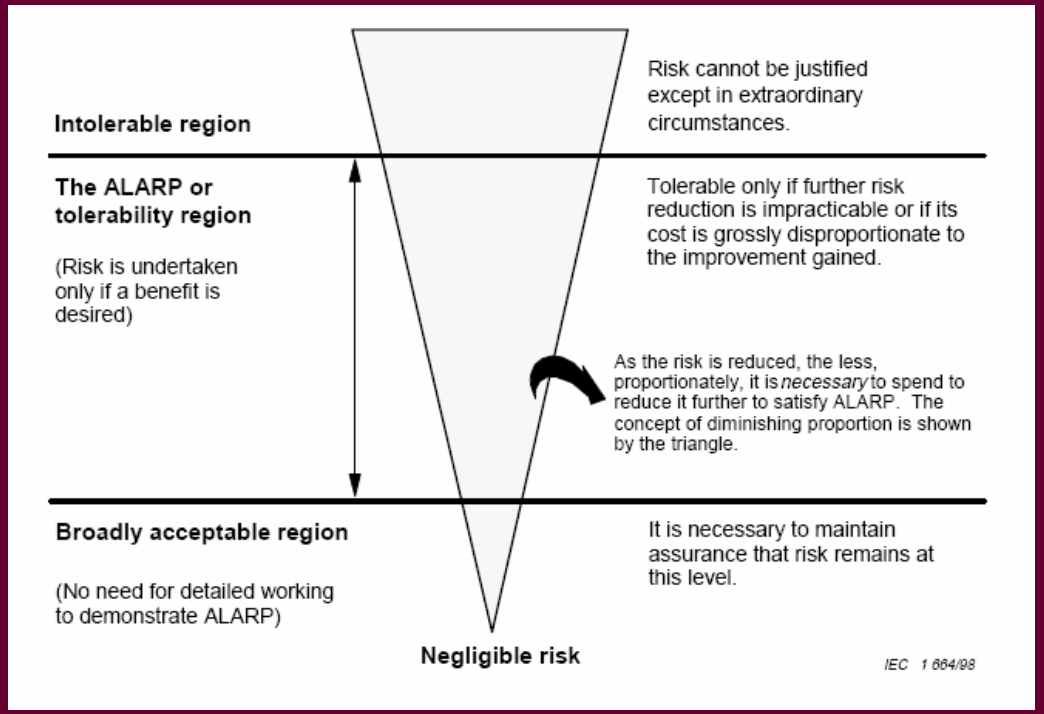
Elemzési példák (2) fékasszisztens



Kockázati paraméter		*Értelmezés*
Következmény	C1	Kisebb sérülés
	C2	Súlyosabb sérülés egy vagy több személynél, vagy egy személy halála
	C3	***Több személy halála.***
	C4	Nagyon sok személy halála, katasztrófa
A veszélyes zónában tartózkodás	***F1***	***Ritkától átlagos gyakoriságig. Vészfékezésre ritkán van szükség.***
	F2	Gyakori tartózkodástól állandó tartózkodásig.
A veszély elkerülésének lehetősége	***P1***	***Lehetséges bizonyos körülmények között. A vészfékezés az asszisztens funkció nélkül is hatásos lehet.***
	P2	Majdnem lehetetlen.
A nem kívánt esemény gyakorisága	W1	Nagyon kis valószínűség.
	W2	Kis valószínűség.
	W3	***Nagy valószínűség. Ha a funkcióra szüksége lenne, további kockázatcsökkentés nem lehetséges.***

61508 – Kockázatelemzési módszerek

- ALARP – As Low As Reasonably Possible



61508 – Kockázatelemzési módszerek

- ALARP – As Low As Reasonably Possible

Cél:
Megfelelő gyakoriság meghatározása

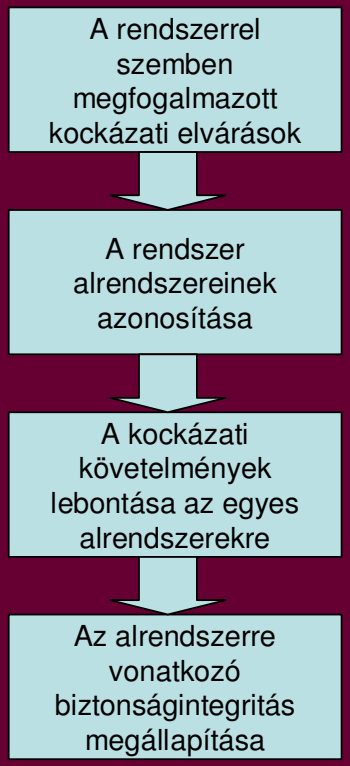
Table B.1 – Example of risk classification of accidents

Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

NOTE 1 – The actual population with risk classes I, II, III and IV will be sector dependent and will also depend upon what the actual frequencies are for frequent, probable, etc. Therefore, this table should be seen as an example of how such a table could be populated, rather than as a specification for future use.

NOTE 2 – Determination of the safety integrity level from the frequencies in this table is outlined in annex C.

61508 – Követelmények allokálása



THR_i

ahol a veszélyes szituációk 1..i között.

J darab alrendszer

THR_{iJ}

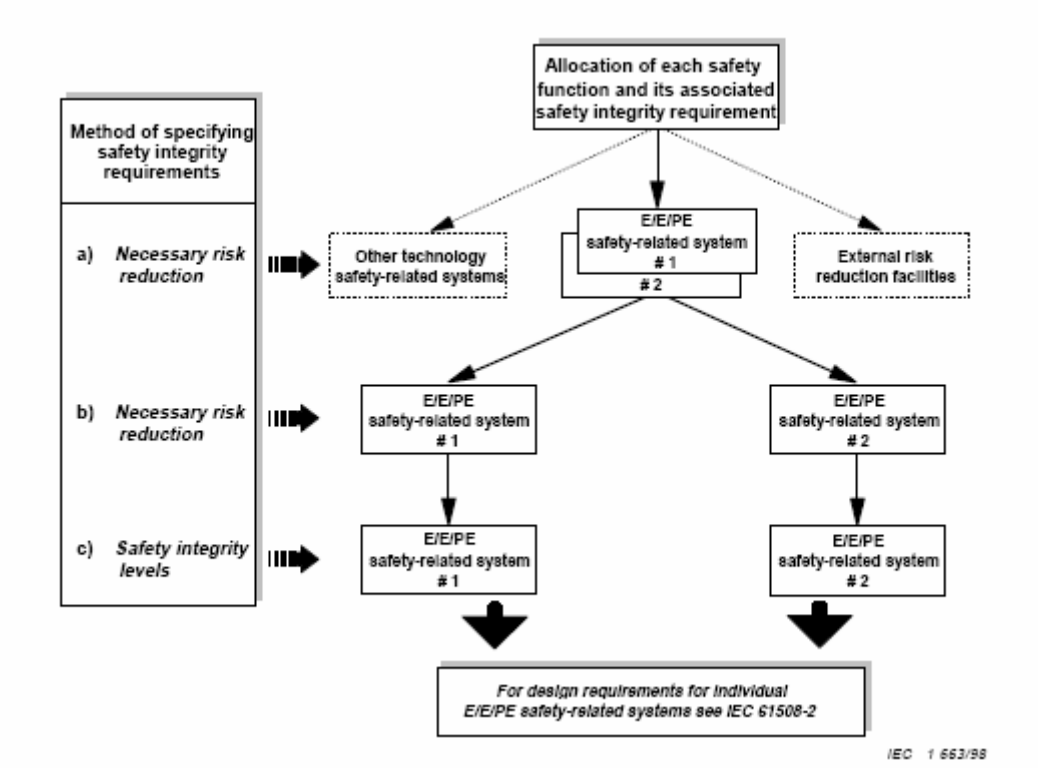
Minden alrendszerre i darab követelményérték

$SIL_{iJ} = f(THR_{iJ})$

Minden alrendszerre i darab SIL követelményszint

Az alrendszernél a max(SIL_{iJ}) veendő figyelembe.

61508 – Követelmények allokálása



Soros rendszer:
-Követelmény nő

Párhuzamos rendszer:
-Követelmény csökken

61508 – Követelmények következményei

Table 2 – Safety integrity levels: target failure measures for a safety function operating in low demand mode of operation

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

Table 3 – Safety integrity levels: target failure measures for a safety function operating in high demand or continuous mode of operation

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure 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 $< 10^{-5}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

61508 – Követelmények következményei (2)

- Egy adott berendezésnek:
  - A THR követelményeket az egyedi funkciókra teljesítenie kell,
  - A SIL követelmények közül a legmagasabbat kell teljesítenie

61508 – hardver SIL

- A hardver által teljesíthető SIL meghatározása három paraméter alapján:
  - A rendszer megismertsége,
    - „A” tip: - meghibásodási módok jól definiáltak; hiba melletti viselkedés determinált; elégséges adat a detektáltság megállapításához.
    - „B” tip: - a fenti valamelyik követelmény nem teljesül
  - Meghibásodási módok biztonsága,
  - Hibatűrés.

61508 – hardver SIL

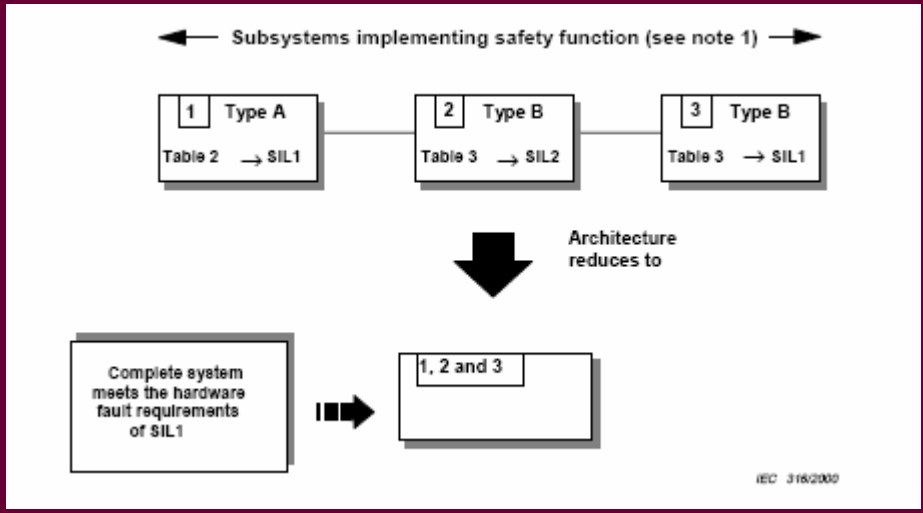
Table 2 – Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % – < 90 %	SIL2	SIL3	SIL4
90 % – < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4
NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table. NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function. NOTE 3 See annex C for details of how to calculate safe failure fraction.			

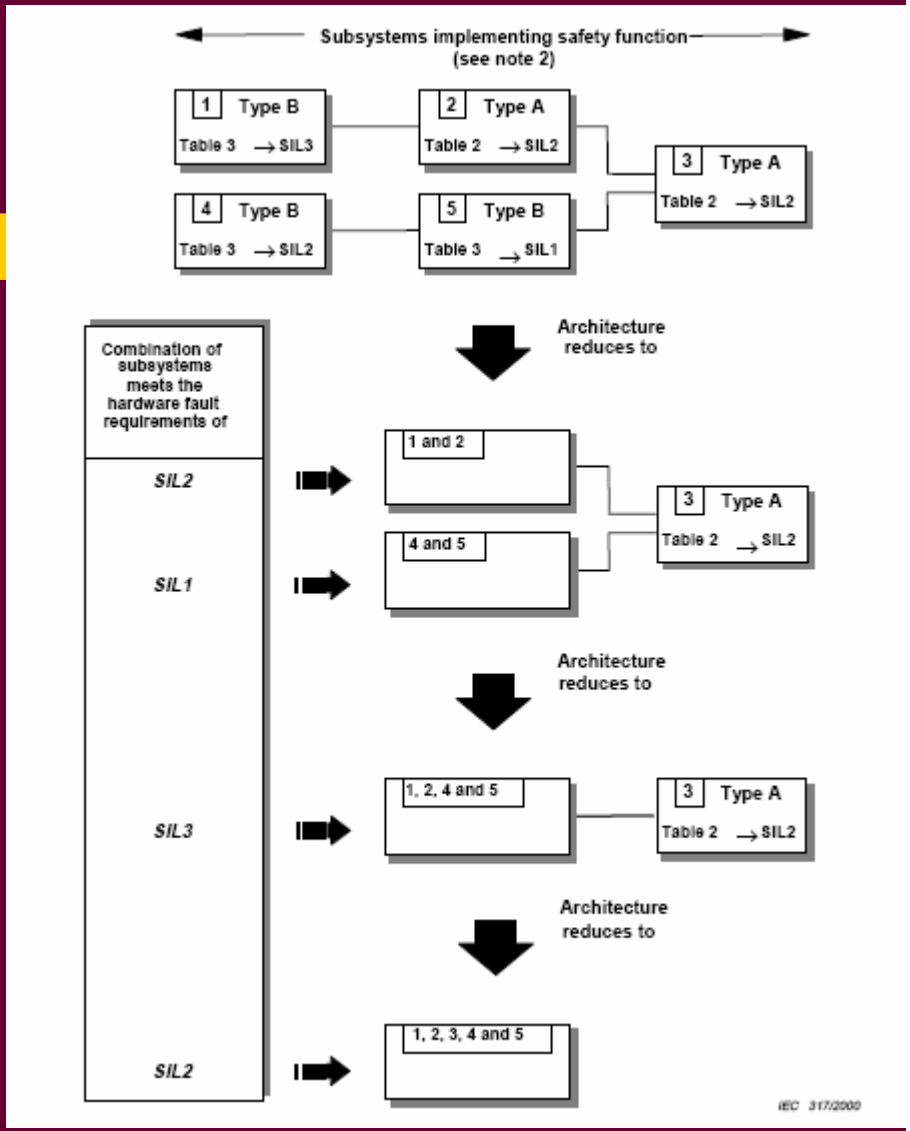
Table 3 – Hardware safety integrity: architectural constraints on type B safety-related subsystems

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4
NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table. NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function. NOTE 3 See annex C for details of how to calculate safe failure fraction.			

61508 – hardver SIL



61508 – hardver SIL



THR követelmények teljesülésének igazolása

- Alapadatok adatbázisból
  - Saját adatok (azonos vagy hasonló alkalmazás)
  - Általános adatok, pl. MIL-HDBK 217F
  - A kettő kombinálása, súlyozása
- Rendszerelemzések
  - FMEA
  - Hibafa
  - Megbízhatósági blokkdiagram

THR követelmények teljesülésének igazolása - alapadatok

MIL-HDBK-217F

5.1 MICROCIRCUITS, GATE/LOGIC ARRAYS AND MICROPROCESSORS

DESCRIPTION

1. Bipolar Devices, Digital and Linear Gate/Logic Arrays
2. MOS Devices, Digital and Linear Gate/Logic Arrays
3. Field Programmable Logic Array (PLA) and Programmable Array Logic (PAL)
4. Microprocessors

$$\lambda_p = (C_1\pi_T + C_2\pi_E)\,\pi_Q\pi_L \quad \text{Failures}/10^6 \text{ Hours}$$

Bipolar Digital and Linear Gate/Logic Array Die Complexity Failure Rate - C_1

Digital		Linear		PLA/PAL	
No. Gates	C_1	No. Transistors	C_1	No. Gates	C_1
1 to 100	.0025	1 to 100	.010	Up to 200	.010
101 to 1,000	.0050	101 to 300	.020	201 to 1,000	.021
1,001 to 3,000	.010	301 to 1,000	.040	1,001 to 5,000	.042
3,001 to 10,000	.020	1,001 to 10,000	.060		
10,001 to 30,000	.040				
30,001 to 60,000	.080				

Temperature Factor For All Microcircuits - π_T

	TTL, ASTTL, CML, HTTL, FTTL, DTL, ECL, ALSTTL	F, LTTL, STTL	BiCMOS, LSTTL	III, I^2L, ISL	Digital MOS, VHSIC CMOS	Linear (Bipolar & MOS)	Memories (Bipolar & MOS), MNOS	GaAs MMIC Active Devices, π_{TA}	GaAs Digital Active Devices, π_{TA}
Ea(eV) → T_J (°C)	.4	.45	.5	.6	.35	.65	.8	1.5	1.4
25	.10	.10	.10	.10	.10	.10	.10	3.20E-09	1.00E-08
30	.13	.13	.14	.15	.13	.15	.15	8.40E-09	2.50E-08
35	.17	.18	.19	.21	.16	.23	.21	2.10E-08	5.90E-08
40	.21	.23	.25	.31	.19	.34	.31	5.20E-08	1.40E-07
45	.27	.3	.34	.43	.24	.49	.43	1.30E-07	3.10E-07
50	.33	.39	.45	.61	.29	.71	.61	2.90E-07	6.60E-07
55	.42	.50	.59	.85	.35	1.0	.85	6.70E-07	1.50E-06
60	.51	.63	.77	1.2	.42	1.4	1.2	1.50E-06	3.10E-06
65	.63	.80	1.0	1.6	.50	2.0	1.6	3.20E-06	6.40E-06
70	.77	1.0	1.3	2.1	.60	2.8	2.1	6.80E-06	1.30E-05
75	.94	1.2	1.6	2.9	.71	3.8	2.9	1.40E-05	2.50E-05
80	1.1	1.5	2.1	3.8	.84	5.2	3.8	2.90E-05	4.90E-05
85	1.4	1.9	2.6	5.0	.98	7.0	5.0	5.70E-05	9.40E-05
90	1.6	2.3	3.3	6.6	1.1	9.3	6.6	1.10E-04	1.70E-04
95	1.9	2.8	4.1	8.5	1.3	12	8.5	2.10E-04	3.20E-04
100	2.3	3.4	5.0	11	1.5	16	11	4.00E-04	5.80E-04
105	2.7	4.1	6.2	14	1.8	21	14	7.50E-04	1.00E-03
110	3.2	4.9	7.5	18	2.1	28	18	1.40E-03	1.80E-03
115	3.7	5.8	9.2	23	2.4	35	23	2.40E-03	3.10E-03
120	4.3	6.9	11	28	2.7	45	28	4.30E-03	5.30E-03
125	5	8.2	13	35	3.1	58	35	7.50E-03	9.00E-03
130	5.8	9.6	16	44	3.5	73	44	1.30E-02	1.50E-02
135	6.7	11	19	54	3.9	92	54	2.20E-02	2.40E-02
140	7.7	13	23	67	4.4	120	67	3.70E-02	3.90E-02
145	8.8	15	27	82	5.0	140	82	6.10E-02	6.30E-02
150	10	18	32	100	5.5	180	100	1.00E-01	1.00E-01
155	11	20	37	120	6.3	220	120	1.60E-01	1.60E-01
160	13	24	43	150	7.0	270	150	2.60E-01	2.40E-01
165	15	27	50	180	7.9	330	180	4.10E-01	3.70E-01
170	18	31	59	210	8.7	400	210	6.40E-01	5.70E-01
175	18	35	68	250	9.8	480	250	9.90E-01	8.50E-01

$$\pi_T = .1 \exp\left(\frac{-E_a}{8.617 \times 10^{-5}}\left(\frac{1}{T_J + 273} - \frac{1}{298}\right)\right)$$ Silicon Devices

$$\pi_T = .1 \exp\left(\frac{-E_a}{8.617 \times 10^{-5}}\left(\frac{1}{T_J + 273} - \frac{1}{425}\right)\right)$$ GaAs Devices

E_a = Effective Activation Energy (eV) (Shown Above)

T_J = Worse Case Junction Temperature (Silicon Devices) or Average Active Device Channel Temperature (GaAs Devices). See Section 5.11 (or Section 5.12 for Hybrids) for T_J Determination.

NOTES:
1. $T_J = T_C + P\theta_{JC}$
   - T_C = Case Temperature (°C)
   - P = Device Power Dissipation (W)
   - θ_{JC} = Junction to Case Thermal Resistance (°C/W)

   θ_{JC} should be obtained from the device manufacturer, MIL-M-38510, or from the default values shown in Section 5.11 for the closest equivalent device.
2. Use Digital MOS column for HC, HCT, AC, ACT, C and FCT technologies.
3. Table entries should be considered valid only up to the rated temperature of the component under consideration.

THR követelmények teljesülésének igazolása - alapadatok

Package Failure Rate for all Microcircuits - C_2

Number of Functional Pins, N_p	Package Type: Hermetic: DIPs w/Solder or Weld Seal, Pin Grid Array (PGA)[1], SMT (Leaded and Nonleaded)	DIPs with Glass Seal[2]	Flatpacks with Axial Leads on 50 Mil Centers[3]	Cans[4]	Nonhermetic: DIPs, PGA, SMT (Leaded and Nonleaded)[5]
3	.00092	.00047	.00022	.00027	.0012
4	.0013	.00073	.00037	.00049	.0016
6	.0019	.0013	.00078	.0011	.0025
8	.0026	.0021	.0013	.0020	.0034
10	.0034	.0029	.0020	.0031	.0043
12	.0041	.0038	.0028	.0044	.0053
14	.0048	.0048	.0037	.0060	.0062
16	.0056	.0059	.0047	.0079	.0072
18	.0064	.0071	.0058		.0082
22	.0079	.0096	.0083		.010
24	.0087	.011	.0098		.011
28	.010	.014			.013
36	.013	.020			.017
40	.015	.024			.019
64	.025	.048			.032
80	.032				.041
128	.053				.068
180	.076				.098
224	.097				.12

THR követelmények teljesülésének igazolása - alapadatok

Environment Factor - π_E

Environment	π_E
G_B	.50
G_F	2.0
G_M	4.0
N_S	4.0
N_U	6.0
A_{IC}	4.0
A_{IF}	5.0
A_{UC}	5.0
A_{UF}	8.0
A_{RW}	8.0
S_F	.50
M_F	5.0
M_L	12
C_L	220

Learning Factor - π_L

Years in Production, Y	π_L
≤ .1	2.0
.5	1.8
1.0	1.5
1.5	1.2
≥ 2.0	1.0

$\pi_L = .01 \exp(5.35 - .35Y)$

Y = Years generic device type has been in production

Quality Factors - π_Q

Description	π_Q
Class S Categories: 1. Procured in full accordance with MIL-M-38510, Class S requirements. 2. Procured in full accordance with MIL-I-38535 and Appendix B thereto (Class U). 3. Hybrids: (Procured to Class S requirements (Quality Level K) of MIL-H-38534.	.25
Class B Categories: 1. Procured in full accordance with MIL-M-38510, Class B requirements. 2. Procured in full accordance with MIL-I-38535, (Class Q). 3. Hybrids: Procured to Class B requirements (Quality Level H) of MIL-H-38534.	1.0
Class B-1 Category: Fully compliant with all requirements of paragraph 1.2.1 of MIL-STD-883 and procured to a MIL drawing, DESC drawing or other government approved documentation. (Does not include hybrids). For hybrids use custom screening section below.	2.0

THR követelmények teljesülésének igazolása – alapadatok (Appendix A)

Generic Failure Rate, λ_g (Failures/10^6 Hours) for Microcircuits. See Page A-4 for π_Q Values
(Defaults: π_T Based on Ea Shown, Solder or Weld Seal DIPs/PGAs (No. Pins as Shown Below), π_L = 1 (Device in Production ≥ 2 Yr.))

Section #	Part Type	Environ. → T_J (°C) →	G_B 50	G_F 60	G_M 65	N_S 60	N_U 65	A_{IC} 75	A_F 75	A_{UC} 90	A_{UF} 90	A_{RW} 75	S_F 50	M_F 65	M_L 75	C_L 60
5.1	Bipolar Technology															
	Gate/Logic Arrays, Digital (Ea = .4)															
	1 - 100 Gates	(16 Pin DIP)	.0036	.012	.024	.024	.035	.025	.030	.032	.049	.047	.0036	.030	.069	1.2
	101 - 1000 Gates	(24 Pin DIP)	.0060	.020	.038	.037	.055	.039	.048	.051	.077	.074	.0060	.046	.11	1.9
	1001 to 3000 Gates	(40 Pin DIP)	.011	.035	.066	.065	.097	.070	.085	.091	.14	.13	.011	.082	.19	3.3
	3001 to 10,000 Gates	(128 Pin PGA)	.033	.12	.22	.22	.33	.23	.28	.30	.46	.44	.033	.28	.65	12
	10,000 to 30,000 Gates	(180 Pin PGA)	.052	.17	.33	.33	.48	.34	.42	.45	.68	.65	.052	.41	.95	17
	30,000 to 60,000 Gates	(224 Pin PGA)	.075	.23	.44	.43	.63	.46	.56	.61	.90	.85	.075	.53	1.2	21
5.1	Gate/Logic Arrays, Linear (Ea = .65)															
	1 - 100 Transistors	(14 Pin DIP)	.0095	.024	.039	.034	.049	.057	.062	.12	.13	.076	.0095	.044	.098	1.1
	101 - 300 Transistors	(16 Pin DIP)	.017	.041	.065	.054	.078	.10	.11	.22	.24	.13	.017	.072	.15	1.4
	301 - 1000 Transistors	(24 Pin DIP)	.033	.074	.11	.092	.13	.19	.19	.41	.44	.22	.033	.12	.26	2.0
	1001 - 10,000 Transistors	(40 Pin DIP)	.050	.12	.18	.15	.21	.29	.30	.63	.67	.35	.050	.19	.41	3.4
5.1	Programmable Logic Arrays (Ea = .4)															
	Up to 200 Gates	(16 Pin DIP)	.0061	.016	.029	.027	.040	.032	.037	.044	.061	.054	.0061	.034	.076	1.2
	201 to 1000 Gates	(24 Pin DIP)	.011	.028	.048	.045	.065	.054	.063	.077	.10	.089	.011	.057	.12	1.9
	1001 to 5000 Gates	(40 Pin DIP)	.022	.052	.087	.082	.12	.099	.11	.14	.19	.16	.022	.10	.22	3.3
5.1	MOS Technology															
	Gate/Logic Arrays, Digital (Ea = .35)															
	1 to 100 Gates	(16 Pin DIP)	.0057	.015	.027	.027	.039	.029	.035	.039	.058	.052	.0057	.033	.074	1.2
	101 to 1000 Gates	(24 Pin DIP)	.010	.028	.045	.043	.062	.049	.057	.066	.092	.083	.010	.053	.12	1.9
	1001 to 3000 Gates	(40 Pin DIP)	.019	.047	.080	.077	.11	.088	.10	.12	.17	.15	.019	.095	.21	3.3
	3001 to 10,000 Gates	(128 Pin PGA)	.049	.14	.25	.24	.36	.27	.32	.36	.51	.48	.049	.30	.69	12
	10,001 to 30,000 Gates	(180 Pin PGA)	.084	.22	.39	.37	.54	.42	.49	.56	.79	.72	.084	.46	1.0	17
	30,000 to 60,000 Gates	(224 Pin PGA)	.13	.31	.53	.51	.73	.59	.69	.82	1.1	.98	.13	.63	1.4	21
5.1	Gate/Logic Arrays, Linear (Ea = .65)															
	1 to 100 Transistors	(14 Pin DIP)	.0095	.024	.039	.034	.049	.057	.062	.12	.13	.076	.0095	.044	.098	1.1
	101 to 300 Transistors	(16 Pin DIP)	.017	.041	.065	.054	.078	.10	.11	.22	.24	.13	.017	.072	.15	1.4
	301 to 1,000 Transistors	(24 Pin DIP)	.033	.074	.11	.092	.13	.19	.19	.41	.44	.22	.033	.12	.26	2.0
	1001 to 10,000 Transistors	(40 Pin DIP)	.05	.12	.18	.15	.21	.29	.30	.63	.67	.35	.05	.19	.41	3.4
5.1	Floating Gate Programmable Logic Array, MOS (Ea = .35)															
	Up to 16K Cells	(24 Pin DIP)	.0046	.018	.035	.035	.052	.035	.044	.044	.070	.070	.0046	.044	.10	1.9
	16K to 64K Cells	(28 Pin DIP)	.0056	.021	.042	.042	.062	.042	.052	.053	.084	.083	.0056	.052	.12	2.3
	64K to 256K Cells	(28 Pin DIP)	.0081	.022	.043	.042	.063	.043	.054	.055	.086	.084	.0081	.053	.13	2.3
	256K to 1M Cells	(40 Pin DIP)	.0095	.033	.064	.063	.094	.065	.080	.083	.13	.13	.0095	.079	.19	3.3
5.1	Microprocessors, Bipolar (Ea = .4)															
	Up to 8 Bits	(40 Pin DIP)	.028	.061	.098	.091	.13	.12	.13	.17	.22	.18	.028	.11	.24	3.3
	Up to 16 Bits	(64 Pin PGA)	.052	.11	.18	.16	.23	.21	.24	.32	.39	.31	.052	.20	.41	5.6
	Up to 32 Bits	(128 Pin PGA)	.11	.23	.36	.33	.47	.44	.49	.65	.81	.65	.11	.42	.86	12
5.1	Microprocessors, MOS (Ea = .35)															
	Up to 8 Bits	(40 Pin DIP)	.048	.089	.13	.12	.16	.16	.17	.24	.28	.22	.048	.15	.28	3.4
	Up to 16 Bits	(64 Pin PGA)	.093	.17	.24	.22	.29	.30	.32	.45	.52	.40	.093	.27	.50	5.6
	Up to 32 Bits	(128 Pin PGA)	.19	.34	.49	.45	.60	.61	.66	.90	1.1	.82	.19	.54	1.0	12

ság

THR követelmények teljesülésének igazolása - rendszerelemzések

- Rendszerelemzések
  - FMEA (Bottom-up)
  - Hibafa (Top-down)
- Módszertan:
  - Hibakatalógus,
  - Strukturálás,
  - Modellalkotás

Hibakatalógus

Table A.1 – Faults or failures to be detected during operation or to be analysed in the derivation of safe failure fraction

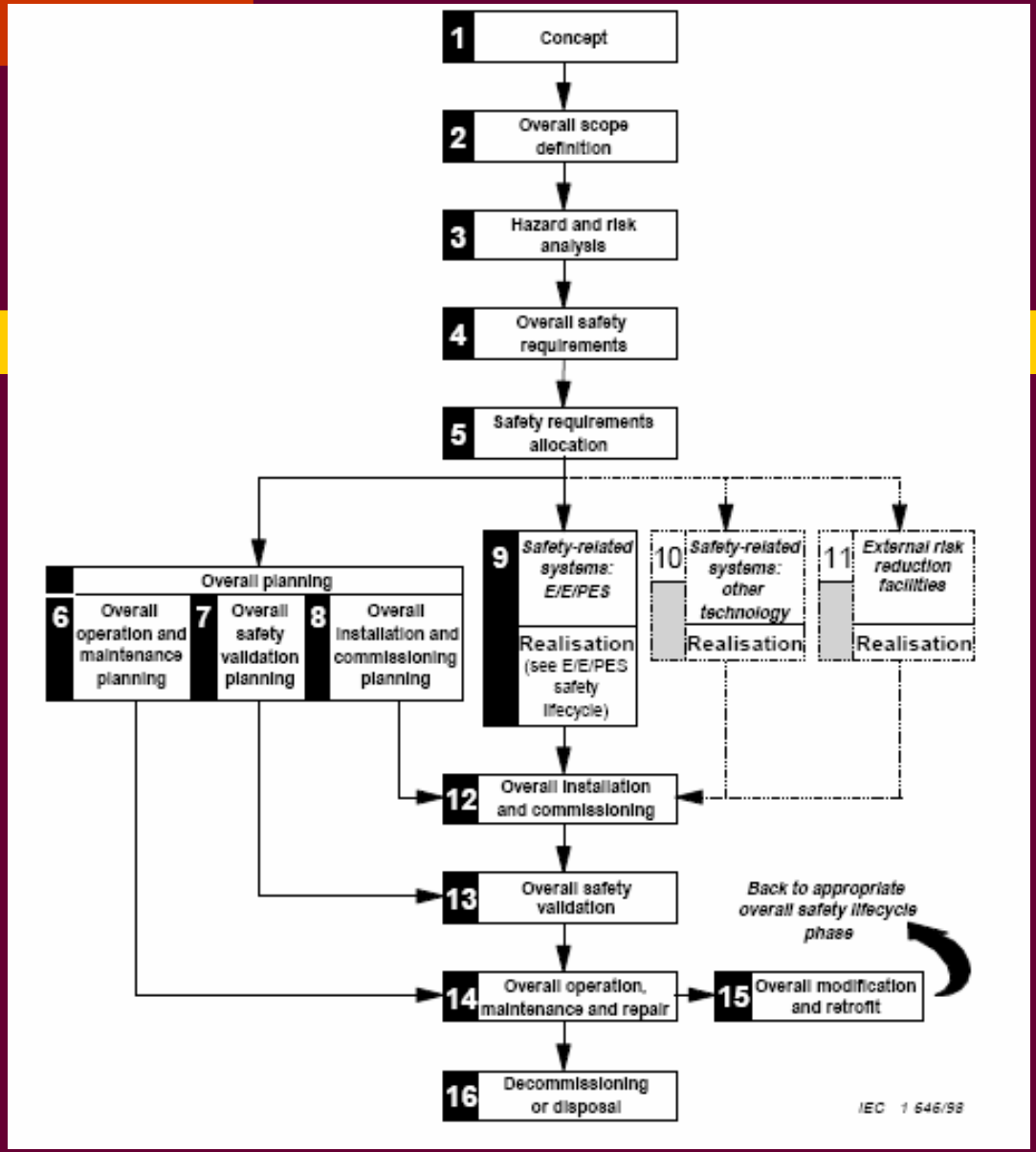
Component	See table(s)	Requirements for diagnostic coverage or safe failure fraction claimed		
		Low (60 %)	Medium (90 %)	High (99 %)
Electromechanical devices	A.2	Does not energize or de-energize	Does not energize or de-energize	Does not energize or de-energize
		Welded contacts	Individual contacts welded	Individual contacts welded No positive guidance of contacts (for relays this failure is not assumed if they are built and tested according to EN 50205 or equivalent)
				No positive opening (for position switches this failure is not assumed if they are built and tested according to EN 60947-5-1, or equivalent)
Discrete hardware	A.3, A.7, A.9, A.11			
Digital I/O		Stuck-at	DC fault model	DC fault model drift and oscillation
Analogue I/O		Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation
Power supply		Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation
Bus	A.3			
General	A.7	Stuck-at of the addresses	Time out	Time out
Memory management unit	A.8	Stuck-at of data or addresses	Wrong address decoding	Wrong address decoding
Direct memory access		No or continuous access	DC fault model for data and addresses	All faults which affect data in the memory
			Wrong access time	Wrong data or addresses
				Wrong access time
Bus-arbitration (see note 1)		Stuck-at of arbitration signals	No or continuous arbitration	No or continuous or wrong arbitration

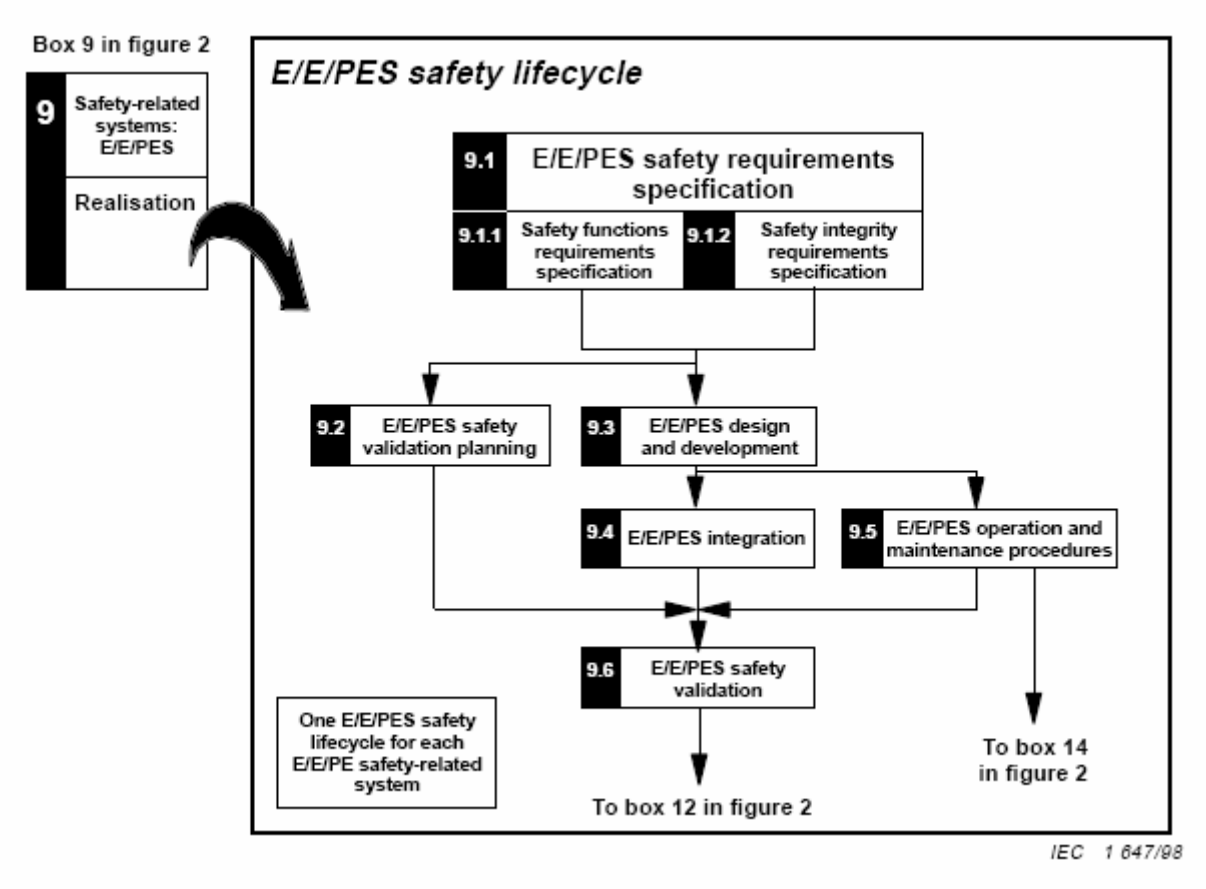
THR követelmények teljesülésének igazolása - FTA

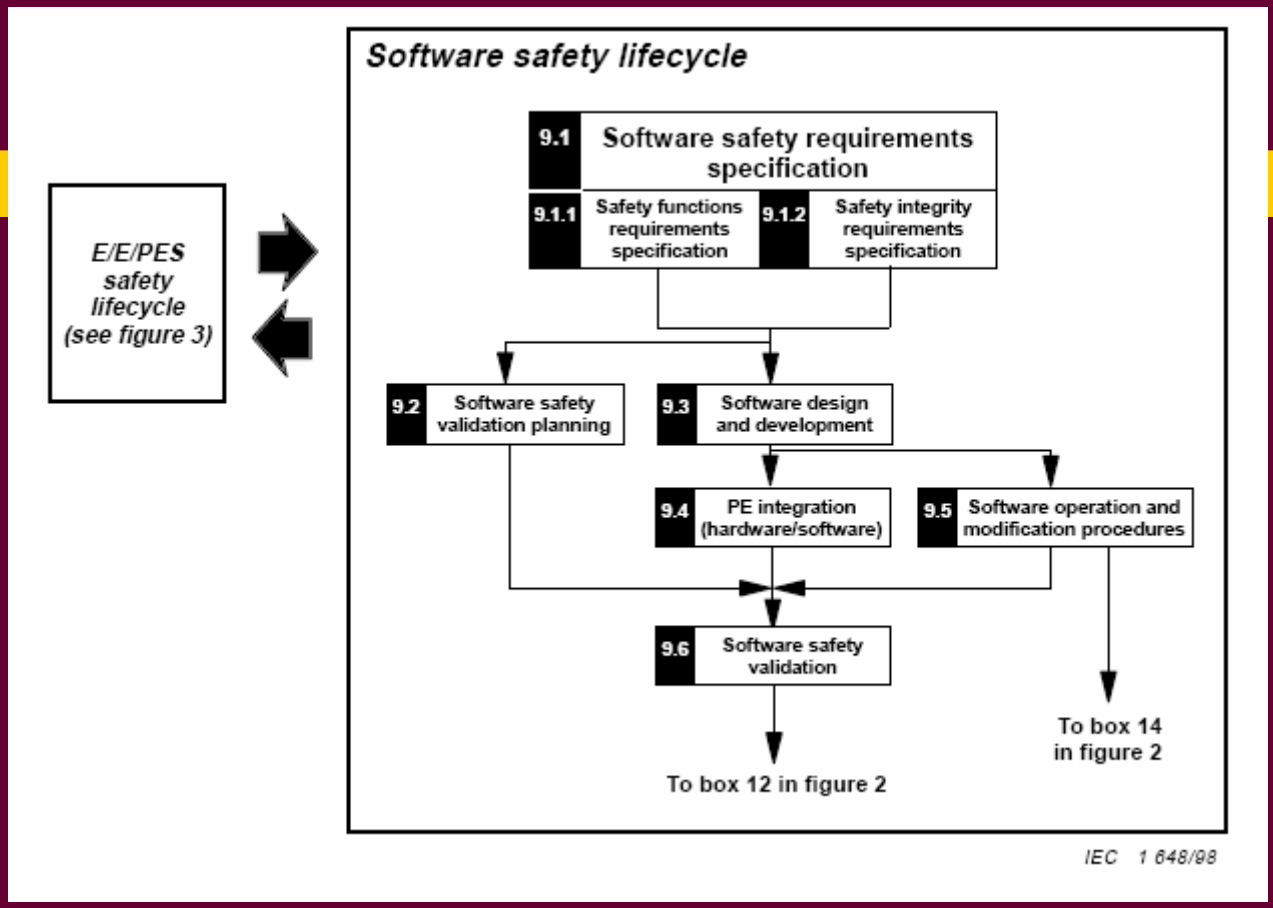
- Rendszermodell, modell-elemek (csúcsesemény, alapesemény, közbenső esemény)
- Számítási típusok (MCS, csúcsesemény P, időfüggő vizsgálatok, érzékenységvizsgálatok)

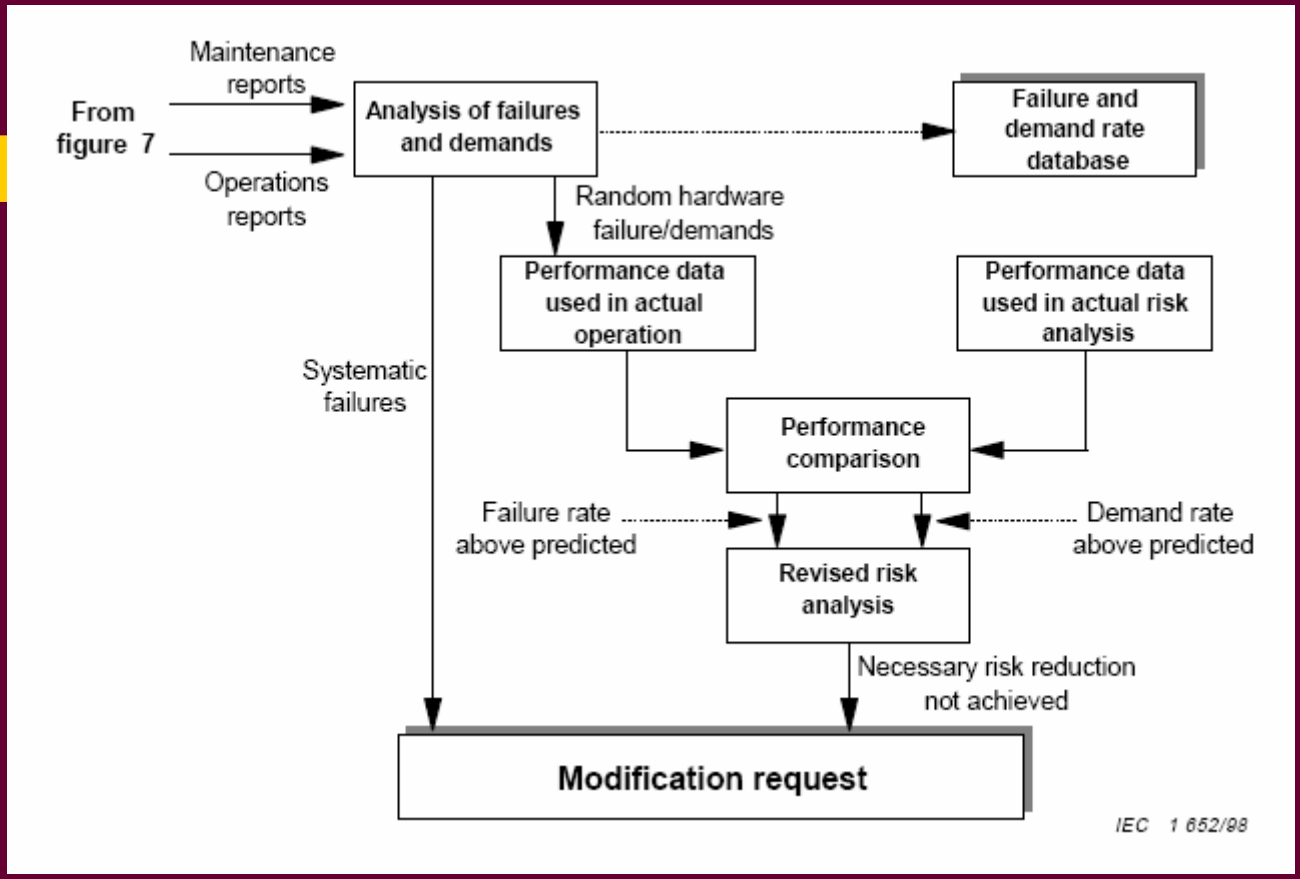
SIL követelmények

- Dokumentáció,
- Biztonsági életciklus követelmények (felelősségek, kompetencia, függetlenségek),
- Életciklus,
- Módszerek és eljárások.


1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety-related systems: E/E/PES
Realisation (see E/E/PES safety lifecycle)
10 Safety-related systems: other technology
Realisation
11 External risk reduction facilities
Realisation
12 Overall installation and commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
16 Decommissioning or disposal
IEC 1 646/98


Box 9 in figure 2
9
Safety-related systems: E/E/PES
Realisation
E/E/PES safety lifecycle
9.1
E/E/PES safety requirements specification
9.1.1
Safety functions requirements specification
9.1.2
Safety integrity requirements specification
9.2
E/E/PES safety validation planning
9.3
E/E/PES design and development
9.4
E/E/PES integration
9.5
E/E/PES operation and maintenance procedures
9.6
E/E/PES safety validation
One E/E/PES safety lifecycle for each E/E/PE safety-related system
To box 12 in figure 2
To box 14 in figure 2
IEC 1 647/98


E/E/PES safety lifecycle (see figure 3)
Software safety lifecycle
9.1 Software safety requirements specification
9.1.1 Safety functions requirements specification
9.1.2 Safety integrity requirements specification
9.2 Software safety validation planning
9.3 Software design and development
9.4 PE integration (hardware/software)
9.5 Software operation and modification procedures
9.6 Software safety validation
To box 12 in figure 2
To box 14 in figure 2
IEC 1 648/98


Maintenance reports
From figure 7
Operations reports
Analysis of failures and demands
Failure and demand rate database
Random hardware failure/demands
Performance data used in actual operation
Performance data used in actual risk analysis
Systematic failures
Performance comparison
Failure rate above predicted
Demand rate above predicted
Revised risk analysis
Necessary risk reduction not achieved
Modification request
IEC 1 652/98

SIL követelmények teljesülésének igazolása: Biztonságértékelés (Functional Safety Assessment)

- Cél: az elért biztonsági szint vizsgálata és döntés a megfelelőségről.
  - Egy vagy több személy,
  - Minden információhoz és résztvevőhöz hozzáfér,
  - Minden fázisra,
  - Terv alapján
  - Megfelelő függetlenséggel.

Table 4 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phases 1 to 8 and 12 to 16 inclusive (see figure 2))

Minimum level of independence	Consequence (see note 2)			
	A	B	C	D
Independent person	HR	HR[1]	NR	NR
Independent department	–	HR[2]	HR[1]	NR
Independent organization (see note 2 of 8.2.12)	–	–	HR[2]	HR
NOTE 1 – See 8.2.12 (including notes) and 8.2.13 for details on interpreting this table.				
NOTE 2 – Typical consequences could be: consequence A – minor injury (for example temporary loss of function); consequence B – serious permanent injury to one or more persons, death to one person; consequence C – death to several people; consequence D – very many people killed.				

Table 5 – Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phase 9, including all phases of E/E/PES and software safety lifecycles (see figures 2, 3 and 4))

Minimum level of Independence	Safety integrity level			
	1	2	3	4
Independent person	HR	HR[1]	NR	NR
Independent department	–	HR[2]	HR[1]	NR
Independent organization (see note 2 of 8.2.12)	–	–	HR[2]	HR
NOTE – See 8.2.12 (including notes), 8.2.13 and 8.2.14 for details on interpreting this table.				

Módszerek és eljárások

- Nem feltétlenül kötelező az alkalmazásuk
  - HR, R, NR
  - Low, medium, high, mandatory
- A megfelelőségről a biztonságértékelő dönt

Módszerek és eljárások (2)

Table B.1 – Recommendations to avoid mistakes during specification of E/E/PES requirements (see 7.2)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Separation of E/E/PE safety-related systems from non-safety-related systems	B.1.3	HR low	HR low	HR medium	HR high
	Structured specification	B.2.1	HR low	HR low	HR medium	HR high
	Inspection of the specification	B.2.6	– low	HR low	HR medium	HR high
	Semi-formal methods	B.2.3, see also table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
	Checklists	B.2.5	R low	R low	R medium	R high
	Computer aided specification tools	B.2.4	– low	R low	R medium	R high
	Formal methods	B.2.2	– low	– low	R medium	R high
All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required.						

Módszerek és eljárások (3)

Table B.2 – Recommendations to avoid introducing faults during E/E/PES design and development (see 7.4)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Observance of guidelines and standards	B.3.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Structured design	B.3.2	HR low	HR low	HR medium	HR high
	Modularisation	B.3.4	HR low	HR low	HR medium	HR high
	Use of well-tried components	B.3.3	R low	R low	R medium	R high
	Semi-formal methods	B.2.3, see also table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
	Checklists	B.2.5	– low	R low	R medium	R high
	Computer-aided design tools	B.3.5	– low	R low	R medium	R high
	Simulation	B.3.6	– low	R low	R medium	R high
	Inspection of the hardware or walk-through of the hardware	B.3.7 B.3.8	– low	R low	R medium	R high
	Formal methods	B.2.2	– low	– low	R medium	R high

All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required.

Módszerek és eljárások (4)

Table B.3 – Recommendations to avoid faults during E/E/PES integration (see 7.5)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Functional testing	B.5.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Black-box testing	B.5.2	R low	R low	R medium	R high
	Field experience	B.5.4	R low	R low	R medium	R high
	Statistical testing	B.5.3	– low	– low	R medium	R high
All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required.						

Módszerek és eljárások (5)

Table B.4 – Recommendations to avoid faults and failures during E/E/PES operation and maintenance procedures (see 7.6)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Operation and maintenance instructions	B.4.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	User friendliness	B.4.2	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Maintenance friendliness	B.4.3	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Limited operation possibilities	B.4.4	– low	R low	HR medium	HR high
	Protection against operator mistakes	B.4.6	– low	R low	HR medium	HR high
	Operation only by skilled operators	B.4.5	– low	R low	R medium	HR high
All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required.						

Módszerek és eljárások (6)

Table B.5 – Recommendations to avoid faults during E/E/PES safety validation (see 7.7)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Functional testing	B.5.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Functional testing under environmental conditions	B.6.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Interference surge immunity testing	B.6.2	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Fault insertion testing (when required diagnostic coverage ≥ 90 %)	B.6.10	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Static analysis, dynamic analysis and failure analysis	B.6.4 B.6.5 B.6.6	– low	R low	R medium	R high
	Simulation and failure analysis	B.3.6 B.6.6	– low	R low	R medium	R high
	"Worst-case" analysis, dynamic analysis and failure analysis	B.6.7 B.6.5 B.6.6	– low	– low	R medium	R high
	Static analysis and failure analysis (see note 4)	B.6.4 B.6.6	R low	R low	NR	NR
	Expanded functional testing	B.6.8	– low	HR low	HR medium	HR high
	Black-box testing	B.5.2	R low	R low	R medium	R high
	Fault insertion testing (when required diagnostic coverage < 90 %)	B.6.10	R low	R low	R medium	R high
	Statistical testing	B.5.3	– low	– low	R medium	R high
	"Worst-case" testing	B.6.9	– low	– low	R medium	R high
	Field experience	B.5.4	R low	R low	R medium	NR

This table is divided into three groups, as indicated by the sidebar shading. All techniques marked "R" in the grey and black shaded groups are replaceable by other techniques within that group, but at least one of the techniques of the grey shaded group (analytical techniques) and at least one of the techniques of the black shaded group (testing techniques) is required.

Módszerek és eljárások - hatékonyság

Table B.6 – Effectiveness of techniques and measures to avoid systematic failures

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Project management (see note)	B.1.1	Definition of actions and responsibilities; scheduling and resource allocation; training of relevant personnel; consistency checks after modifications	Validation independent from design; project monitoring; standardised validation procedure; configuration management; failure statistics; computer aided engineering; computer-aided software engineering
Documentation (see note)	B.1.2	Graphical and natural language descriptions, for example block-diagrams, flow-diagrams	Guidelines for consistent content and layout across organization; contents checklists; computer-aided documentation management, formal change control
Separation of E/E/PE safety-related systems from non safety-related systems	B.1.3	Well-defined interfaces between E/E/PE safety-related systems and non-safety-related systems	Total separation of E/E/PE safety-related systems from non-safety-related systems, i.e. no write access of non-safety-related systems to E/E/PE safety-related systems and separate physical locations to avoid common cause influences
Structured specification	B.2.1	Manual hierarchical separation into subrequirements; description of the interfaces	Hierarchical separation described using computer-aided engineering tools; automatic consistency checks; refinement down to functional level
Formal methods	B.2.2	Used by personnel experienced in formal methods	Used by personnel experienced in formal methods in similar applications, with computer support tools
Semi-formal methods	B.2.3	Describing some critical parts with semi-formal methods	Describing total E/E/PE safety-related systems with different semi-formal methods to show different aspects; consistency check between the methods
Computer-aided specification tools	B.2.4	Tools without preference for one particular design method	Model-oriented procedures with hierarchical subdivision; description of all objects and their relationships; common data base; automatic consistency checks
Checklists	B.2.5	Prepared checklists for all safety life-cycle phases; concentration	Prepared detailed checklists for all safety life-cycle phases

IEC61511 – folyamatirányítási szektor