SZÉCHENYI ISTVÁN EGYETEM
SZE - GYŐR

Ipari biztonsági rendszerek

Alapok

Ballagi Áron
Automatizálási Tanszék

Biztonsági rendszerek feladata

- Az emberek, a gépek és a környezet védelme
- A munkafolyamatok kockázatának minimalizálása illetve (szabványos) elfogadható szinten tartása

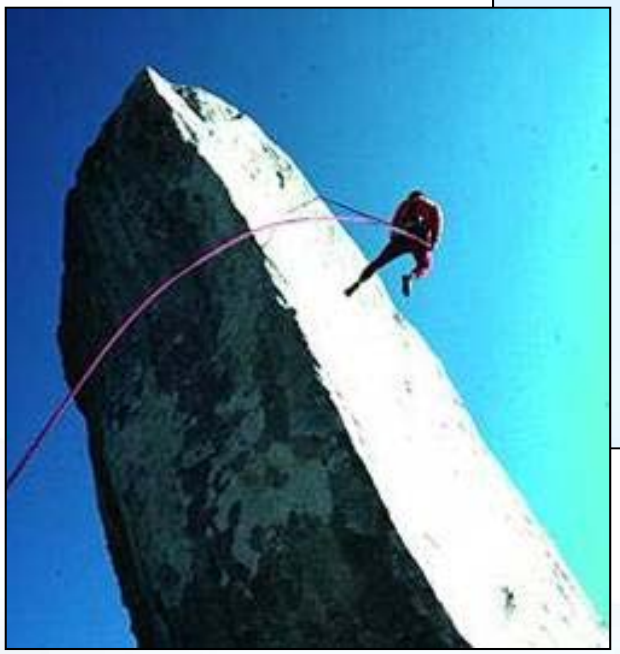
Miért van szükség biztonsági rendszerekre?

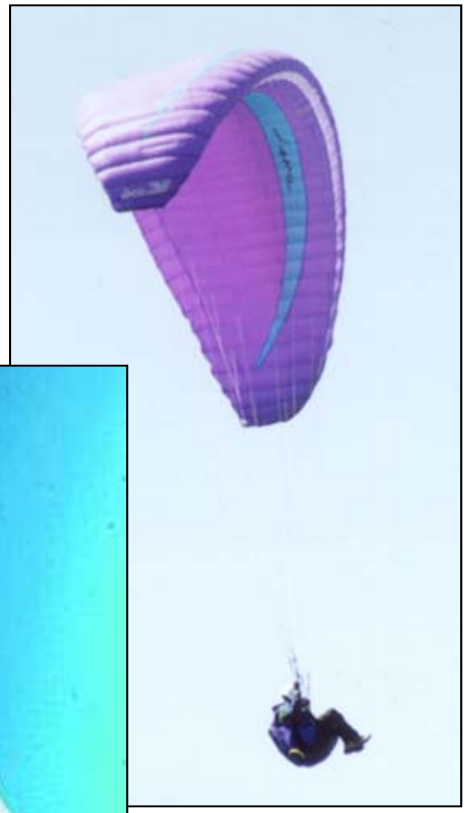
Miért van szükség biztonsági rendszerekre?

Miért van szükség biztonsági rendszerekre?

Elfogadható kockázat

- Kockázat mindig van!

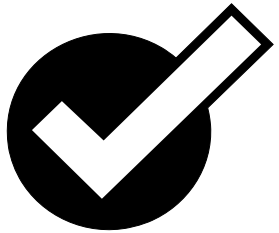




Kockázat - helyfüggő

- Ugyan az a veszélyforrás más-más kockázati szintet jelenthet a földrajzi elhelyezkedés függvényében


+

=


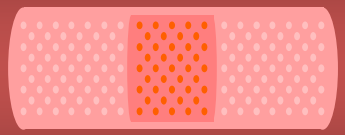
+

=


A kockázat felmérése

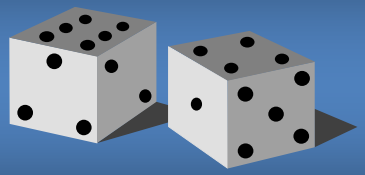
Kockázat

Következmény



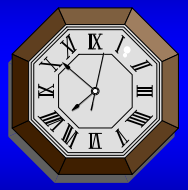
Mekkora bajt okoz?

Esély



Mi a valószínűsége?

Gyakoriság



Milyen gyakran?

Kockázat csökkentés

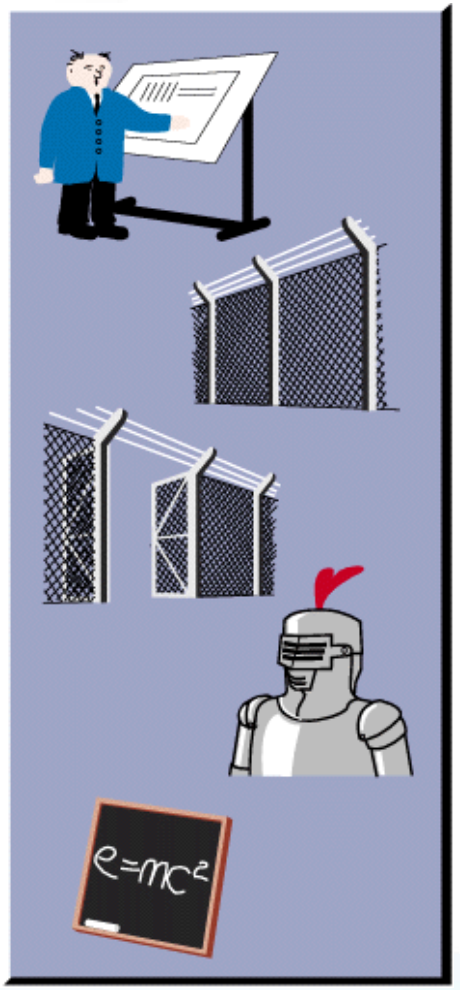
Tervezéssel

Fix mechanikai védelem

Monitorozás és vezérlés

Tréning és felülvizsgálat

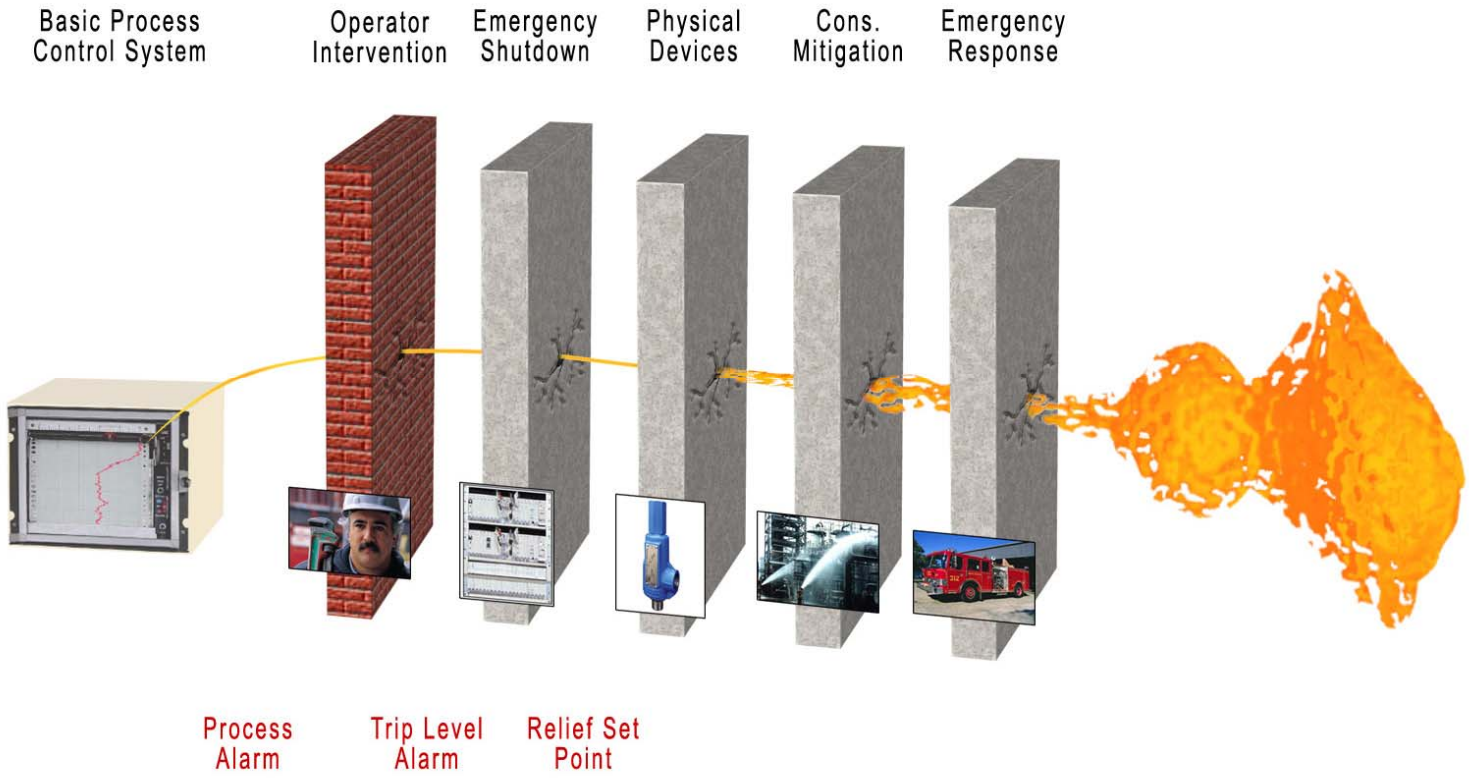
Személyes védőeszközök



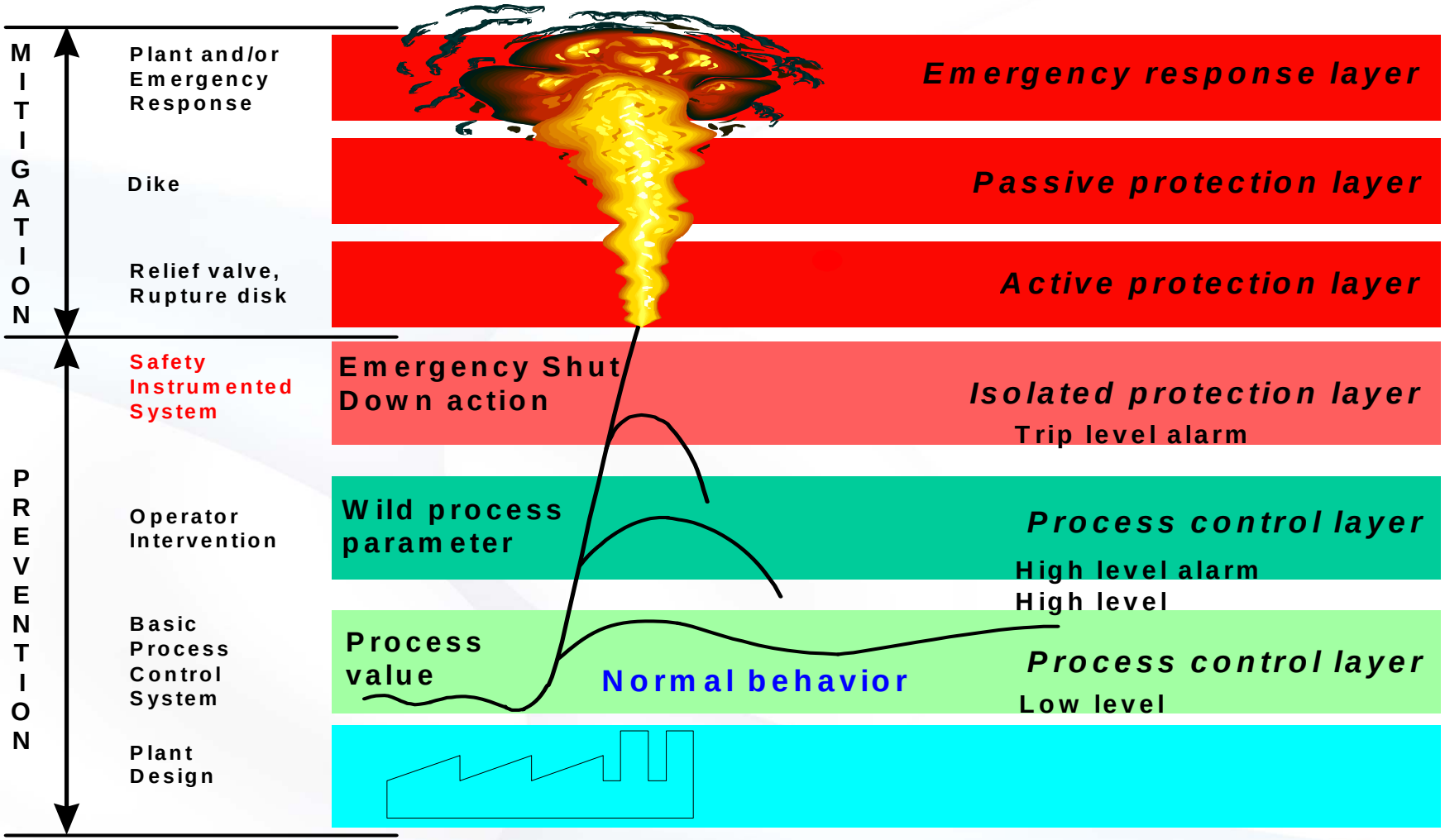
Legjobban preferált

Legkevésbé preferált

Védelmi, biztonsági rétegek



Független védelmi réteg



Szabványok

- Minden biztonsági eszköznek és rendszernek speciális szabványoknak kell megfelelnie
  - EN 954-1 (Safety Categories)
  - IEC 61508 (Safety Integrity Levels for Programmable Safety Systems)
  - EN 1088 (Safety Interlocks)

- Az eszközök professzionális szakértő harmadik fél által minősítettek
  - Pl.: TÜV Rheinland, TÜV Nord and BG

TÜV

www.tuv.com

Szabványok története

1984	TUV Guidelines for PES (SK Safety Classes 1-9)
1987	HSE PES Guidelines Parts 1 & 2
1989	DIN 19250/ VDE 0801 for PES (AK Safety Classes 1 - 8)
1994	Appendix to VDE 0801 - Harmonisation Document
1996	**ISA SP84 - Safety Lifecycle, Quantitative Approach**
1997	IEC 61508 - Safety Lifecycle, Quantitative and Qualitative Approach
2003	**ANSI/ISA 84.01 = IEC61511 - Functional Safety, SIS for the Process industry sector**
2004	DIN 19250 visszavonása és az új Machine Safety Standard IEC 62061megjelenése

Szabványok: Safety Instrumented Systems (SIS)

- Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA 84.01, *Application of Safety Instrumented Systems for the Process Industry*, 1996 (revised 2004).
- International Electrotechnical Commission (IEC), IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Sector

Safety „szavak”

SIS – Safety Instrumented System

SIF – Safety Instrumented Function

SIL – Safety Integrity Level

PFD – Probability of Failure on Demand

PHA – Process Hazard Analysis

LOPA – Layer Of Protection Analysis

SRS – Safety Requirement Specification

PES – Programmable Electronic System

BPCS – Basic Process Control System

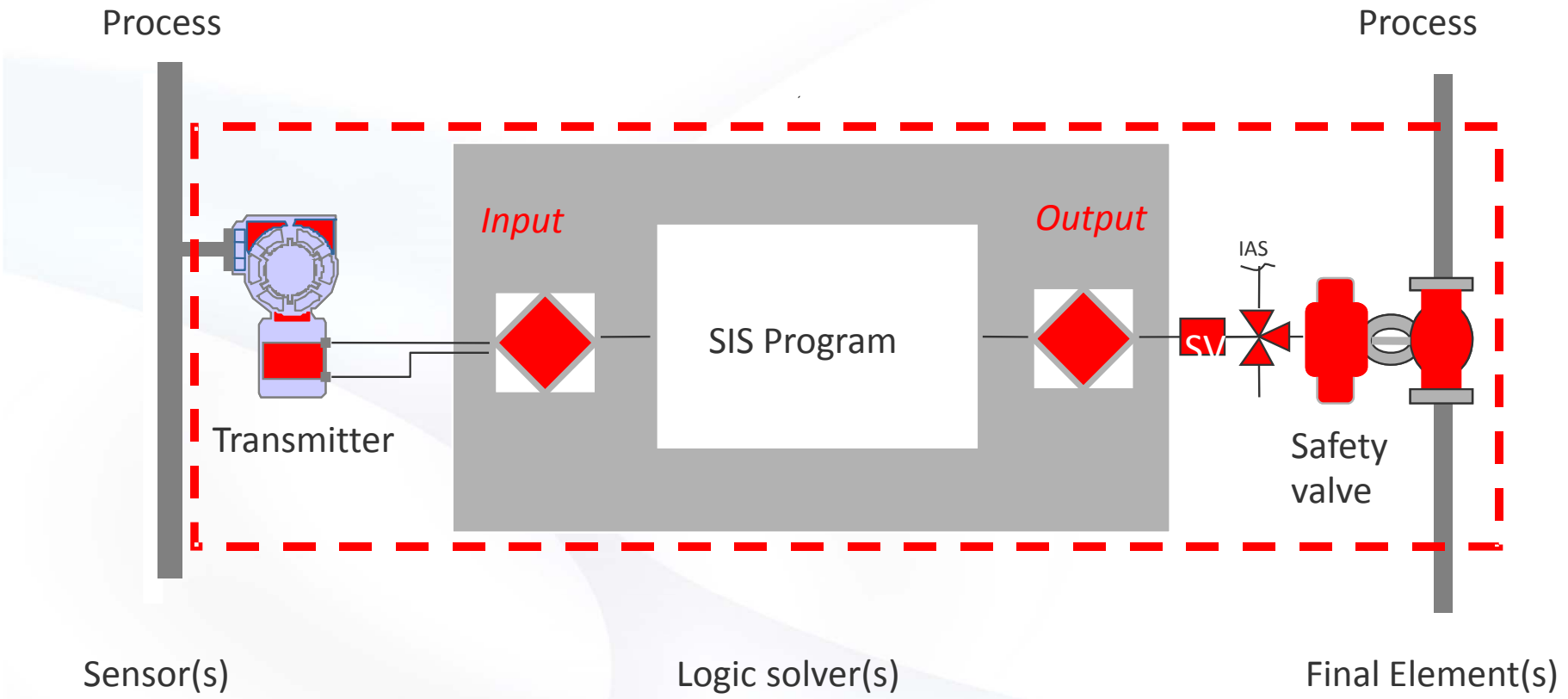
Gyakran használt rövidítések

- ESD (Emergancy Shut Down system) Biztonsági rendszer.
- SIL (Safety Integrity Level) Integrált biztonság szintje.
- SIF (Safety Instrumented Function), Műszerezett Biztonsági függvény
- SIS (Safety Instrumented System) Biztonságosan műszerezett rendszer.
- BPCS (Basic Process Control System), Folyamatirányító rendszer (PLC, DCS).
- MTBF (Mean Time Between Failure), Meghibásodások közti átlagos idő.
- MTTF (Mean Time To Failure,)Javításokra fordított átlagos idő.
- PFD (Probability of Failure on Demand), Annak a valószínűsége, hogy a rendszer nem működik, amikor működnie kellene, évre vetítve
- PFH (Probability of Failure on Hour). Annak a valószínűsége, hogy a rendszer nem működik, amikor működnie kellene, órára vetítve.
- LOPA (Layer of Protection Analysis), Biztonsági rétegek elemzése
- HAZOP (Hazard and Operation Analysis), Hazárd helyzetek és a működtetések elemzése.

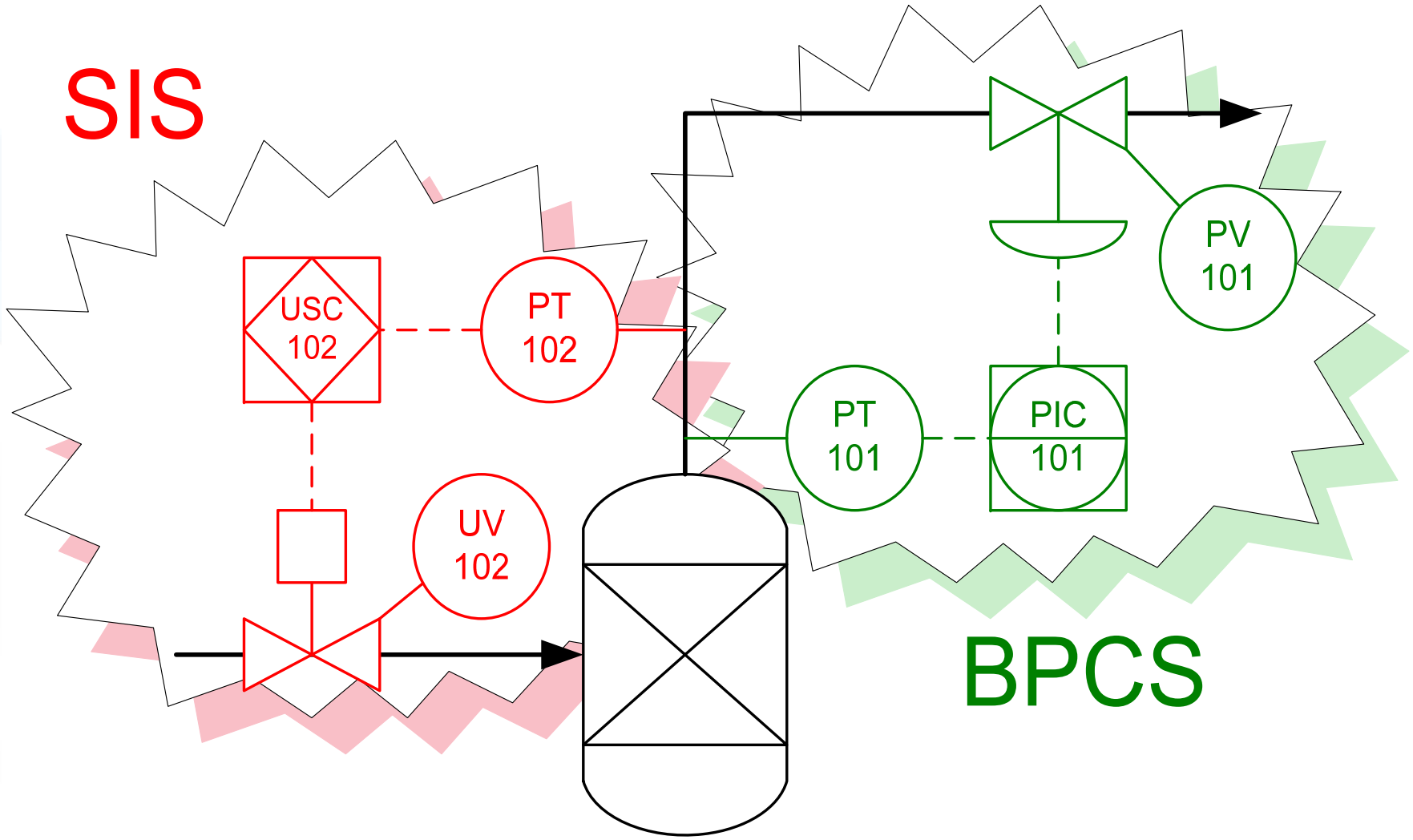
Mi az a SIS

- Formális definíció:
  - SIS – "olyan műszerezett rendszer, mely egy vagy több műszerezett biztonsági függvényt (SIF) implementál. A SIS, szenzorok, logikai egységek és végrehajtó elemek kombinációjából épül fel." (IEC 61511 / ISA 84.01)
- Informális definíció:
  - Olyan műszerezett vezérlő rendszer, mely felismeri az „felügyelet alól kilépő rendszert" és automatikusan valamilyen biztonságos állapotba hozza azt
  - „A védelem utolsó vonala"
  - Nem BPCS (alap folyamatirányítási rendszer)

Miből áll egy SIS rendszer?



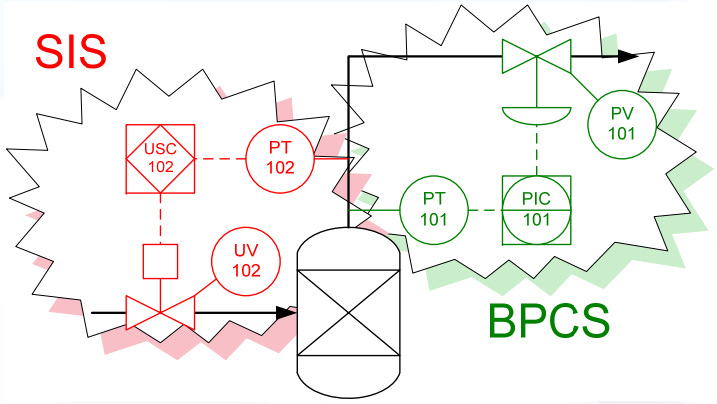
Mi a különbség a SIS és a BPCS között?



Hol használunk SIS-t?

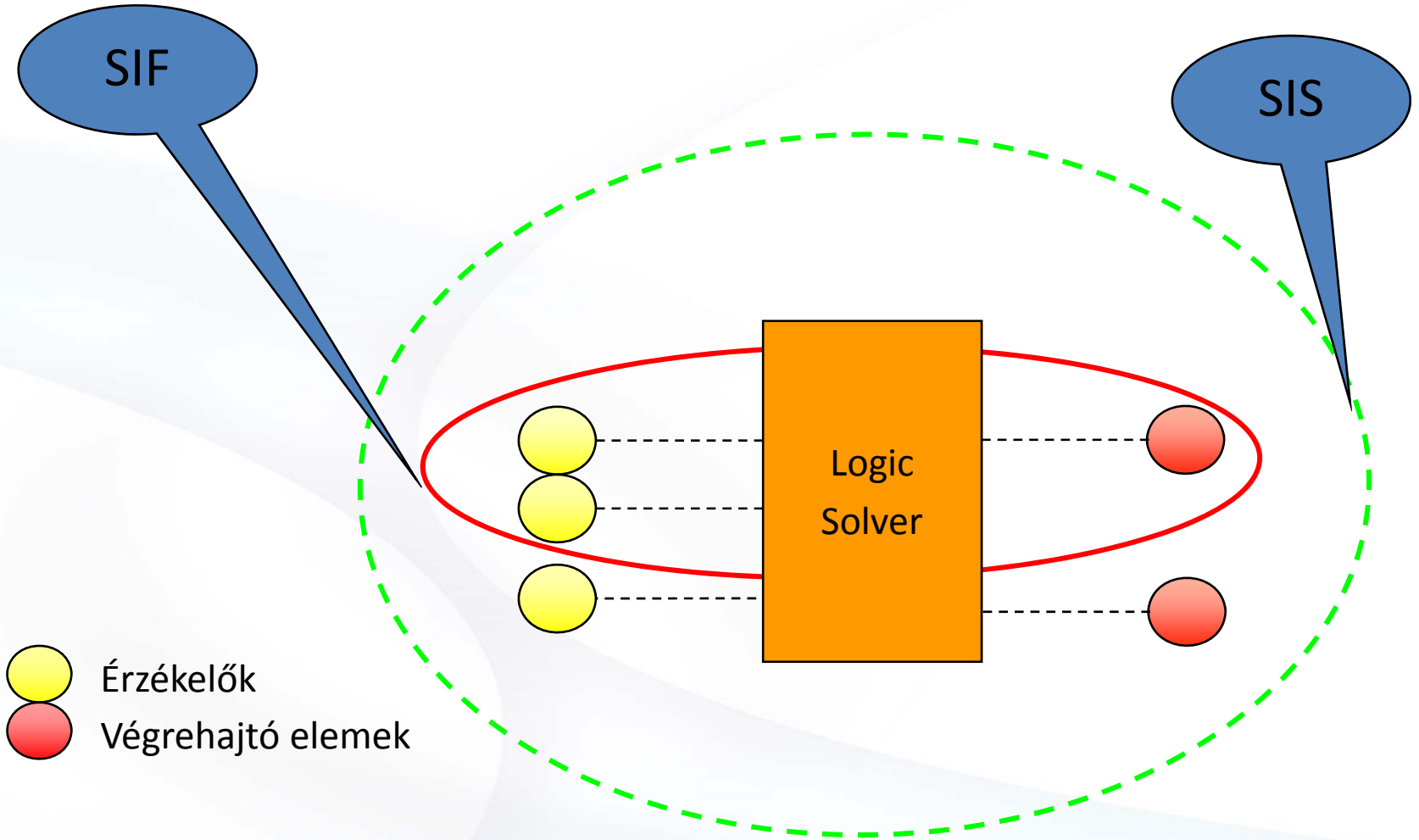
- Tipikus SIS alkalmazások:
  - ESD: **E**mergency **S**hut **D**own System
  - F&G: **F**ire and **G**as System
  - BMS: **B**urner **M**anagement **S**ystem
  - TMC: **T**urbo **M**achinery **C**ontrol System
  - HIPPS: **H**igh **I**ntegrity **P**ressure **P**rotection **S**ystem
  - WHCP: **W**ell **H**ead **C**ontrol **P**anel

Safety Instrumented Function (Műszerezett Biztonsági függvény)

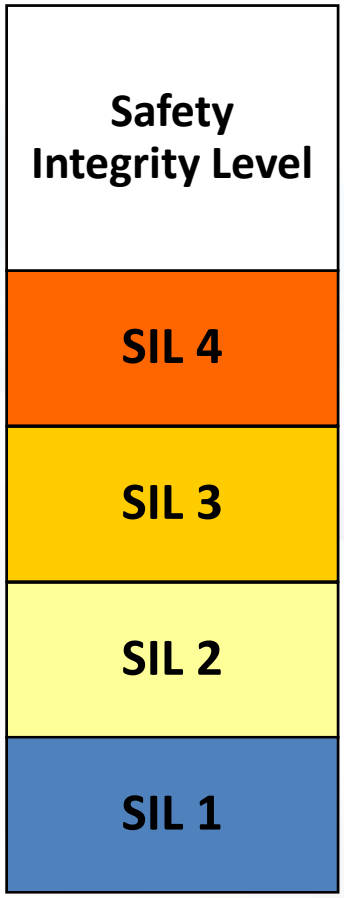


- Formális definíció:
  - SIF – "olyan, a SIS által implementált funkció, mely automatikusan eléri és fenntartja a folyamat biztonságos állapotát figyelembe véve egyes speciális veszélyes eseményeket"(IEC61511 ISA SP 84.01)
- Informális definíció:
  - Független biztonsági kör vagy retesz, mely automatikusan biztonságos állapotba viszi a folyamatot valamely meghatározott esemény hatására

SIS vagy SIF



SIL - Safety Integrity Level (Integrált biztonság szintje)



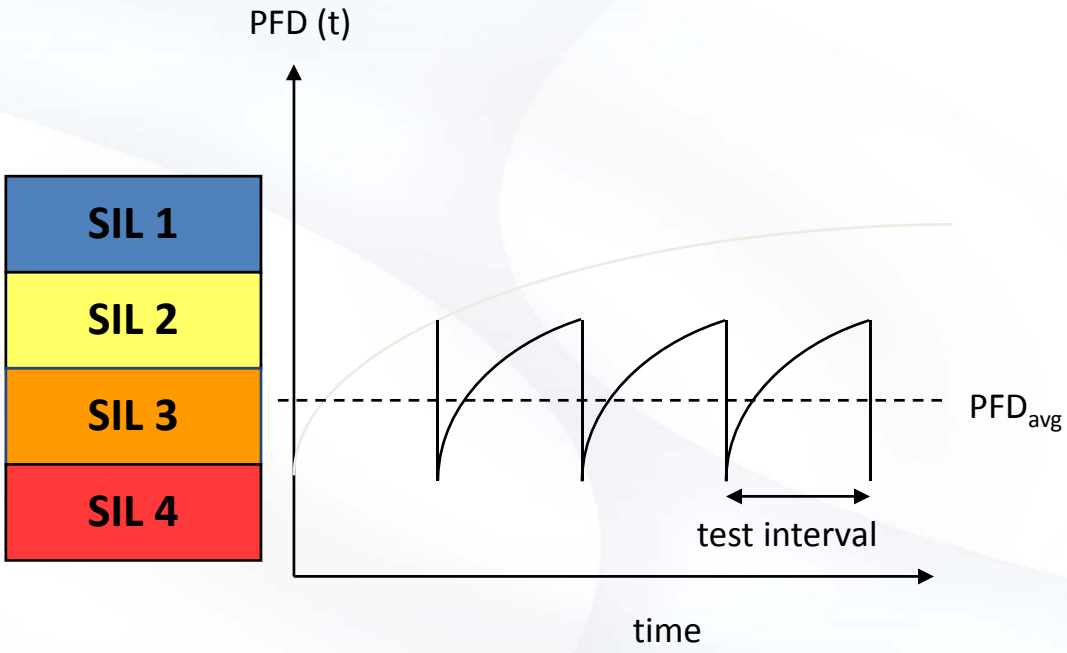
- Informális definíció:
  - SIL ..egy, a SIS által implementált műszerezett biztonsági funkció (SIF)integrált biztonsági szintje (SIL)

  vagy

  - Egy specifikus műszerezett biztonsági funkció által elérhető kockázat csökkentés mértéke

SIL leírása PFD-ként

$$PFD_{avg} = \lambda_{DU} TI / 2$$



PFD:
Probability of Failure on Demand

λ_{DU}:
Dangerous Undetected Failures

TI:
Test Interval (proof)

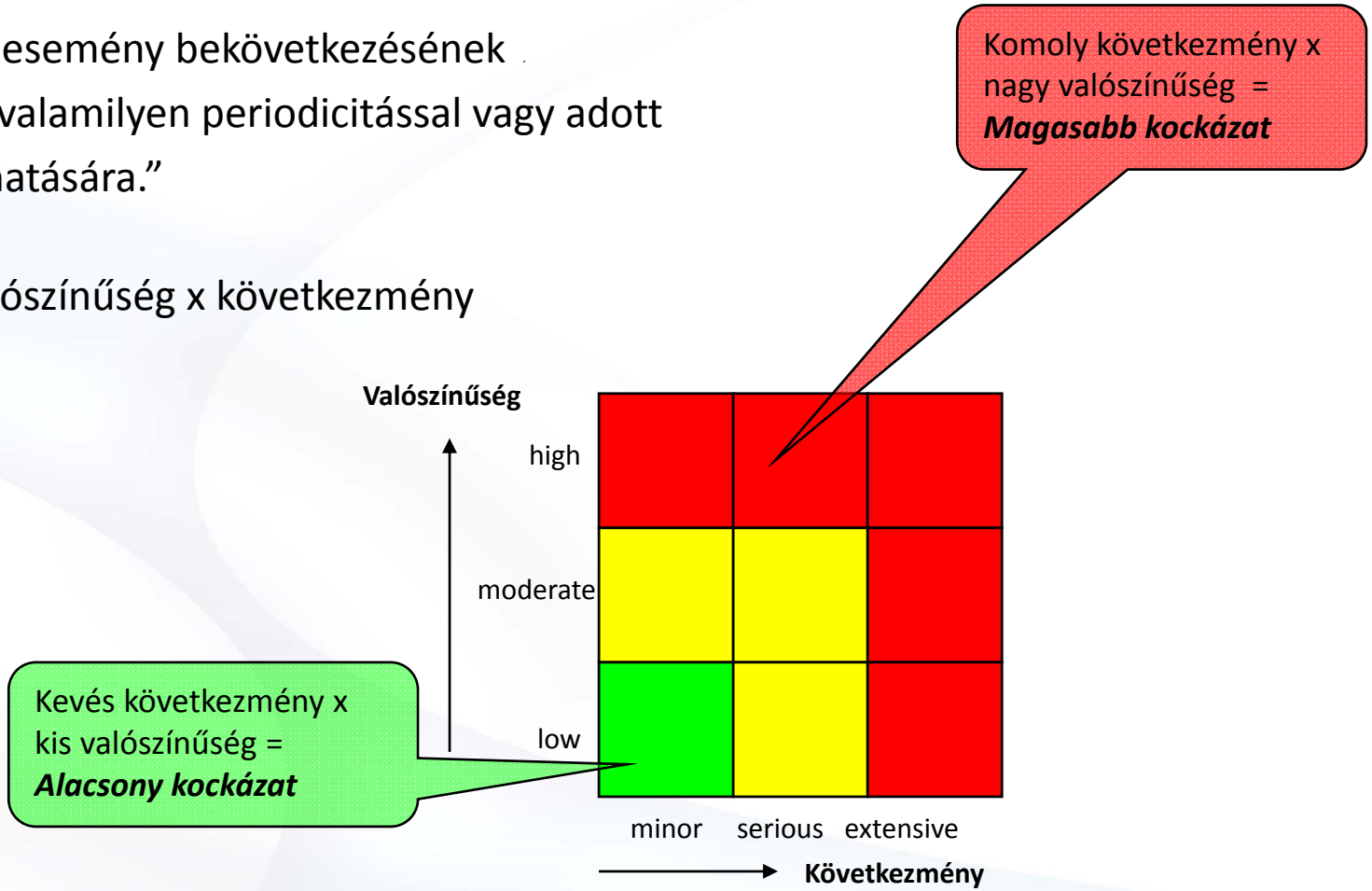
SIL szintek

Safety Integrity Level	Safety	Probability of Failure on Demand	Risk Reduction Factor
SIL 4	> 99.99%	0.001% to 0.01%	100,000 to 10,000
SIL 3	99.9% to 99.99%	0.01% to 0.1%	10,000 to 1,000
SIL 2	99% to 99.9%	0.1% to 1%	1,000 to 100
SIL 1	90% to 99%	1% to 10%	100 to 10

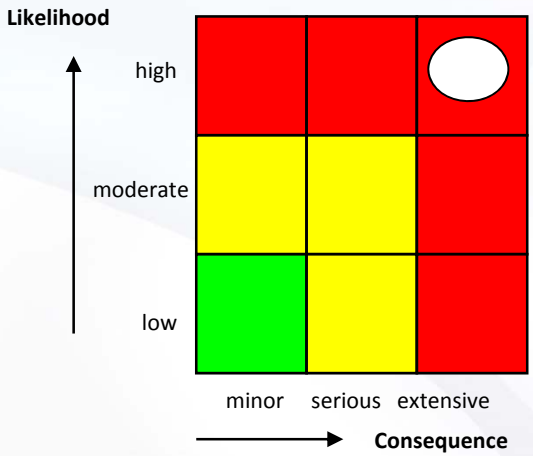
A kockázat

"Egy nem várt esemény bekövetkezésének valószínűsége valamilyen periodicitással vagy adott körülmények hatására."

Kockázat = valószínűség x következmény



A túl nagy kockázatvállalás következményei

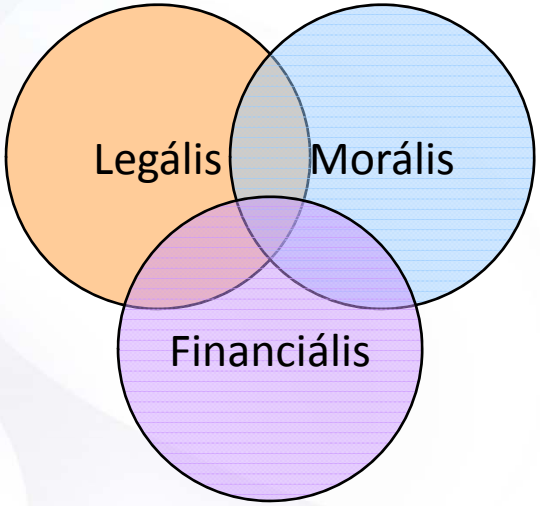


- Személyi sérülés, halál
- Környezet károsítás
- Eszközök megsérülése, megsemmisülése
- Üzleti partnerek elvesztése
- Felelősségre vonás
- Rossz kép a cégről
- Piacvesztés

Elfogadható kockázat

- Törvények, pénzügyi mutatók és a moralitás korlátoz
- A törvényi minimum az OSHA (Occupational Safety and Health Administration - Munkahelyi Biztonság és Egészségvédelem) előirányzat

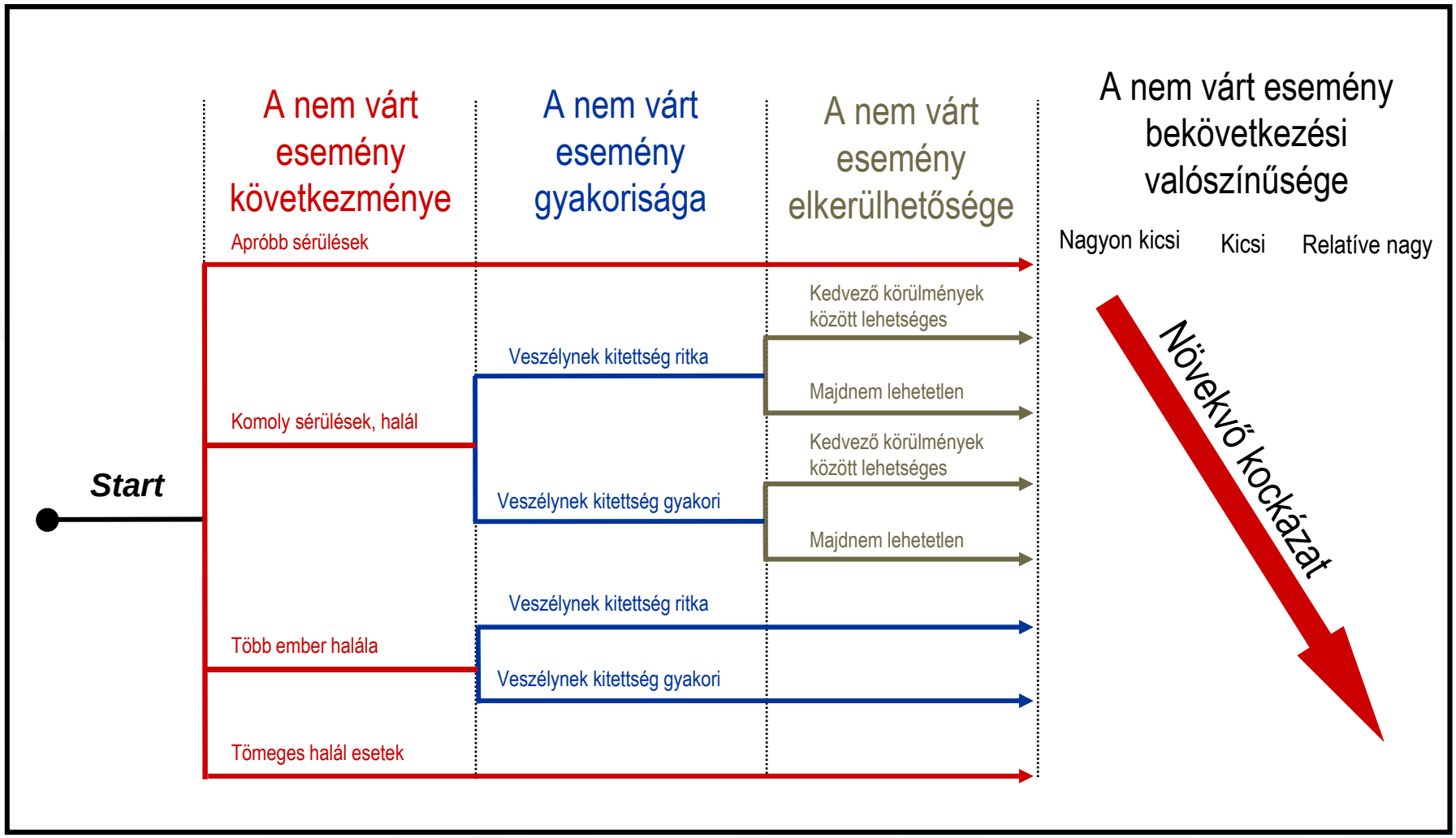
A törvényi előírásoknak megfelelő biztonság



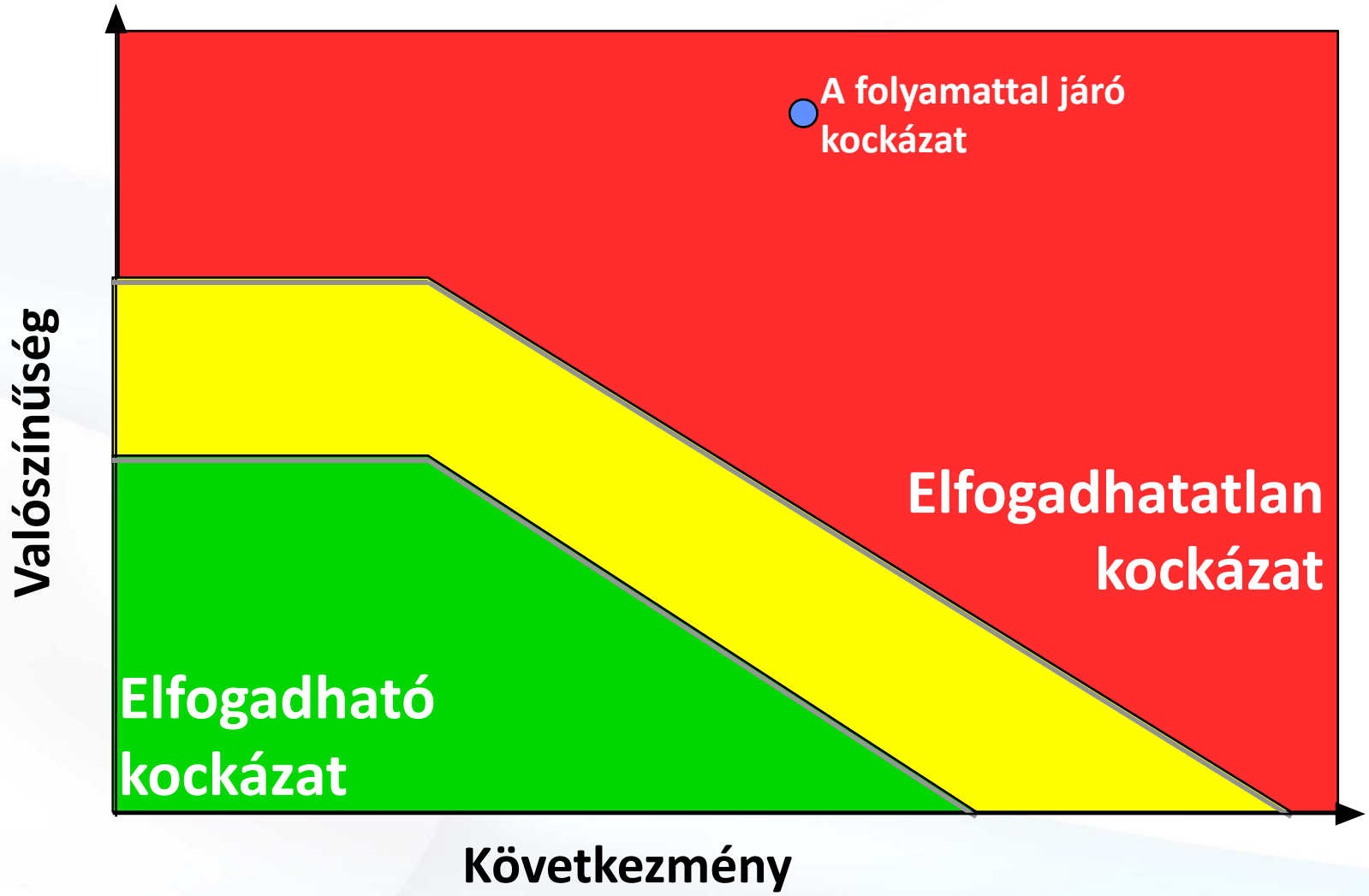
A lehető legbiztonságosabb munkahelyek kialakítása

A legolcsóbb biztonság

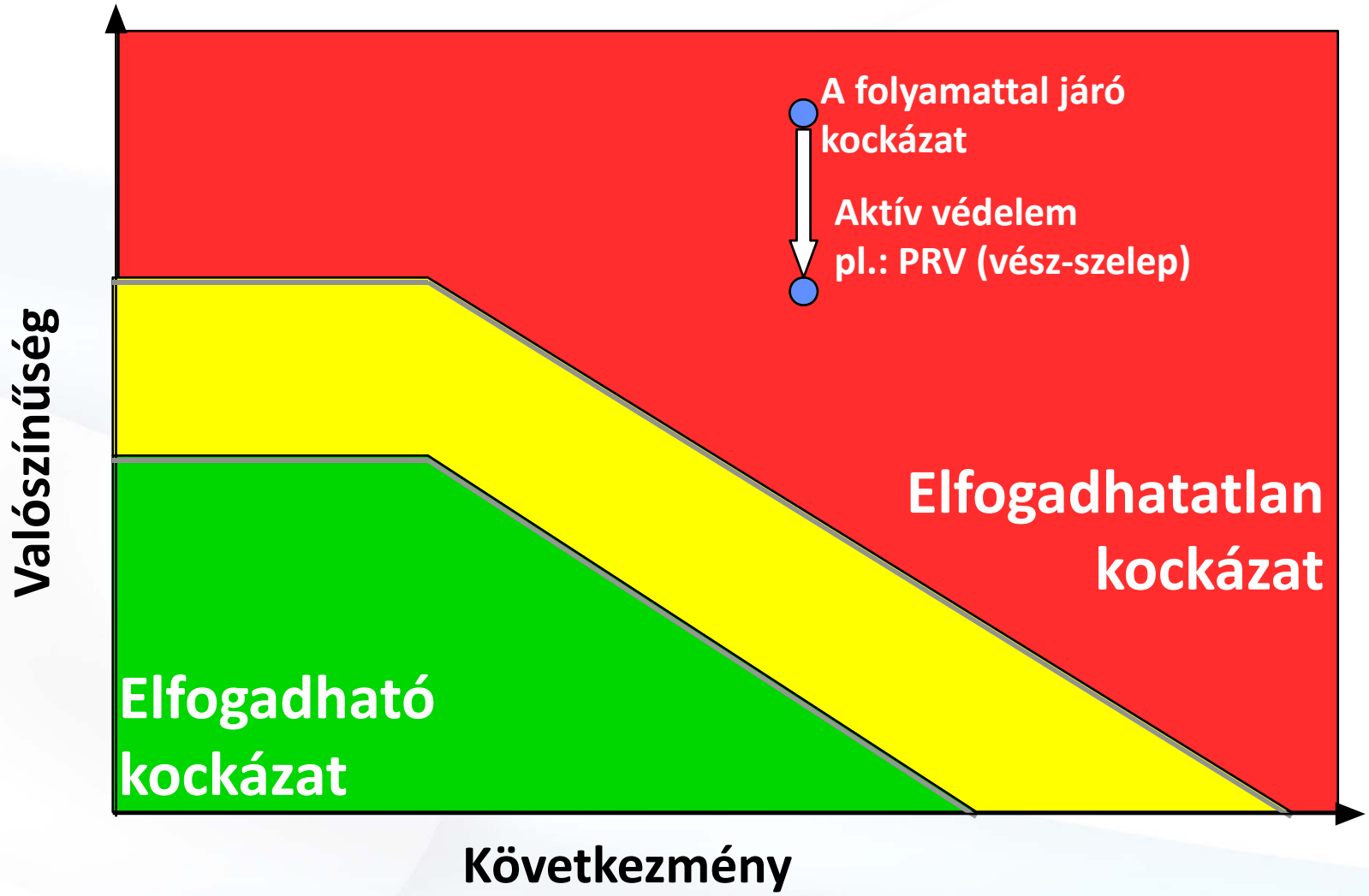
Kockázat elemzés kockázati gráf



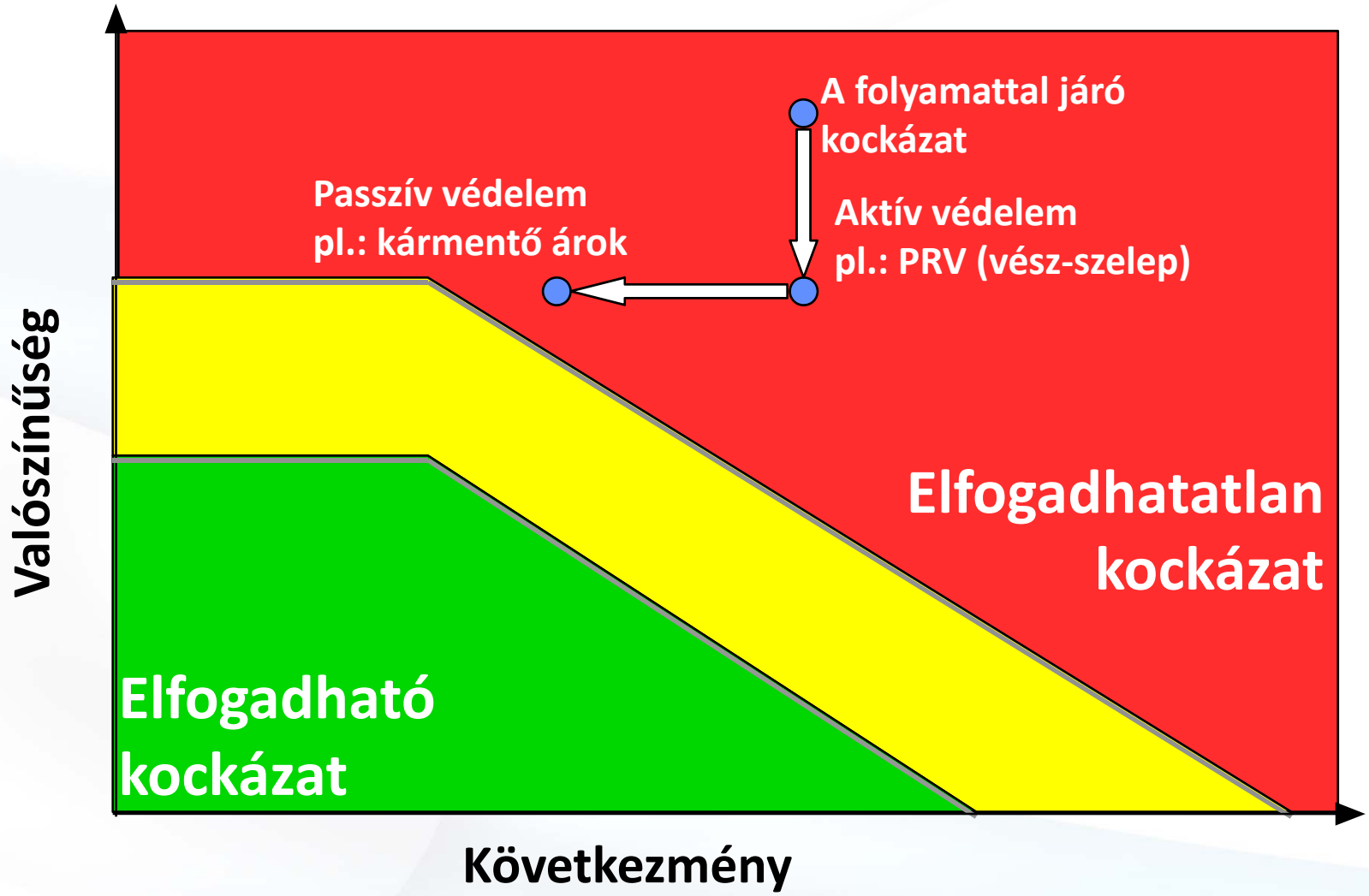
Kockázatok csökkentése



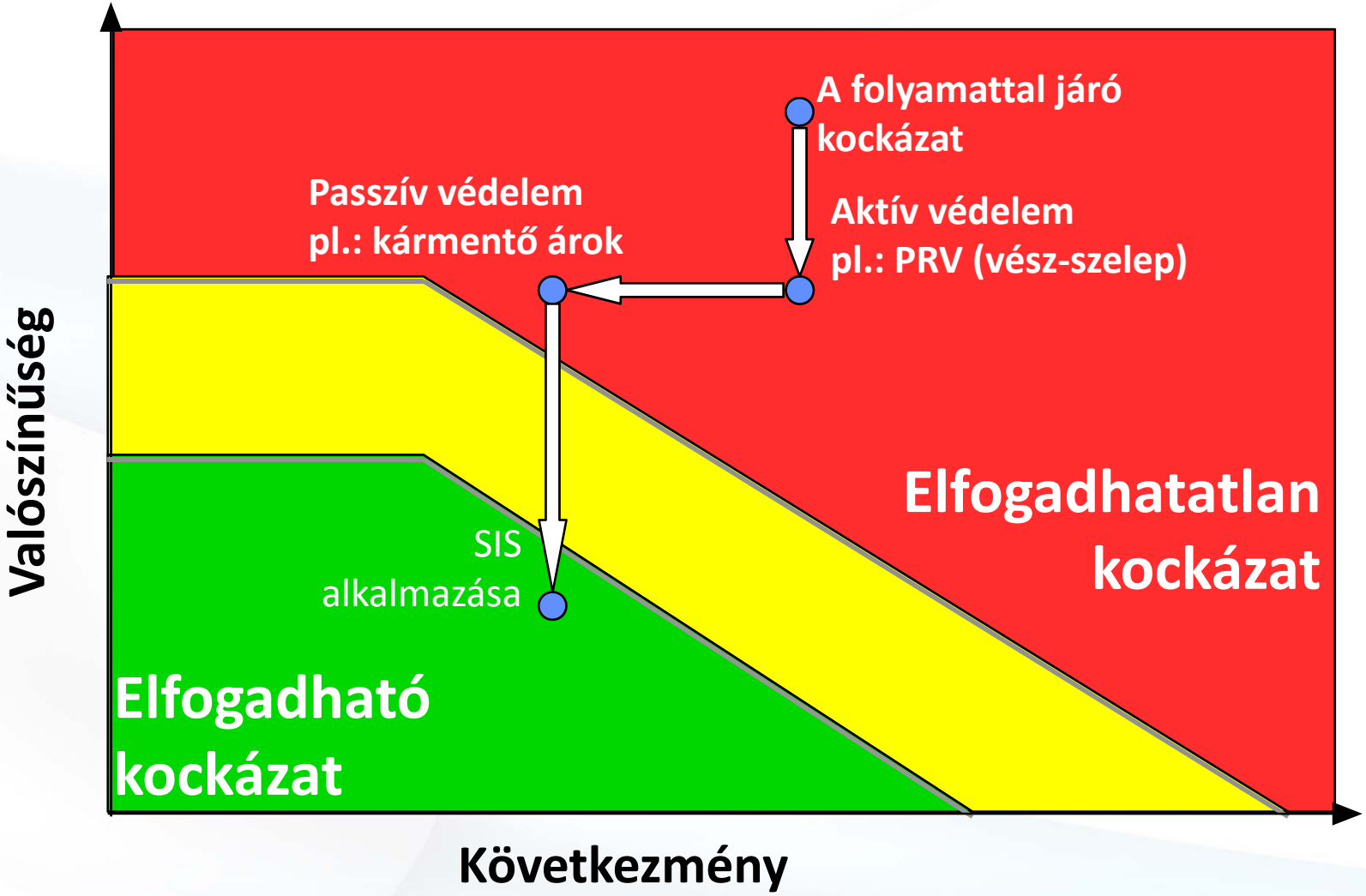
Kockázatok csökkentése



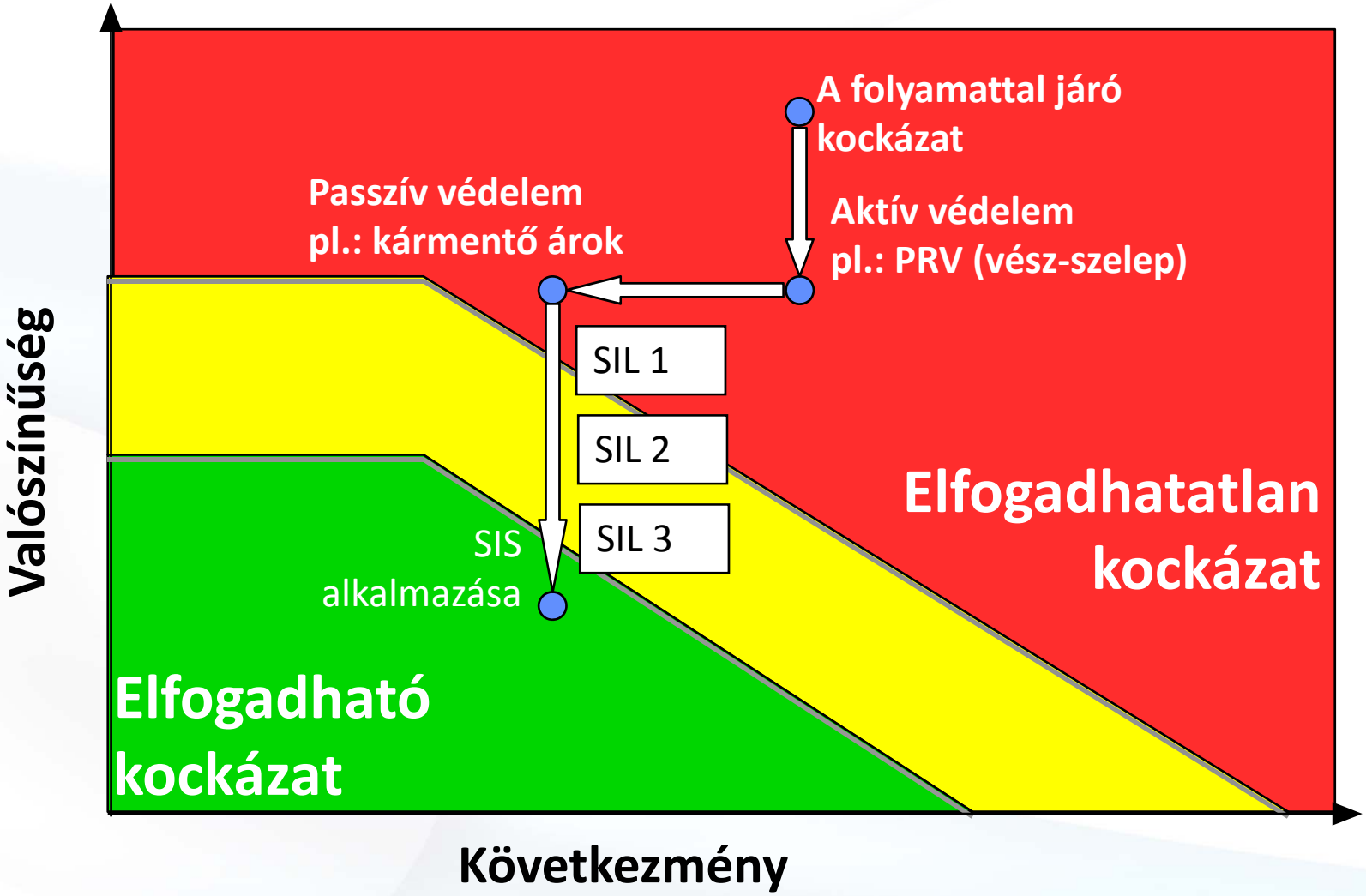
Kockázatok csökkentése



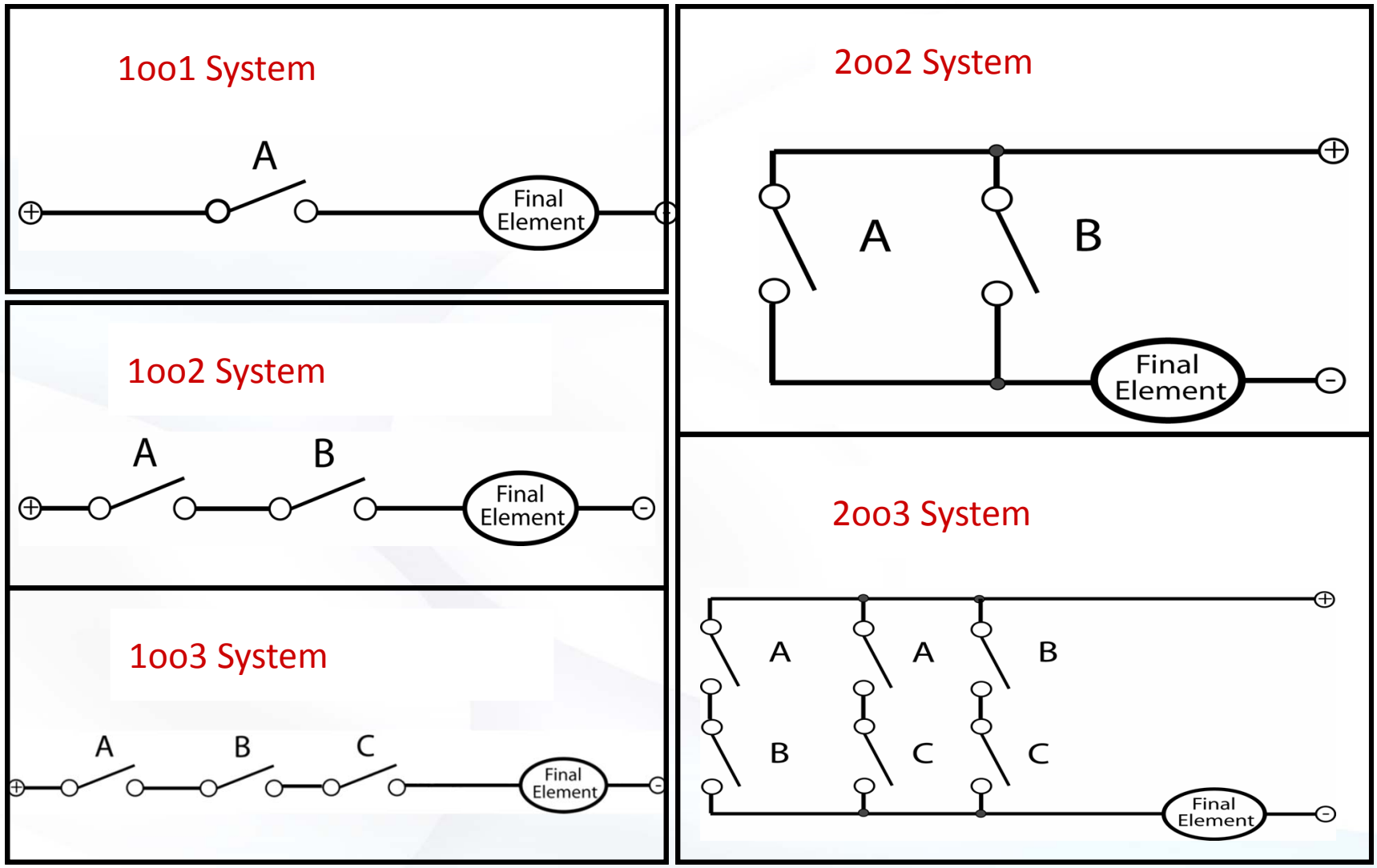
Kockázatok csökkentése



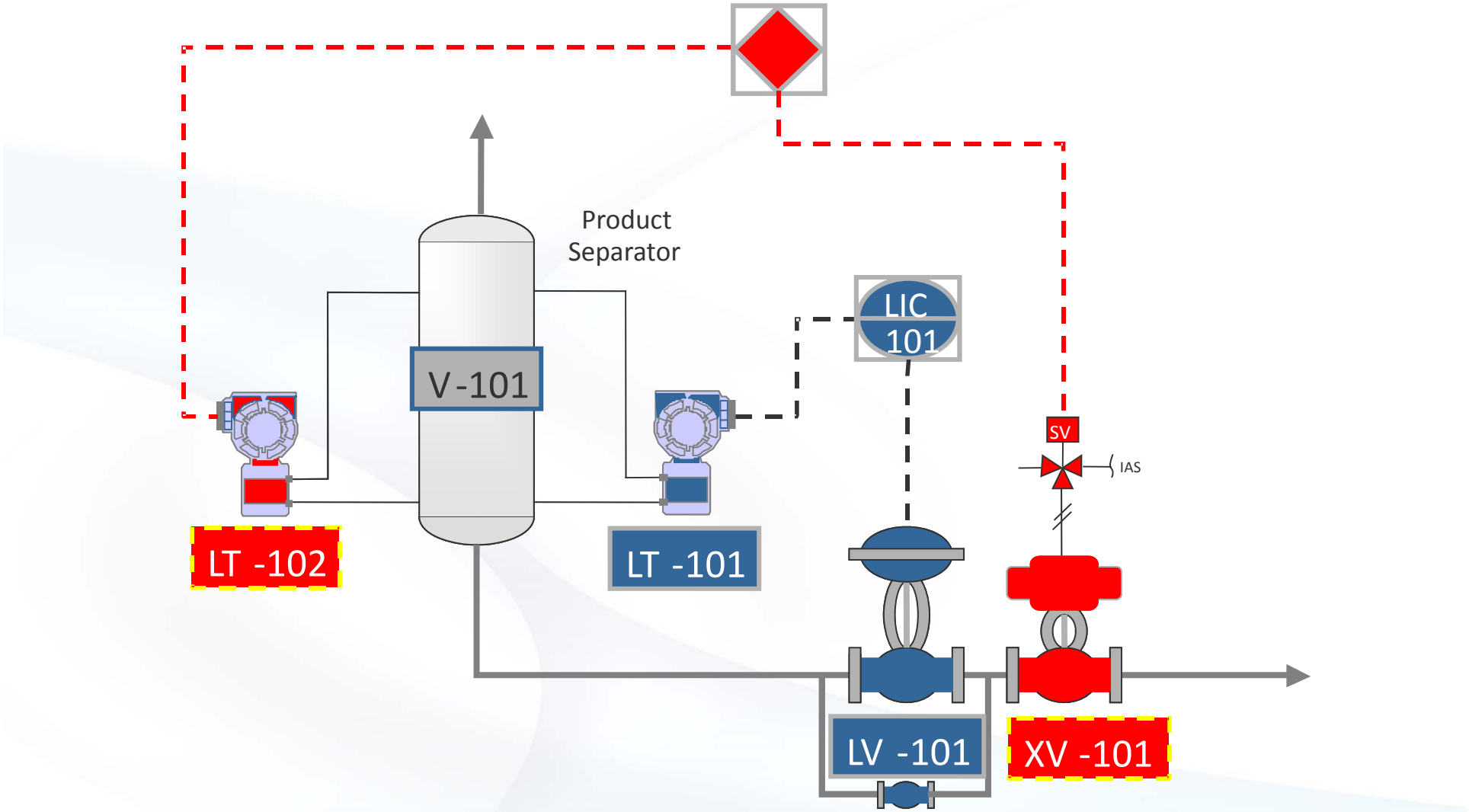
Kockázatok csökkentése



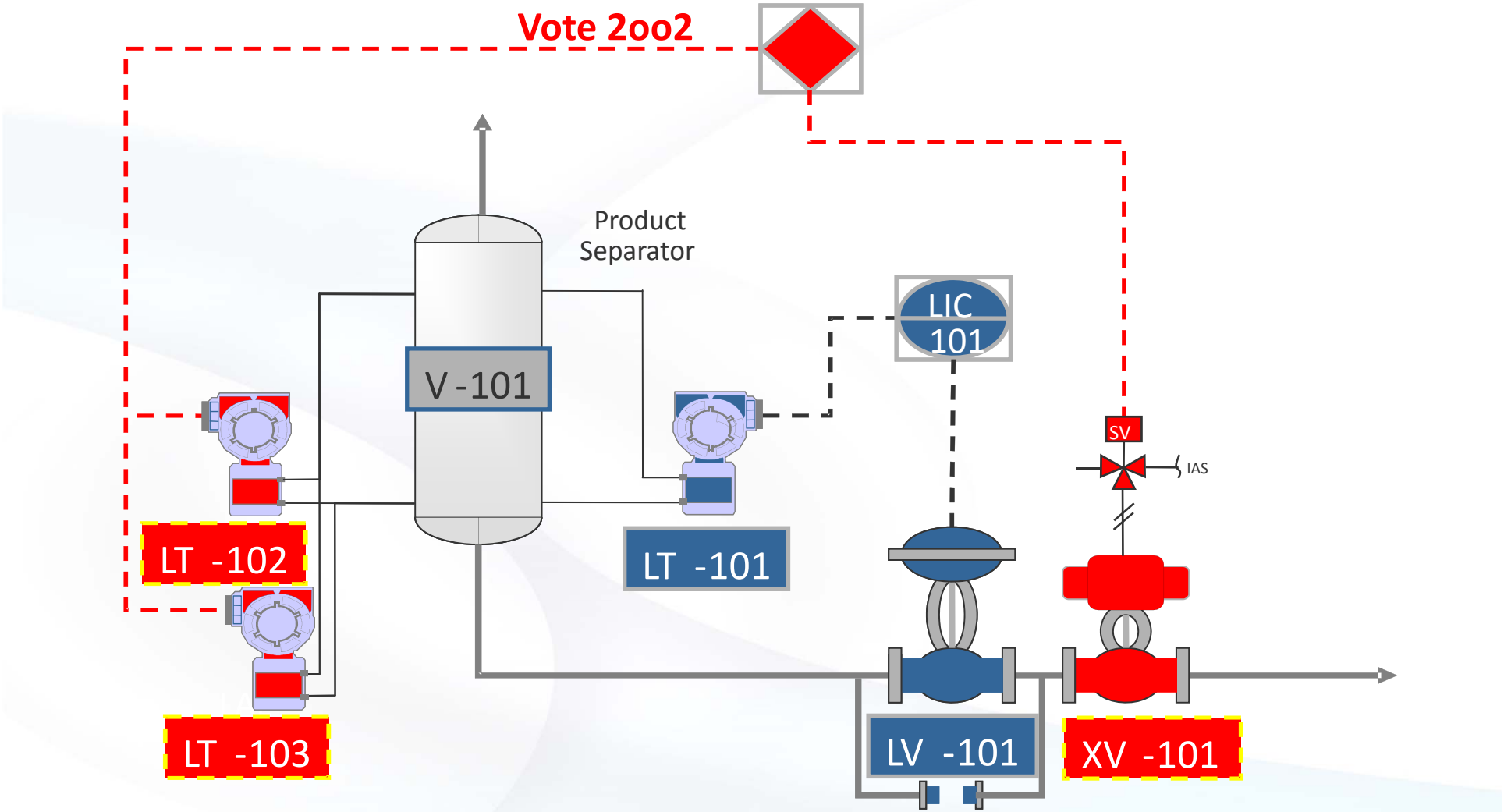
Rendszer architektúrák



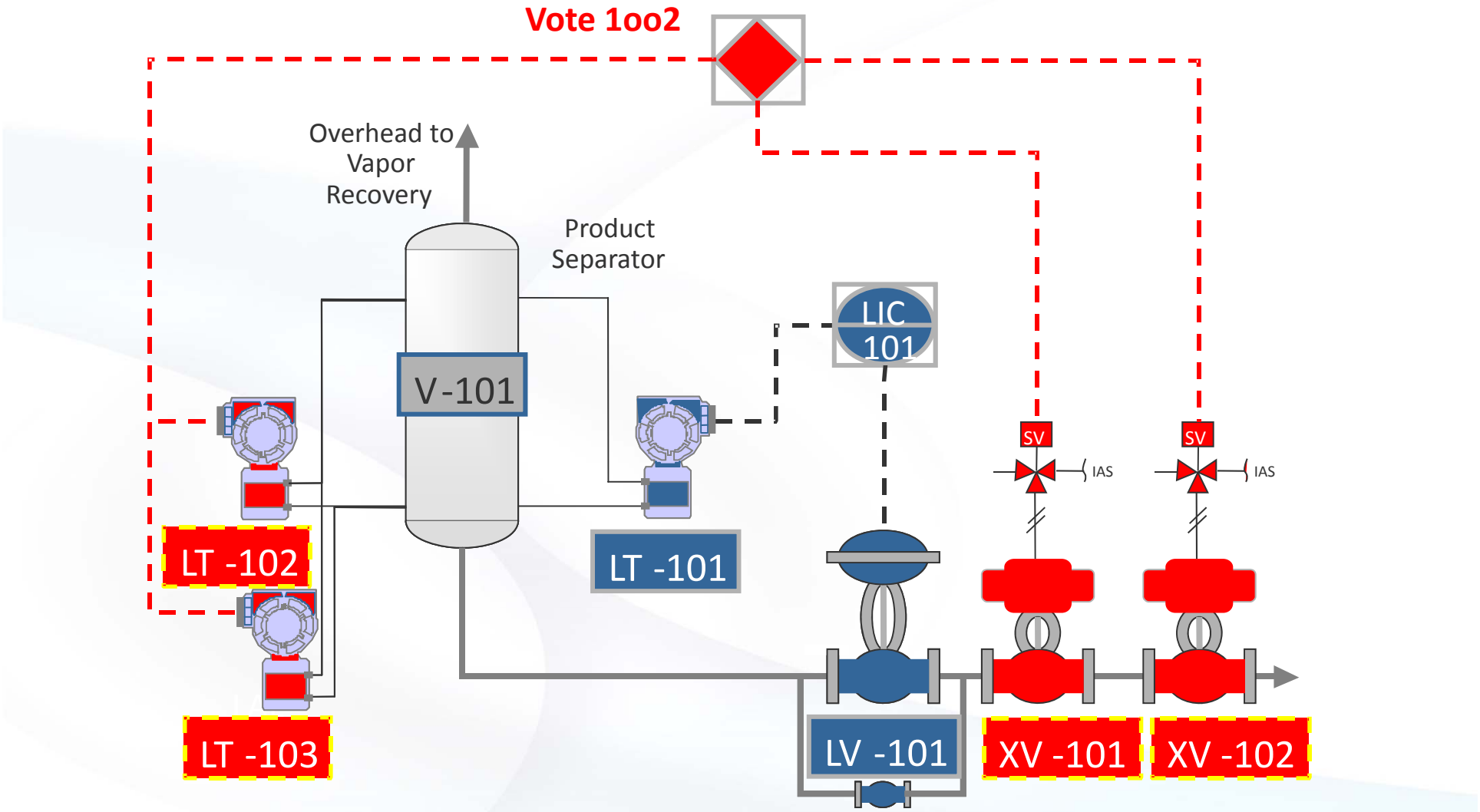
SIL 1 példa


Product
Separator
V-101
LIC
101
SV
IAS
LT -102
LT -101
LV -101
XV -101

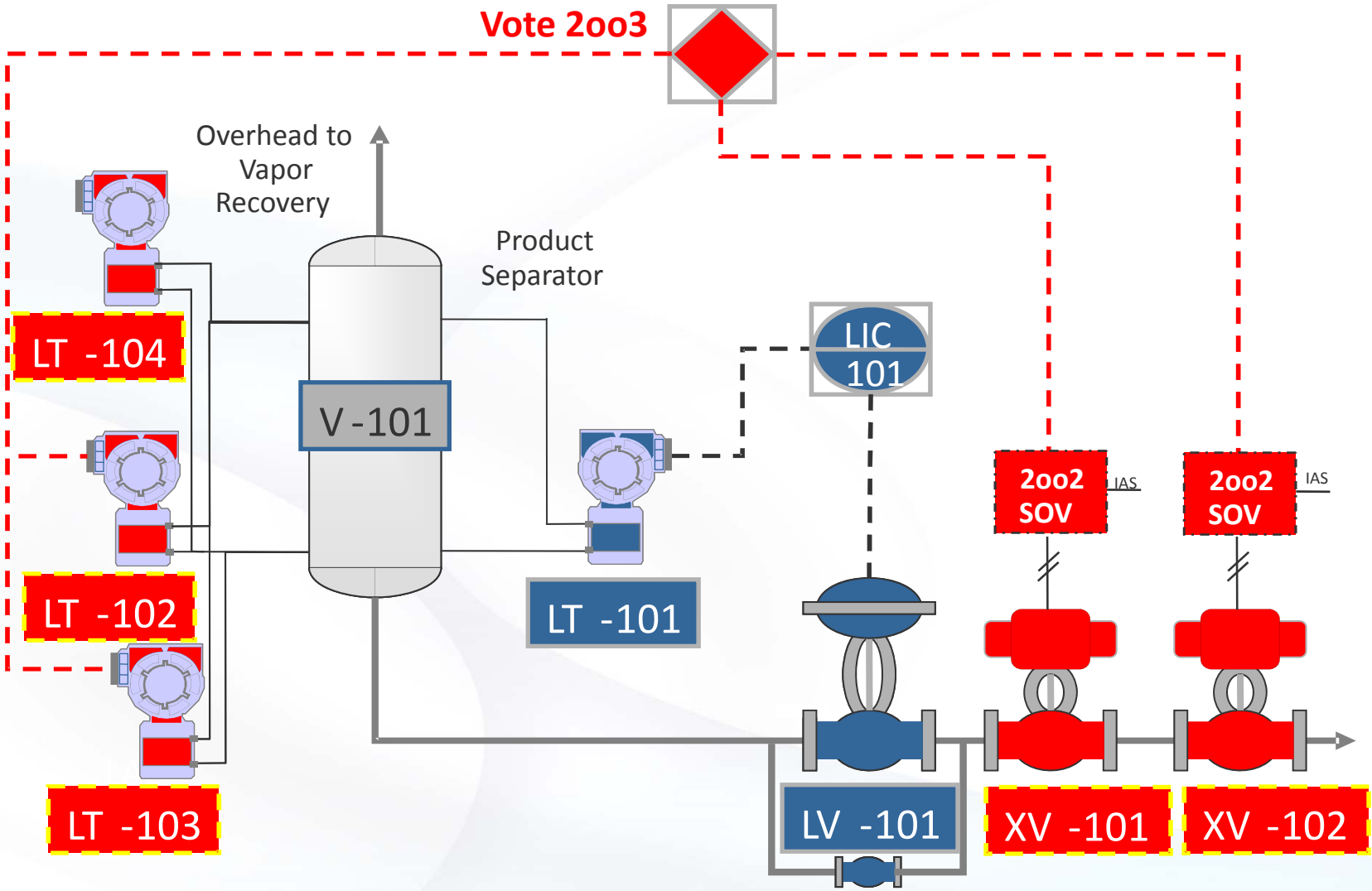
SIL 1 példa


Vote 2oo2
Product
Separator
V -101
LIC
101
SV
IAS
LT -102
LT -101
LT -103
LV -101
XV -101

SIL 2 példa

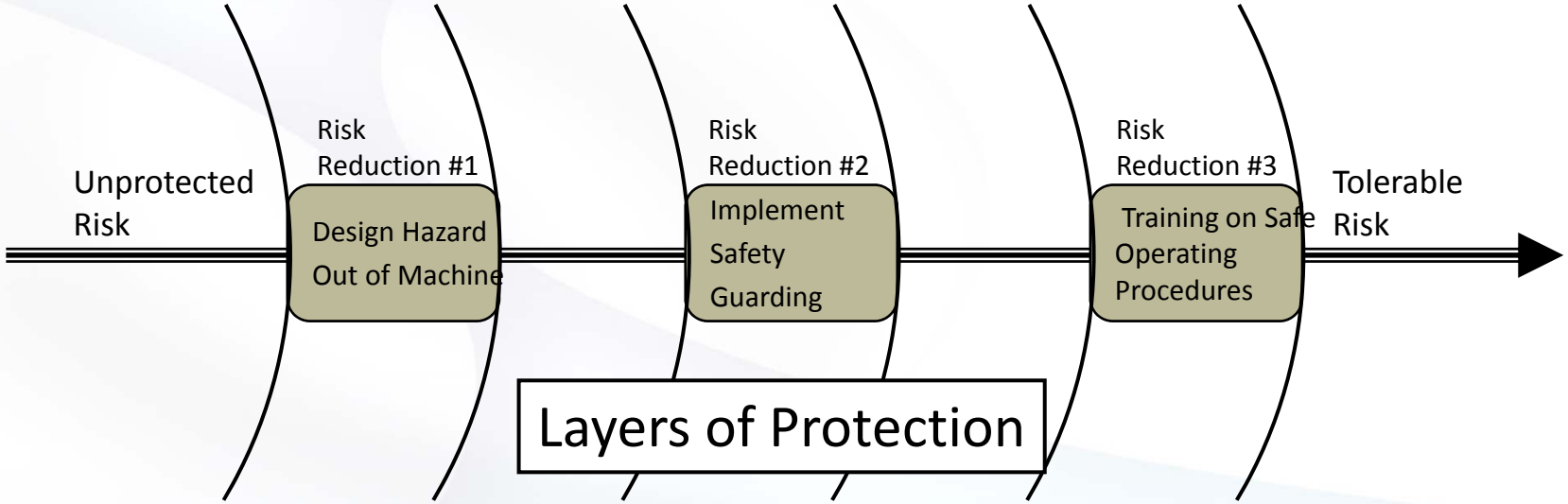

Vote 1oo2
Overhead to Vapor Recovery
Product Separator
V-101
LIC 101
LT -102
LT -101
LT -103
SV
IAS
SV
IAS
LV -101
XV -101
XV -102

SIL 2 példa


Vote 2oo3
Overhead to Vapor Recovery
Product Separator
LT -104
LT -102
LT -103
V -101
LT -101
LIC 101
2oo2 SOV
IAS
2oo2 SOV
IAS
LV -101
XV -101
XV -102

Kockázatok csökkentése

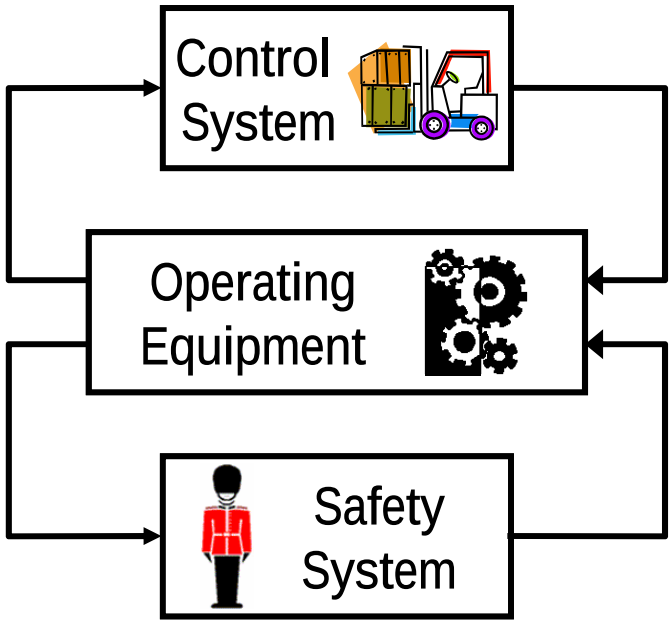
- A kockázat elemzéssel (Risk Assessment) mérjük fel az egyes folyamatok, gépek veszélyforrásait (Hazards)
- Minden veszélyforrásnál egy védelmi rétegre van szükség



Biztonsági rendszer funkciói

- A biztonsági rendszer feladata a folyamat vagy gép monitorozása és vezérlése a célból, hogy a veszélyhelyzeteket, azok kialakulását, fokozódását megakadályozza.

- A biztonsági rendszerek párhuzamosan futnak a gyártás irányítórendszerekkel
  - A gyártásirányítás célja: produktivitás
  - A biztonsági rendszer célja : védelem



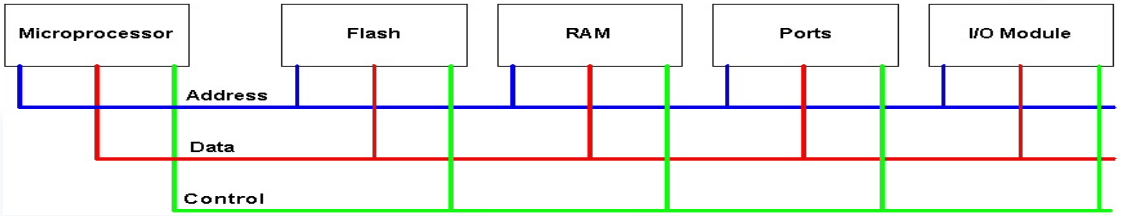
A biztonsági „3-D”

- **Duality** – ***dualitás, redundancia***
  - Ha valami hibázik, van másik ami képes a rendszert biztonságos állapotba hozni
  - Párhuzamos inputok és soros outputok

- **Diversity - diverzitás**
  - Védelem az azonos időben azonos módon való meghibásodás ellen
  - Pl.: NO és NC kontaktusok együttes használata
  - Pl.: egy magas és egy alacsony jelszintű input csatorna használata a biztonsági eszközökhöz

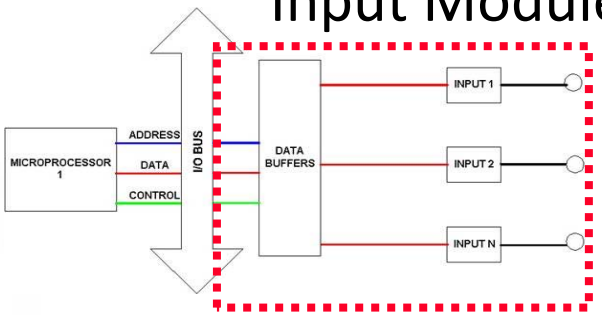
- **Diagnostics - diagnosztika**
  - A biztonsági rendszerek folyamatos öndiagnosztikát végeznek
  - Probléma esetén a rendszert „biztonságos állapotba” állítja és a probléma megszűnéséig ott is tartja
  - Pl.: Egy biztonsági PLC öndiagnosztikai rátája jóval nagyobb mint egy hagyományos PLC-é (> 90% vs. ≈ 50%)

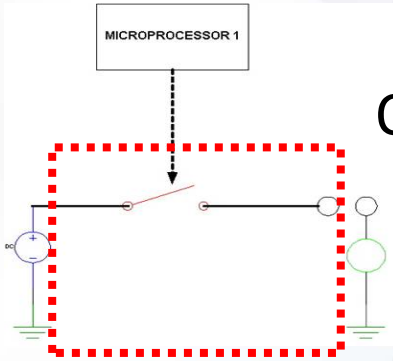
Standard PLC struktúra



Standard PLC

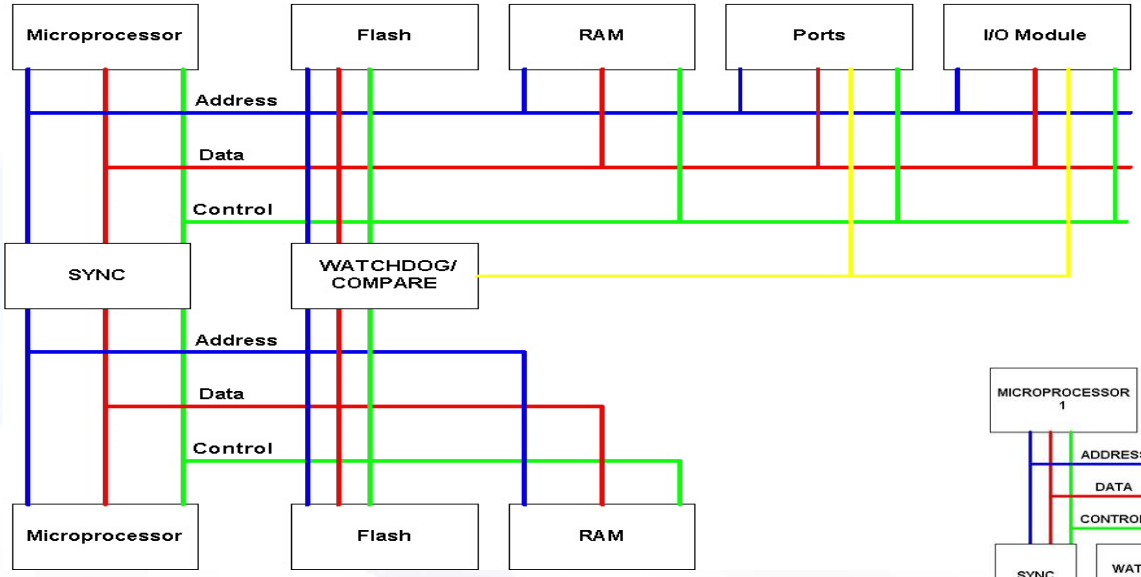
Input Module





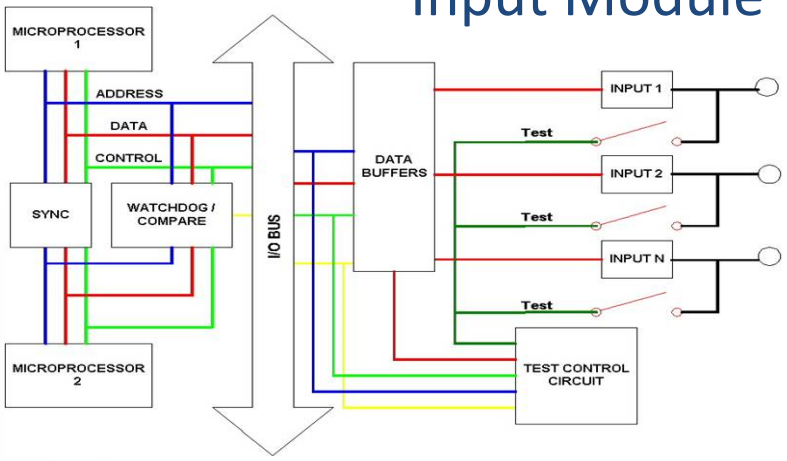
Output Module

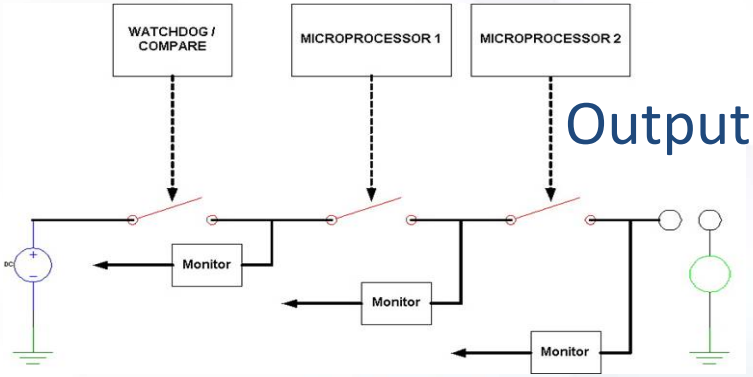
Biztonsági PLC struktúrája



Safety PLC

Input Module

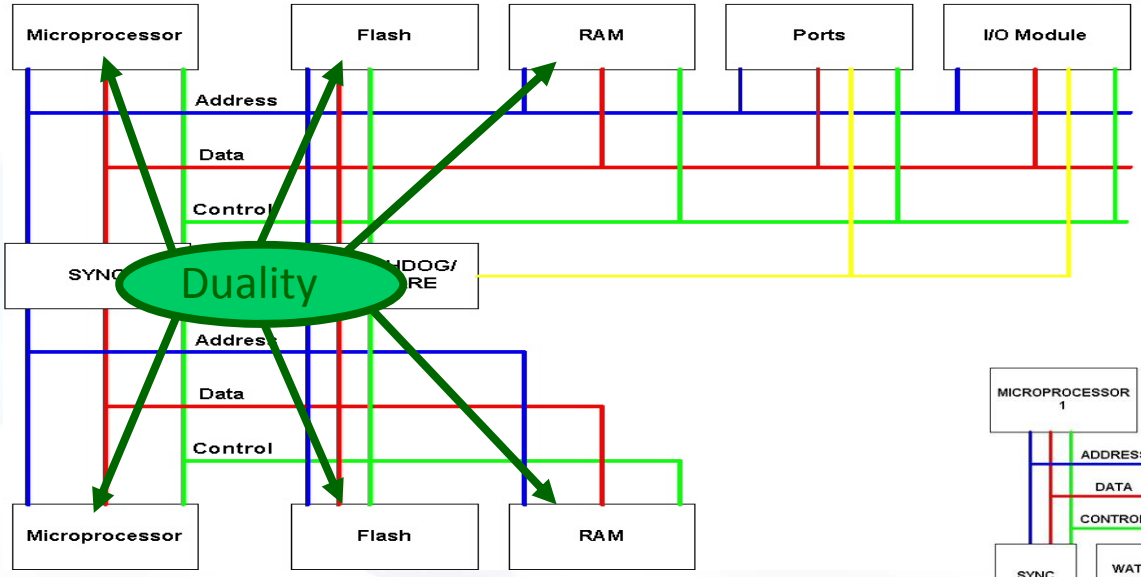




Output Module

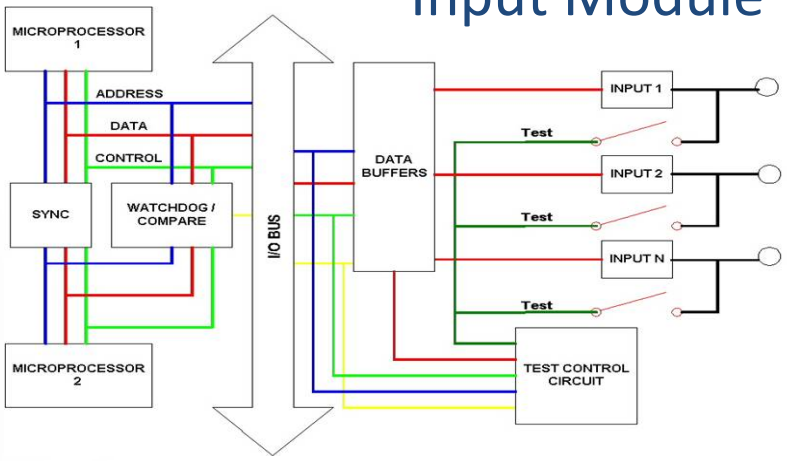
Hol van a „3-D” ???

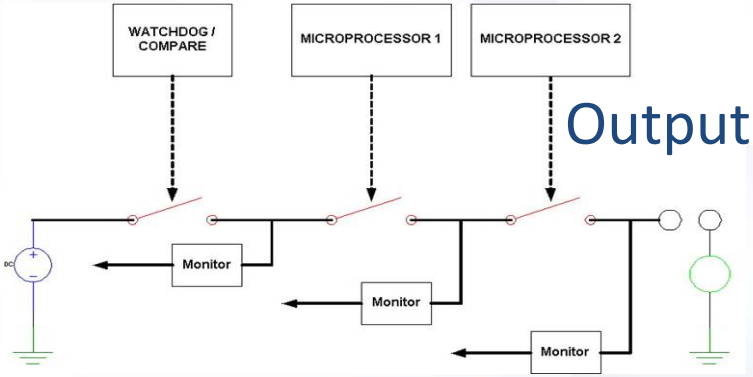
Biztonsági PLC struktúrája



Safety PLC

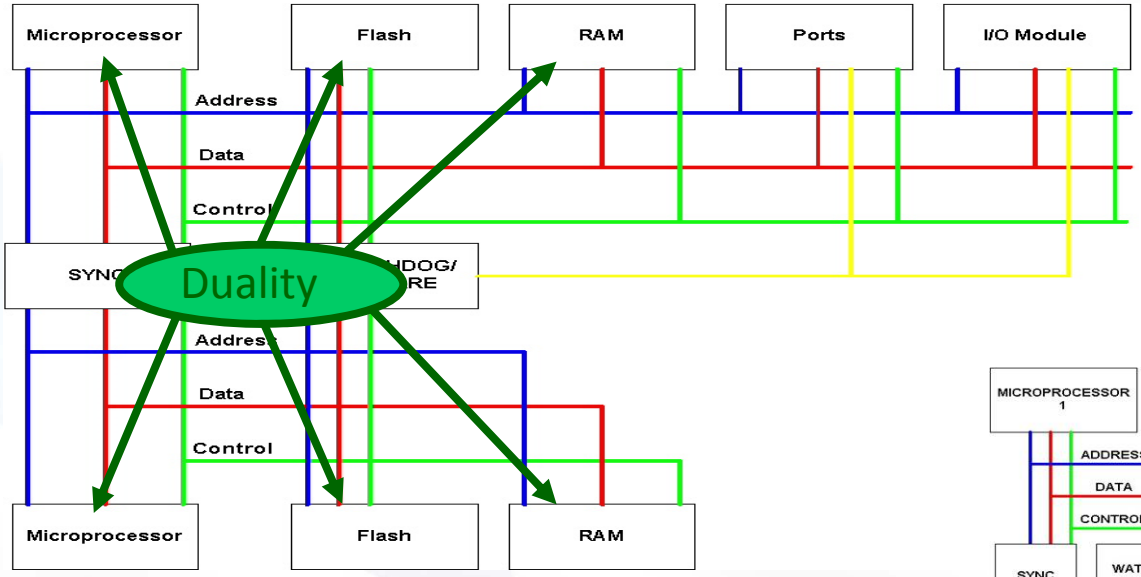
Input Module





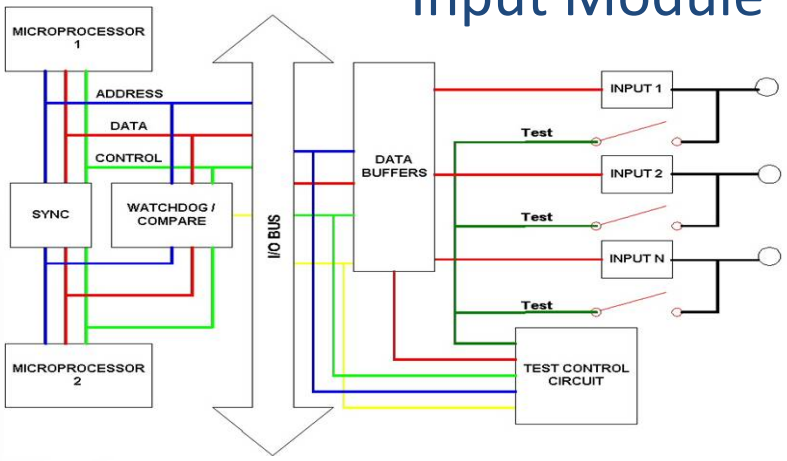
Output Module

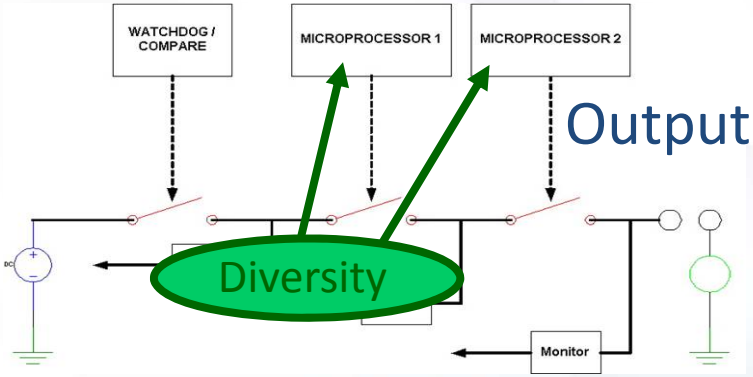
Biztonsági PLC struktúrája



Safety PLC

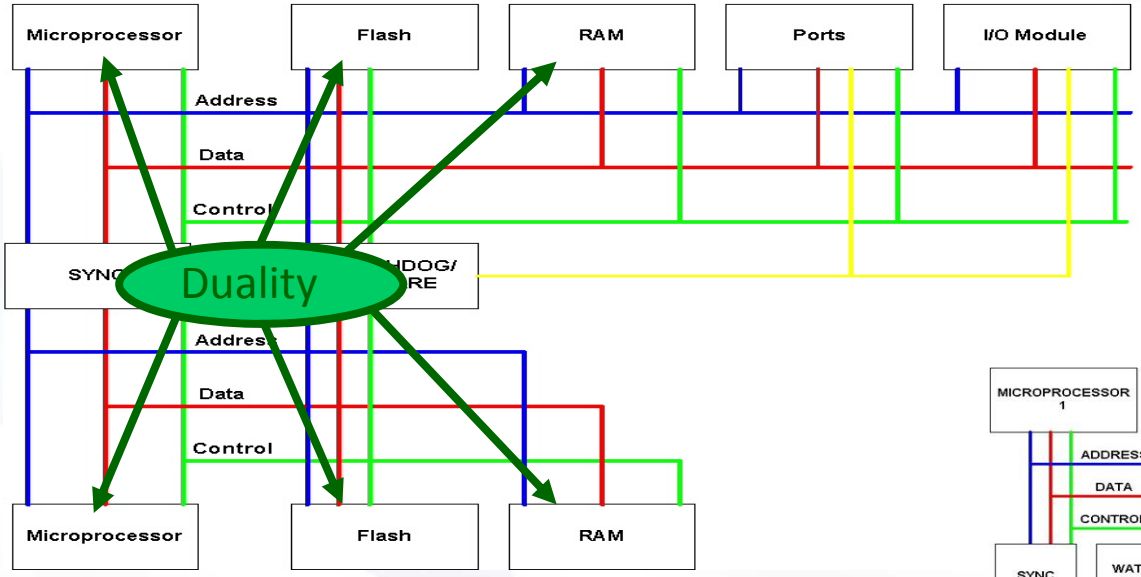
Input Module





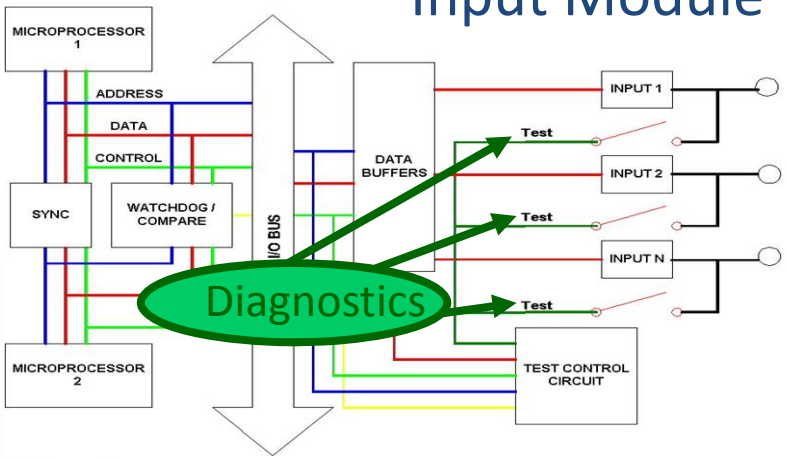
Output Module

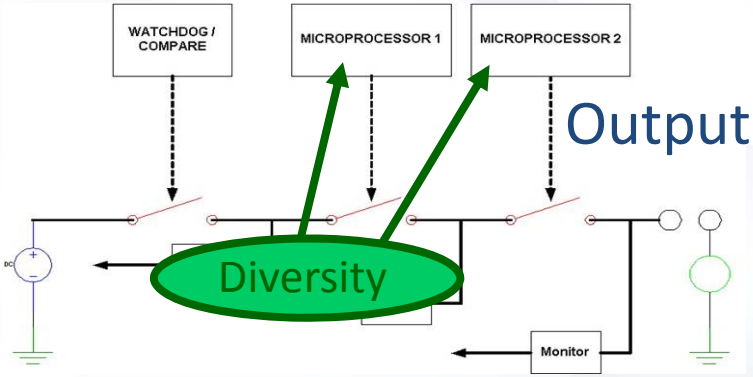
Biztonsági PLC struktúrája



Safety PLC

Input Module

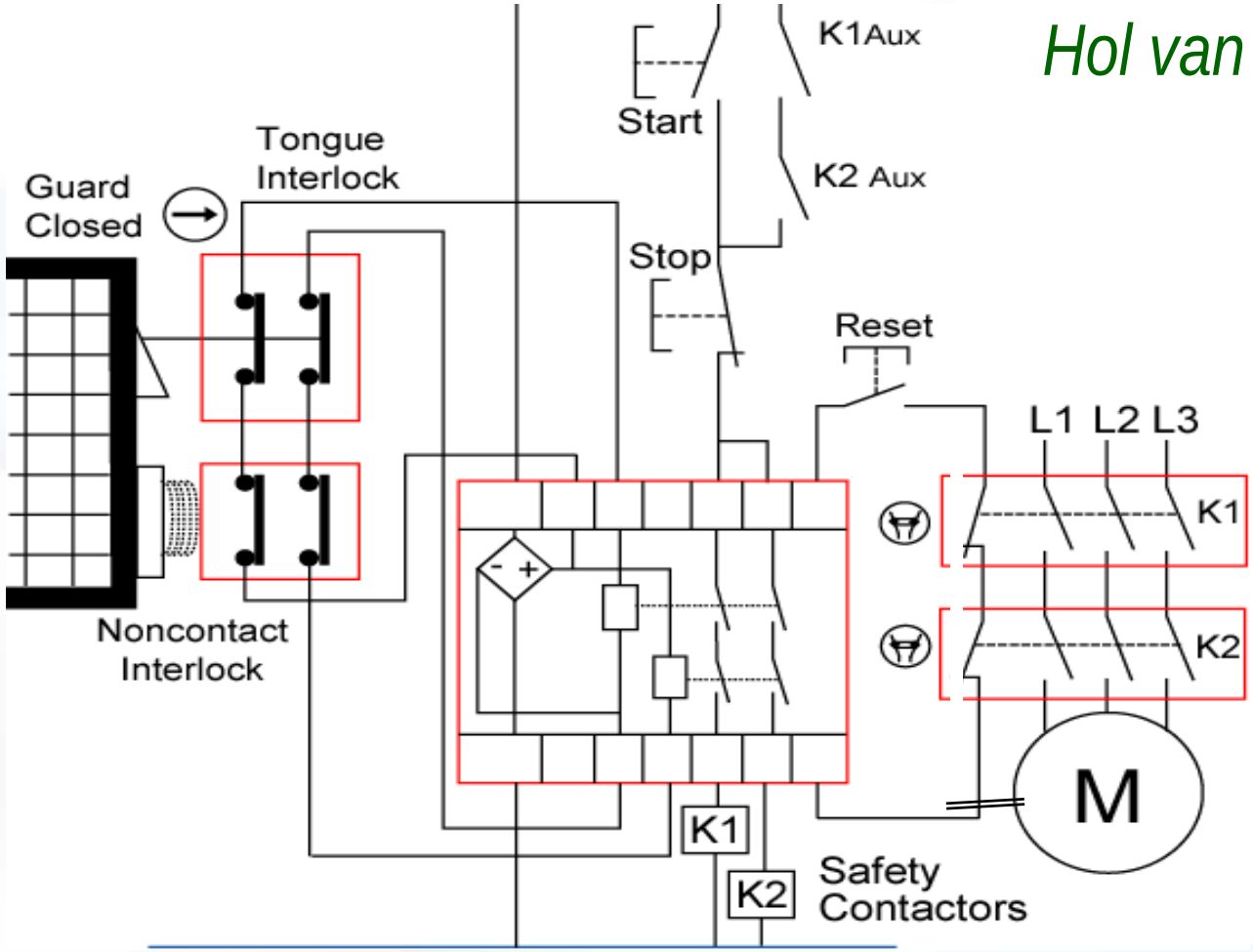




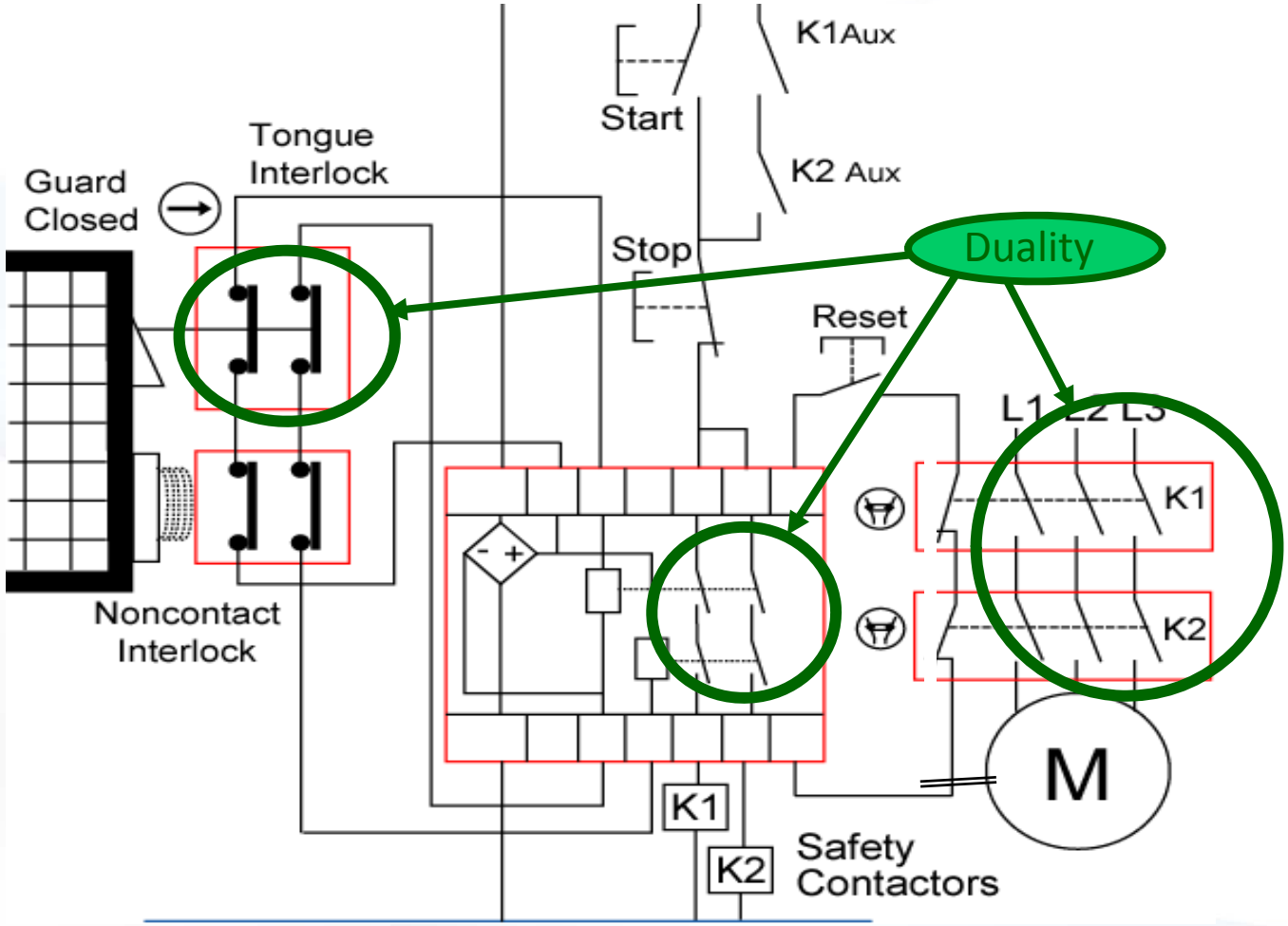
Output Module

Biztonsági Relé struktúrája

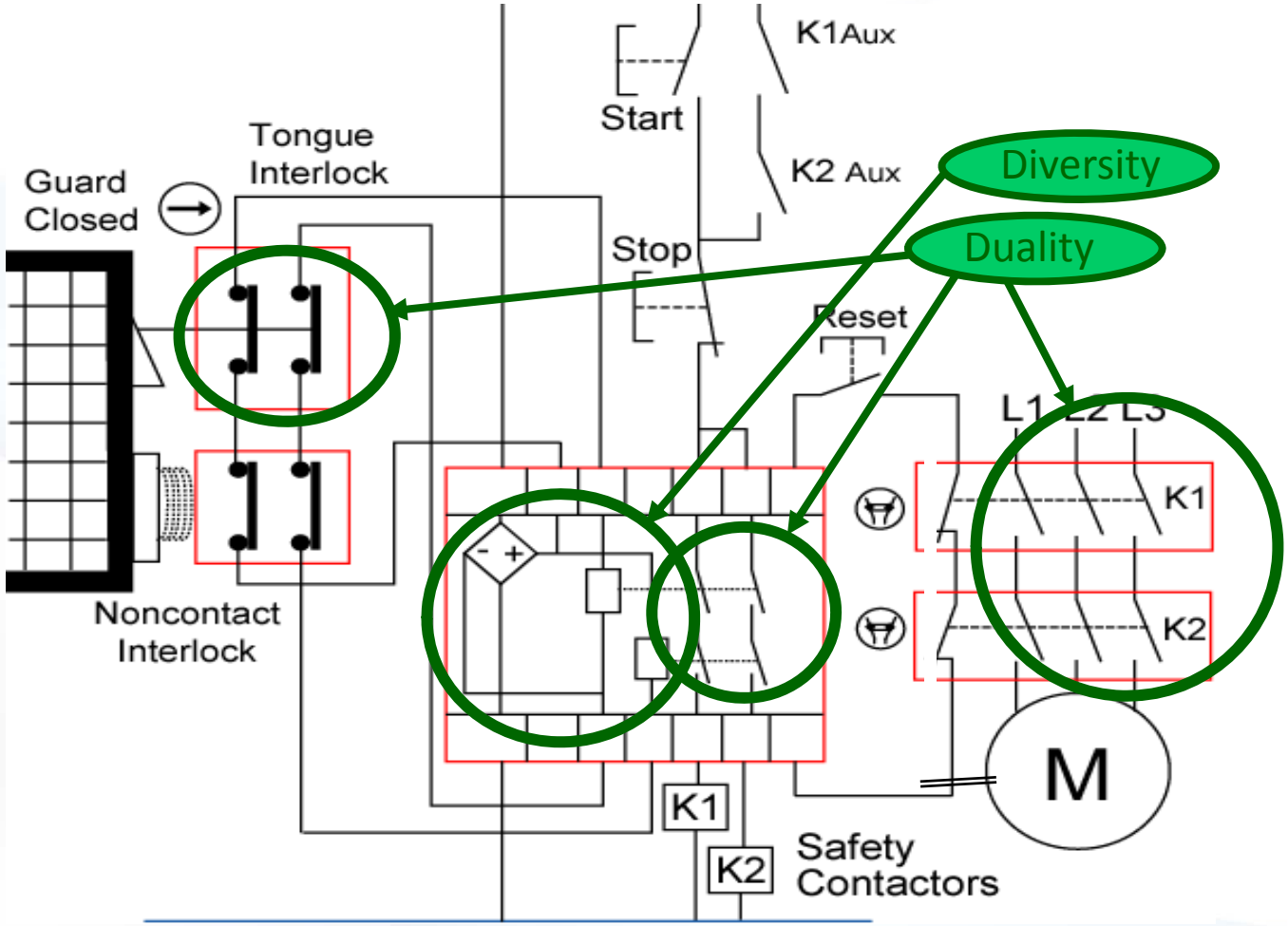
Hol van a „3-D” ???



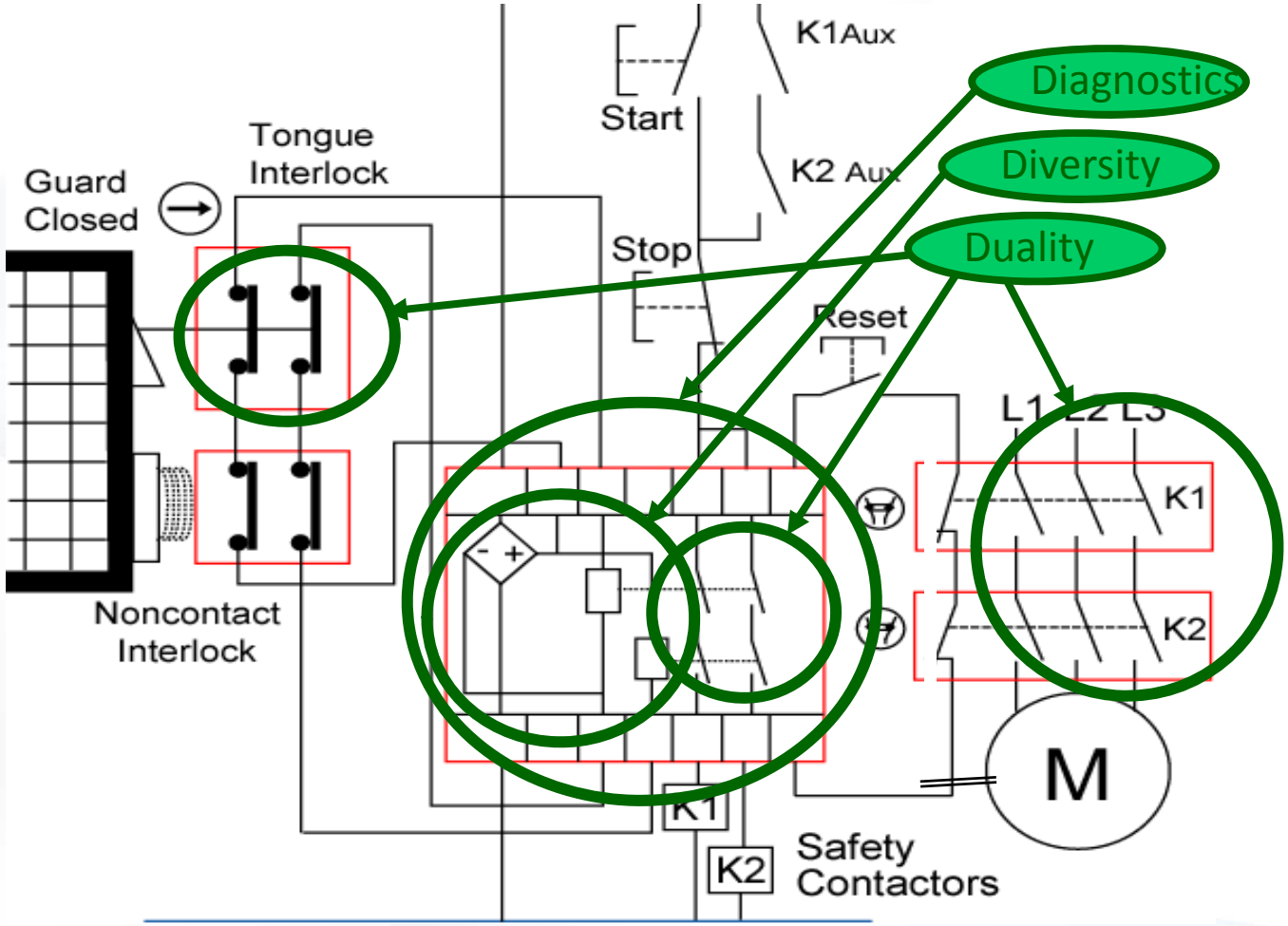
Biztonsági Relé struktúrája



Biztonsági Relé struktúrája



Biztonsági Relé struktúrája



PLC és Biztonsági PLC (Safety PLC)

- PLC-ben nem determináltak a hibaállapotok
- SPLC garantálja a „biztonságos” hibaállapotot a megfelelő SIL 1, 2 vagy 3 szerint
- SPLC harmadik fél által (TÜV) minősítetten megfelel a szabványoknak (IEC 61508, IEC 61511)
- SPLC-t csak megfelelően képzett és minősített személy konfigurálhat

SZÉCHENYI ISTVÁN EGYETEM
SZE - GYŐR

KÉRDÉS?

Köszönöm a figyelmet!

SZÉCHENYI ISTVÁN EGYETEM
SZE - GYŐR

Ipari biztonsági rendszerek

Implementálás

Ballagi Áron
Automatizálási Tanszék

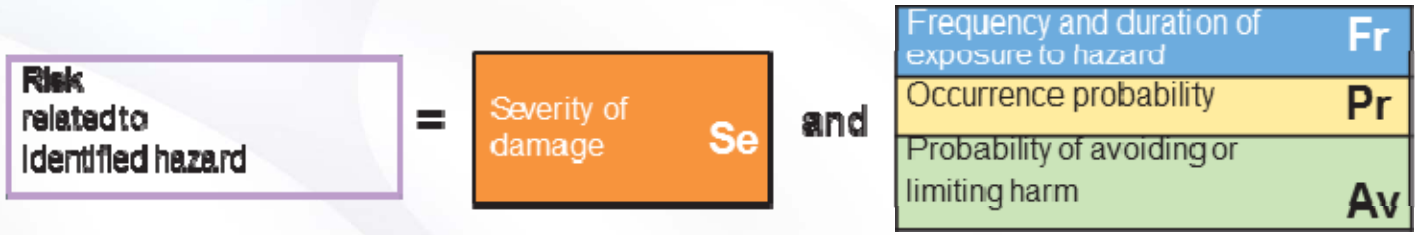
Biztonsági rendszerek implementálási eljárása

- A gépgyártó lépései
  - Kockázat elemzés
  - Kockázat csökkentés
    - 1. lépés: Biztonsági rendszerterv
    - 2. lépés: Védelemi technikák mértéke
    - 3. lépés: Felhasználó informálása a maradék kockázatokról
  - A gép validálása
  - A gép piacra dobása
- Technikai dokumentációk
  - Minden lépés részletesen dokumentált

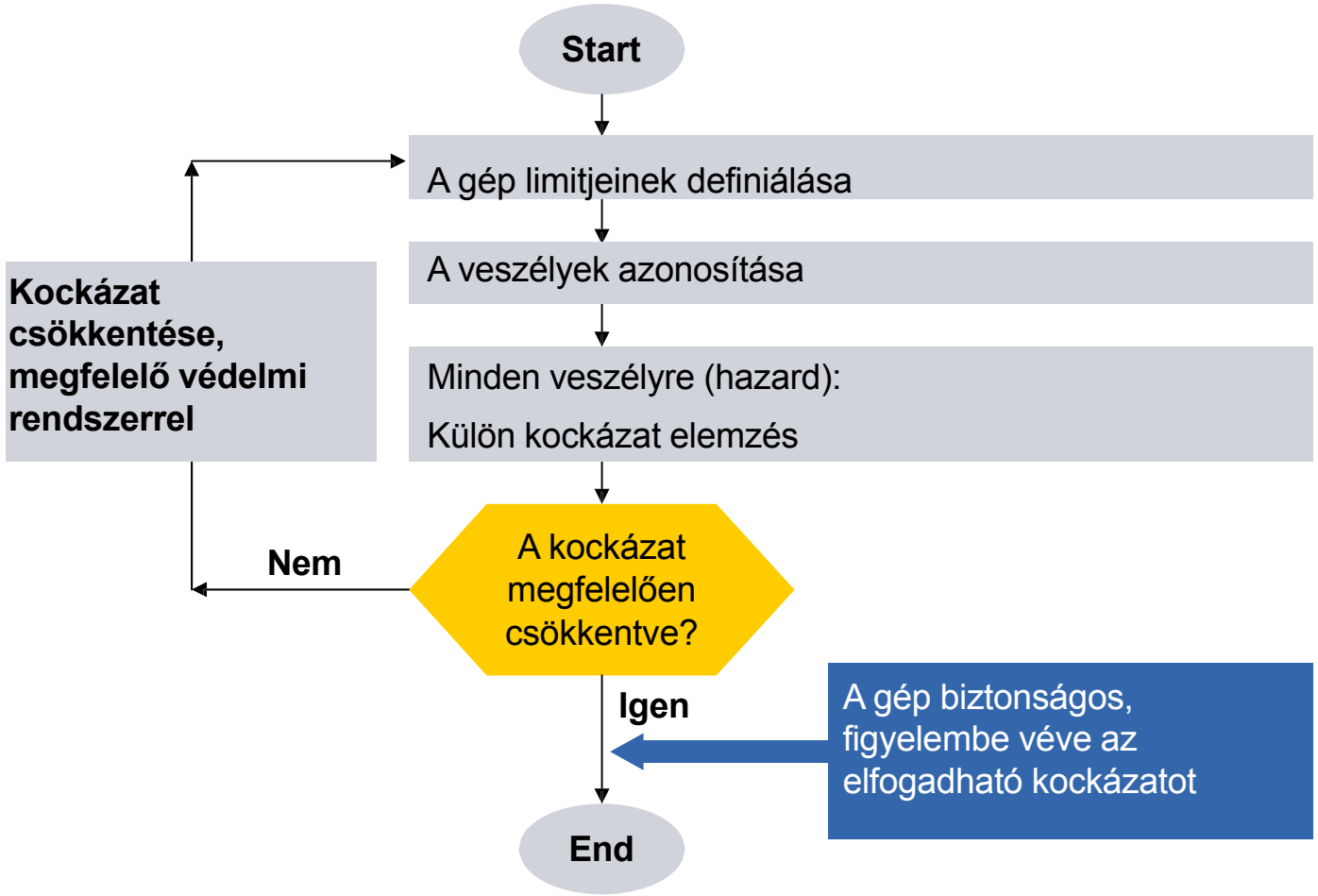
Kockázat elemzés

A kockázati elemek (Se, Fr, Pr és Av) a EN 62061 és EN ISO 13849-1 szabványok bemenetei.

- EN 62061 a szükséges „safety integrity level” (SIL) határozza meg
- EN ISO 13849-1, a "performance level" (PL) a kimenet



A gép kockázati elemzése



Releváns Szabványok

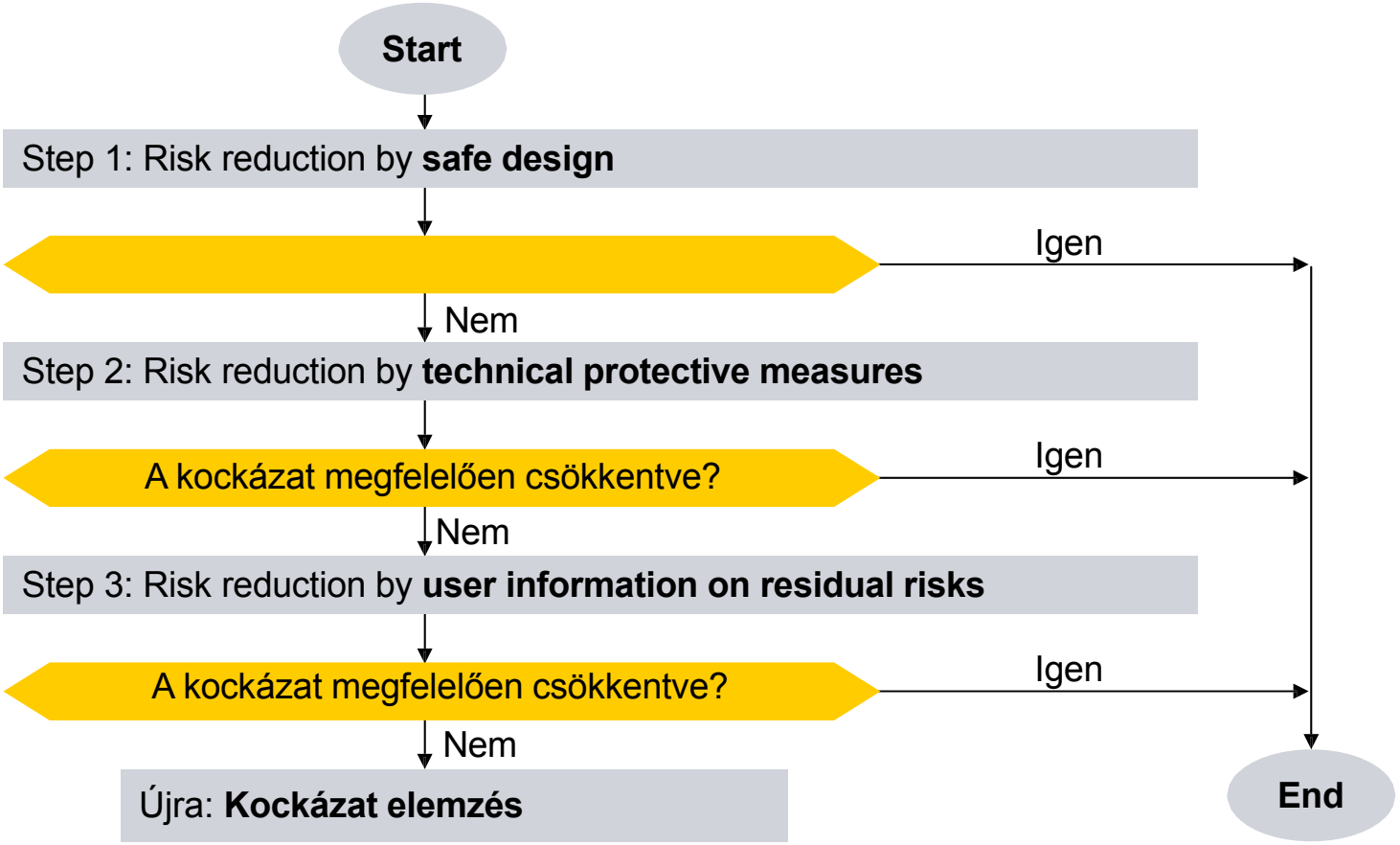
- **EN ISO 12100**
- **Safety of machinery – Biztonsági Gépgyártás**
- **Alap koncepciók, tervezés szabályai**
  - Lehetséges veszélyek leírása
  - Kockázat csökkentési stratégiák
  - Cél: biztonságos géptervezés, elfogadható maradék kockázattal
- **EN ISO 14121**
- **Safety of machinery – Kockázat elemzés szabályai**
  - A kockázat tényezői

Kockázat minimalizálási stratégiák (EN ISO 12100-1 sec.1)

- A gép fizikai és időbeli korlátainak felmérése
- Veszélyek feltárása, kockázat elemzés
- A kockázat meghatározása minden egyes feltárt veszélyes szituációra
- Kockázatok elemzése és minimalizálásuk lehetőségeinek feltárása
- Veszély elnyomás és védelem, kockázat csökkentés a „3 lépés módszerrel" – tervezés, védelem technikai mérőszámok, használati információk

Kockázat csökkentés a „3 lépés” módszer (EN ISO 12100)

Minden egyes veszély kockázatát csökkenteni kell:



1. lépés: Biztonsági rendszerterv

- Biztonsági rendszerterv
  - A gép tervezésénél integrálva a biztonság
  - Kockázat elemzés előtérben

- A biztonsági tervezés aspektusai (pl)
  - Élek letörése
  - Áramütés védelem
  - Vész esetén megállási terv
  - Üzemeltetés és karbantartási koncepciók
  - …

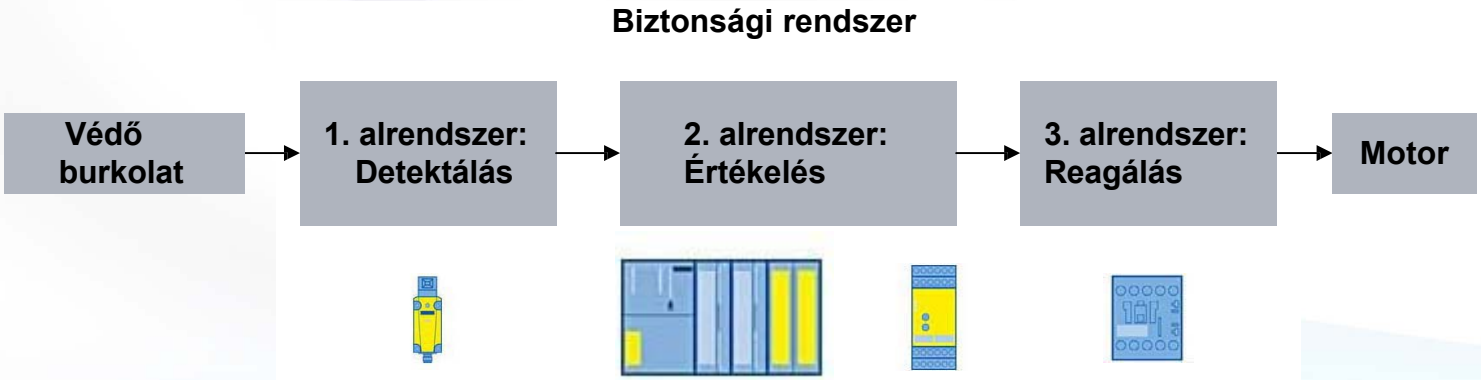
2. lépés: Védelemi technikák mértéke

- Védelmi technikák mértéke
  - Biztonsági funkciók minden kiküszöbölhetetlen veszélyhez
  - Biztonsági rendszer végzi a védelmet

- Pl. :Biztonsági funkció, biztonsági rendszer nélkül
  - Veszélyes részek folyamatos mechanikai elzárása (kerítés)
- Pl.: Biztonsági funkció, biztonsági rendszerrel
  - Ha védő burkolat nyitva, akkor a motor nem foroghat

2. lépés: Védelemi technikák mértéke

- Biztonsági rendszer
  - Biztonsági funkciókat lát el
  - Biztonsági alrendszerekből áll
- Biztonsági alrendszerek
  - Érzékelés, detektálás (pozíció kapcsoló, fény függőny,…)
  - Értékelés (biztonsági PLC, biztonsági vezérlő, …)
  - Reagálás (motorvédő kapcsoló, frekvencia váltó, …)



2. lépés: Védelemi technikák mértéke

A gépgyártás biztonsági tervezési és megvalósítási szabványai

EN 954-1 (2009 végéig)

EN ISO 13849-1

EN 62061 (IEC 62061)

2. lépés: Védelemi technikák mértéke

- Alap eljárások a biztonsági funkciók felépítésénél
  - Biztonsági funkció specifikálása
  - A szükséges védelmi szint meghatározása
  - A biztonsági funkció tervezése
  - Az elért biztonsági szint determinálása
  - A funkció realizálása és tesztelése

2. lépés: Védelemi technikák mértéke - Biztonsági funkció specifikálása

- A Biztonsági funkció peremfeltételei
  - Milyen veszély ellen véd
  - Személyi érintettség
  - A gép működési módjai
  - …
- A biztonsági funkcióval szemben támasztott követelmények
  - Reakciók a hibára
  - Elvárt reagálási idő
  - Elektromechanikus eszközök működtetése

2. lépés: Védelemi technikák mértéke
A szükséges védelmi szint meghatározása

- A szükséges védelmi szint a biztonsági funkció hatékonyságának mértéke
- Függ a:
  - Sérülés súlyosságától
  - A bekövetkezési gyakoriságtól / expozíciós időtől
  - Elkerülhetőségtől
- Minél súlyosabb a sérülés és nagy az előfordulás valószínűsége (gyakorisága) annál magasabb szintű védelemre van szükség
- Az EN 62061 és az ISO 13849 mutat eljárásokat a szükséges biztonsági szint meghatározására

2. lépés: Védelemi technikák mértéke
A szükséges védelmi szint meghatározása

Az EN 62061 specifikációi: SIL 1 -től SIL 3 -ig

Frekvencia/ expozíciós idő	Fr
< 1 óra	5
1 óra – 1 nap	5
1 nap – 2 hét	4
2 hét – 1 év	3
> 1 év	2

+

Előfordulás valószínűsége	Pr
Gyakori	5
Valószínű	4
Lehetséges	3
Ritka	2
Elhanyagolható	1

+

Elkerülhetőség	P
Lehetetlen	5
Lehetséges	3
Valószínű	1

Sérülés súlyossága	Se
Visszafordíthatatlan, pl.: végtag elvesztése	4
Visszafordíthatatlan, pl.: comb törés	3
Visszafordítható, pl.: korházi megfigyelést igényel	2
Visszafordítható: pl.: elsősegélyt igényel	1

Se	Class Cl = Fr + Pr + P				
	3 - 4	5 - 7	8 - 10	11 - 13	14 - 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3			SIL 1	SIL 2	SIL 3
2				SIL 1	SIL 2
1					SIL 1

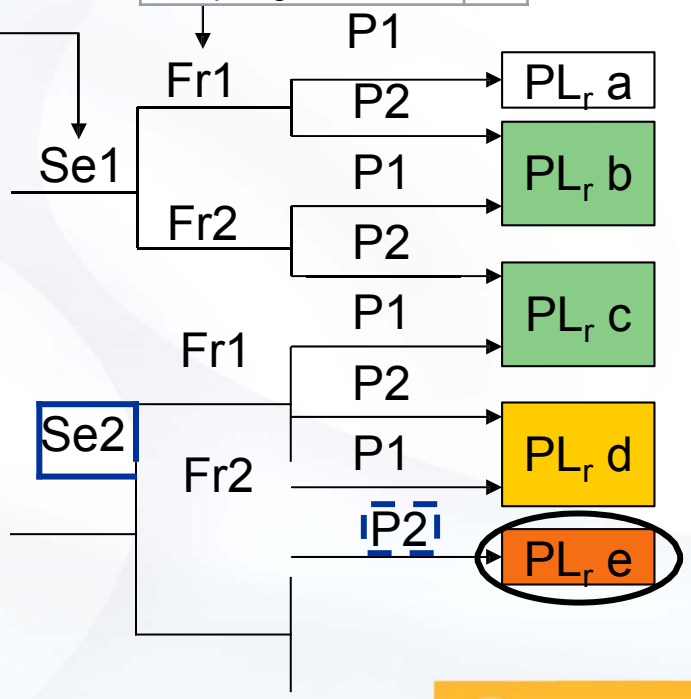
2. lépés: Védelemi technikák mértéke
A szükséges védelmi szint meghatározása

Az EN ISO 13849 specifikációi: PLr a -tól PLr e -ig

Sérülés súlyossága	Se
Visszafordíthatatlan sérülés	Se2
Visszafordítható sérülés	Se1

Frekvencia/ expozíciós idő	Fr
Gyakoritól a folyamatosig / hosszú	Fr2
Ritkától a közepesig / rövid	Fr1

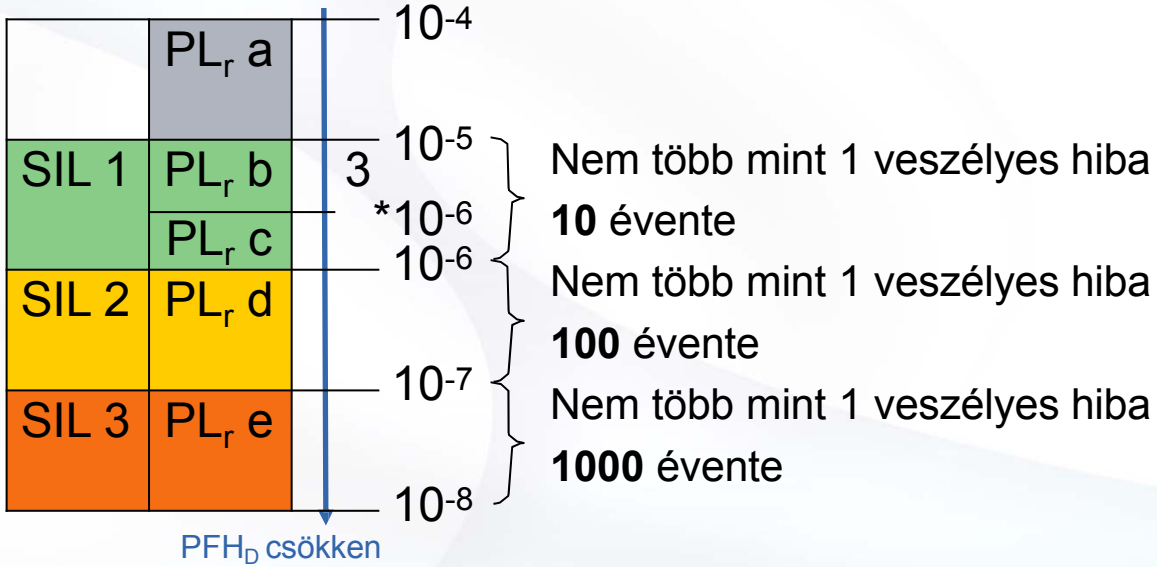
Elháríthatóság	P
Alig lehetséges	P2
Lehetséges	P1



2. lépés: Védelemi technikák mértéke
A szükséges védelmi szint meghatározása

Biztonsági szintekkel szembeni elvárás: a meghibásodás valószínűsége

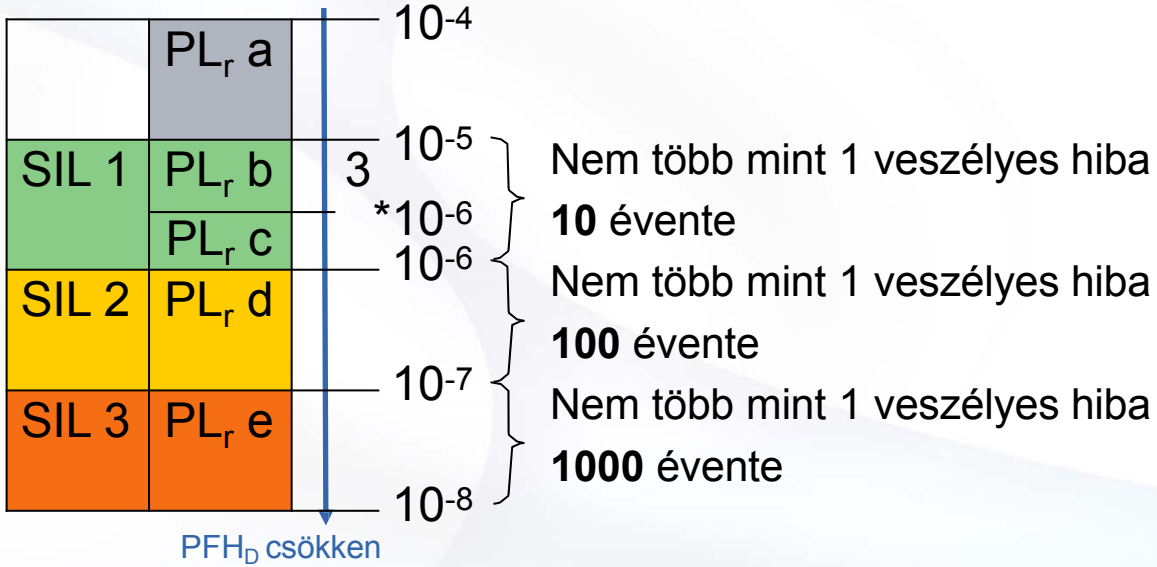
- Az EN 62061 és az EN ISO 13849 előírják a biztonsági funkciók meghibásodásának elfogadható valószínűségét:
  - A veszélyes hibák esélye óránként, PFH_D
  - Nagyobb biztonság – kisebb PFH_D



2. lépés: Védelemi technikák mértéke
A szükséges védelmi szint meghatározása

Biztonsági szintekkel szembeni elvárás: a meghibásodás valószínűsége

- Az EN 62061 és az EN ISO 13849 előírják a biztonsági funkciók meghibásodásának elfogadható valószínűségét:
  - A veszélyes hibák esélye óránként, PFH_D
  - Nagyobb biztonság – kisebb PFH_D



3. lépés: Felhasználó informálása a maradék kockázatokról

- A maradék és elfogadható kockázatok ismertetése
- Nem helyettesíti a:
  - Biztonsági tervezést
  - Védelmi technikákat

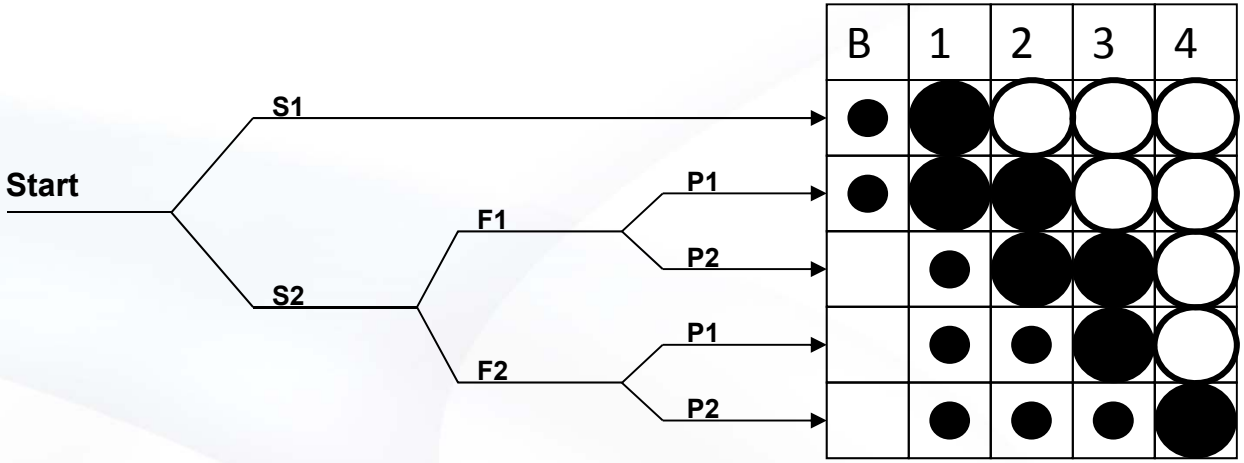
- Pl.:
  - Figyelmeztetések a felhasználói leírásban
  - Speciális munka instrukciók
  - Ikonok
  - Személyi védő felszerelés

Robotok és biztonságtechnika

- Robot biztonságtechnikai HW elemek
- Vezérlések biztonságtechnikai eszközei
- Szoftver és Hardver fejlesztések
- Virtuális robotkörnyezet

Kockázatelemzés

Biztonsági Kategóriák



Kockázati paraméterek:

S sérülés komolysága
S1 csekély (normál, visszafordítható sérülés)
S2 komoly (maradandó sérülés, halál)
F gyakorisága és feltétele a kockázatnak
F1 ritkán és rövid ideig fennálló kockázat
F2 folyamatos és hossza tartó kockázati állapot
P a kockázat vagy sérülés elkerülésének lehetősége
P1 bizonyos feltételekkel lehetséges
P2 szinte lehetetlen

Biztonsági besorolási kategóriák

Gyakori besorolások

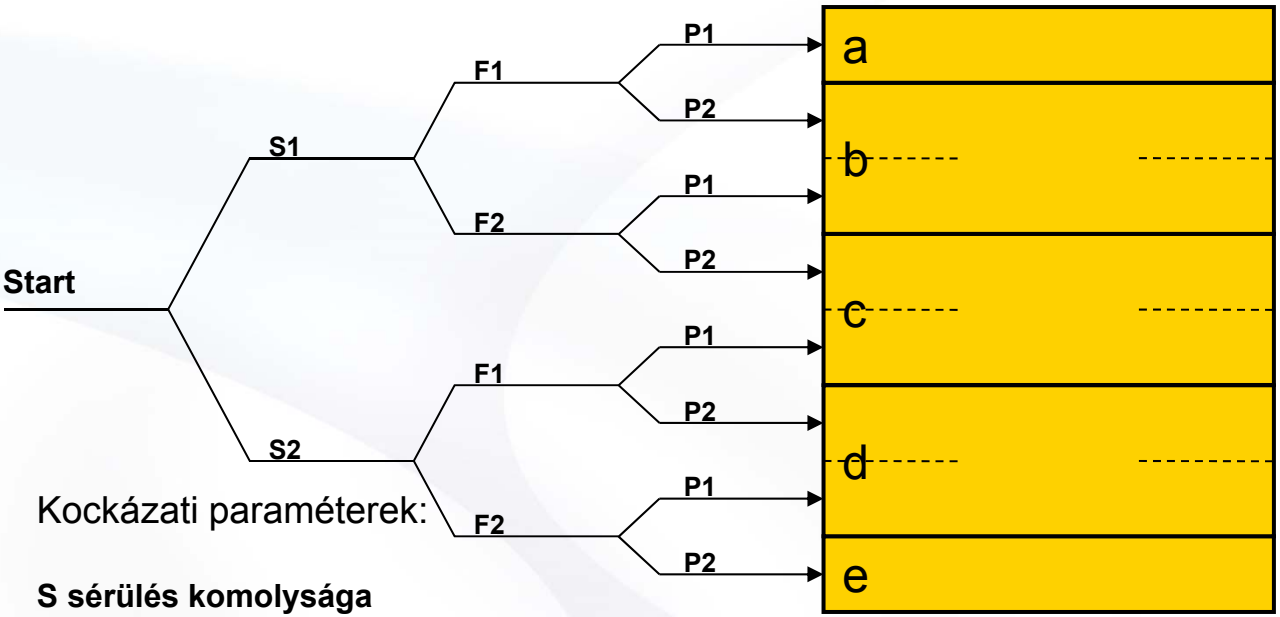
További vizsgálatot/elemzést igénylő kategóriák

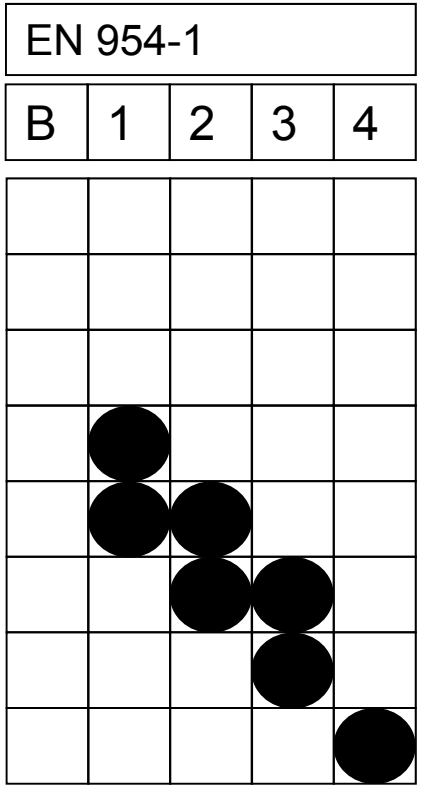
A valós kockázathoz képest túlbiztosított helyzetek

EN 954-1

Kockázatelemzés

Biztonsági Kategóriák





Kockázati paraméterek:

S sérülés komolysága
- S1 csekély (normál, visszafordítható sérülés)
- S2 komoly (maradandó sérülés, halál)

F gyakorisága és feltétele a kockázatnak
- F1 ritkán és rövid ideig fennálló kockázat
- F2 folyamatos és hossza tartó kockázati állapot

P a kockázat vagy sérülés elkerülésének lehetősége
- P1 bizonyos feltételekkel lehetséges
- P2 szinte lehetetlen

Direktíva megfelelőség:
Cat 3 → PL d
Cat 4 → PL e

EN 954-1& ISO 13949-1

- ISO 13949-1 besorolási tényezők:
- **Sérülés komolysága**
  - S1: zúzódás és/vagy zúzott seb
  - S2: amputáció vagy halál

- **F gyakorisága és feltétele a kockázatnak**
  - F1: Időről időre lép fel (eseti)
  - F2: ismétlődően fellép az automatikusan végzett ciklusok során
  - Figyelem: Ha óránként legalább egyszer fellép a kockázati tényező, akkor már F2 a besorolás

- **P1, P2 állapot elkerülésének lehetősége**
  - P1: csak akkor választható, ha a baleset elkerülésének vagy a hatásának csökkentésére reális esély mutatkozik
  - P2: ha gyakorlatilag nincs esély a kockázat csökkentésére.

- Konklúzió:
  - Általában a robotos alkalmazások CAT 3 / PLd
  - Csak kivételesen veszélyes körülmények között sorolandóak a CAT 4 / Ple kategóriába

Példa

A gépkezelő egy kiszolgálási feladatot lát el, semmi nem akadályozza, hogy ellépjen a robottól.

Szigorúság:

Nagy robot, komoly sérülést okozhat, tehát S2

Gyakoriság

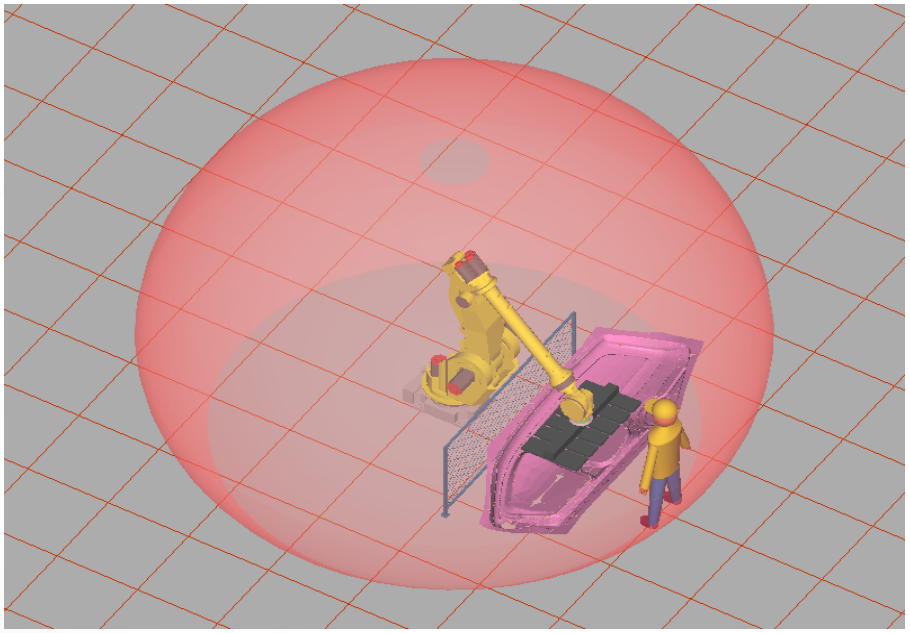
Minden ciklusban, tehát F2

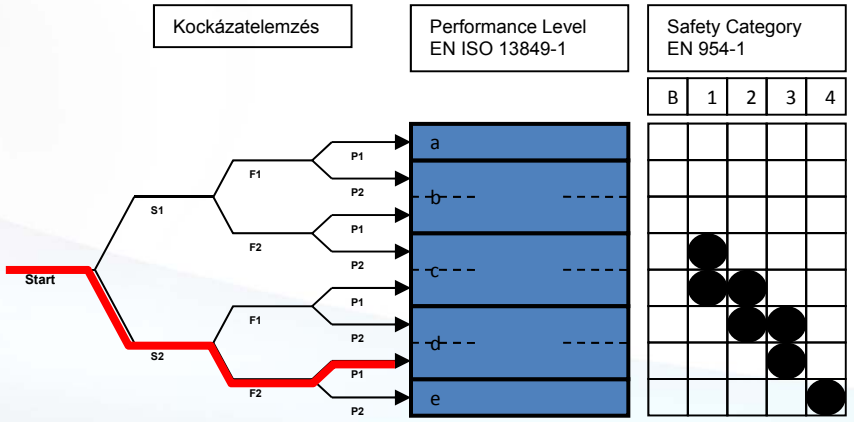
Elkerülési lehetőség

Könnyen elkerülhető, tehát P1

Eredmény

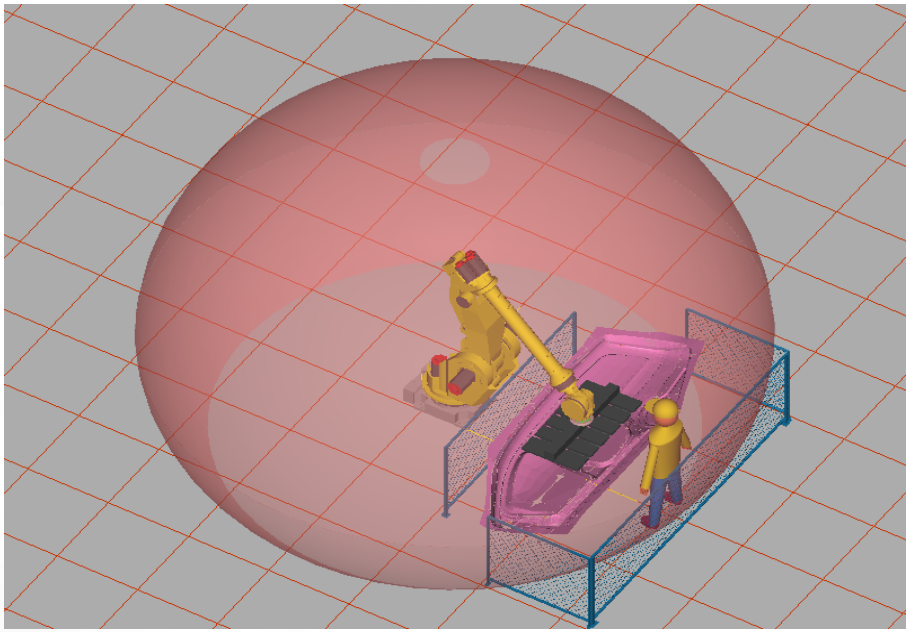
CAT 3 / PL d





Példa

A gépkezelő egy kiszolgálási feladatot lát el, semmi nem akadályozza, hogy ellépjen a robottól.



Szigorúság:

Nagy robot, komoly sérülést okozhat, tehát S2

Gyakoriság

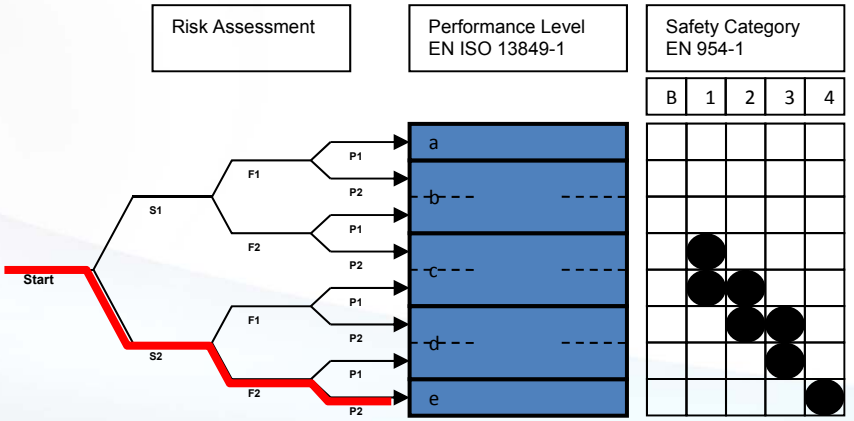
Minden ciklusban, tehát F2

Elkerülési lehetőség

Nehezen elkerülhető, tehát P2

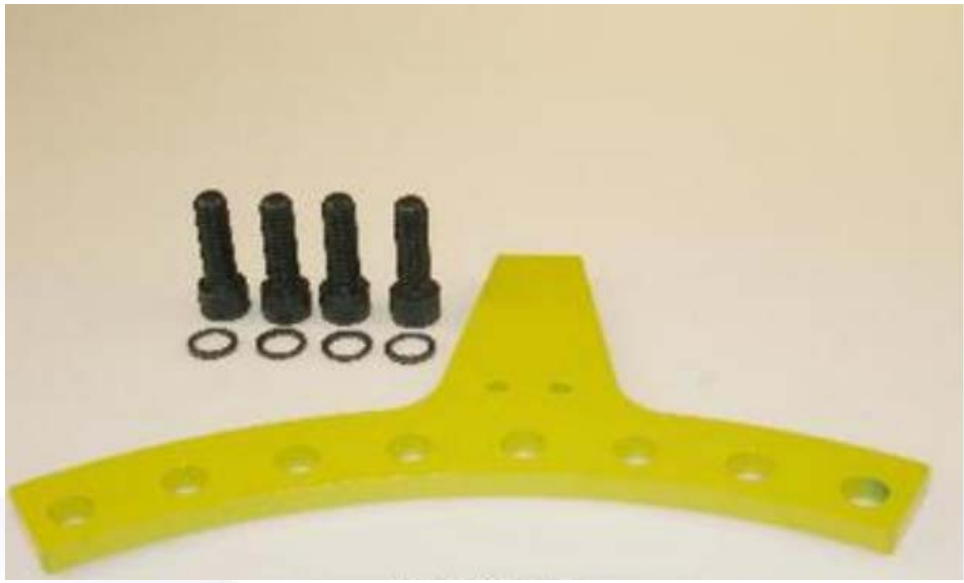
Eredmény

CAT 4 / PL e



Biztonságtechnikai HW elemek

- SW korlátozás (nincs Safety besorolás)
- Mechanikus ütközők

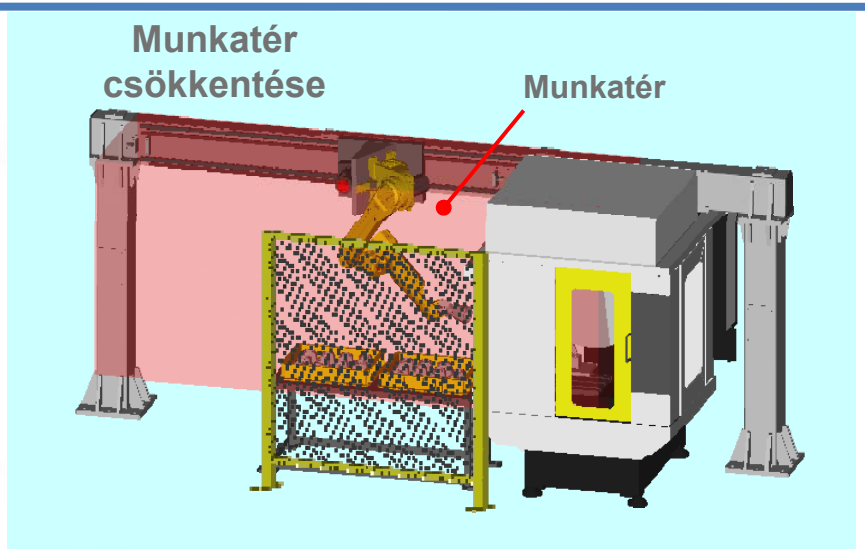


Biztonságtechnikai HW elemek

- SW korlátozás (nincs Safety besorolás)
- Safety végálláskapcsolók

DCS (Dual Check Safety)

- Safety funkció, Safety SW
- DCS Position/Speed check, 3 mozgástípus monitorozása “Safety speed check” ,“Safety zone check”, “T1 mode check”
- TÜV általi biztonsági besorolás (for ISO 13849 & EN954)
- E-Stop, Fence > Cat4, Ple
- DCS > Cat3, Pld
- Biztonsági HW elhagyása költségcsökkenést eredményez



DCS (Dual Check Safety)

- Cat4 > E-Stop, Fence
- Cat3 > DCS (T1 Mode, Joint, Cartesian)
- Jelszavas védelem
- Biztonsági (szabályozott) megállás
- Vészmegállás
- 4 biztonsági bemenet (R-30iA)

TÜVRheinland®

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EL 358.03/09

Prüfgegenstand Product tested	Robot Controller	Zertifikats-inhaber Holder of the certificate	FANUC LTD Oshino-Mura Yamanashi Prefecture 401-0597 Japan
Typbezeichnung Type designation	Dual Check Safety for FANUC SYSTEM R-30iA and FANUC SYSTEM R-30iA Mate	Verwendungs-zweck Intended application	Safety Related Programmable Electronic System for robot control and Emergency-Shut-Down, where the safe state is the de-energized state
Prüfgrundlagen Codes and standards forming the basis of testing	ANSI/RIA R15.06:1999 EN 13849-1:2008 EN 61508 parts 1 to 4:1998		
Prüfungsergebnis Test results	The products described in the test report are suitable for PL=d or PL=e (EN 13849-1) and SIL 2 or SIL 3 (EN 61508) depending on the safety function. The Emergency Stop function fulfils the requirements for Control Reliability (ANSI/RIA R15.06). The Emergency Stop and Safe I/O functions were qualified up to PL=e (EN 13849-1) and SIL 3 (EN 61508), if the conditions of the test report are taken into account.		
Besondere Bedingungen Specific requirements	The contents and requirements stated in the test report and the user manual need to be complied with.		

Der Prüfbericht-Nr. 968/EL 358.03/09 vom 20.08.2009 ist Bestandteil dieses Zertifikates.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen. Es wird ungültig bei jeglicher Änderung der Prüfgrundlagen für den angegebenen Verwendungszweck.

The test report-no. 968/EL 358.03/09 dated 2009-08-20 is an integral part of this certificate.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 00 51, 51101 Köln

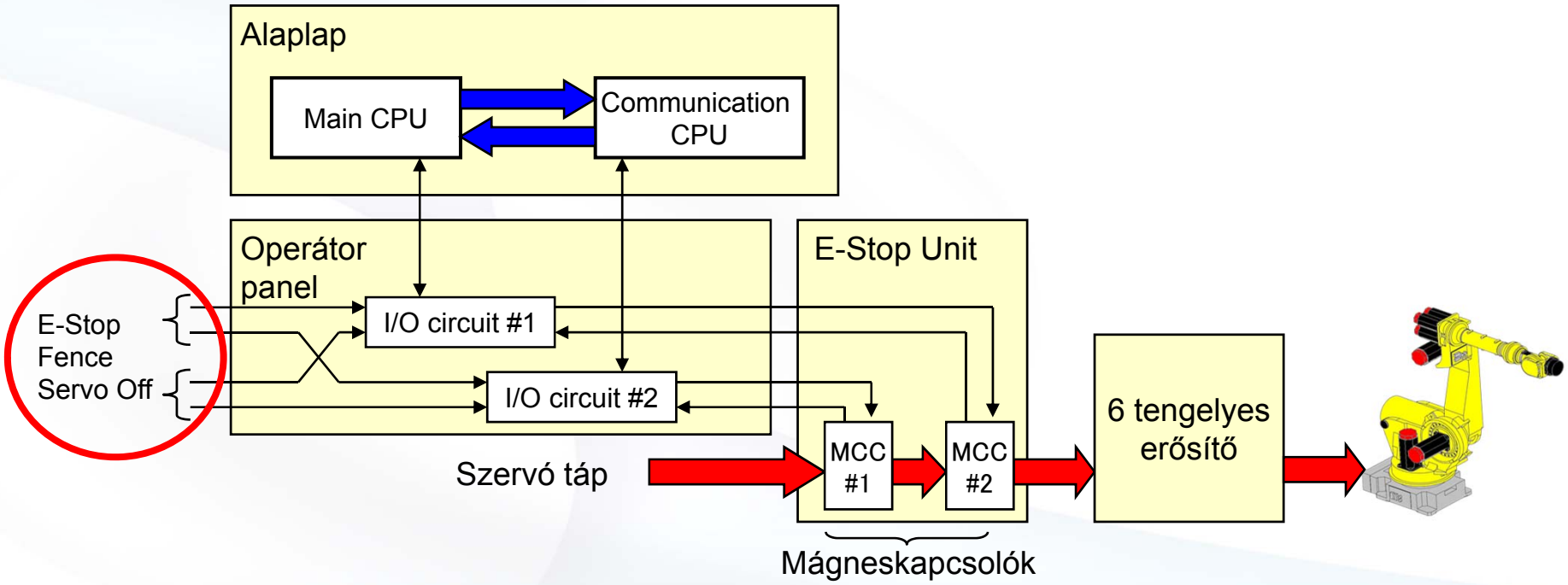
2009-08-20
Datum/Date

Firmenstempel/Company stamp

Dipl.-Ing. Heinz Gall

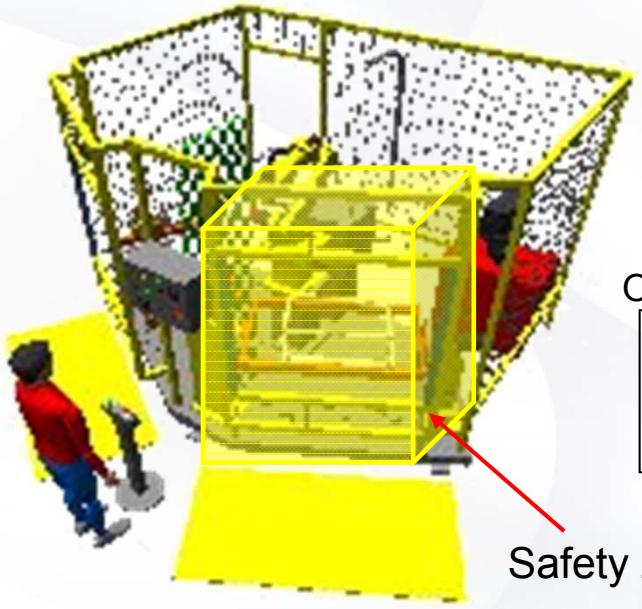
DCS (Dual Check Safety)

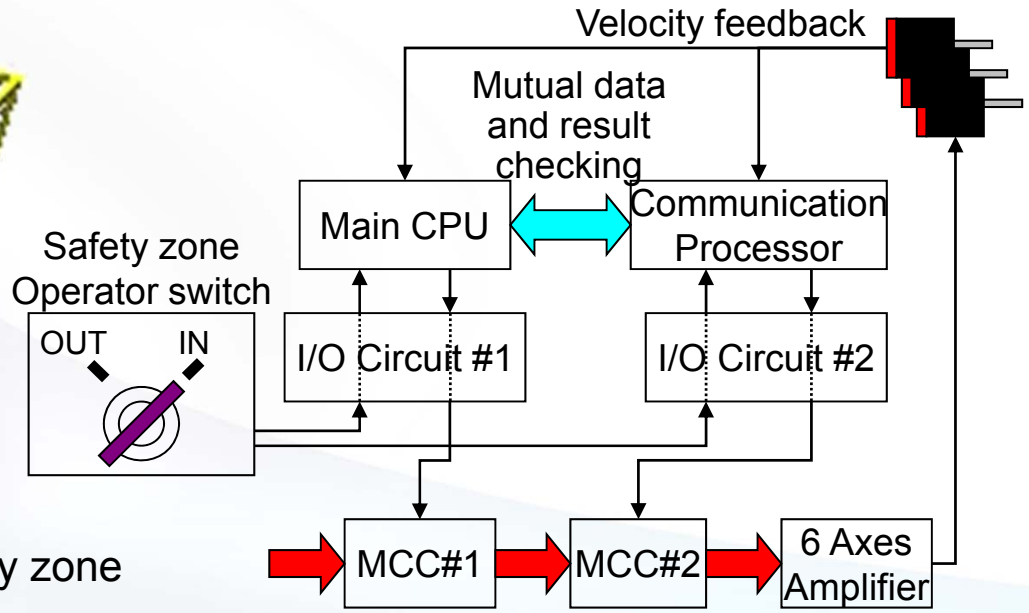
– Dual Check Safety Hardware > Redundáns mágneskapcsolók, I/O-csatornák és CPU-k
  - Fő CPU és kommunikációs CPU.



DCS (Position Checking)

- Biztonsági zóna folytonos monitorozása (2 független processzoron)
- Biztonsági zóna elhagyása azonnali szervóleállítást eredményez
- Cat3

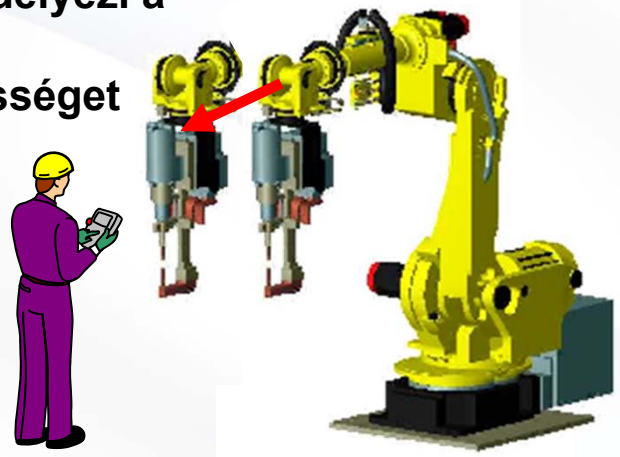




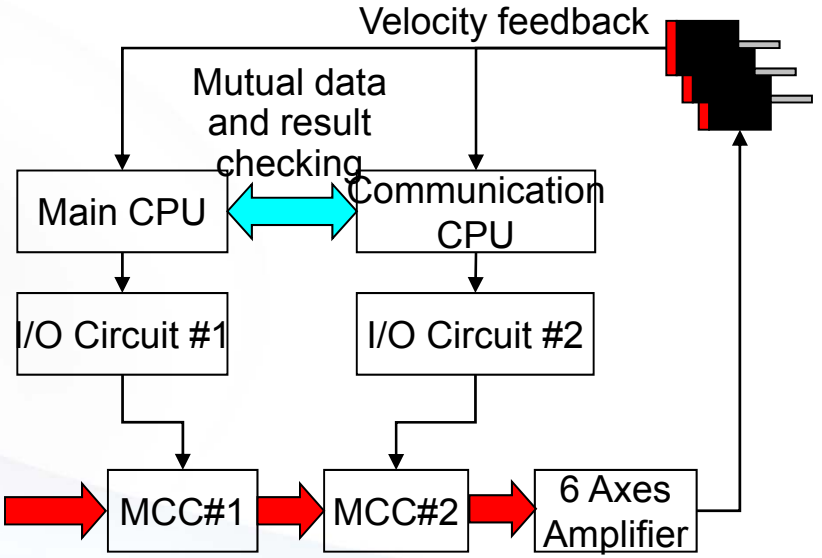
DCS (Speed Check)

- Mozgási sebesség maximalizálása
  - Szervó azonnali leállítása sebesség túllépés esetén
  - Cat3

Nem engedélyezi a nagy sebességet

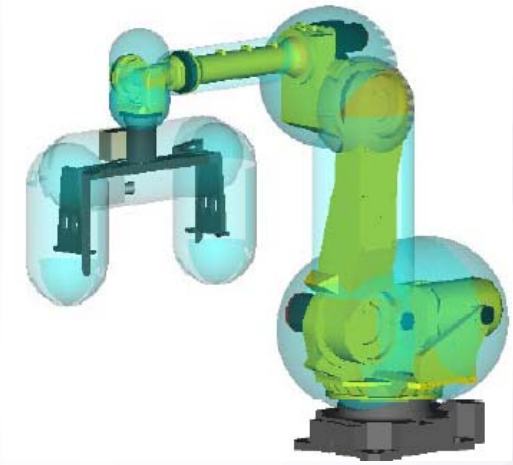


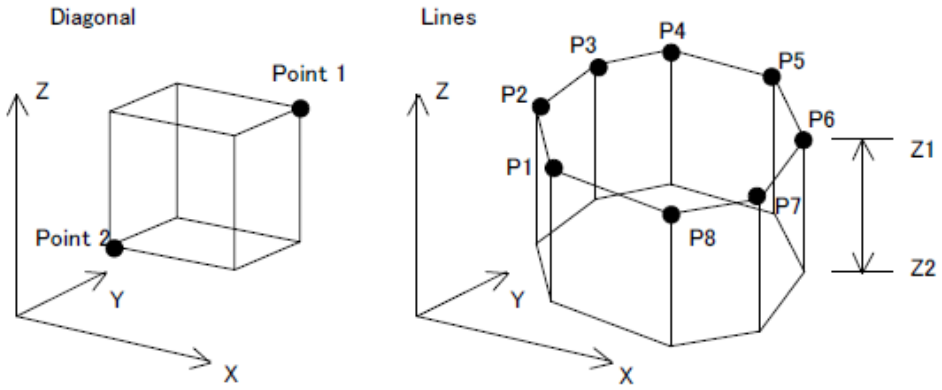
Karbantartás esetén mozgatás



DCS (Shape Models)

- A robotkar, megfogó és egyéb hardverek (gömb, henger és téglatest definiálása)
- **"SRVO-402 DCS Cart. pos. limit„** hiba lép fel, ha definiált robotkar kilép a DCS zónából (azonnali megállás)
- Safety I/O segítségével lehetséges a Positioin Check ki/bekapcsolása
- Biztonsági zónák (téglalap vagy sokszög alapon, Z irányú eltolással)

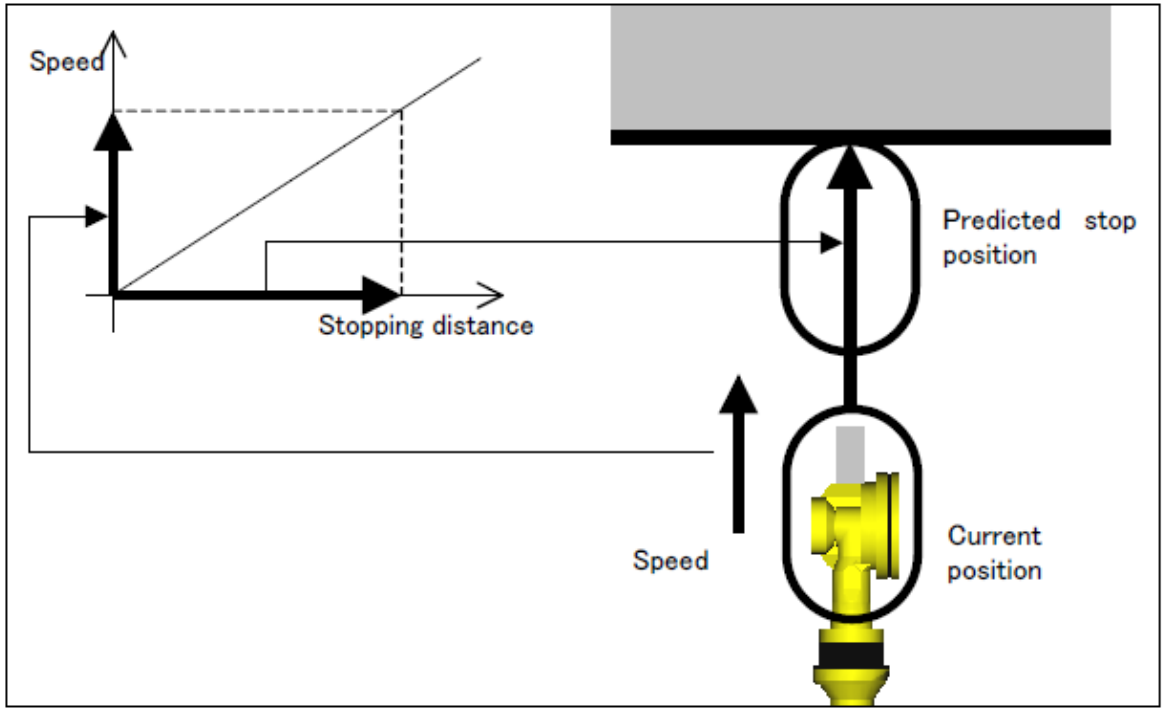




Methods to define a Safe zone

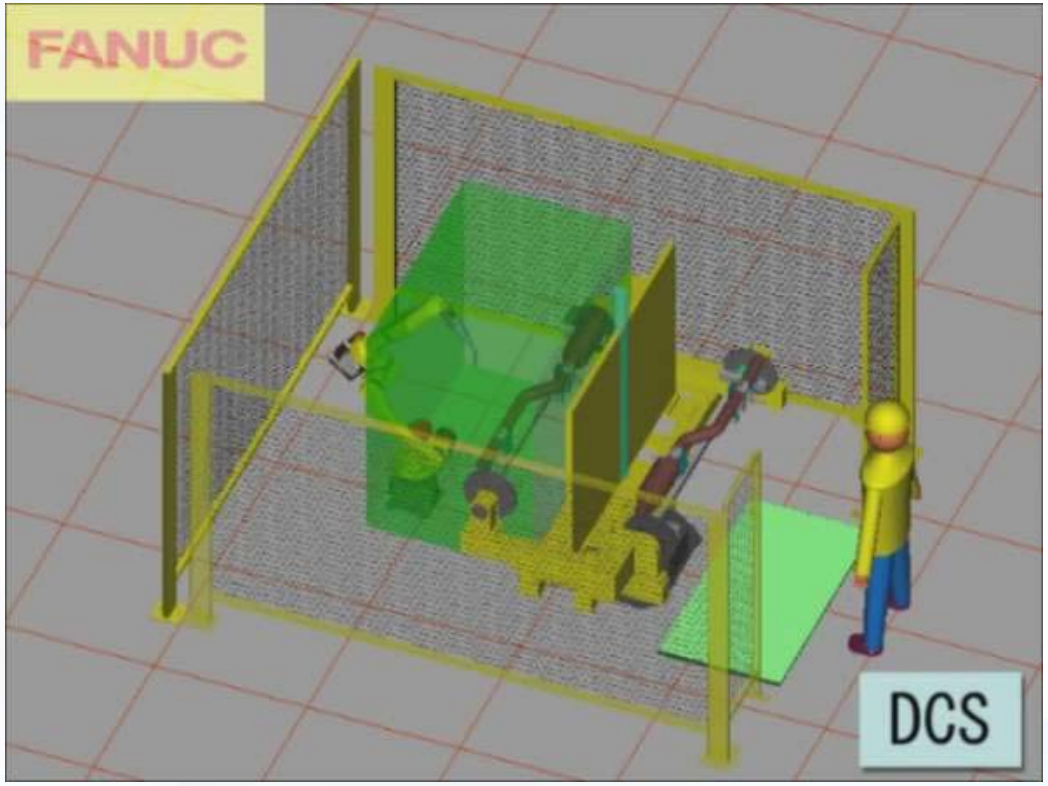
DCS (Shape Models)

- A terhelés, sebesség és megállás típusa szerint definiálhatóak Safety zónák
- A robot időben (ütközés, káresemény előtt) meg tud állni
- Max. 7 mozgáscsoport, külső tengelyeket is beleértve (POS, LIN)



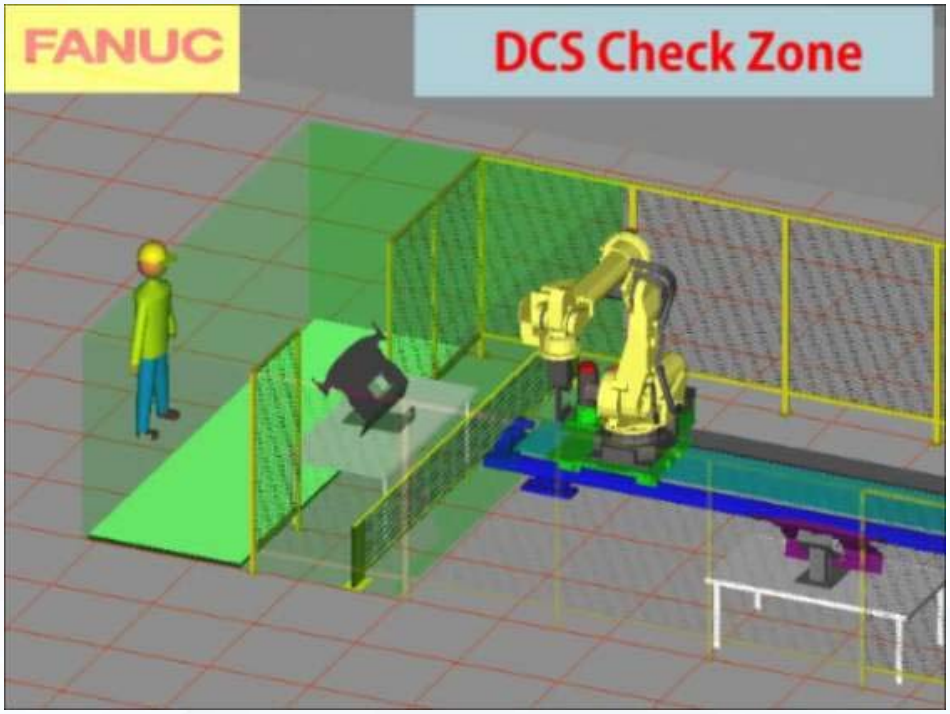
DCS (Példák)

- Forgatóasztal sebesség/poz. felügyelete
  - DCS Speed Check és 1 Safety Input
  - A körasztal sebessége DCS által felügyleve, amikor a gépkezelő a biztonsági szőnyegen áll.



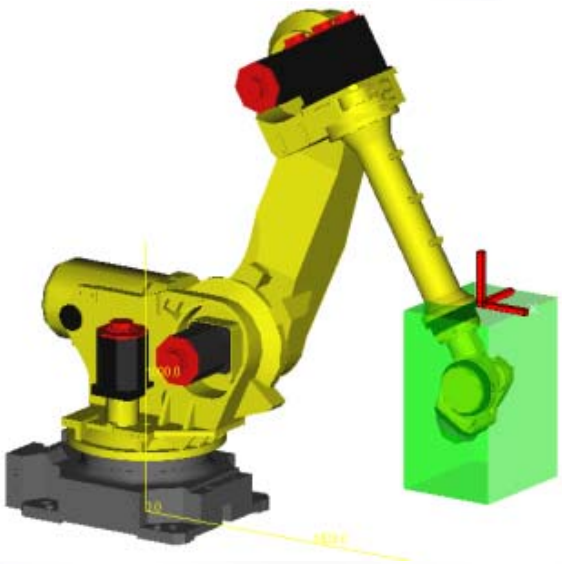
DCS (Példák)

- A robot nem érheti el a dolgozót.
  - Position check és egy safety input
  - Ha a robot a DCS zónában van és a dolgozó a szőnyegre lép, azonnal megáll
  - Biztonságos távolság szavatolt a dolgozó és a robot között.

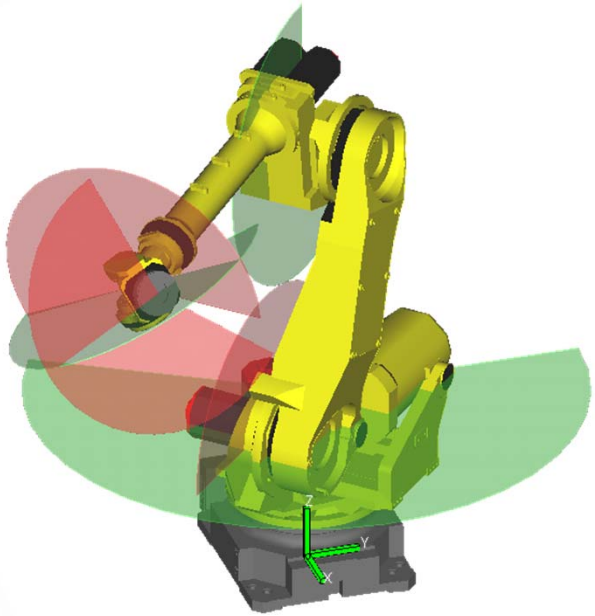


DCS (Példák)

Beállító képernyő



Vizuális Cartesian Safe Zone

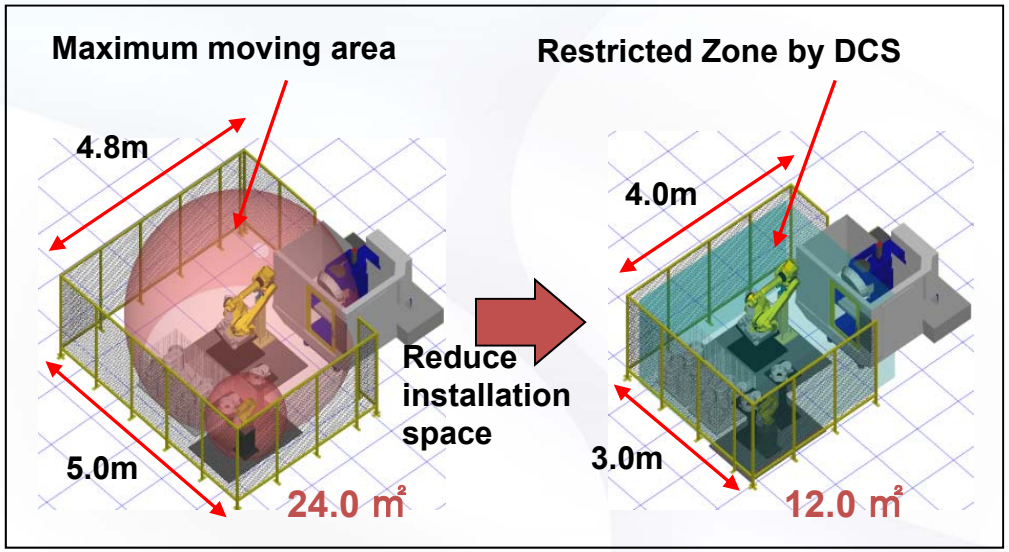


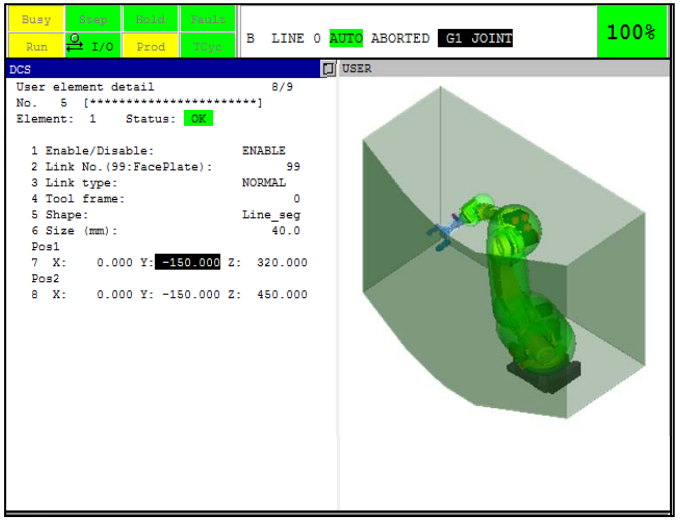
Vizuális Joint Safe Zones

Egyszerű és biztonságos vizuális biztonsági zóna beállítás

DCS (R-30iB)

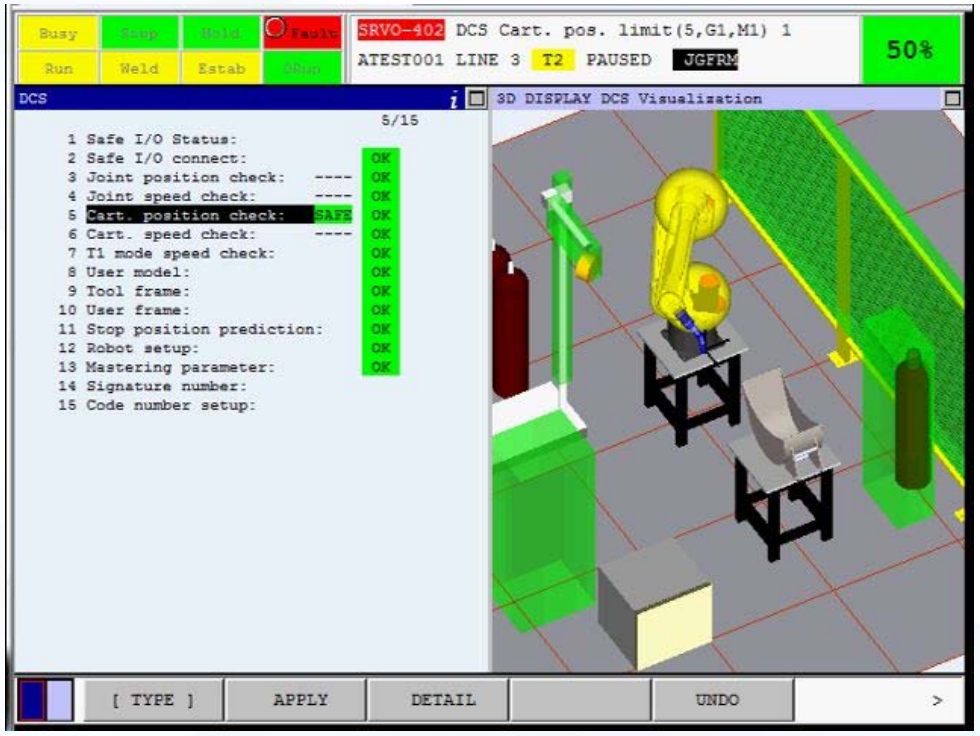
- iPendantról paraméterezhető DCS funkciók.





DCS (R-30iB)

- iPendantról paraméterezhető DCS funkciók.
  - Aktív DCS zónák vizuális megjelenítése
  - Nézőpont mozgatása, zoom, forgatás, Safety I/O megjelenítés
  - Robot mozgás közbeni nyomonkövetése



SZÉCHENYI ISTVÁN EGYETEM
SZE - GYŐR

KÉRDÉS?

Köszönöm a figyelmet!