Wyznaczanie poziomów SIL funkcji bezpieczeństwa urządzeń (SIF)

TR Automatyka Sp z o.o.

Lechicka 14

02-156 Warszawa

POLAND

www.trautomatyka.pl

biuro@trautomatyka.pl

G.M. International s.r.l

Via San Fiorano, 70

20058 Villasanta (Milano)

ITALY

www.gmintsrl.com

info@gmintsrl.com

Standard Definitions

Tytuł IEC 61508: Standard for Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related System

Bezpieczeństwo funkcjonalne elektrycznych / elektronicznych / programowalnych elektronicznych systemów związanych z bezpieczeństwem

Norma IEC 61508 została stworzona w celu określenia i ujednolicenia metod zmniejszenia zagrożeń dla człowieka i / lub zmniejszenia strat dobytku we wszystkich przemysłowych i nieprzemysłowych środowiskach.

Tytuł IEC 61511: Safety Instrumented Systems for the Process Industry

Systemy Automatyki Zabezpieczeniowej dla Procesów Przemysłowych

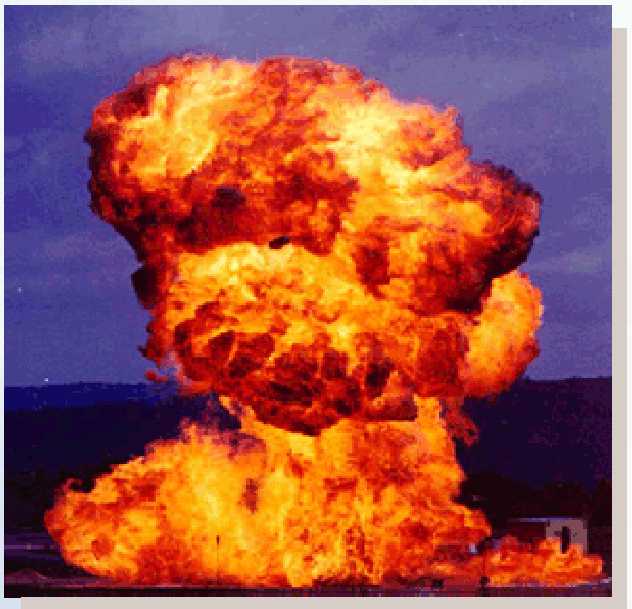
Norma IEC 61511 została stworzona jako rozwinięcie Sektora Procesowego normy IEC 61508.

Spełnienie powyższych standardów jest niezbędnym minimum do zagwarantowania bezpieczeństwa zakładu. On sam nie jest w stanie zagwarantować, że proces będzie bezpieczny.

Zaniechanie realizacji norm bezpieczeństwa z pewnością doprowadzi do wystąpienia niebezpieczeństwa w procesie.

Co oznacza bezpieczeństwo?

“Ograniczenie ryzyka do akceptowalnego poziomu”



Rys. Przykład eksplozji par cieczy (BLEVE)

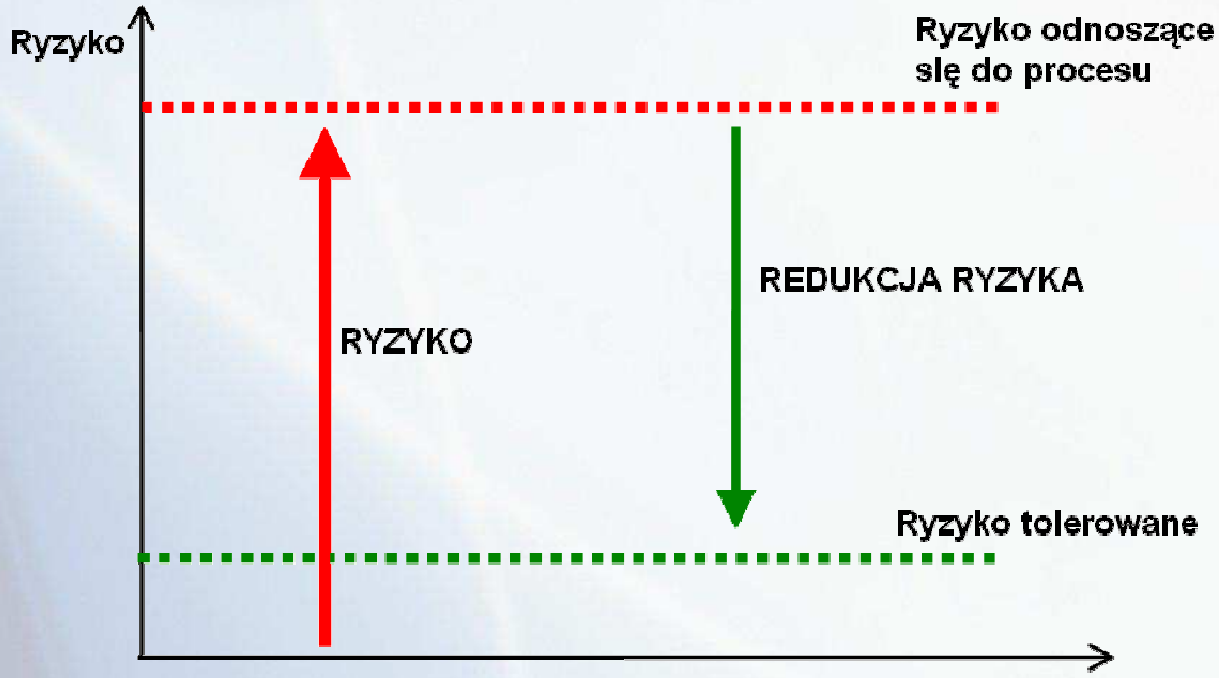
Poziomy Nienaruszalności Bezpieczeństwa IEC 61508

SIL Poziom Nienaru-szalności Bezpie-czeństwa	PFDavg Średnie prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego na rok (tryb pracy na żądanie)	(1- PFDavg) Dyspozycyjn-ość bezpieczeń-stwa	RRF Współczynnik Redukcji Ryzyka	PFDavg Średnie prawdopodobieństwo wystąpienie uszkodzenia niebezpiecznego na godzinę (tryb pracy ciągłej)
SIL 4	≥ 10-5 do 10-4	99.99 do 99.999%	100000 do 10000	≥ 10-9 do 10-8
SIL 3	≥ 10-4 do 10-3	99.9 do 99.99 %	10000 do 1000	≥ 10-8 do 10-7
SIL 2	≥ 10-3 do 10-2	99 do 99.9 %	1000 do 100	≥ 10-7 do 10-6
SIL 1	≥ 10-2 do 10-1	90 do 99 %	100 do 10	≥ 10-6 do 10-5

Tab. Współczynnik redukcji ryzyka, jako funkcja poziomów SIL oraz Dyspozycyjności

Redukcja Ryzyka

$$RRF = \frac{\text{Częst. występowania uszkodzeń w systemie bez ochrony}}{\text{Tolerowana częstość występowania uszkodzeń}} = \frac{1}{PFDavg}$$



Rys. Główna koncepcja redukcji ryzyka

Współczynnik Redukcji Ryzyka (RRF)

- Liczba wypadków na rok bez ochrony: 10
- Liczba tolerowanych wypadków: 1 na 100 lat
- 10 x 100 / 1 = 1000 = RRF
  (Współczynnik Redukcji Ryzyka)
- 1 / 1000 = 0.001 = PFDavg na rok
  (Średnie prawdopodobieństwo wystąpienia uszkodzenia w trybie pracy na żądanie)
- Oznacza to uzyskanie niedostępności bezpieczeństwa funkcji SIF równej 1/1000 w ciągu jednego roku (ok,. 10h)

A.L.A.R.P. baza Norma E51508-5:2001

Obszar Ryzyka Niedopuszczalnego

Ryzyko niedopuszczalne, z wyjątkiem nadzwyczajnych okoliczności

ALARP lub Obszar Ryzyka Dopuszczalnego

Dopuszczamy ryzyko jeśli mamy z tego korzyść.

Ryzyko jest dopuszczalne tylko, jeśli dalsza jego redukcja jest niemożliwa lub jeśli koszty jego zmniejszenia są niewspółmiernie wysokie w stosunku do korzyści.
Im ryzyko jest bardziej zmniejszane, tym proporconalnie mniejsze jest niezbędne wydatkowanie na dalszą jego redukcję, aby spełnić ALARP.
Koncepcja malejących proporconalnie wymaganych nakładów, zobrazowana jest w postaci trójkąta.

Obszar Ryzyka Zasadniczo Akceptowalnego
Brak potrzeby podejmowania działań w celu redukcji ALARP

Niezbędne jest utrzymywanie pewności, że ryzyko pozostanie na tym poziomie

RYZYKO JEST POMIJALNE

Rys. Ryzyko i strefy ALARP

Korzyści / Koszty w strefie ALARP

$$\frac{\text{Korzyści}}{\text{Koszty}} = \frac{F_{NO\,SIS} \times EV_{NO\,SIS} - F_{SIS} \times EV_{SIS}}{COST_{SIS} + COST_{NT}}$$

Gdzie:

- stosunek K/K: Stosunek Korzyści do Kosztów
- $F_{NO\text{-}SIS}$: Częstość niepożądanych zdarzeń bez systemu SIS.
- $EV_{NO\text{-}SIS}$: Wartość spodziewanych całkowitych strat ze zdarzeń bez systemu SIS.
- F_{SIS} : Częstość niepożądanych zdarzeń z systemem SIS.
- EV_{SIS} : Wartość spodziewanych całkowitych strat ze zdarzeń z systemem SIS.
- $COST_{SIS}$: Koszt całkowitego cyklu życia systemu SIS (roczny).
- $COST_{NT}$: Poniesione koszty spowodowane pomyłkami (roczne)

Przykład:

System SIS został zainstalowany w celu ochrony przed ogniem. Podczas pożaru firma poniosła koszty $1,000,000.

Częstość wystąpienia ognia, przed zastosowaniem systemu SIS, została wyznaczona raz na każde 10 lat.

Po zainstalowaniu systemu SIS, spodziewana częstość zdarzenia wynosi raz na 1000 lat i jego roczny koszt wyniesie w przybliżeniu $66.000.

Koszty poniesione pomyłkami są pomijalne (bezpieczna pozycja pracy F&G - bez energii).

Jaki jest stosunek korzyści do kosztów dla projektu F&G?

Relacja Korzyści/Koszty będzie:

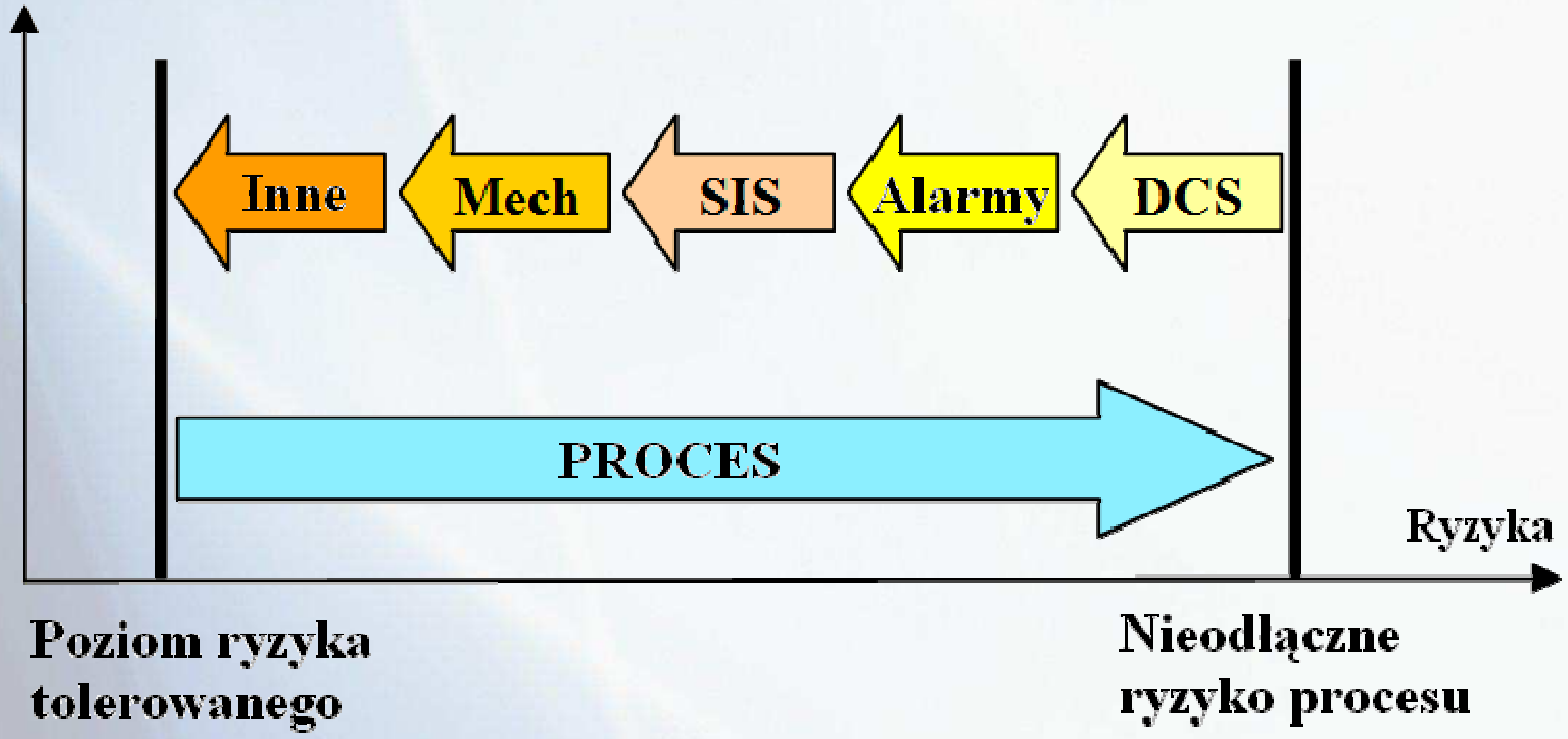
$$\text{Korzyści} = \left(\frac{1}{10} \times 1000000\right) - \left(\frac{1}{1000} \times 1000000\right) = 99000$$

$$\text{Koszty} = (66000 + 0) = 66000$$

$$\frac{\text{Korzyści}}{\text{Koszty}} = \frac{99000}{66000} = 1.5$$

Stosunek Korzyści/Koszty równy 1,5 oznacza, że za każdy zainwestowany $1 w zakładzie, właściciel może spodziewać się $1.5 zysku.

Redukcja Ryzyka z Warstwami Ochrony



Rys. Redukcja ryzyka z kilkoma warstwami ochrony

Warstwy Ochrony

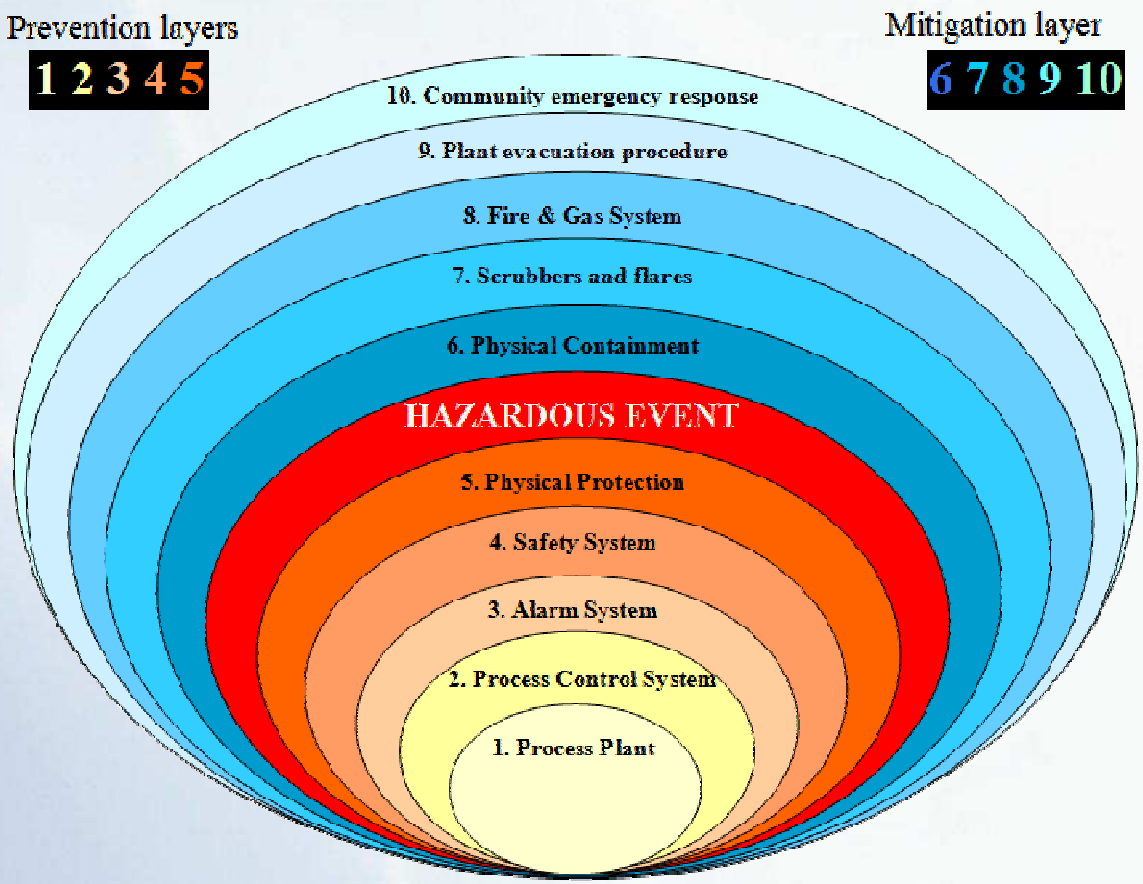
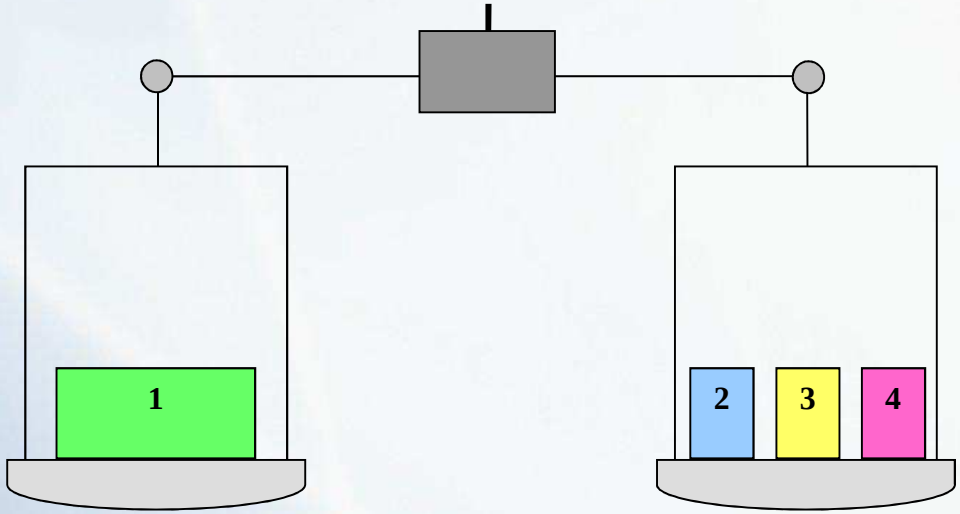


Figure 5, Prevention and mitigation layers of the hazardous event

Wyważenie Ryzyko-Ochrona

Ryzyko musi zostać wyważone poprzez Warstwy Ochronne

(Optymalne Wyważenie Bezpieczeństwa)



RYZYKO

1. Zakład Przemysłowy, Proces i Środowisko

ZAPOBIEGANIE

2. DCS

3. SIS / ESD

4. Fizyczna Ochrona

Niebezpieczne Wydarzenie / Wypadek

Rys. Przykład pożaru zbiornika

Warstwy Łagodzące

- Warstwy łagodzące są wprowadzane w celu redukcji konsekwencji zdarzenia (wypadku), które miało miejsce.
- Mogą one ograniczać, rozpraszać lub neutralizować wyciek niebezpiecznych substancji.

MTBF

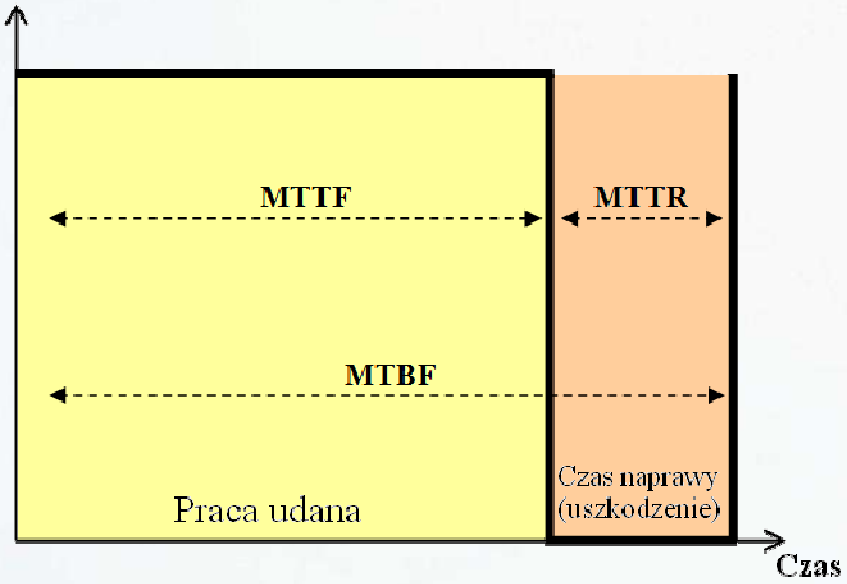
MTTF jest wskaźnikiem średniego czasu poprawnej pracy urządzenia (systemu) przed wystąpieniem uszkodzenia w jakiejkolwiek postaci.

- **MTBF:** Średni Czas Pracy Bezawaryjnej
- **MTBF = MTTF + MTTR**
- **MTTF = MTBF - MTTR**
- **MTTR:** Średni Czas Naprawy Uszkodzenia

- Ponieważ **(MTBF >> MTTR)**

  MTBF ≠ MTTF

  (bardzo bliskie w wartościach)



Rys. Schematyczne przedstawienie czasów MTTF, MTTR, MTBF

MTBF i Współczynnik Uszkodzeń

$$\text{Współczynnik Uszkodzeń} = \lambda = \frac{\text{Ilość uszkodzeń w jednostce czasu}}{\text{Ilość komponentów narażonych na błąd funkcjonalny}}$$

$$\text{MTBF} = \frac{1}{\lambda}$$

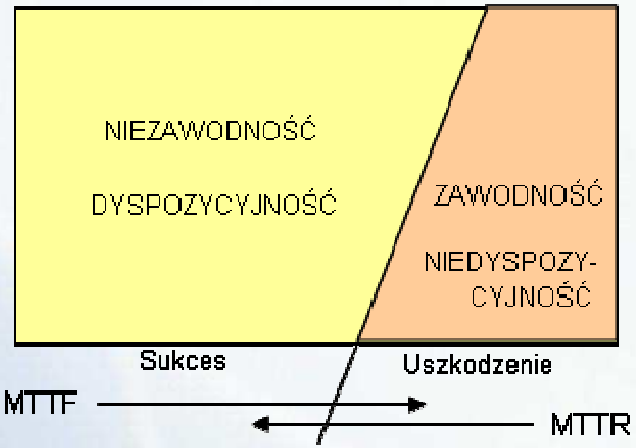


Diagram Venna: Niezawodność-Zawodność;
Dyspozycyjność-Niedyspozycyjność oraz relacje MTTF i MTTR

MTBF i Współczynnik Uszkodzeń

Relacja pomiędzy MTBF i Współczynnikiem Uszkodzeń λ

$$\lambda = \frac{\text{Liczba uszkodzeń w czasie}}{\text{Ilość narażonych urządzeń}} = \frac{1}{\text{MTBF}}$$

$$\text{MTBF} = \frac{1}{\lambda} = \frac{\text{Ilość narażonych urządzeń}}{\text{Liczba uszkodzeń w czasie}}$$

MTBF - Przykład

- Współczynnik uszkodzeń jest zwykle używany jako miara niezawodności.
- Np. 300 Barier pracuje przez 10 lat. Wydarzyły się 3 uszkodzenia. Średni współczynnik uszkodzeń dla bariery wynosi:

$$\lambda = \frac{\text{Liczba uszkodzeń w czasie}}{\text{Ilość narażonych urządzeń}} = \frac{3}{300*10*8760} =$$

= 0.000000038 na godzinę = 0.001 na rok
= 38 FIT (Uszkodzenie na miliard godzin) =
= 38 prawdopodobieństwo uszkodzenia na miliard godzin.
= 0.001 prawdopodobieństwo uszkodzenia na rok

- MTBF = 1 / λ = 1000 lat (dla stałego współczynnika uszkodzeń)

Dyspozycyjność

Czas dyspozycyjności (godz)	Czas naprawy (godz)	Dyspozycyjność (%)
1000	10	99
10000	10	99,9
100000	10	99,99
1000000	10	99,999

- Co oznacza dyspozycyjność 99,99% dla określonego komponentu lub systemu?

  Oznacza, że komponent lub system mógłby przestać pracować raz na..

- .. miesiąc przy czasie naprawy 4.3 minut.
- .. rok przy czasie naprawy 53 minut.
- .. 10 lat przy czasie naprawy 8.8 godzin.

FIT

Uszkodzenia w czasie (FIT). Ilość uszkodzeń na miliard godzin pracy urządzenia.

1 FIT =

= 1 Uszkodzenie na 10^9 godzin

= 10^{-9} Uszkodzeń na godzinę

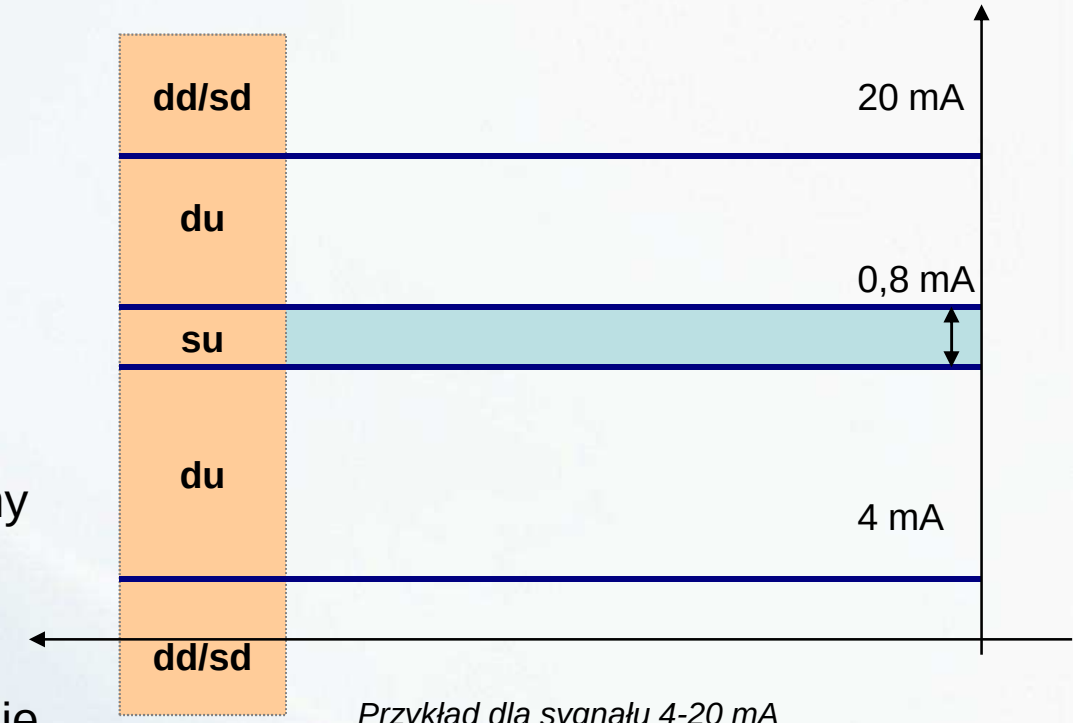
Kategorie Współczynnika Uszkodzeń

λ tot = λ bezpieczny + λ niebezpieczny
λ s = λ sd + λ su
λ d = λ dd + λ du
λ tot = λ sd + λ su + λ dd + λdu

Gdzie:

sd = Bezpieczny wykrywalny
su = Bezpieczny niewykrywalny
dd = Niebezpieczny wykrywalny
du = Niebezpieczny niewykrywalny

λ tot = λ bezpieczny + λ niebezpieczny
(MTBF = MTBFs + MTBFd)
λ bezpieczny: fałszywe wyzwolenie (kłopotliwe wyzwolenie)
λ niebezpieczny: bezpieczne wyzwolenie



Przykład dla sygnału 4-20 mA

Przykład analizy FMEDA

ID	Component type	λ (FIT)	% of failure rate	Simulated failure type	Effect on output signal	λ_{SD} (FIT)	λ_{SU} (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)
C1A	Cond. MC 10 nF 50V 10 % x 7R 0805 SMD	31.8	80 20	Open Short	SD SU	25.4	6.36		
C2A	Cond. MC 10 nF 50V 10 % x 7R 0805 SMD	31.8	80 20	Open Short	DU SU		6.36		15.4
C12A	Cond. MC 10 nF 50V 10 % x 7R 0805 SMD	28.6	80 20	Open Short	DD SU		5.72	22.8	
R48A	Res.TF392KR 1/8 W 1% 100 ppm 0805 SMD	9.6	20 40 15 25	Open Short 0,5 x R 2 x R	SU SD SD SD	 3.88 1.46 2.43	1.94		
R52A	Res. TF 1KR 1/8 W 1% 100 ppm 0805 SMD	9.6	50 50	Open Short	DU DD SU SU		 1.46 2.43	3.88	1.94
T1A	Tras. EF16 1p/1s 45/95 s Vds 90 V Ids 300 mA 2.8/12.6 mH		50 50	Open Short	SD DD	8.9		8.9	
TR5A	Trans. 2N7002 Nmos Vds 60V Ids 300 mA Rds 0,1R SOT23 SMD	25	50 50	Open Short	SD SU	12.5	12.5		
TR7A	Trans. 2N7002 Nmos Vds 60V Ids 300 mA Rds 0,1R SOT23 SMD	25	50 50	Open Short	DU DD			12.5	7.5
IC3A	Integ. TLC272 Ampl. Operaz. SO8 SMD	2.7	40 40 20	Open Short Unstable	SD SU DU		1.08 1.08		15.4 0.054
IC4A	Integ. TLC272 Ampl. Operaz. SO8 SMD	2.7	40 40 20	Open Short Unstable	SU SD DU	1.08	1.08		 0.054
					Total Failure Rates	55.65	40.01	48.16	24.95

Table 31, Example of FMEDA analysis

Analiza i Współczynniki Bezpieczeństwa

Analiza D1014 SIL 3

Separator - zasilacz sygnałów analogowych D1014 kompatybilny z Hart

Table 12: Failure rates

Failure category	Failure rates in FIT
Total FAIL Dangerous Detected	147
Fail Dangerous Detected (internal diagnostics or indirectly)	0
Fail High (detected by the logic solver)	42
Fail Low (detected by the logic solver)	105
Fail Dangerous Undetected	22
No Effect	182
No Part	15
MTBF = MTTF + MTTR	312 years
$MTTF_S = 1/\lambda s$	627 years
$MTTF_D = 1/\lambda du$	5189 years

Table 13: Failure rates according to IEC 61508

Failure rate category	λsd	λsu	λdd	λdu	SFF	DCs	DCd
Rates	0 FIT	182 FIT	147 FIT	22 FIT	93.86%	0%	87%

Table 14: PFDavg values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 9.43 E-05 Valid for **SIL 3**	PFDavg = 4.71 E-04 Valid for **SIL 2**	PFDavg = 9.43 E-04 Valid for **SIL 2**
See Note 4 Section 6	See Note 3 Section 6	See Note 3 Section 6

Udział Uszkodzeń Bezpiecznych (SFF)

$$SFF = \frac{\sum \lambda_{DD} + \sum \lambda_{SD} + \sum \lambda_{SU}}{\sum \lambda_{DD} + \sum \lambda_{DU} + \sum \lambda_{SD} + \sum \lambda_{SU}} = 1 - \frac{\sum \lambda_{DU}}{\sum \lambda_{DD} + \sum \lambda_{DU} + \sum \lambda_{SD} + \sum \lambda_{SU}}$$

SFF	Tolerancja defektów sprzętu (HFT) 0	Tolerancja defektów sprzętu (HFT) 1	Tolerancja defektów sprzętu (HFT) 2
< 60%	SIL 1	SIL 2	SIL3
60% - < 90%	SIL 2	SIL 3	SIL 4
90% - < 99%	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

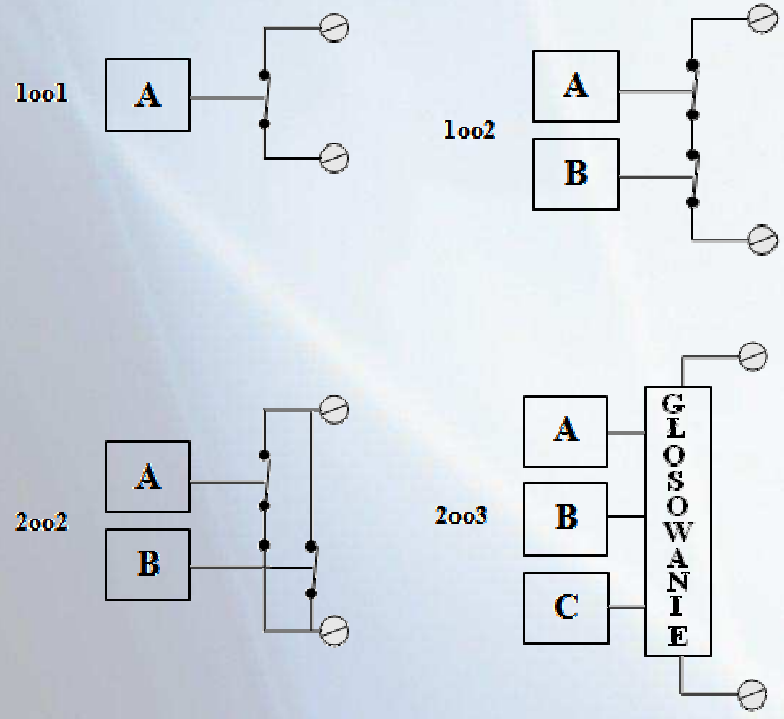
Tab. Udział uszkodzeń bezpiecznych dla komponentów typu A

- Komponenty **Typu A** są opisane jako proste urządzenia z dobrze znanymi rodzajami uszkodzeń i pełną historią pracy.
- Urządzenia **Typu B** są to złożone komponenty z potencjalnie nieznanymi rodzajami uszkodzenia, np. mikroprocesor, ASIC, itd.

SFF	Tolerancja defektów sprzętu (HFT) 0	Tolerancja defektów sprzętu (HFT) 1	Tolerancja defektów sprzętu (HFT) 2
< 60%	Nie dopuszcza się	SIL 1	SIL2
60% - < 90%	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Tab. Udział uszkodzeń bezpiecznych dla komponentów typu B

Architektury systemu



Rys. Schematyczne diagramy niektórych architektur systemu

Architektura	Prawdopod. bezpiecznego uszkodzenia na rok	$MTTF_S$ (lata)	Prawdopod. niebezp. uszkodzenia na rok	$MTTF_D$ (lata)
1oo1	0,0400	25	0,0200	50
1oo2	0,0800	12,5	0,0004	2500
2oo2	0,0016	625	0,0400	25
2oo3	0,0048	208	0,0012	833

Tabela 7, Wpływ redundancji

Uproszczone równania PFDavg

Architecture	PFDavg TI = 1 year	PFDavg TI = 3 years	PFDavg TI = 5 years	PFDavg TI = 10 years
1oo1	$\frac{\lambda_{DU}}{2}$	$3\times\frac{\lambda_{DU}}{2}$	$5\times\frac{\lambda_{DU}}{2}$	$10\times\frac{\lambda_{DU}}{2}$
1oo2	$\frac{\lambda_{DU}^2}{3}$	$9\times\frac{\lambda_{DU}^2}{3}$	$25\times\frac{\lambda_{DU}^2}{3}$	$100\times\frac{\lambda_{DU}^2}{3}$
2oo2	λ_{DU}	$3\times\lambda_{DU}$	$5\times\lambda_{DU}$	$10\times\lambda_{DU}$
2oo3	λ_{DU}^2	$9\times\lambda_{DU}^2$	$25\times\lambda_{DU}^2$	$100\times\lambda_{DU}^2$
1oo3	$\frac{\lambda_{DU}^3}{4}$	$27\times\frac{\lambda_{DU}^3}{4}$	$125\times\frac{\lambda_{DU}^3}{4}$	$1000\times\frac{\lambda_{DU}^3}{4}$
2oo4	λ_{DU}^3	$27\times\lambda_{DU}^3$	$125\times\lambda_{DU}^3$	$1000\times\lambda_{DU}^3$

Tabela. Uproszczone równania dla obliczania PFDavg

Wspólne przyczyny / Współczynnik Beta

Architektura	Równanie uproszczone	Równanie uproszczone ze współczynnikiem β
1oo2	$\frac{1}{3}\times(\lambda_{DU}\times TI)^2$	$\frac{1}{3}\times\left[(1-\beta)\times(\lambda_{DU}\times TI)\right]^2+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$
1oo2D	$\frac{1}{3}\times(\lambda_{DU}\times TI)^2$	$\frac{1}{3}\times\left[(1-\beta)\times(\lambda_{DU}\times TI)\right]^2+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$
2oo2	$\lambda_{DU}\times TI$	$\left[(1-\beta)\times(\lambda_{DU}\times TI)\right]+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$
2oo3	$(\lambda_{DU}\times TI)^2$	$\left[(1-\beta)\times(\lambda_{DU}\times TI)\right]^2+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$
1oo3	$\frac{1}{4}\times(\lambda_{DU}\times TI)^3$	$\frac{1}{4}\left[(1-\beta)\times(\lambda_{DU}\times TI)\right]^3+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$

Dla podsystemów redundancji, w których używane są komponenty elektroniczne, wartość współczynnika **β** wynosi od 1% do 10%.

Drugi człon w równaniach określa udział wartości PFDavg, z powodu obecności **współczynnika β**, wprowadzony poprzez architekturę 1oo1**.**

Przykład: λdu = 0.01 / yr; TI = 1 yr; β = 0.05

Dla 1oo2 równanie na postać:

$$\frac{1}{3}\times\left[(1-\beta)\times(\lambda_{DU}\times TI)\right]^2+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)=$$

$$=\frac{1}{3}\times[0.95\times0.01]^2+\frac{1}{2}\times(0.05\times0.01\times1)=$$

$$=0.00003+0.00025=0.00028/yr$$

Uwzględnienie Współczynnika β

Porównanie użycia różnych wartości współczynnika β:

[PFDavg] 1oo1 = 0.005 / yr	[RRF] 1oo1 = 200
[PFDavg] 1oo2 = 0.00003 / yr (no β factor)	[RRF] 1oo2 = 33.333 = 200 x **166.6**
[PFDavg] 1oo2 = 0.000082 / yr (with 1% β factor)	[RRF] 1oo2 = 12.195 = 200 x **61**
[PFDavg] 1oo2 = 0.00028 / yr (with 5% β factor)	[RRF] 1oo2 = 3571 = 200 x **17.8**
[PFDavg] 1oo2 = 0.000527 / yr (with 10% β factor)	[RRF] 1oo2 = 1897 = 200 x **9.48**

Rozważania:

- Wartość 0.00003 jest 166.6 razy mniejsza niż 0.005.
- Wartość 0.000082 jest 61 razy mniejsza niż 0.005.
- Wartość 0.00028 jest 17.8 razy mniejsza niż 0.005.
- Wartość 0.000527 jest 9.48 razy mniejsza niż 0.005.
- Bez współczynnika β wartość PFDavg, architektury 1oo2, jest 166.6 razy lepsza niż wartość PFDavg architektury 1oo1.
- Z 1% współczynnika β wartość PFDavg, architektury 1oo2, jest 61 razy lepsza niż wartość PFDavg architektury 1oo1.
- Z 5% współczynnika β wartość PFDavg, architektury 1oo2, jest 17.8 razy lepsza niż wartość PFDavg architektury 1oo1.
- Z 10% współczynnika β wartość PFDavg, architektury 1oo2, jest 9.48 razy lepsza niż wartość PFDavg architektury 1oo1.

Obliczanie PFDavg w architekturze 1oo1

Równanie dla pętli w architekturze 1oo1

$$PFDavg\ (T1) = \lambda dd\ *\ RT + \lambda du\ *\ T1/2$$

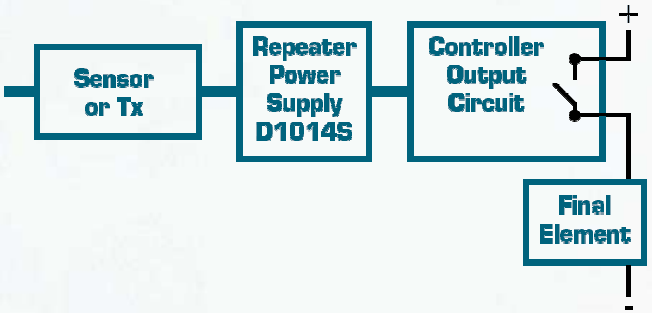
Gdzie:

RT = czas naprawy w godzinach (umownie 8 godzin)

T1 = T-proof, czas pomiędzy funkcjonalnymi testami obwodu (1-5-10 lat)

λ_{dd} = współczynnik uszkodzeń dla uszkodzeń niebezpiecznych wykrywalnych

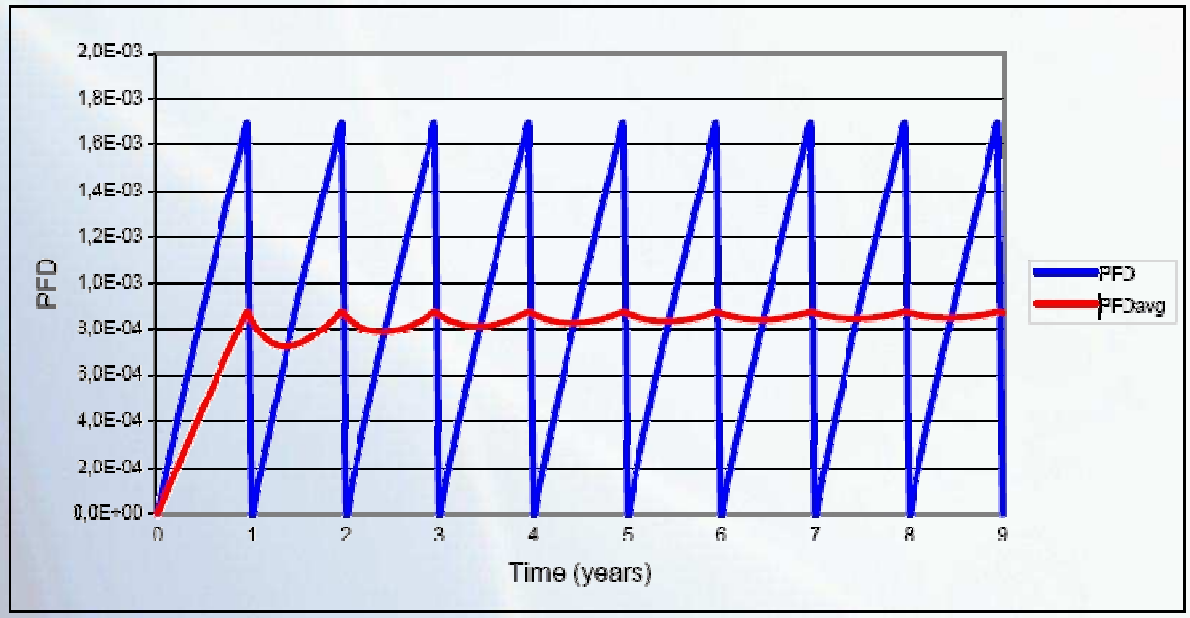
λ_{du} = współczynnik uszkodzeń dla uszkodzeń niebezpiecznych niewykrywalnych



PFD a czas T- proof (TI)

PFD pogarsza się w czasie.

Prawdopodobieństwo uszkodzenia dowolnego wyposażnia (dlatego wyznacza się PFD dla funkcji bezpieczeństwa uszkodzeń SIF), wzrasta z czasem (liniowo dla stałego współczynnika uszkodzeń).



Jak PFD zmienia się w czasie

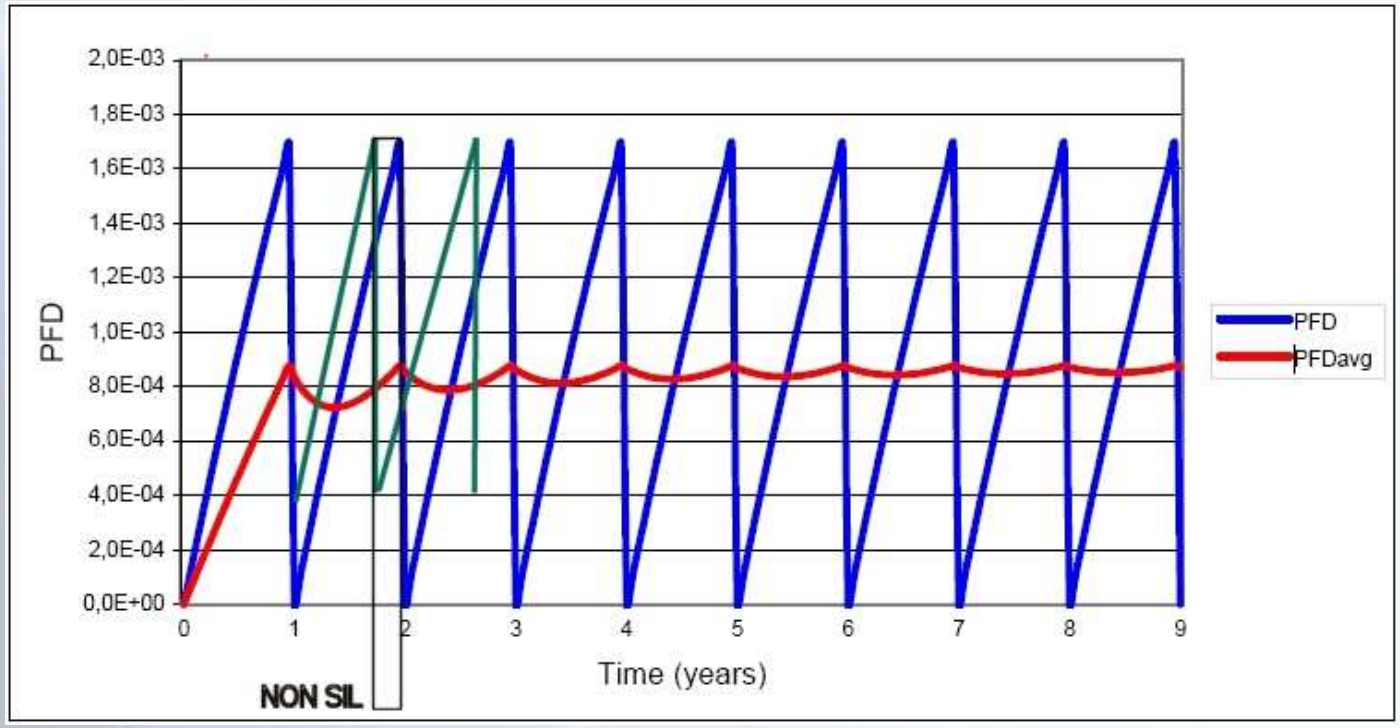
- Ponieważ PFD wzrasta z czasem, jego wartość może być utrzymywana pod kontrolą poprzez wprowadzanie testów sprawdzających w pewnych odstępach czasu.

- Okresowy test z przedziałem T-proof (określonym przez producenta), umożliwia identyfikację każdego niebezpośrednio wykrywalnego uszkodzenia w sprzęcie (błędy niebezpieczne niewykrywalne).

- Stopień skuteczności testu wpływa na wartość, do której jest następnie przywracany PFDavg.

Jak PFD zmienia się w czasie

Jeżeli efektywność wynosi (99-100%) wyposażenie jest traktowane “jak nowe”, z punktu widzenia prawdopodobieństwa błędu, jeżeli jest niższa niż 100% (70-80-90%), to poziom SIL może być nieaktualny i nie osiągać wymaganego poziomu SIL.



Test okresowy dla D1014 – 50%

Test okresowy (Proof test) 1: Zawiera następujące kroki, opisane w poniższej tabeli 57.

Tabela 57: Kroki dla testu okresowego 1.

Krok	Działanie
1	Wykonaj bypass sterownika bezpieczeństwa PLC lub wykonaj inne działania, zapobiegające wystąpieniu fałszywego wyzwolenia.
2	Wyślij komendę HART do modułu, ustawiającą wysoki alarm na wyjściu prądowym i zweryfikuj czy sygnał analogowy osiągnął zadaną wartość. Test ten sprawdza, czy występują problemy związane z niskim napięciem zasilania pętli oraz wzrastającą rezystancją okablowania.
3	Wyślij komendę HART do modułu, ustawiającą niski alarm na wyjściu prądowym i zweryfikuj czy sygnał analogowy osiągnął zadaną wartość. Test ten sprawdza możliwość wystąpienia prądów spoczynkowych, mających związek z uszkodzeniem.
4	Przywróć pętlę do pełnej funkcjonalności.
5	Usuń bypass ze sterownika bezpieczeństwa PLC i przywróć układ do normalnej pracy.

Test ten wykrywa w przybliżeniu 50% możliwych „du” uszkodzeń w module.

Test okresowy dla D1014 – 99%

Test okresowy (Proof test) 2: Zawiera następujące kroki, opisane w poniższej tabeli 58.

Tabela 58: Kroki dla testu okresowego 2.

Krok	Działanie
1	Wykonaj bypass sterownika bezpieczeństwa PLC lub wykonaj inne działania, zapobiegające wystąpieniu fałszywego wyzwolenia.
2	Powtórz kroki 2 i 3 z testu okresowego 1 (tabela 57).
3	Wykonaj dwupunktową kalibrację (np. dół i góra skali) podłączonego przetwornika i zweryfikuj czy wartość wyjścia prądowego utrzymuje się we właściwych wartościach.
4	Przywróć pętlę do pełnej funkcjonalności.
5	Usuń bypass ze sterownika bezpieczeństwa PLC i przywróć układ do normalnej pracy.

Test ten wykrywa w przybliżeniu 99% możliwych „du” uszkodzeń w module.

“Waga” PFDavg w SIF

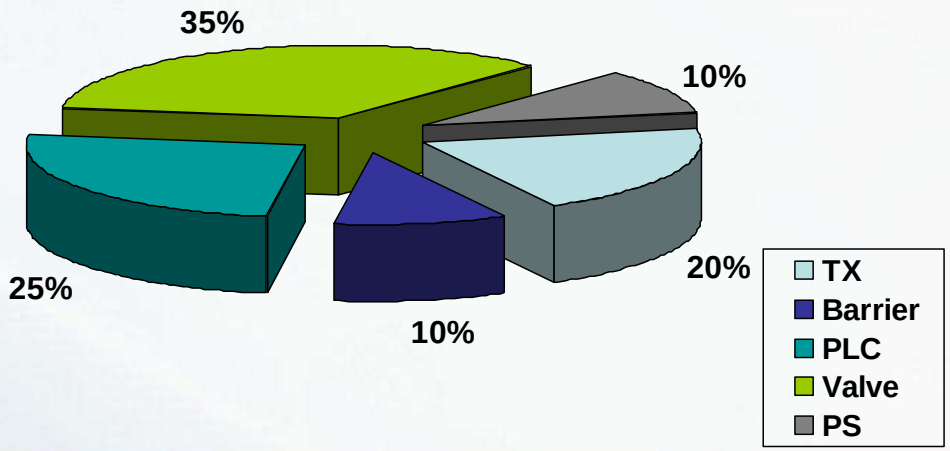
Dla każdego systemu PFDavg jest wartością procentową w odniesieniu do całości.

Wytwórcy podzespołów podają w swoich materiałach wartość współczynnika bezpieczeństwa PFDavg uzyskaną od instytucji certyfikujących (TUV, EXIDA, FM, itp.)

Instytucje te stosują konwencjonalne “wagi” PFDavg komponentu jako rezultatu ważności tego komponentu w całej pętli, co pokazano w następującej tabeli:

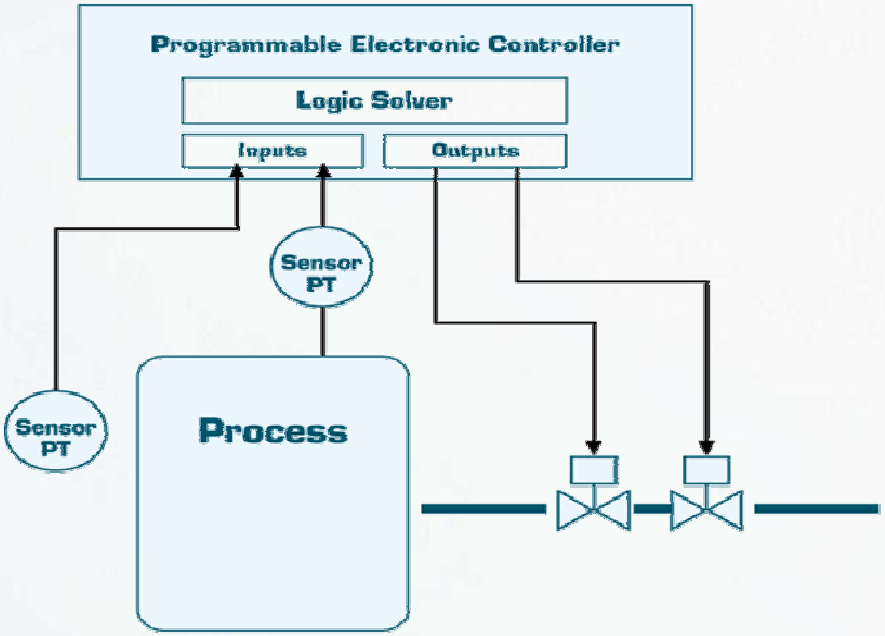
Subsystem	PFDavg 1oo1 (%)
Transmitter	20 %
Barrier	10 %
PLC	25 %
Valve	35 %
Power Supply	10%
Total (SIF)	100 %

Table 5, PFDavg “weighing” for 1oo1 system architecture



Safety Instrumented Systems (SIS)

- Prosty SIS, oparty o jeden układ logiczny, spełnia funkcję bezpieczeństwa pokazaną na rysunku.
- Na SIS składa się wiele funkcji SIF: po jednej na każdy warunek bezpieczeństwa.
- Jego zadaniem jest zbieranie i analiza danych z czujników dla określenia, czy wystąpiło uszkodzenie niebezpieczne i w konsekwencji uruchomienie sekwencji czynności przenoszących proces do stanu bezpiecznego.
- Potencjalna możliwość wystąpienia uszkodzenia niebezpiecznego jest nazywana „żądaniem“.

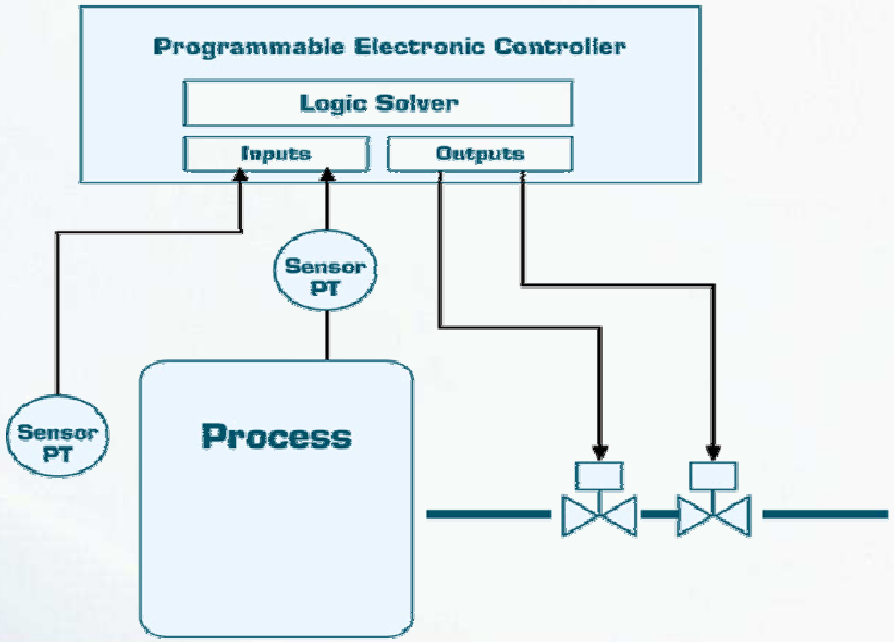


Safety Instrumented Systems (SIS)

- Większość systemów SIS jest oparta na koncepcji odcinania zasilania po wystąpieniu zdarzenia. W warunkach normalnej pracy wejścia i wyjścia są zasilane. (w systemach F&G jest odwrotnie)

- Dla każdej SIF, wyznaczany jest Współczynnik Redukcji Ryzyka (RRF).

- IEC 61508 and IEC 61511, to rozpoznawane standardy, określające wymogi bezpieczeństwa.



Obliczanie PFDavg w architekturze 1oo1

Równanie dla pętli w architekturze 1oo1

$$PFDavg\ (T1) = \lambda dd\ *\ RT + \lambda du\ *\ T1/2$$

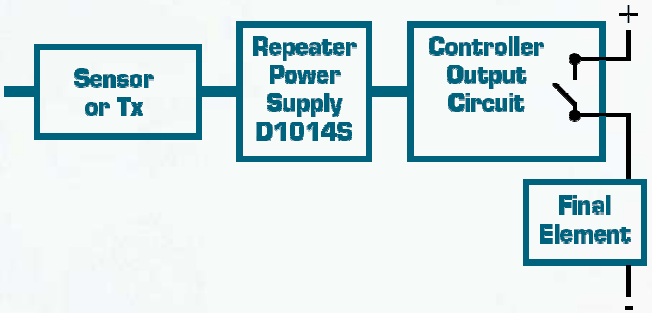
Gdzie:

RT = czas naprawy w godzinach (umownie 8 godzin)

T1 = T-proof, czas pomiędzy funkcjonalnymi testami obwodu (1-5-10 lat)

λ_{dd} = współczynnik uszkodzeń dla uszkodzeń niebezpiecznych wykrywalnych

λ_{du} = współczynnik uszkodzeń dla uszkodzeń niebezpiecznych niewykrywalnych



Obliczanie Pętli PFD_{avg}

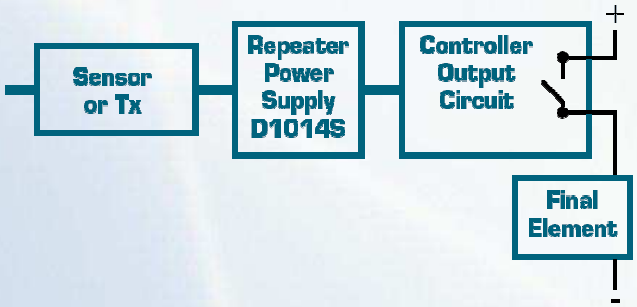
$$PFDavg\ (T1) = \lambda dd * RT + \lambda du * T1/2$$

Jeśli T1 = 1 rok, wtedy

$$PFDavg = \lambda dd * 8 + \lambda du * 4380$$

ale λ_{dd} * 8 jest dużo mniejsze niż λ_{du} * 4380

$$PFDavg = \lambda du * T1/2$$

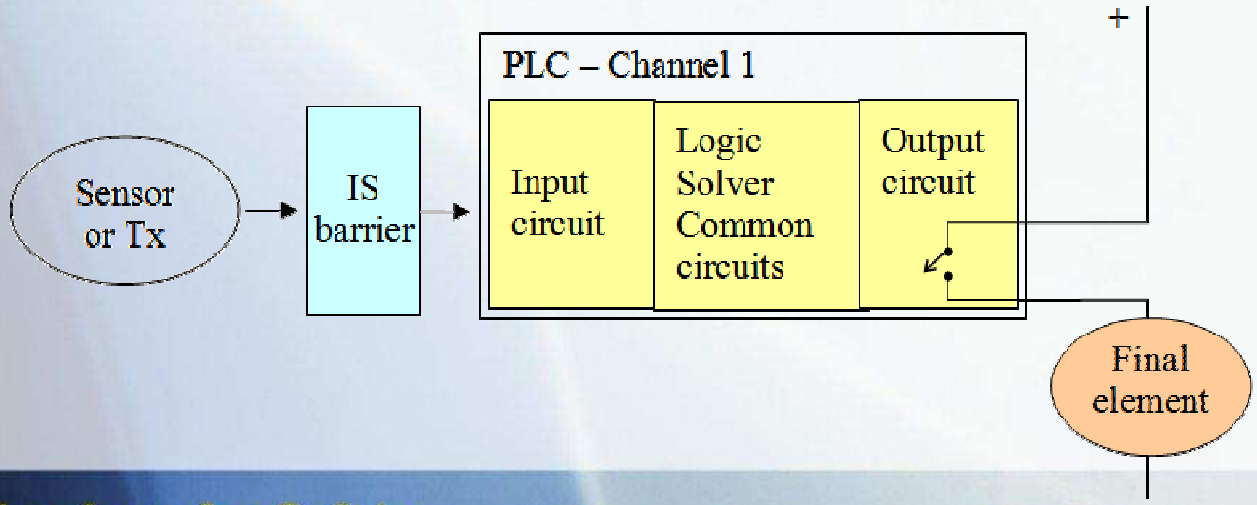


Przykład SIF

Wyliczone wartości MTBF, PFDavg, RRF dla możliwego poziomu SIL danej SIF.

Poniższe wartości podawane są przez wytwórców:

Tx:	MTBF = 102 lata;	λDU = 0,00080 / r;	λDD = 0,0010 / r;	λS = 0,00800 / r
Bariera:	MTBF = 314 lat;	λDU = 0,00019 / r;	λDD = 0,0014 / r;	λS = 0,00159 / r
PLC:	MTBF = 685 lat;	λDU = 0,00001 / r;	λDD = 0,0001 / r;	λS = 0,00135 / r
Zasilacz:	MTBF = 167 lat;	λDU = 0,00070 / r;	λDD = 0,0000 / r;	λS = 0,00530 / r
Zawór:	MTBF = 12 lat;	λDU = 0,02183 / r;	λDD = 0,0200 / r;	λS = 0,0400 / r



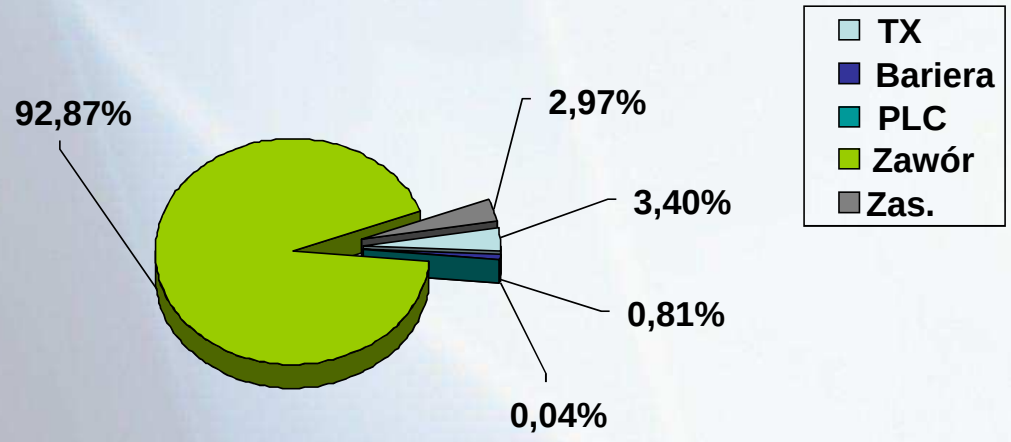
Tablica podsumowująca dla SIL 1

Pod-system	MTBF (rok)	λ / rok = 1/MTBF	MTBFs= 1/ λ_S (rok)	λ_S / rok	λ_{DD} /rok	λ_{DU} / rok	PFDavg 1oo1 = $\lambda_{DU}/2$	% całk. PFDavg	RRF = 1/PFDavg	SFF	Poziom SIL
Tx	102	0.00980	125	0.00800	0.0010	0.00080	0.000400	3.40 %	2500	91.8 %	SIL 2
Bariera D1014S	314	0.00318	629	0.00159	0.0014	0.00019	0.000095	0.81 %	10526	94.0 %	SIL 3
PLC	685	0.00146	741	0.00135	0.0001	0.00001	0.000005	0.04 %	200000	99.3 %	SIL 3
Zawór *	12	0.08333	24	0.04150	0.0200	0.02183	0.010915	92.87 %	92	73.8 %	SIL 1
Zasilacz	167	0.00600	189	0.00530	0.0000	0.00070	0.000350	2.97 %	2857	88.3 %	SIL 3
Razem (SIF)	**10**	**0.10377**	**17**	**0.05774**	**0.0225**	**0.02353**	**0.011765**	**100 %**	**85**	**-**	**SIL 1**

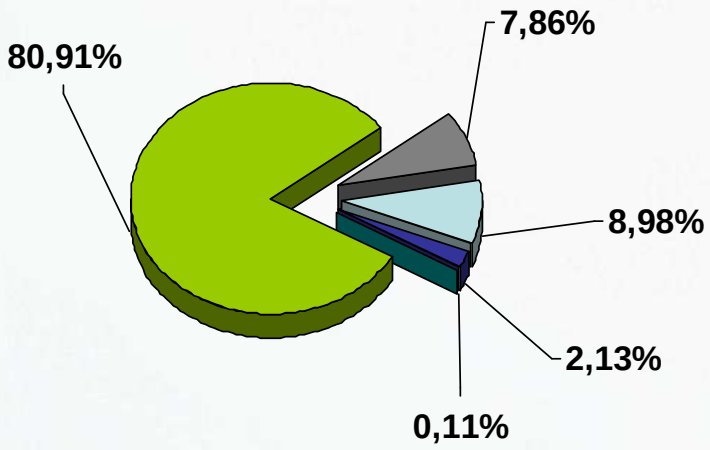
Tablica podsumowująca dla SIL 2

Pod-system	MTBF (rok)	λ = 1/MTBF na rok	MTBFs= 1/ λ_S (rok)	λ_S / rok	λ_{DD} / rok	λ_{DU} / rok	PFDavg 1oo1 = $\lambda_{DU}/2$	% całkowit. PFDavg	RRF = 1/PFDavg	SFF	Poziom SIL
Tx	102	0.00980	125	0.00800	0.0010	0.00080	0.000400	8.98 %	2500	91.8 %	SIL 2
Bariera D1014S	314	0.00318	629	0.00159	0.0014	0.00019	0.000095	2.13 %	10526	94.0 %	SIL 3
PLC	685	0.00146	741	0.00135	0.0001	0.00001	0.000005	0.11 %	200000	99.3 %	SIL 3
Zawór 4 Months TProof	36	0.02750	73	0.01370	0.0066	0.00720	0.003602	80.91 %	278	73.8 %	SIL 2
Zasilacz	167	0.00600	189	0.00530	0.0000	0.00070	0.000350	7.86 %	2857	88.3 %	SIL 3
Razem (SIF)	**21**	**0.04794**	**33**	**0.02994**	**0.00910**	**0.00890**	**0.004452**	**100 %**	**225**	**-**	**SIL 2**

SIF Zestawienie PFDavg



SIL 1



SIL 2

Tablica testowa dla SIL 2 SIF

Dla tej funkcji SIF i poziomu integralności bezpieczeństwa SIL 2 okresowe testy sprawdzające powinny być wykonywane zgodnie z poniższą tabelą:

Podsystem	T-proof test time interval
Przekaźnik	1 rok
Bariera	10 lat
PLC	20 lat
Zawór	4 miesiące

SIF Przykład 2

Wyliczone wartości MTBF, PFDavg, RRF dla możliwego poziomu SIL danej SIF.

Poniższe wartości podawane są przez wytwórców:

Tx:	MTBF = 102 lata;	λDU = 0,00080 / r;	λDD = 0,0010 / r;	λS = 0,00800 / r
Bariera:	MTBF = 314 lat;	λDU = 0,00019 / r;	λDD = 0,0014 / r;	λS = 0,00159 / r
PLC:	MTBF = 685 lat;	λDU = 0,00001 / r;	λDD = 0,0001 / r;	λS = 0,00135 / r
Zasilacz:	MTBF = 167 lat;	λDU = 0,00070 / r;	λDD = 0,0000 / r;	λS = 0,00530 / r
Zawór:	MTBF = 12 lat;	λDU = 0,02183 / r;	λDD = 0,0200 / r;	λS = 0,00400 / r

Zastosowano te same dane dla architektury 1oo1 co w pierwszym przykładzie, ale wprowadzono współczynnik β równy 5% (0.05) dla podsystemów redundantnych.

Tabela 1oo2

Podsystem	PFDavg 1oo1	RRF 1oo1	MTBF 1oo1		PFDavg 1oo2[1]	RRF 1oo2	MTBF 1oo2	SFF	SIL Level
Tx *	0.000400	2500	125		0.00002019	49528	62.5	91.8 %	SIL 3
Bariera D1014D *	0.000095	10526	629		0.00000476	210051	314.4	94.0 %	SIL 4
PLC	0.000005	200000	741		0.00000500	200000	741	99.3 %	SIL 3
Zawór *	0.010915	92	24		0.00068768	1454	12	73.8 %	SIL 3
Zasilacz *	0.000350	2857	189		0.00001765	56670	94.3	88.3 %	SIL 3
Razem (SIF)	**0.011765**	**85**	**17**		**0.00073528**	**1360**	**8.5**	**-**	**SIL 3**

Tabel podsumowująca - architektura 1oo2

Uwaga 1:

Powyższa tabela ukazuje przewagę architektury 1oo2 względem 1oo1. Poziom integralności bezpieczeństwa dla funkcji SIF przesunął się z SIL 1 do SIL 3 przy utrzymaniu tego samego przedziału testów okresowych 1 rok.

Uwaga 2:

Przy zastosowaniu takiej konfiguracji systemu silnie wzrasta współczynnik redukcji ryzyka. Jeżeli wymagany jest poziom SIL 2 zamiast SIL 3, to można wydłużyć okres między testami (TI).
Tabela 10 pokazuje, jak 1oo2 SIF zmieniałby się dla TI = 3, 5 i 10 lat.

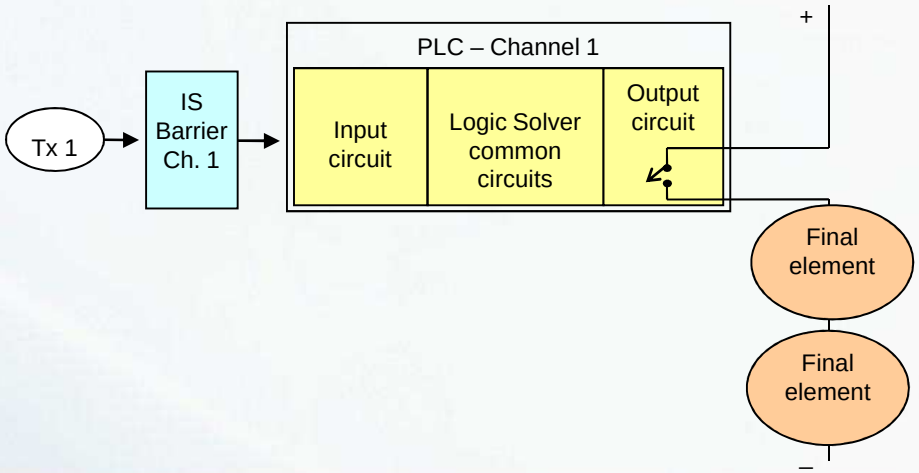
Tabela 10 - pokazuje, jak architektura 1oo2 funkcji SIF zmieniałby się dla TI = 3,5 i 10 lat.

System	PFDavg 1oo2	RRF	Max SIL
$1oo2\|_{TI=1}$	0.00073528	**1360**	**SIL 3**
$1oo2\|_{TI=3}$	0.00220582	**453**	**SIL 2**
$1oo2\|_{TI=5}$	0.003676377	**272**	**SIL 2**
$1oo2\|_{TI=10}$	0.007352755	**136**	**SIL 2**

Architektura 1oo2, tylko dla elementów wykonawczych

Podsystem	PFDavg 1oo1	RRF 1oo1	MTBF 1oo1		PFDavg 1oo2 (tylko zawór)	RRF	MTBF	SFF	Poziom SIL
Tx	0.000400	2500	125		0.000400	2500	125	91.8 %	SIL 2
Bariera D1014D	0.000095	10526	629		0.000095	10526	629	94.0 %	SIL 3
PLC	0.000005	200000	741		0.000005	200000	741	99.3 %	SIL 3
Zawór	0.010915	92	24		0.00068768	1454	12	73.8 %	SIL 3
Zasilacz	0.000350	2857	189		0.00001765	56670	189	88.3 %	SIL 2
Razem (SIF)	**0.011765**	**85**	**17**		**0.00120533**	**829**	**10**	**-**	**SIL 2**

Redundancja zaworów pozwala funkcji SIF osiągnąć poziom SIL 2 z bardziej niż satysfakcjonującą wartością RRF.



Architektura 1oo2, element finalny

- Dodanie redundancji zaworu, założony współczynnik β = 5%, RRF = 1454.
- Wartość PFDavg wynosi teraz 1/1454 = 0.00068, dla testu okresowego z interwałem 1 rok (SIL3).

Rozważania:

Regulacja czasu T-proof i redundancja elementu finalnego, umożliwia uzyskanie lepszego poziomu SIL w całkowitej funkcji SIF, nawet uzyskanie poziomu SIL3.

Tabela podsumowująca - 1oo2, element finalny

Uwaga 1:

Tabel podkreśla korzyści architektury 1oo2 w przypadku elementu finalnego.

Poziom nienaruszalności bezpieczeństwa funkcji SIF został zmieniony z SIL 1 na SIL 2, poprzez utrzymanie czasu T-proof o interwale 1 rok.

Tabela 10b pokazuje, jak zmienia się poziom SIL elementu finalnego w architekturze 1oo2 dla czasów TI = 3, 5 i 10 lat.

System	PFDavg 1oo2	RRF	Max SIL Level
$1oo2\|_{TI=1}$	0.00120533	**829**	**SIL 2**
$1oo2\|_{TI=3}$	0.00361599	**276**	**SIL 2**
$1oo2\|_{TI=5}$	0.00602665	**165**	**SIL 2**
$1oo2\|_{TI=10}$	0. 0120533	**82**	**SIL 1**

Przykład 3 - SIF

Wyliczone wartości MTBF, PFDavg, RRF dla możliwego poziomu SIL danej SIF.

Poniższe wartości podawane są przez wytwórców:

Tx:	MTBF = 102 lata;	λDU = 0,00080 /rok;	λDD = 0,0010 /rok;	λS = 0,00800 /rok
Barrier:	MTBF = 314 lat;	λDU = 0,00019 /rok;	λDD = 0,0014 /rok;	λS = 0,00159 /rok
PLC:	MTBF = 685 lat;	λDU = 0,00001 /rok;	λDD = 0,0001 /rok;	λS = 0,00135 /rok
Supply:	MTBF = 167 lat;	λDU = 0,00070 /rok;	λDD = 0,0000 /rok;	λS = 0,00530 /rok
Valve:	MTBF = 12 lat;	λDU = 0,02183 /rok;	λDD = 0,0200 /rok;	λS = 0,00400 /rok

Zastosowano te same dane dla architektury 2oo3 co w pierwszym przykładzie, ale wprowadzono współczynnik β równy 5% (0.05) dla podsystemów redundantnych.

Tabela - architektura 2oo3

Subsystem	PFDavg 1oo1	RRF 1oo1	MTBFs 1oo1	PFDavg 2oo3[4]	RRF 2oo3	MTBFs 2oo3	SFF	SIL Level
Tx *	0.000400	2500	125	0.00002058	48597	2893518	91.8 %	SIL 3
Barrier D1014D *	0.000095	10526	629	0.00000478	209092	73250735	94.0 %	SIL 4
PLC	0.000005	200000	741	0.00000500	200000	741	99.3 %	SIL 3
Valve *	0.010915	92	24	0.00097584	1025	107525	73.8 %	SIL 3
Power Supply *	0.000350	2857	189	0.00001794	55734	6592566	88.3 %	SIL 3
Total (SIF)	**0.011765**	**85**	**17**	**0.00102414**	**976**	**55546**	-	**SIL 2**

Tabela podsumowująca – architektura 2oo3

Uwaga 1:

Korzyści zastosowania architektury 2oo3 w odniesieniu do architektury 1oo1 są inne niż te uzyskane dla systemu z architekturą 1oo2.
Poziom nienaruszalności bezpieczeństwa funkcji SIF został zmieniony z SIL 1 na SIL 2, poprzez utrzymanie czasu T-proof o interwale 1 rok.
Bardzo wysoka wartość współczynnik RRF, pokazuje, że SIL2 może być łatwo utrzymany nawet z dłuższymi okresami przeglądów TI.

Uwaga 2:

Stosując taką konfigurację systemu, współczynnik redukcji ryzyka bardzo wzrasta. Jeśli wymagany jest poziom SIL 2 zamiast SIL 3, możliwe jest rozszerzenie interwału czasu T-proof TI.

Tabela 10c pokazuje, jak zmienia się poziom SIL elementu finalnego w architekturze 2oo3 dla czasów TI = 3, 5 i 10 lat.

System	PFDavg 1oo2	RRF	Max SIL Level
$2oo3\|_{TI=1}$	0.00102414	**976**	**SIL 2**
$2oo3\|_{TI=3}$	0.00307242	**325**	**SIL 2**
$2oo3\|_{TI=5}$	0.0051207	**195**	**SIL 2**
$2oo3\|_{TI=10}$	0. 0102414	**80**	**SIL 1**

Porównanie pomiędzy architekturami

SIF Architecture	$MTBF_S$ (yr)	PFDavg	RRF	Max. SIL Level
1oo1	17	0.011765	85	SIL 1
1oo2	8.5	0.000735	1360	SIL 3
2oo3	55546	0.001024	976	SIL 2

Tabela13, Porównanie pomiędzy architekturami

- Redundancja w architekturze podnosi poziom SIL.
- Architektura 2oo3 zasadniczo uzasadnia powód wysokiej wartości MTBFs.

  Oznacza ona, że prawie nigdy produkcja nie zostanie przerwana przez nieuzasadnione (fałszywe) wyzwolenie funkcji bezpieczeństwa.
- Architektura 1oo2 jest prostsza, tańsza oraz ma lepszy współczynnik RRF.

  Jednak współczynnik MTBFs jest bardzo niski.
- Wybór powiniein również uwzględniać przedział testów okresowych (T-proof time).

Tabele porównawcze dla wartości PFDavg w różnych architekturach

Architecture	λdu/yr	PFDavg	RRF	Possible SIL level
1oo1	0.01	0.005900000	169	SIL 2
1oo2	0.01	0.000042350	23613	SIL 4
2oo2	0.01	0.010900000	92	SIL 1
2oo3	0.01	0.000127049	7871	SIL 3

Tabela 14, TI = 1 rok, TD = 0.0009 rok (8 godz.)

Architecture	λdu/yr	PFDavg	RRF	Possible SIL level
1oo1	0.01	0.015300000	65	SIL 1
1oo2	0.01	0.000309005	3236	SIL 3
2oo2	0.01	0.030300000	33	SIL 1
2oo3	0.01	0.000927016	1079	SIL 3

Tabela 15, TI = 3 lat, TD = 0.0009 lat (8 godz)

Architecture	λdu/yr	PFDavg	RRF	Possible SIL level
1oo1	0.01	0.025180	39	SIL 1
1oo2	0.01	0.000842	1187	SIL 3
2oo2	0.01	0.050180	20	SIL 1
2oo3	0.01	0.002527	396	SIL 2

Tabela 16, TI = 5 lat, TD = 0.0009 lat (8 godz)

Architecture	λdu/yr	PFDavg	RRF	Possible SIL level
1oo1	0.01	0.050090	20	SIL 1
1oo2	0.01	0.003342	299	SIL 2
2oo2	0.01	0.100090	10	SIL 0
2oo3	0.01	0.010027	99	SIL 1

Tabela 17, TI = 10 lat, TD = 0.0009 lat (8 godz)

Rola PFDavg i rozważania o SIL

- Wiedza, że dwa różne elementy wyposażenia bezpieczeństwa mają ten sam poziom SIL nie jest wystarczająca do całościowego oszacowania. Wartości PFDavg mogą się różnić od 1 do 10 razy.

- Zawsze preferowana jest niższa wartość PFDavg ze względu na mniejszy wpływ na całkowity poziom SIL funkcji SIF oraz ze względu na możliwość (najczęściej) stosowania dłuższych okresów międzytestowych.

SIL Safety Integrity Level	**PFDavg** Average probability of failure on demand per year (low demand)	**(1-PFDavg)** Safety availability	**RRF** Risk Reduction Factor	**PFDavg** Average probability of failure on demand per hour (high demand)
SIL 4	**$\geq 10^{-5}$ to $< 10^{-4}$**	**99.99 to 99.999 %**	**100000 to 10000**	**$\geq 10^{-9}$ to $< 10^{-8}$**
SIL 3	**$\geq 10^{-4}$ to $< 10^{-3}$**	**99.9 to 99.99 %**	**10000 to 1000**	**$\geq 10^{-8}$ to $< 10^{-7}$**
SIL 2	**$\geq 10^{-3}$ to $< 10^{-2}$**	**99 to 99.9 %**	**1000 to 100**	**$\geq 10^{-7}$ to $< 10^{-6}$**
SIL 1	**$\geq 10^{-2}$ to $< 10^{-1}$**	**90 to 99 %**	**100 to 10**	**$\geq 10^{-6}$ to $< 10^{-5}$**

Table 26, Risk reduction factor, as function of SIL levels and Availability

Prawda czy fałsz?

Poziom SIL nie zmienia się w czasie

NIEPRAWDA!

Poziomy nienaruszalności SIL zależą od prawdopodobieństwa wystąpienia uszkodzenia, które wzrasta w czasie.

Prawda czy fałsz?

Instrukcja Bezpieczeństwa musi być dostarczona przez producenta.

PRAWDA!

Instrukcja Bezpieczeństwa jest integralnym dokumentem każdego komponentu, posiadającego poziom SIL. Precyzuje informacje z certyfikatów SIL i warunki jego obowiązywania.

Prawda czy fałsz?

Dwa produkty o klasie SIL2 oferują tę sam poziom bezpieczeństwa.

NIEPRAWDA!

1) Przykład: SIL 2 oznacza RRF = od 100 do 1000.

2) Klasy SL nadawane są na pewien okres czasu.
Przykład: SIL 2 na lat 10 różni się od SIL2 na rok.

Prawda czy fałsz?

Testy okresowe są wymagane do utrzymania poziomu SIL.

PRAWDA!

Dopóki cześć błędów jest niewykrywalnych podczas normalnego użytkowania (dangerous undetected failures) testy okresowe są wymagane aby przywrócić współczynnik SIF do warunków “jak-nowy” (efektywność 100%)

Testy okresowe są istotne dla utrzymania poziomu SIL.

Prawda czy fałsz?

Przedział czasu T-Proof jest określony przez personel techniczny zakładu.

NIEPRAWDA!

Jest określony w Specyfikacji Sprzętu przez producenta i zweryfikowany przez jednostkę notyfikowaną.

Prawda czy fałsz?

Klient (użytkownik) określa typ komponentu (A czy B).

NIEPRAWDA!

Typ komponentu jest określony przez producenta.

Prawda czy fałsz?

Skrócenie czasu T-Proof podnosi klasę SIL.

PRAWDA!

Skrócenie okresu pomiędzy testami T-proof, zmniejsza prawdopodobieństwo wystąpienia uszkodzenia (PFDavg) w czasie.

Przykład: SIL1 na rok równoważny jest SIL2 na 3 miesiące.

Prawda czy fałsz

Wartość PFDavg funkcji SIF jest największą z wartości PFDavg spośród wszystkich komponentów

NIEPRAWDA!

Wartość PFDavg funkcji bezpieczeństwa (SIF) jest sumą wartości PFDavg wszystkich komponentów.

Prawda czy fałsz?

Współczynniki SFF i PFD muszą być dopasowane do wymagań SIL w zależności od typu komponentu.

PRAWDA!

Wartość SFF każdego z komponentów funkcji SIF musi być zgodna z tabelą wymagań A lub B w celu wyznaczenia danego poziomu SIL.

Prawda czy fałsz?

Możliwe jest dokonanie zmian w oprogramowaniu bez wcześniejszej analizy.

NIEPRAWDA!

Analiza musi być przeprowadzona dla wszystkich zmian dokonywanych w oprogramowaniu oraz w sprzęcie w zakładie.

Prawda czy fałsz?

Urządzenia w klasie SIL 3 mogą być użyteczne w funkcjach SIL2.

PRAWDA!

Używanie wyższego poziomu SIL niż jest wymagany pozwala zredukować częstotliwość testów T-proof oraz ma mniejszy wpływ na całkowity PFDavg funkcji SIF.

Przykład: SIL3 na rok równoważny jest SIL2 na 10 lat.

Prawda czy fałsz?

Przeglądy serwisowe muszą być uwzględnione w fazie projektowania.

PRAWDA!

Funkcja bezpieczeństwa w czasie przeglądu jest niedostępna, dlatego długość czasu naprawy musi zostać uwzględniona.

Udoskonalenie uzyskane w postacie zastosowanej redundancji jest utracone.

Prawda czy fałsz?

Wszystkie uszkodzenia mają te sam wpływ na bezpieczeństwo.

FAŁSZ!

Uszkodzenia mogą być BEZPIECZNE lub NIEBEZPIECZNE.

Bezpieczne – prowadzą do zdarzeń, które nie powodują szkody, ale oznaczają zatrzymanie produkcji.

Niebezpieczne – powodują niedostępność funkcji bezpieczeństwa.

Prawda czy fałsz?

MTBF zawiera czas naprawy.

PRAWDA!

MTBF = MTTF + MTTR.
Dla większości aplikacji, MTTR jest pomijalny, dlatego MTBF ≈ MTTF.
W aplikacjach o wysokich wymaganiach, nawet kilka godzin niedostępności może być krytyczne i należy brać go pod uwagę.

Prawda czy fałsz?

Inżynierowie HSE są odpowiedzialni za utrzymanie poziomu SIL w okresie życia instalacji.

FAŁSZ!

Inżynierowi utrzymania ruchu są odpowiedzialni za utrzymanie poziomu SIL narzuconego w początkowych obliczeniach. Dla SIL2 ich praca musi zostać poddana inspekcji przez oddzielny departament. Dla SIL3 i SIL4 – przez zewnętrzną agencję.

Rozważania o SIL

- Ogólnie domniemywa się, że funkcja bezpieczeństwa lub urządzenie, dla którego wyznaczamy SIL (1-2-3) będzie takie zawsze.

- Wiemy, że to nieprawda: Poziom SIL zależy od wartości PFDavg, ponadto, poziom SIL jest aktualny dla pewnego ustalonego wcześniej okresu czasu: Okresu Między Testami.

Rozważania o SIL

- Poziom SIL, który jest utrzymywany przez 1 rok, jest bardzo różny od tego utrzymywanego przez 10 lat; Jednakże, oba są stosowane dla tej samej funkcji bezpieczeństwa.

- Interwał testu diagnostycznego jest więc czasem, dla którego spełnione są warunki utrzymania pewnego poziomu SIL.

PFDavg: Równania i przykłady

Dla każdego komponentu funkcji SIF, gdy efektywność okresowego testu diagnostycznego wykrywającego niebezpieczne uszkodzenia wynosi 100%, uproszczone równanie na PFDavg jest:

$$\mathrm{PFDavg} = \lambda_{DU} \times \frac{TI}{2}$$

Gdy efektywność nie wynosi 100%, uproszczone równanie na PFDavg jest:

$$\mathrm{PFDavg} = (Et \times \lambda_{DU} \times \frac{TI}{2}) + \left[(1 - Et) \times \lambda_{DU} \times \frac{SL}{2} \right]$$

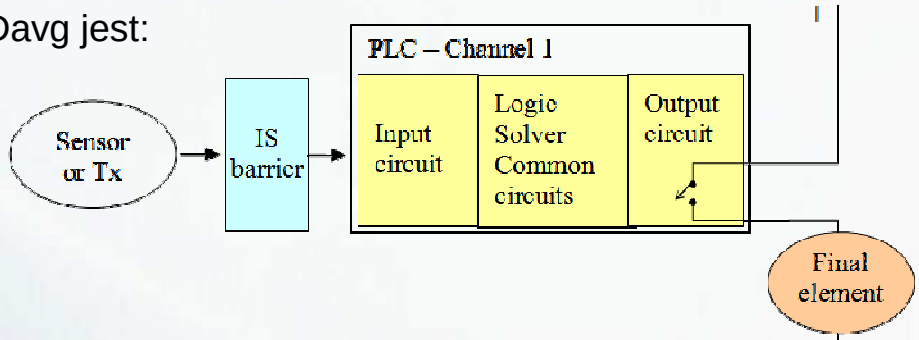
gdzie:

Et: **efektywność okresowego testu diagnostycznego (np. 90%)**

SL: interwał testu diagnostycznego systemu lub urządzenia przy efektywności 99-100% lub między dwoma kompletnymi wymianami urządzenia lub czas życia systemu lub urządzenia, jeżeli nigdy nie był całkowicie wymieniany lub testowany.

dla TI = 1 rok i SL = 12 lat, uproszczone równanie na PFDavg jest:

$$\mathrm{PFDavg}\Big|_{TI=1,SL=12} = (Et \times \frac{\lambda_{DU}}{2}) + \left[(1 - Et) \times \lambda_{DU} \times \frac{12}{2} \right]$$

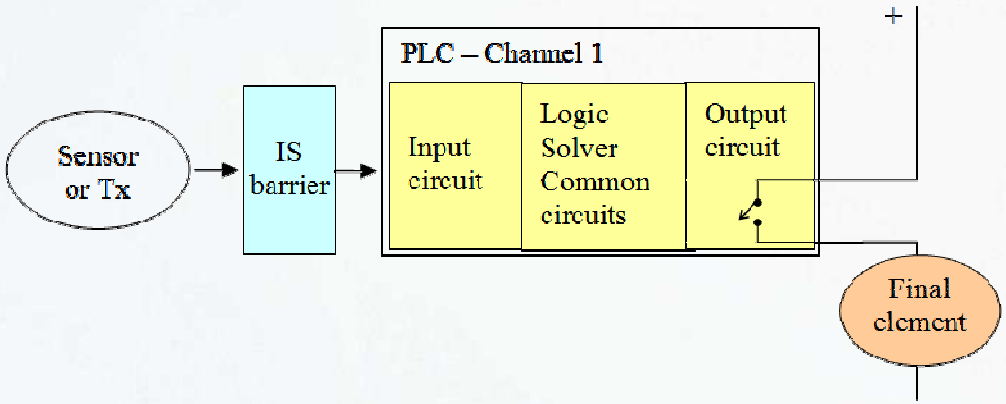


PFDavg: Równania i przykłady

$$PFDavg\Big|_{TI=1,SL=12} = \left(Et \times \frac{\lambda_{DU}}{2}\right) + \left[(1-Et) \times \lambda_{DU} \times \frac{12}{2}\right]$$

Przykład a:

λdu = 0,01 / rok
TI = 1 rok
Et = 90% = 0,9
SL = 12 lat



W instalacji:

PFDavg = 0,01 / 2 = 0,005
RRF = 1 / PFDavg = 1 / 0,005 = **200**

Po roku:

PFDavg = (0,9 x 0,01 / 2) + (0,1 x 0,01 x 6) = 0,0105
RRF = 1 / PFDavg = 1 / 0,0105 = **95**

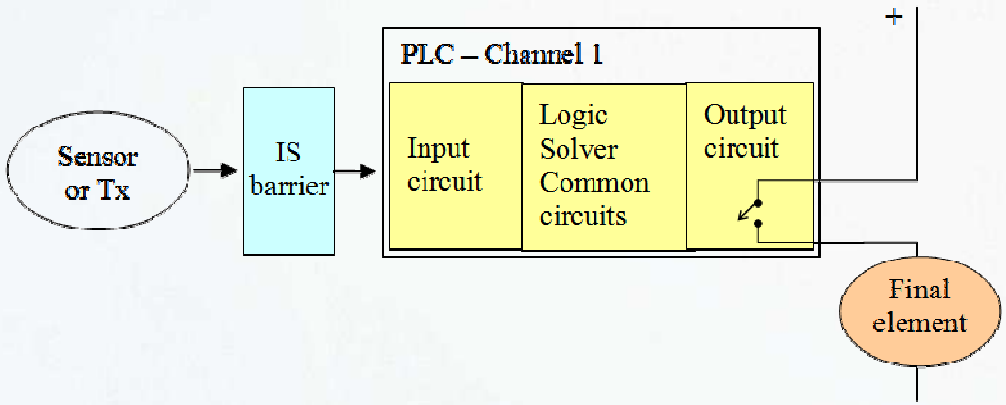
Uwaga: **po roku (lub po każdym teście okresowym) poziom SIL 2 stał się SIL 1.**

PFDavg: Równania i przykłady

$$PFDavg\Big|_{TI=1,SL=12} = \left(Et \times \frac{\lambda_{DU}}{2}\right) + \left[(1-Et) \times \lambda_{DU} \times \frac{12}{2}\right]$$

Przykład b:

λdu = 0,01 / rok
TI = 1 rok
Et = 99% = 0,99
SL = 12 lat



Po roku:

PFDavg = (0,99 x 0,01 / 2) + (0,01 x 0,01 x 6) = 0,0056
RRF = 1 / PFDavg = 1 / 0,006 = **178**

Note: **po roku (lub po każdym teście okresowym) poziom SIL2 jest wciąż utrzymany.**

Wpływ interwału testu PFDavg

- Dla przetestowania systemu bezpieczeństwa on-line (np. przy uruchomionym procesie), część systemu bezpieczeństwa musi być zbocznikowana dla zabezpieczenia przed kłopotliwymi sygnałami wyzwalającymi. Czas trwania ręcznego testu diagnostycznego może mieć znaczący wpływ na ogólną wydajność systemu bezpieczeństwa.

$$\mathrm{PFDavg} = \lambda_{DU} \times \frac{TI}{2}$$

- W czasie testu prosty system 1oo1 musi być odłączony. Jego dostępność jest wobec tego zerowa. Natomiast systemy redundantne nie muszą być całkowicie bocznikowane na czas testu. Tylko jedna odnoga lub fragment systemu redundantnego może być bocznikowany.

$$\mathrm{PFDavg} = \lambda_{DU} \times \frac{TI}{2} + \frac{TD}{TI}$$

- W czasie testu podwójny system jest redukowany do prostego pojedynczego, a potrójny redukowany do podwójnego.

Interwał testu i jego wpływ na PFD_{avg}

Przykład c:

λdu = 0,002 / rok
TI = 1 rok
TD = 8 godzin (Czas Trwania Testu)
PFDavg = 0,001 + 0,0009 = 0,0019;
RRF = 1/ 0,0019 = **526**
(użyteczne dla poziomu **SIL 2**)

Przykład d:

λdu = 0,002 / rok
TI = 1 rok
TD = 96 godzin
PFDavg = 0,001 + 0,01 = 0,011;
RRF = 1/ 0,011 = **90**
(użyteczne dla poziomu **SIL 1**)

$$PFDavg = \lambda_{DU} \times \frac{TI}{2}$$

$$PFDavg\Big|_{TI=1,SL=12} = \left(Et \times \frac{\lambda_{DU}}{2}\right) + \left[(1-Et) \times \lambda_{DU} \times \frac{12}{2}\right]$$

$$PFDavg = \lambda_{DU} \times \frac{TI}{2} + \frac{TD}{TI}$$

$$PFDavg = \left(Et \times \frac{\lambda_{DU}}{2}\right) + \frac{TD}{TI} + \left[(1-Et) \times \lambda_{DU} \times \frac{SL}{2}\right]$$

Uwaga:

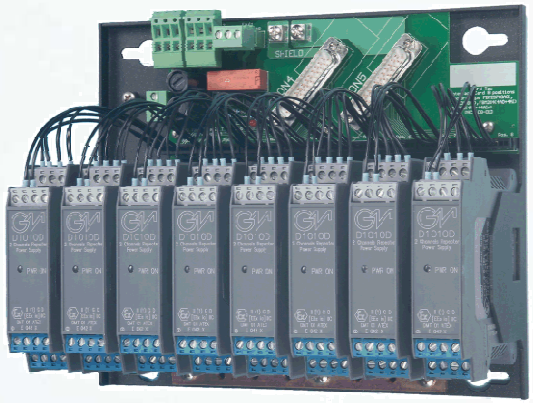
Kombinacja efektywności i czasu trwania testu daje następujące równanie na PFDavg dla architektury 1oo1.

Strategie utrzymania bezpieczeństwa w SIS

Rozważania:

- Podanie wyłącznie poziomu SIL wyposażenia daje częściowy i niepełny obraz poszukiwanego rozwiązania dla funkcji SIF.

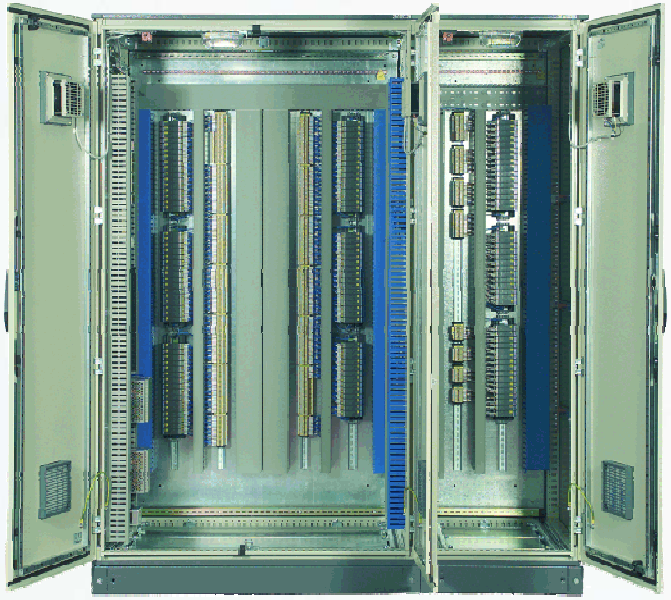
- Należy rozważyć:
  - Częstości uszkodzeń bezpiecznych i niebezpiecznych,
  - Wartości PFDavg dla 1-3-5-10 lat ciągłej pracy,
  - Interwały Testów Diagnostycznych,
  - Procedury testowe oraz ich procentowa efektywność w wykrywaniu niebezpiecznych, niewykrywalnych uszkodzeń powinny być dostępne w Podręczniku Bezpieczeństwa wyposażenia. (analizie)



Strategie utrzymania bezpieczeństwa w SIS

- Dla każdego składnika łańcucha funkcji SIF wymagany jest plan utrzymania systemu, by możliwe było odtworzenie początkowej wartości PFD oraz poziomu SIL.

- Utrzymanie, w formie okresowych testów w wyznaczonych interwałach, normalnie wymaga zbocznikowania testowanego sprzętu na czas testu i często implikuje krytyczne operacje, dlatego interwał czasowy pomiędzy testami powinien być jak najdłuższy, a procedury testowe powinny być efektywne i tak szybkie, jak to tylko możliwe.



Strategie utrzymania bezpieczeństwa w SIS

Wybór komponentów do systemów bezpieczeństwa:

- Wybierz wyposażenie o najniższym PFDavg i najwyższym interwale Testu Diagnostycznego, dla tego samego poziomu SIL.
- Rozważ także Czas Naprawy dla Testu diagnostycznego (wybierz najkrótszy czas naprawy).
- Weź pod uwagę procentową efektywność testu diagnostycznego i oblicz ponownie wartość PFDavg dla sprawdzenia, czy odpowiada ona wymaganemu poziomowi SIL.
- Jeżeli to możliwe, wybierz wyższy poziom SIL niż wymagany, dla uzyskania dłuższych interwałów międzytestowych i dla redukcji kosztów utrzymania.

Powody wyboru SIL 3

1:

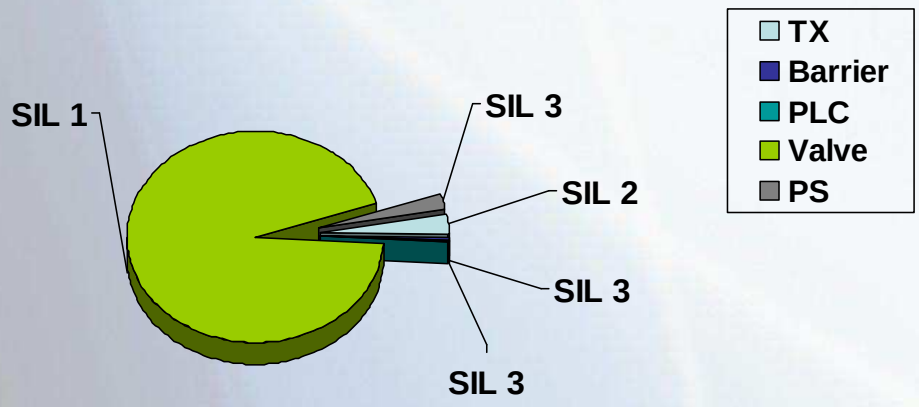
wyposażenie posiadające klasę SIL 3 na rok może być używane w klasie SIL 2 funkcji SIF dla 5 lub 10 letniego interwału testu diagnostycznego, w zależności od jego wartości PFDavg.

Jest to główny powód stosowania urządzeń SIL 3 w fukcji SIF o poziomie SIL 2.

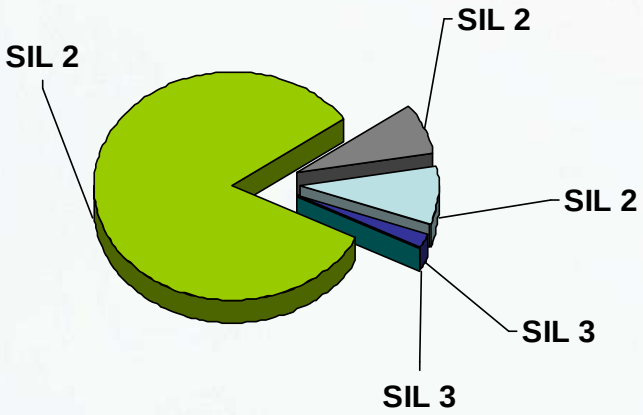
Powody wyboru SIL 3

2:

Wyposażenie posiadające SIL 3 zmniejsza ogólny PFDavg dla funkcji SIF, pozwalając na użycie pozostałych urządzeń z większymi wartościami PFDavg.



SIL 1 SIF

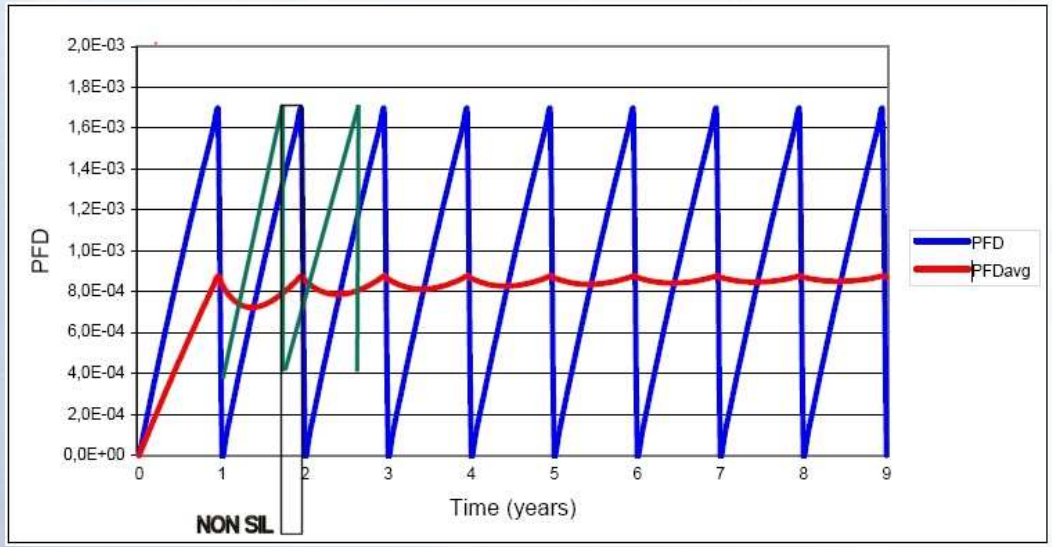


SIL 2 SIF

Powody wyboru SIL 3

3:

Wyposażenie posiadające SIL 3 może być użyte dla funkcji SIF poziomu SIL 2 nawet z mniej niż 100% efektywnością testu.



G.M. International s.r.l
Via San Fiorano, 70
20058 Villasanta (Milan)
ITALY
www.gmintsrl.com
info@gmintsrl.com

TR Automatyka Sp. z o.o.
ul. Lechicka 14
02-156 Warszawa
POLAND
www.trautomatyka.pl
biuro@trautomatyka.pl