FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE

CONFINDUSTRIA

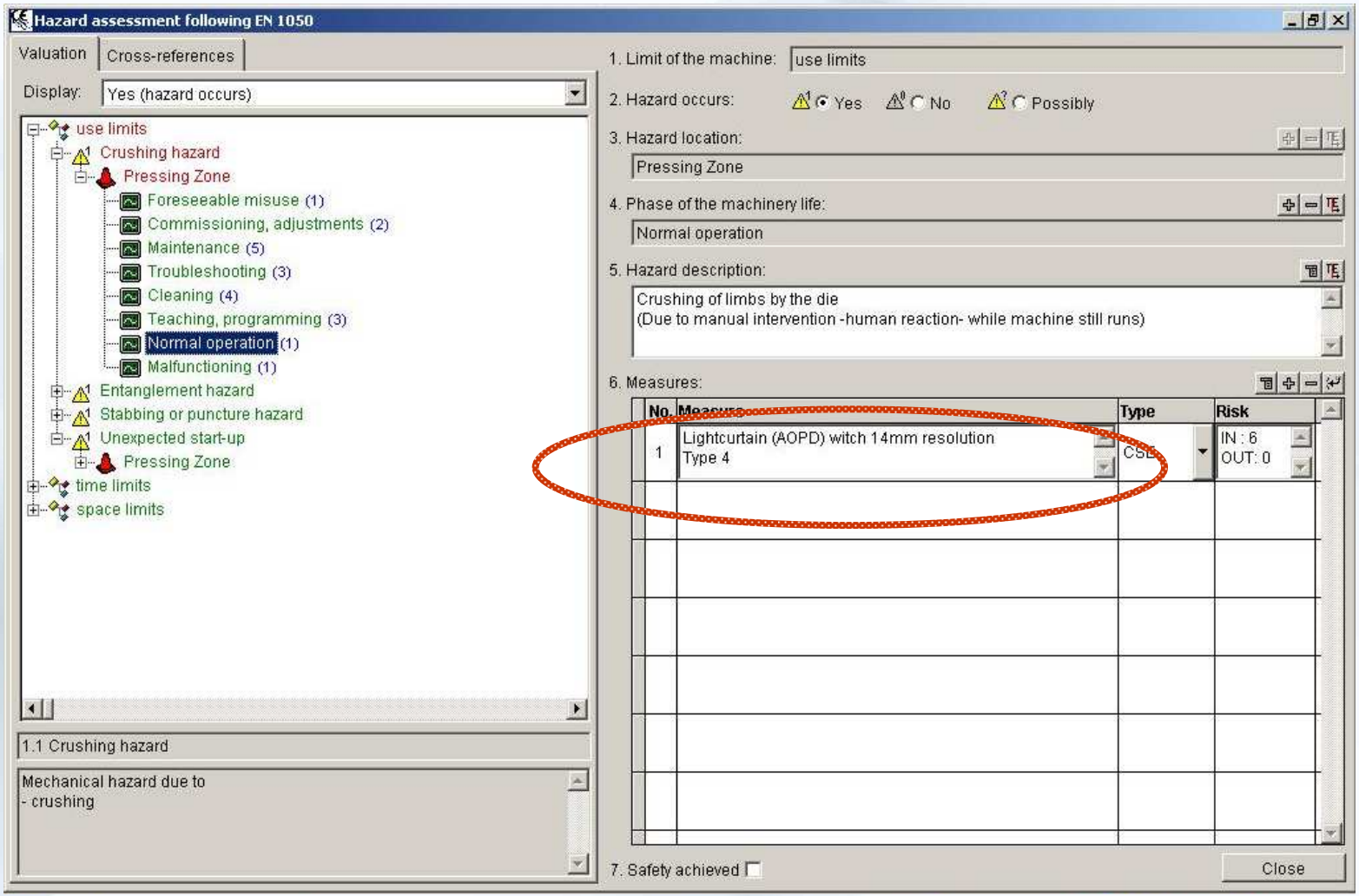
DAL 1945 IL VALORE DELL'INNOVAZIONE

Esempio di applicazione delle norme EN ISO 13849-1 e EN IEC 62061

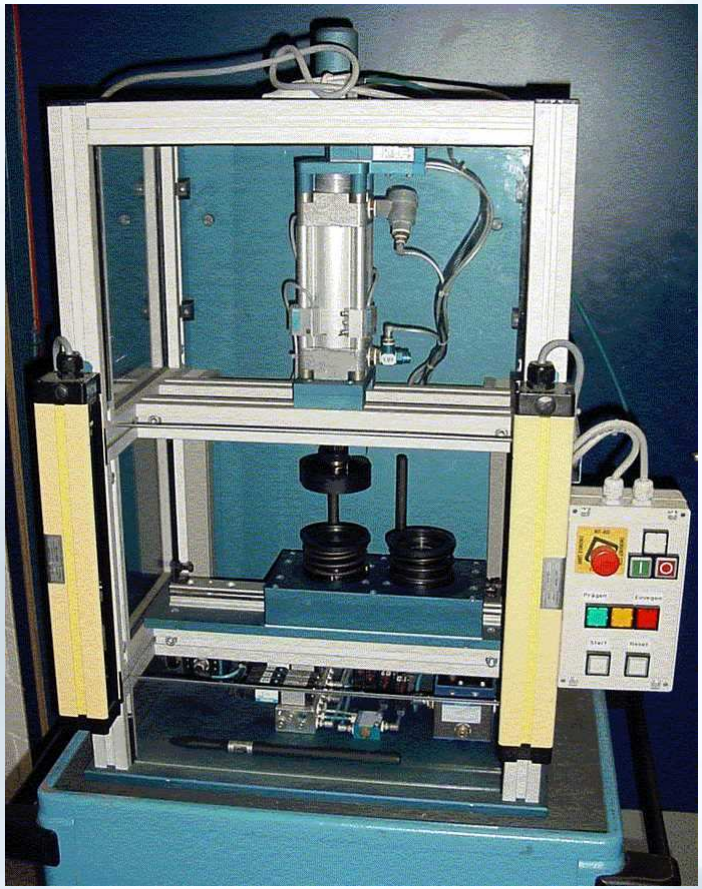
Esempio: Pressa per cuscinetti

Valutazione del rischio
Secondo EN ISO 14121

Valutazione del rischio



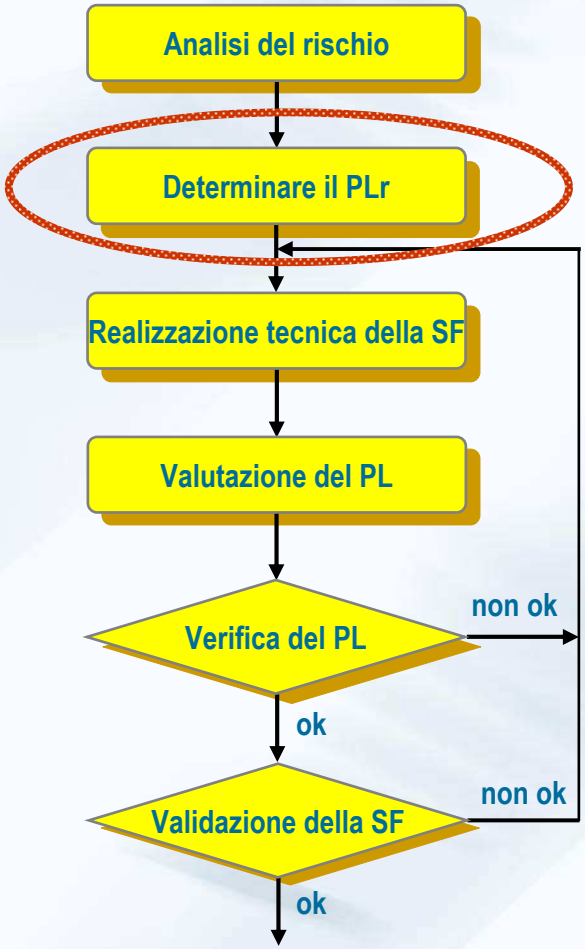
Funzione di sicurezza



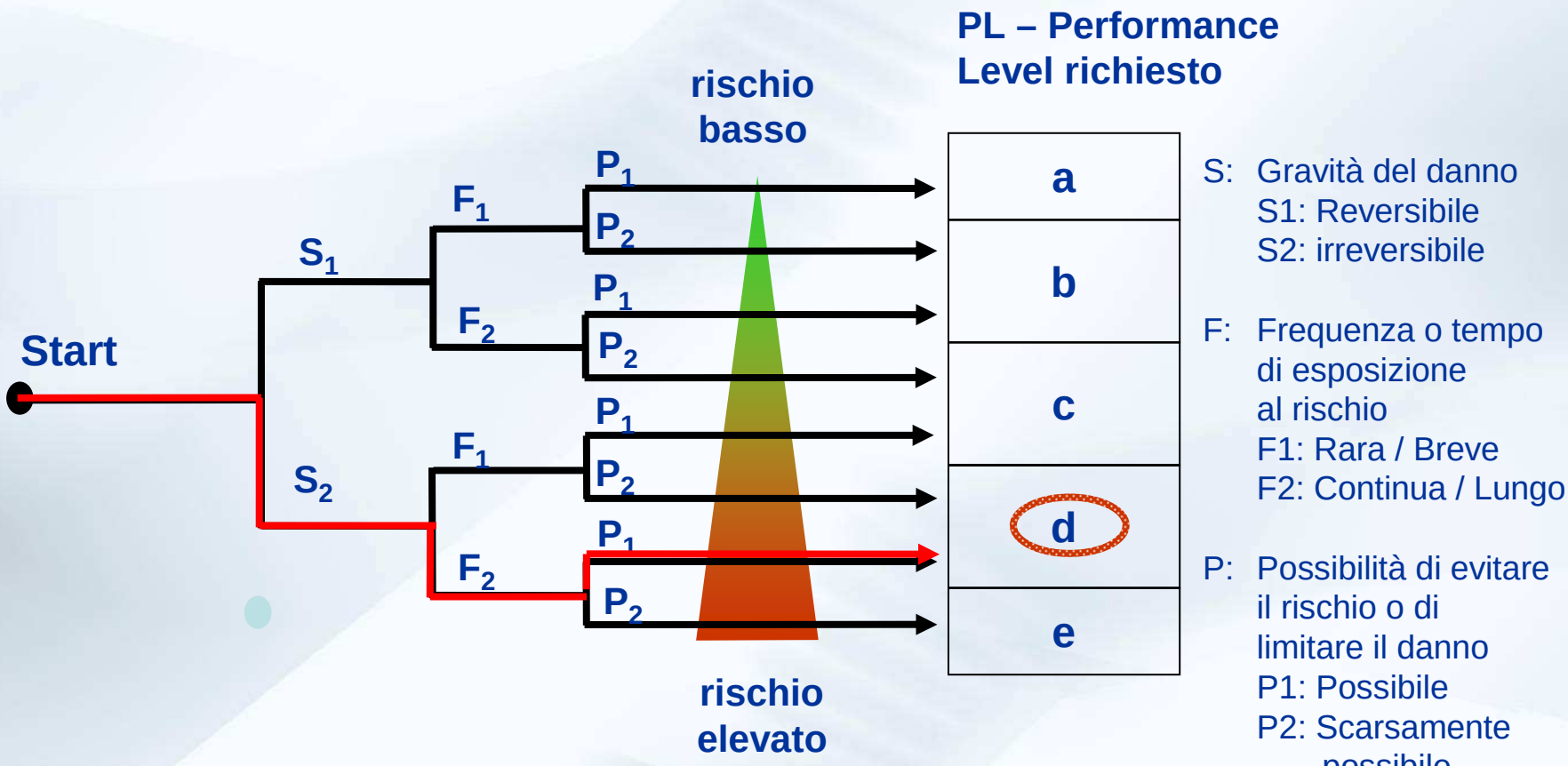
SF:

Il movimento del cilidro deve essere fermato quando il campo protetto della barriera viene infranto

Riduzione del rischio

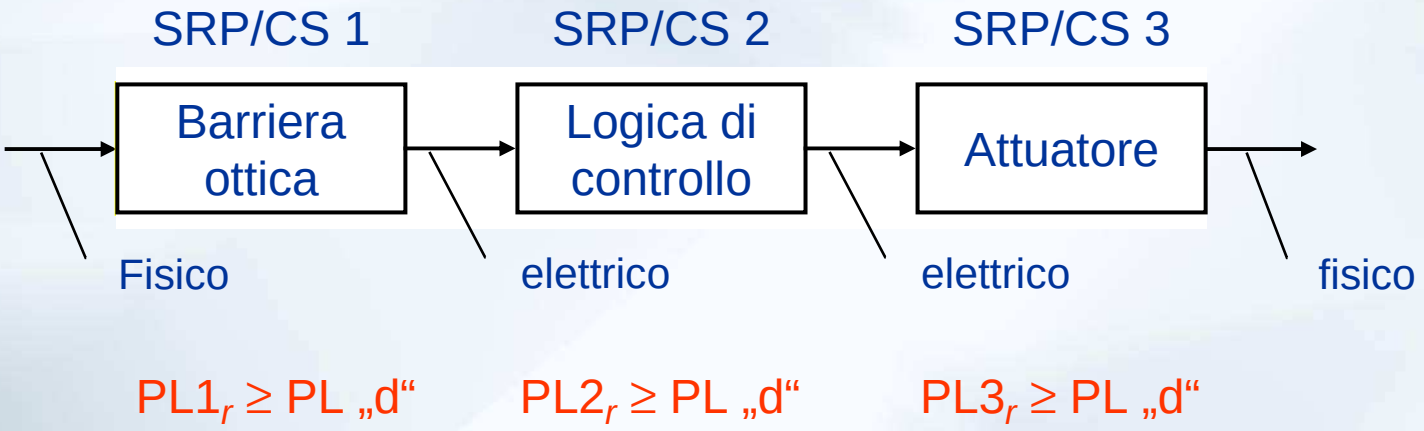


Determinazione del PLr



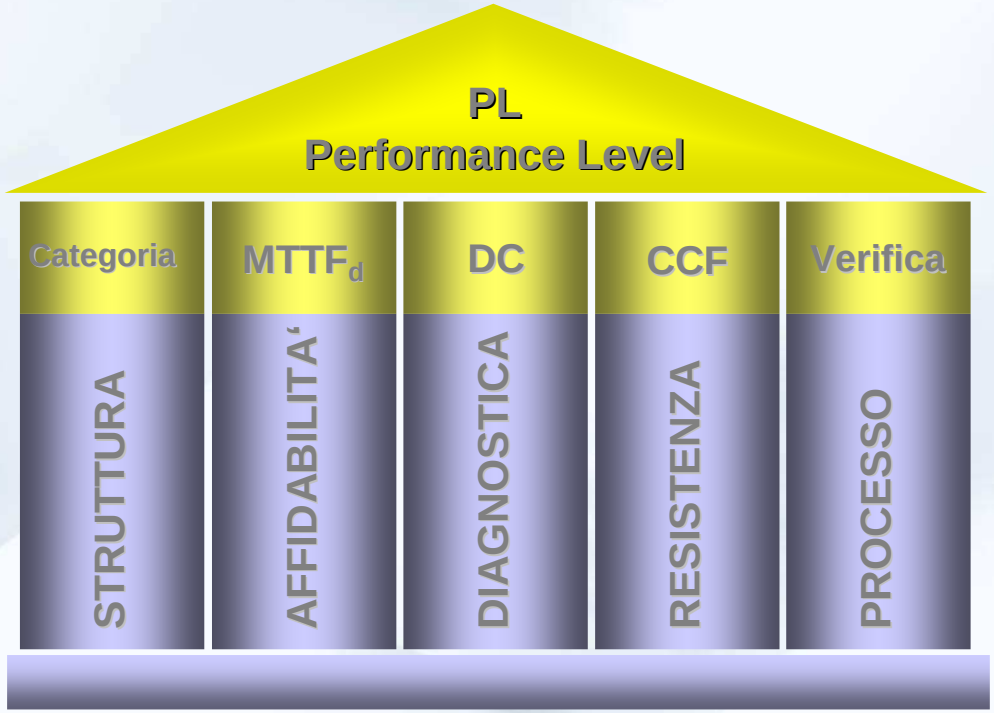
Progettare il sistema di sicurezza

Parti relative alla sicurezza dei sistemi di controllo



„Una funzione di sicurezza può essere composta da uno o più SRP/CS, e più funzioni di sicurezza possono utilizzare gli stessi SRP/CS “

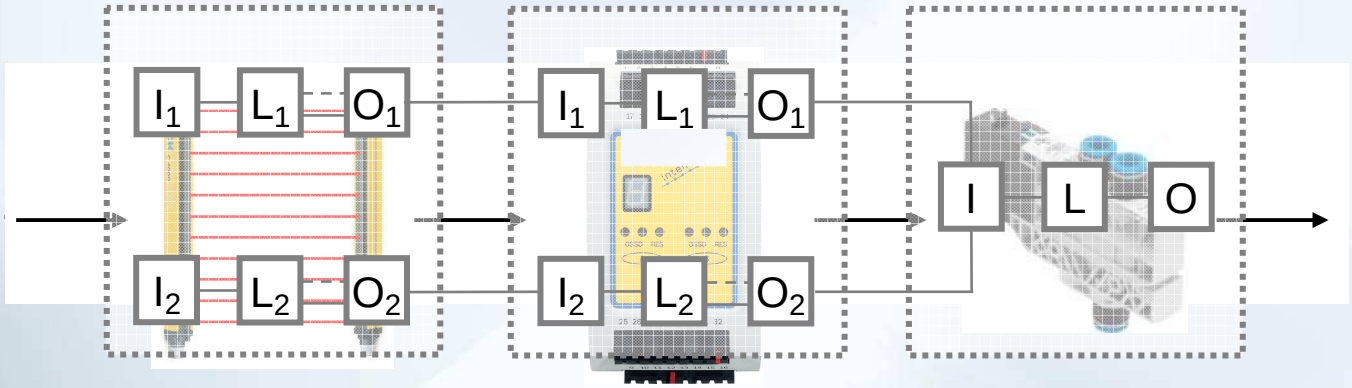
Determinare il PL per SRP/CS



Aspetti strutturali

Circuito di stop di sicurezza

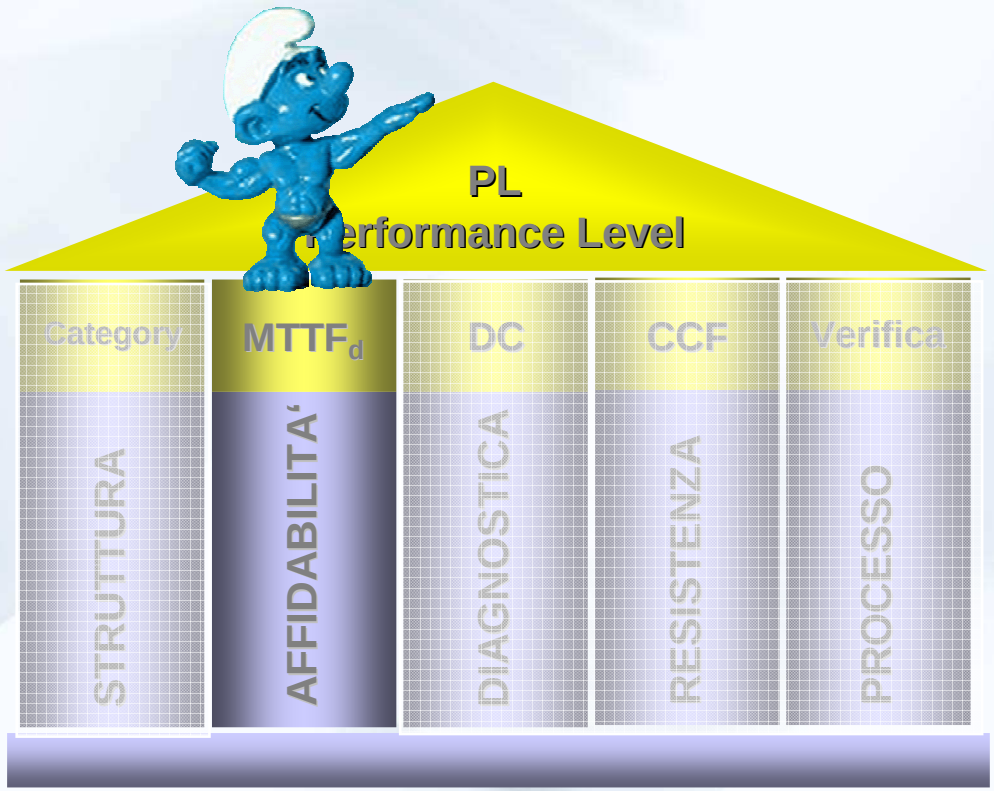
SRP/CS 1 | SRP/CS 2 | SRP/CS 3



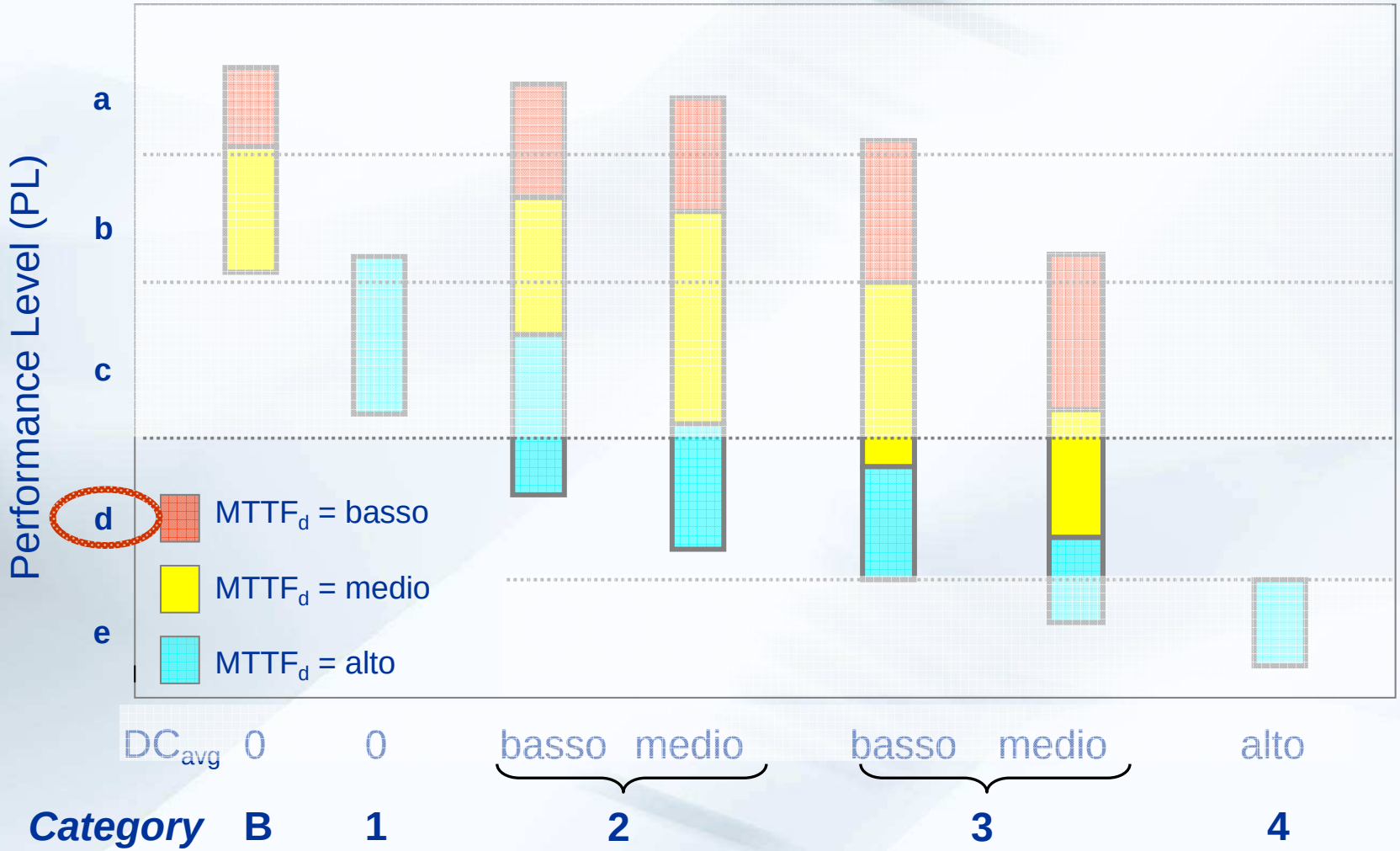
Categoria 4 | Categoria 4 | Categoria 1

$PL1_r \geq$ PL „d“ | $PL2_r \geq$ PL „d“ | $PL3_r \geq$ PL „d“

Aspetti di affidabilità

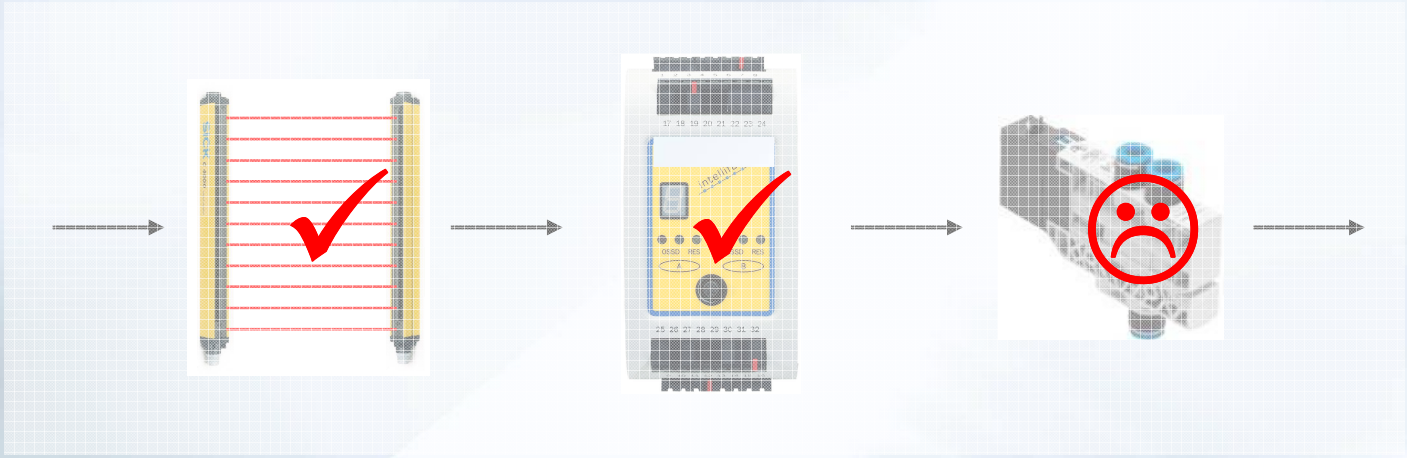


Relazione MTTF e Categoria con PL



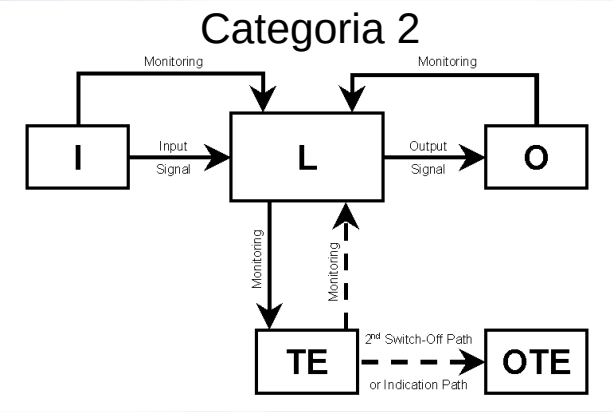
Circuito di stop di sicurezza

SRP/CS 1	SRP/CS 2	SRP/CS 3



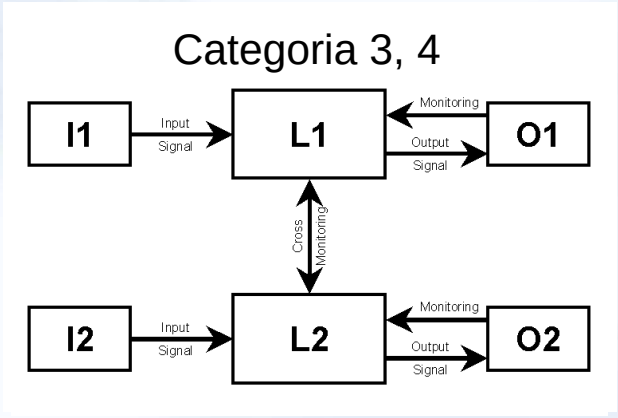
Categoria 4	Categoria 4	Categoria 1
$PL1_r \geq$ PL „d“	$PL2_r \geq$ PL „d“	$PL3_r \geq$ PL „d“

Struttura alternativa



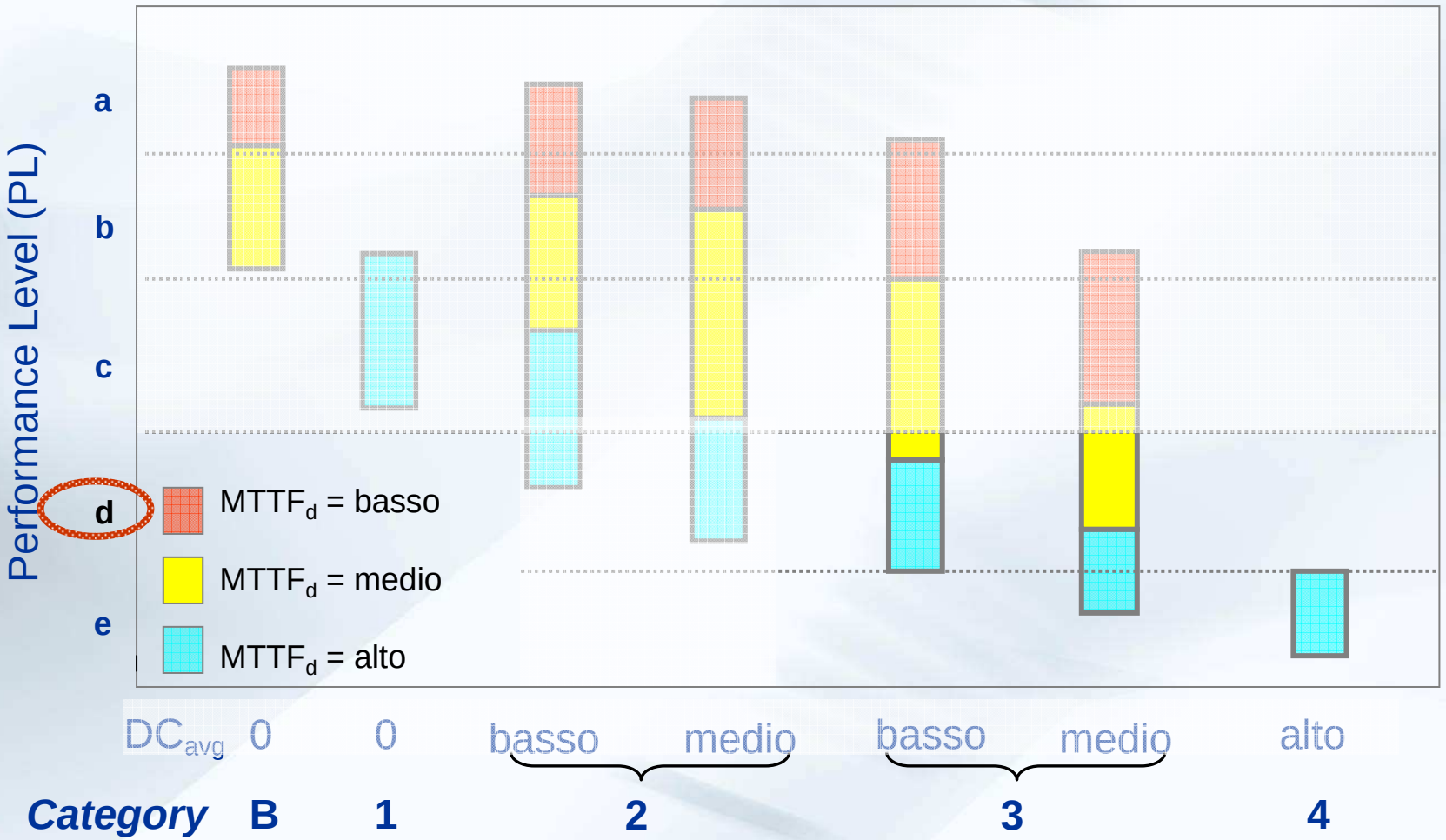
„Per categoria 2: freq. Della richiesta £ 1/100 ·freq. Di test“

Struttura alternativa

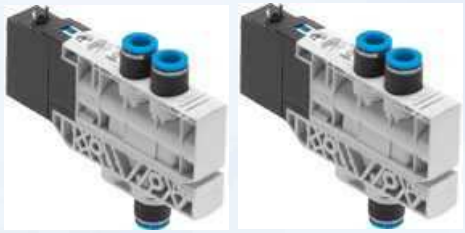


„Corto circuito controllato da un PLC di sicurezza“

Relazione MTTF e Categoria con PL



Calcolo di $MTTF_d$



$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$

$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot d_{op} \cdot h_{op} \cdot C}$$

$$MTTF_d = \frac{20.000.000}{0{,}1 \cdot 220\,{}^{d}\!/_{a} \cdot 8\,{}^{h}\!/_{d} \cdot 60\,{}^{1}\!/_{h}}$$

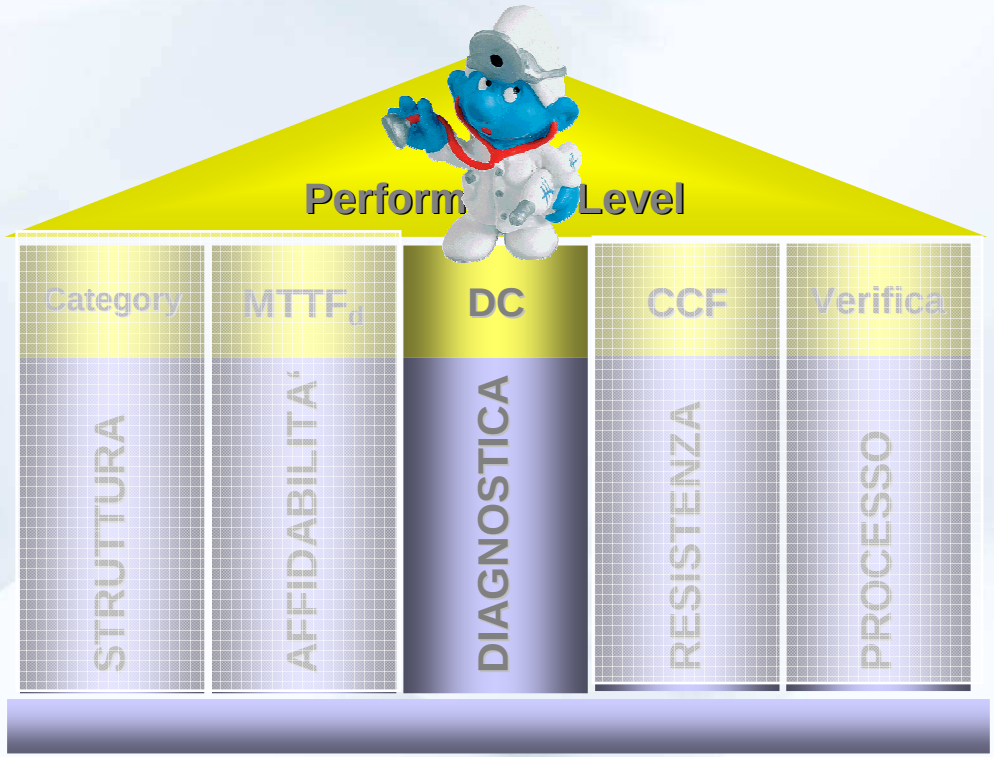
$$\boxed{MTTF_d = 100\,a}$$

ISO 13849:
$B10_d$ = 20.000.000 Cicli di commutazione

Assumendo che:
C = 60 /h
d_{op} = 220 d/a
h_{op} = 8 h/d

$MTTF_d$ = „alto“

Aspetti di diagnostica



Diagnostic coverage

λ_{du} Percentuale di guasti pericolosi non rilevati

λ_d Percentuale di guasti pericolosi

λ_{dd} Percentuale di guasti pericolosi rilevati

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \lambda_{du}}$$

Stima del DC

Table E.1 — Abstract: Estimates for diagnostic coverage (DC)

	Measure	DC
Input	Cyclic test stimulus by dynamic change of the input signals	90%
Input	Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99%
Input	Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60%
Input	Cros monitoring if inputs without dynamic test	0%..99% (dependig on signal change frequency)
Logic	Dynamic principle (all components of the logic are required to change the state ON-OFF-ON when the safety function is demanded), e.g. interlocking circuit implemented by relays	99%
Logic	Processing unit: Self test by software	60%..90%
Output	Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment	90%
Output	Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%
General	Fault Detection by process	0%..99% (not alone for PL „e“)

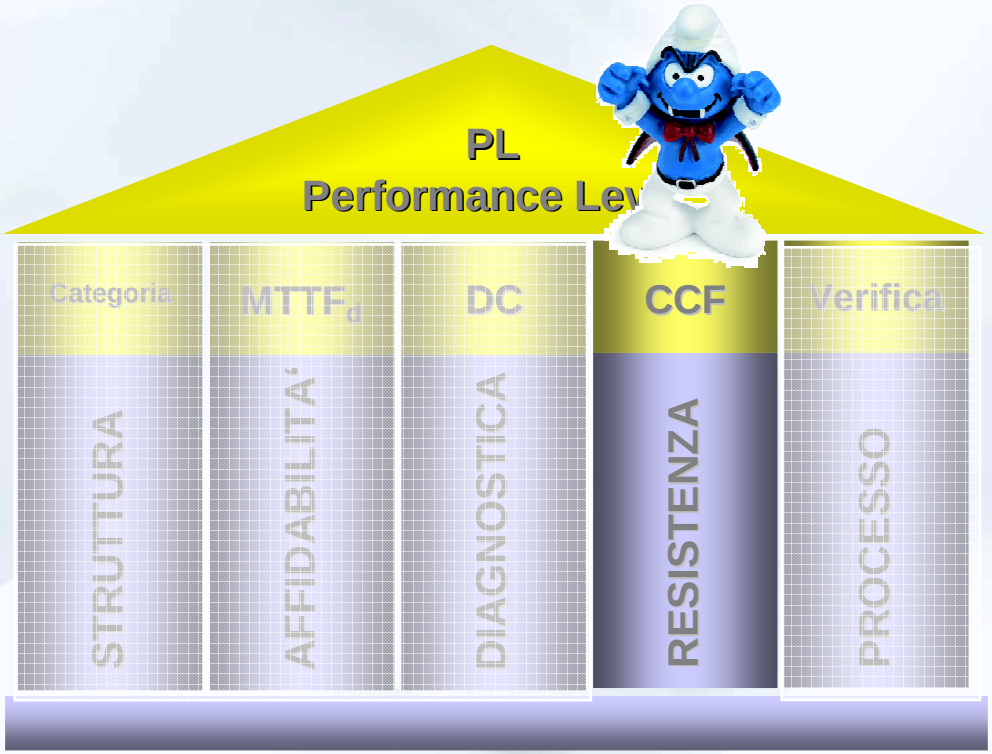
Valori legati al DC

Table 6 — Diagnostic coverage (DC)

Denotation of DC	Range of DC
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC
NOTE For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in this standard in Figure 5, Clause 6 and E.2.	

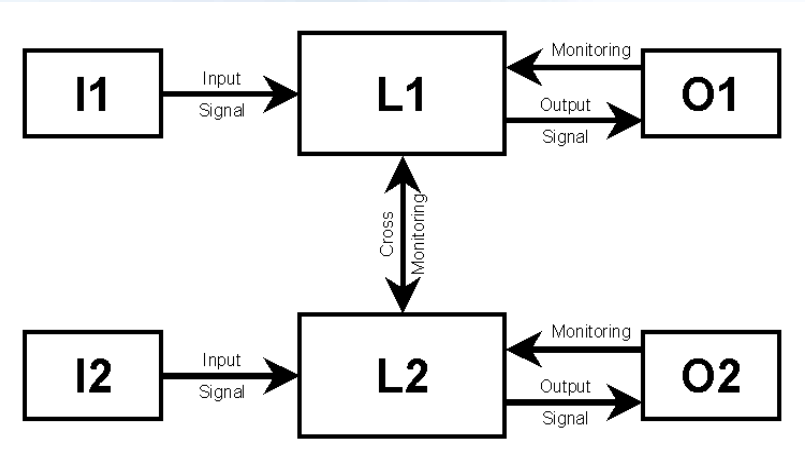
DC = „alto“

Aspetti legati alla resistenza



Cause comuni di guasto

Categoria 3, 4



„Guasto che causa guasti contemporanei su due o più canali in un sottoinsieme multicanale“

Misure contro CCF

Table I.1 - Estimation of the measures against CCF

Item	Max. Score
Separation / segregation	15
Diversity	20
Design / application / experience	20
Assessment / analysis	5
Competence / training	5
Environmental	25
Other influences	10

Totale 100

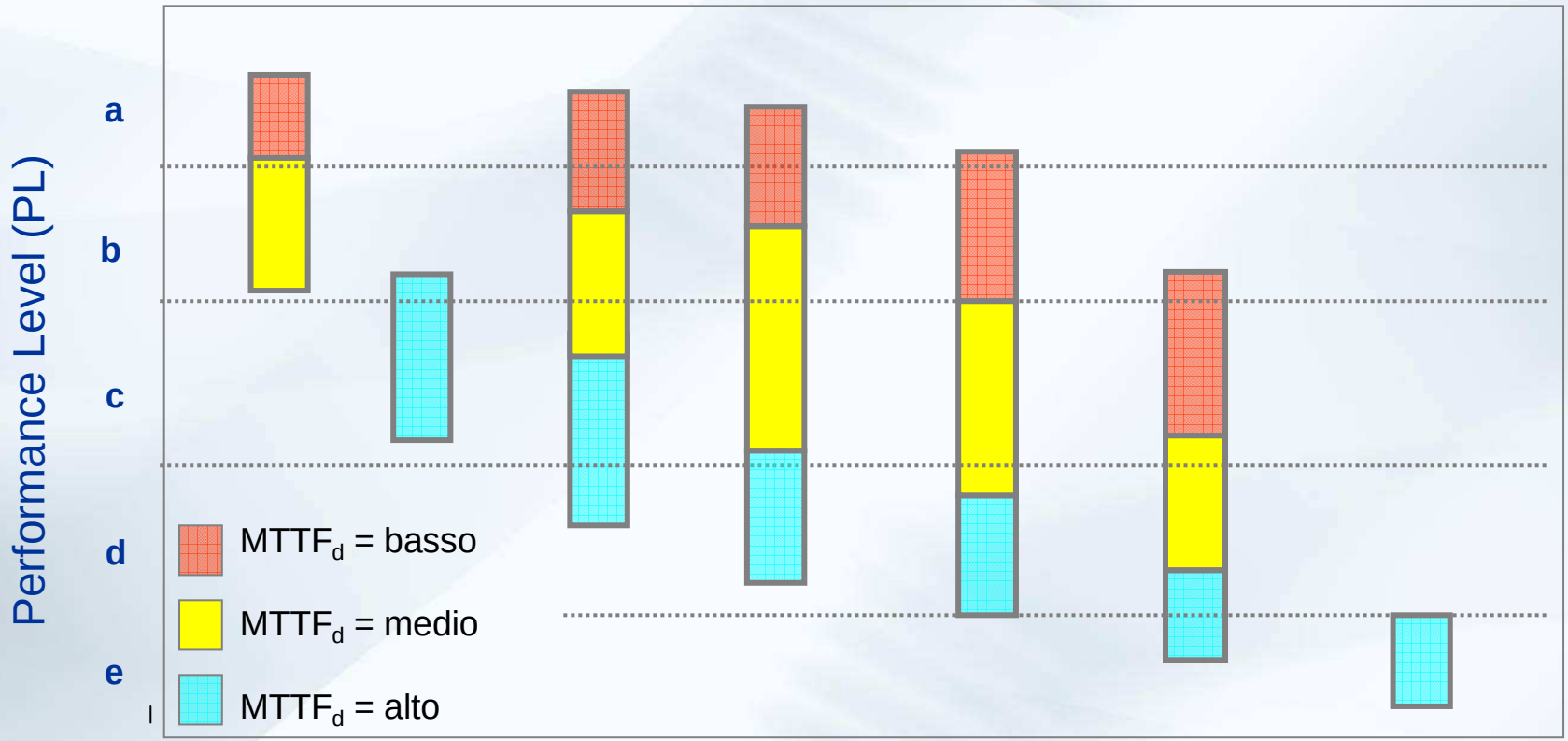
Score ≥ 65

CCF - Tabella

Table I.1 — Estimation of the measures against CCF for example B

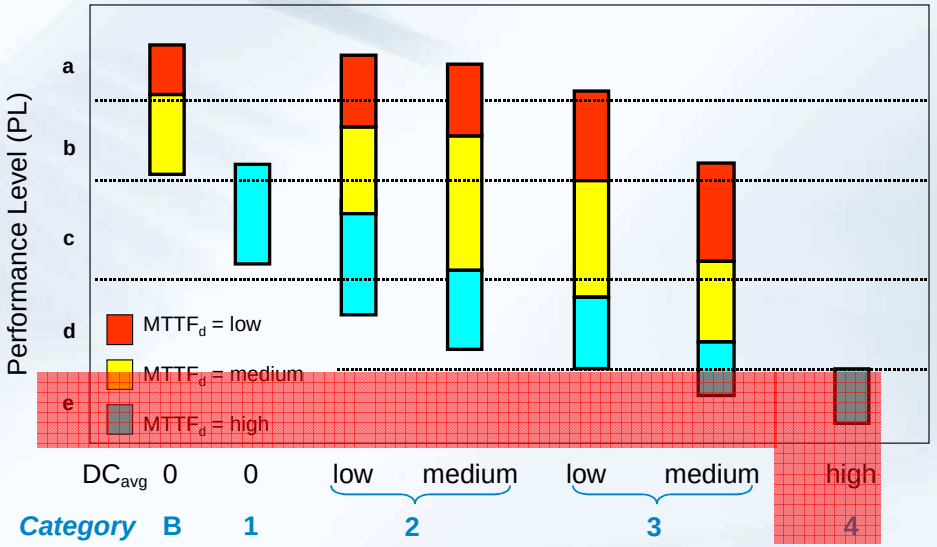
No.	Item	Score for control circuit	Maximum possible score
1	**Separation/segregation**		
	Physical separation between signal paths		15
2	**Diversity**		
	Different technologies/design or physical principles are used		20
3	**Design/application/experience**		
3.1	Protection against over–voltage, over–pressure, over–current, etc.		15
3.2	Components used are well-tried		5
4	**Assessment/analysis**		
	Are the results of a failure mode and effect analysis taken into account to avoid common cause failures in design.		5
5	**Competence/ training**		
	Are designers been trained to understand the causes and consequences of common cause failures		5
6	**Environmental**		
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards		25
6.2	Other Influences Are the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards) considered		10
	Total		max. 100

PL per un SRP/CS



Performance level

Categoria 3/4



$$MTTF_d = 100\,a$$

Table 5 — Mean time to dangerous failure of each channel ($MTTF_d$)

Denotation of $MTTF_d$ of each channel	Range of $MTTF_d$ of each channel
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ ≤ 100 years

Table 6 — Diagnostic coverage (DC)

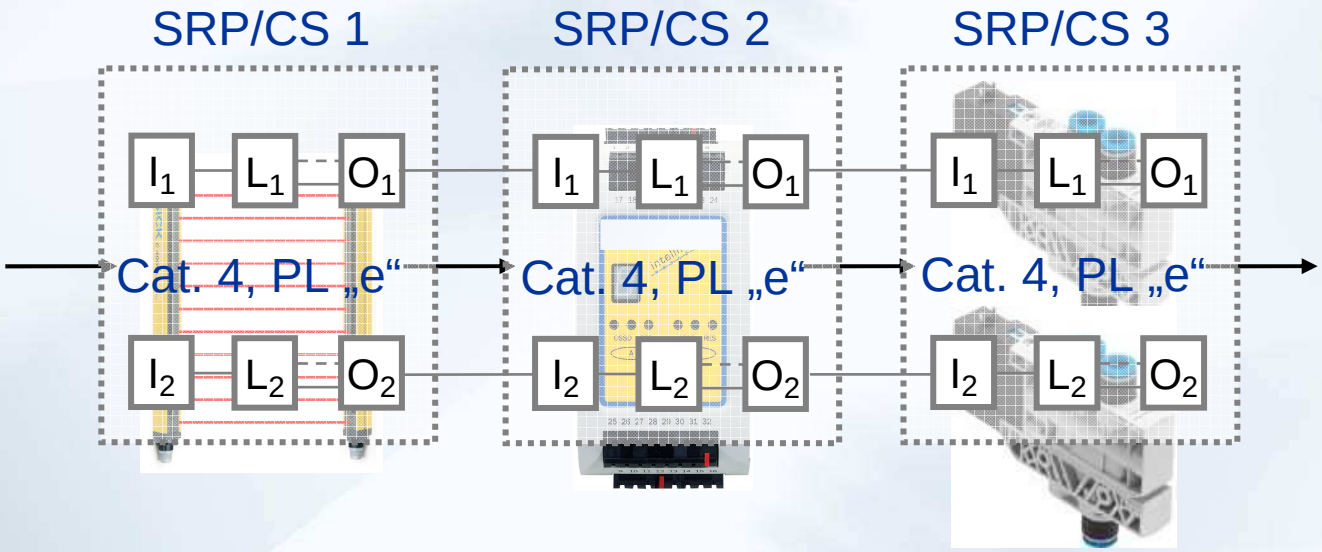
Denotation of DC	Range of DC
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC

NOTE For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in this standard in Figure 5, Clause 6 and E.2.

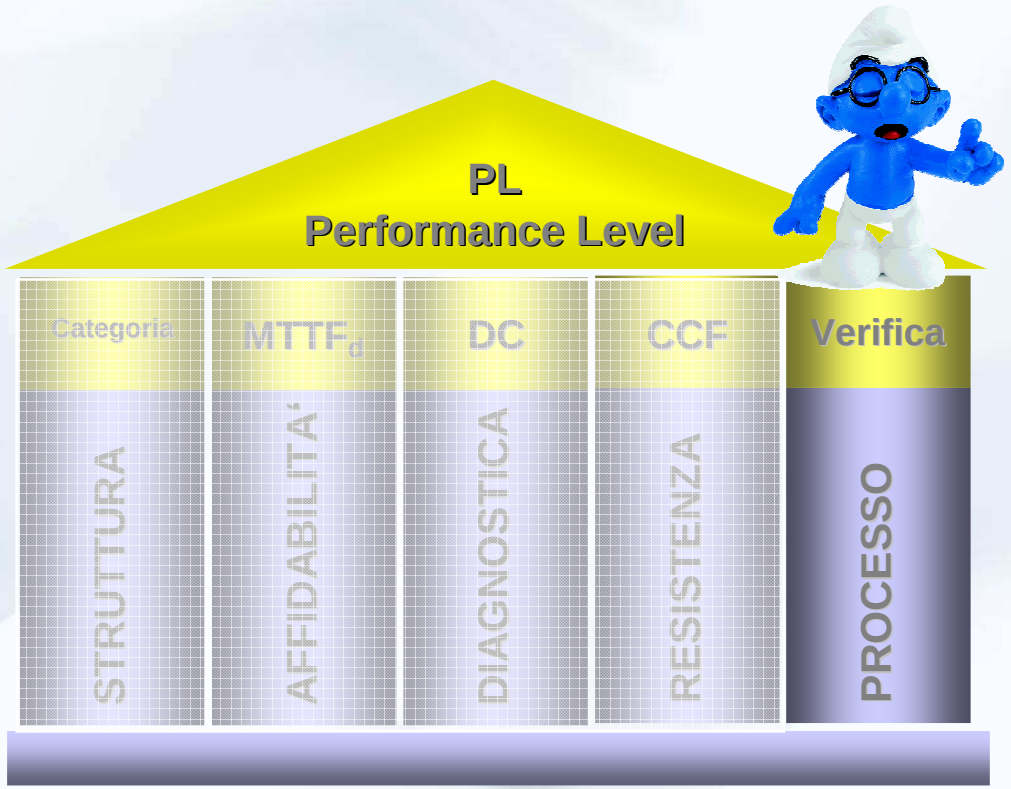
Table I.1 — Estimation of the measures against CCF for example B

No.	Item	Score for control circuit		Maximum possible score
1	**Separation/segregation**			
	Physical separation between signal paths	15		15
2	**Diversity**			
	Different technologies/design or physical principles are used	20		20
3	**Design/application/experience**			
3.1	Protection against over–voltage, over–pressure, over–current, etc.	none	15	15
3.2	Components used are well-tried	5	5	5
4	**Assessment/analysis**			
	Are the results of a failure mode and effect analysis taken into account to avoid common cause failures in design.	5	5	5
5	**Competence/ training**			
	Are designers been trained to understand the causes and consequences of common cause failures	none	5	5
6	**Environmental**			
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards	25	25	25
6.2	Other Influences Are the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards) considered	10	10	10
	Total	80	65	max. 100

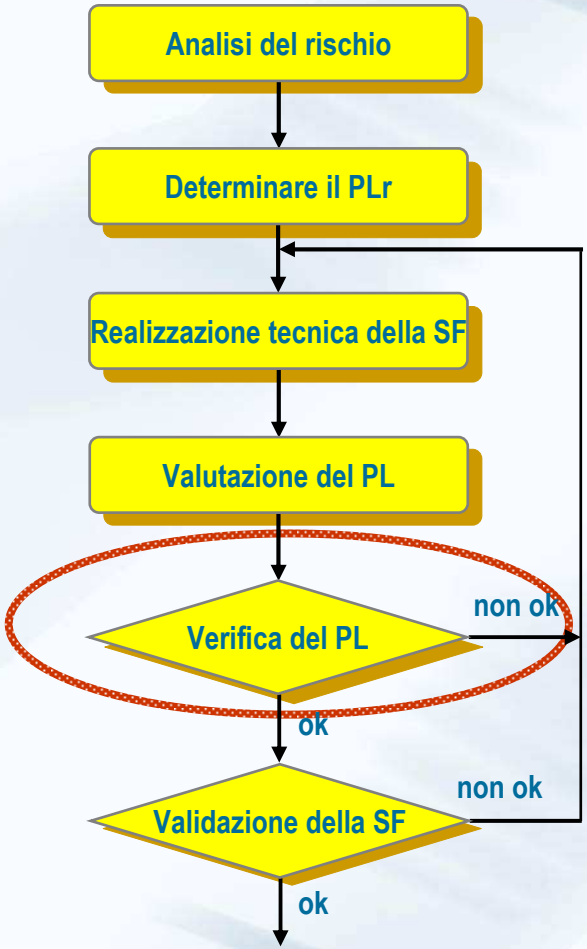
Circuito di stop di sicurezza



Processo di progettazione



Riduzione del rischio



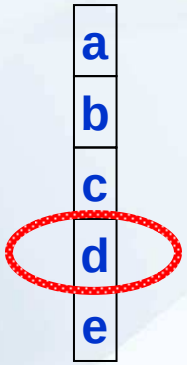
Validazione e manutenzione

La validazione serve a dimostrare che la combinazione dei vari SRP/CS che provvedono ad ogni funzione di sicurezza, è in accordo con tutte le richieste di questo standard

Manutenzione preventiva o correttiva, possono essere necessarie per mantenere le performance specificate per le parti relative alla sicurezza. Le informazioni per l'uso degli SRP/CS, devono contenere le istruzioni per la manutenzione (compresa l'ispezione periodica)

Livello di sicurezza raggiunto

Livello di sicurezza richiesto PL_r



Livello raggiunto PL

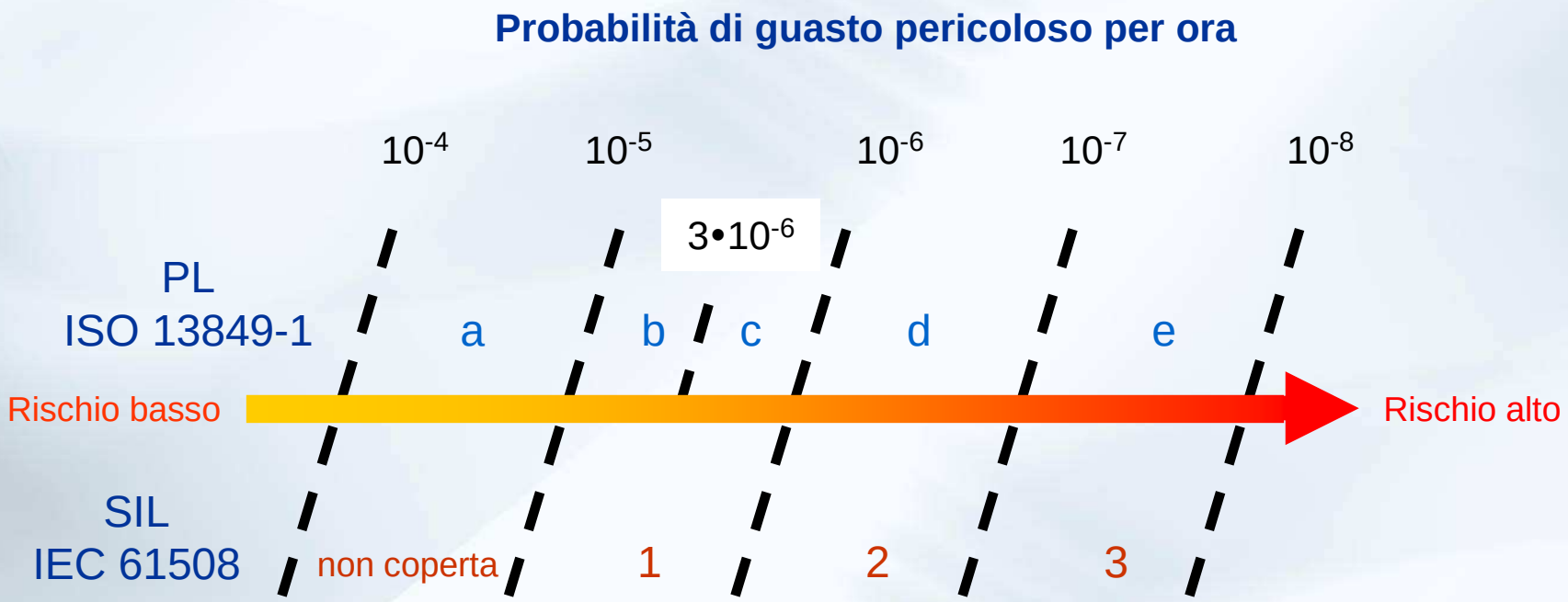
PL(low)	n (low)		PL
a	> 3	=>	--
	≤ 3	=>	a
b	> 2	=>	a
	≤ 2	=>	b
c	> 2	=>	b
	≤ 2	=>	c
d	> 3	=>	c
	≤ 3	=>	d
e	> 3	=>	d
	≤ 3	=>	e

Rappresentazione numerica

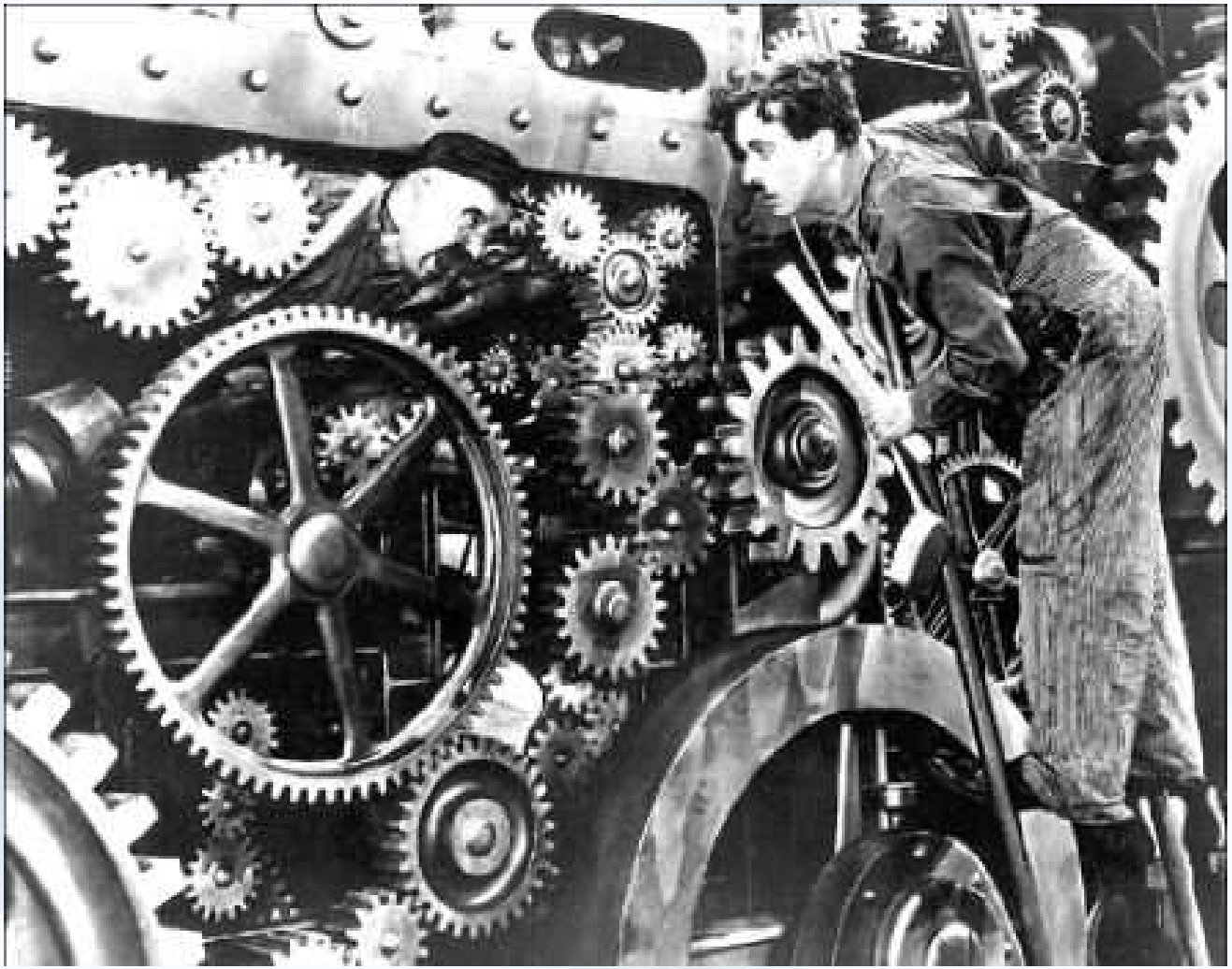
	Average probability of a dangerous failure per hour [1/h] and corresponding performance level (PL)															
$MTTF_d$ for each channel y	Cat. B DC_{avg} = none	PL	Cat. 1 DC_{avg} = none	PL	Cat. 2 DC_{avg} = low	PL	Cat. 2 DC_{avg} = medium	PL	Cat. 3 DC_{avg} = low	PL	Cat. 3 DC_{avg} = medium	PL	Cat. 4 DC_{avg} = high	PL
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-6}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-6}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		

	Average probability of a dangerous failure per hour [1/h] and corresponding performance level (PL)															
$MTTF_d$ for each channel y	Cat. B DC_{avg} = none	PL	Cat. 1 DC_{avg} = none	PL	Cat. 2 DC_{avg} = low	PL	Cat. 2 DC_{avg} = medium	PL	Cat. 3 DC_{avg} = low	PL	Cat. 3 DC_{avg} = medium	PL	Cat. 4 DC_{avg} = high	PL
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

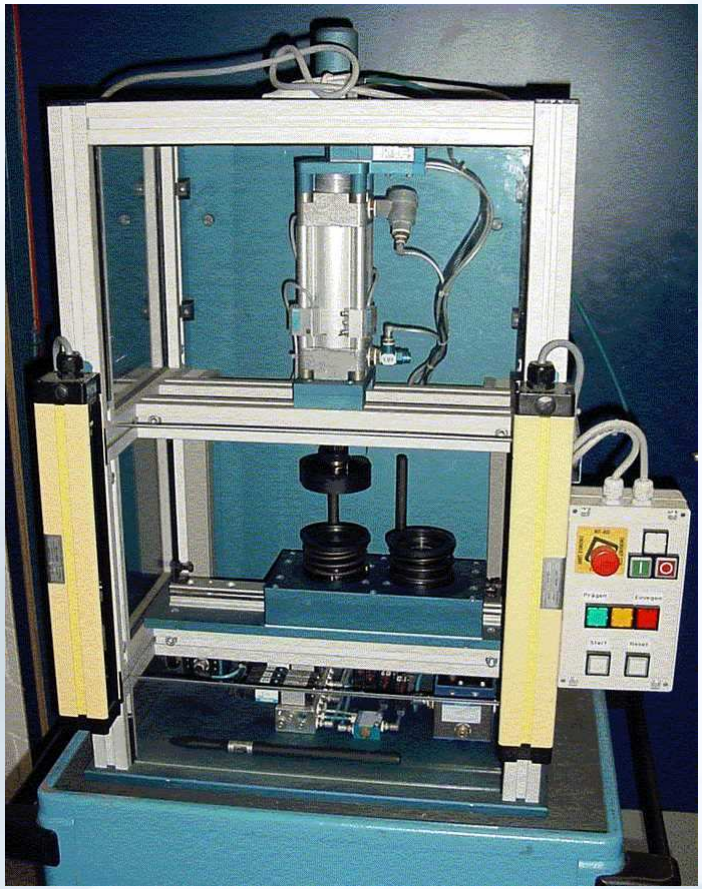
Relazione PFH_D - PL/SIL



Identificare la funzione di sicurezza



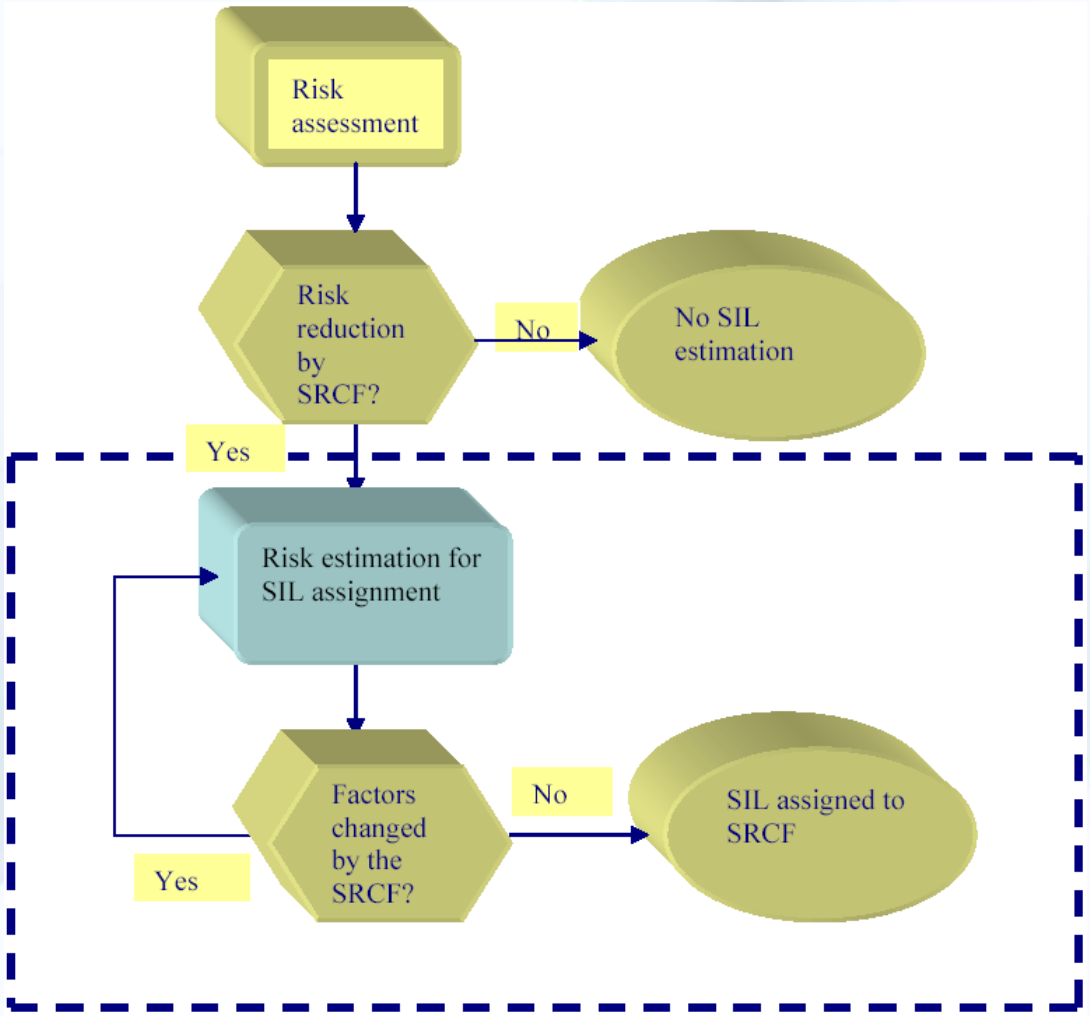
Funzione di controllo relativa alla sicurezza



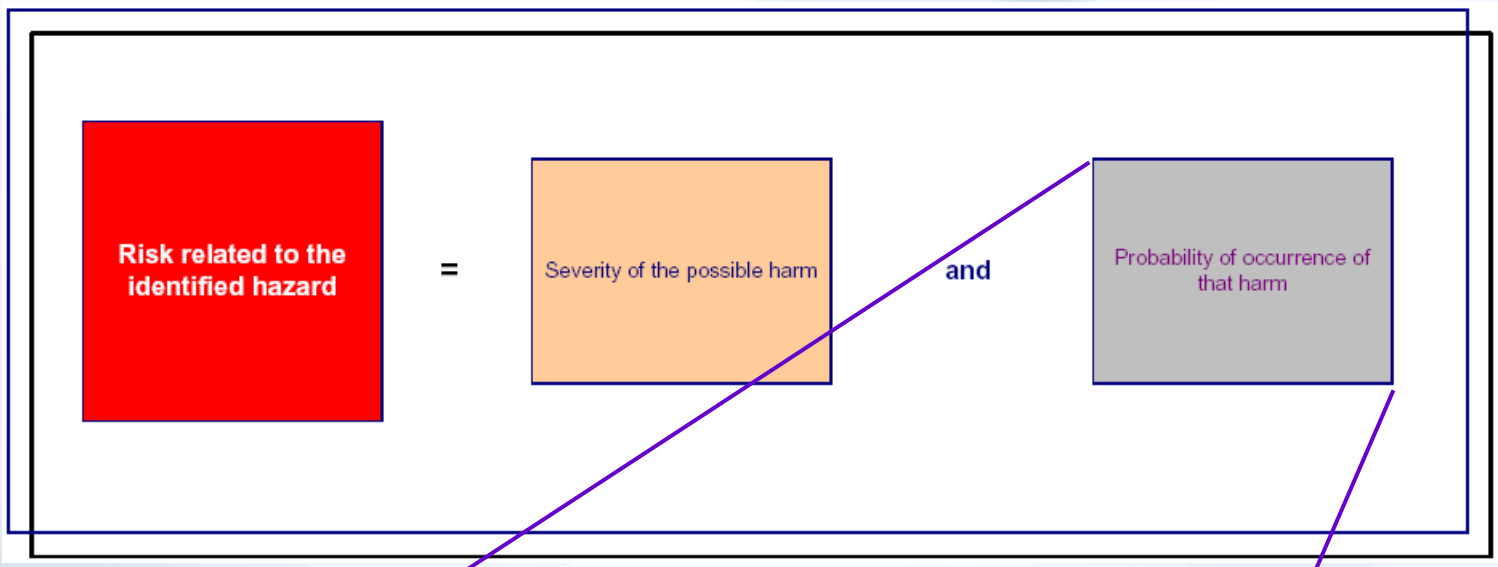
SRCF:

Il movimento del cilidro deve essere fermato quando il campo protetto della barriera viene infranto

Processo di riduzione del rischio



Stima del rischio



- Frequenza e durata dell'esposizione (Fr)
- Probabilità dell'accadere di un evento pericoloso (Pr)
- Probabilità di evitare o limitare il danno (Av)

Assegnazione del SIL

SIL assignment and safety measures

Document No.: _____
Part of: _____

Product: _____
Issued: _____
verified: _____
Date: _____

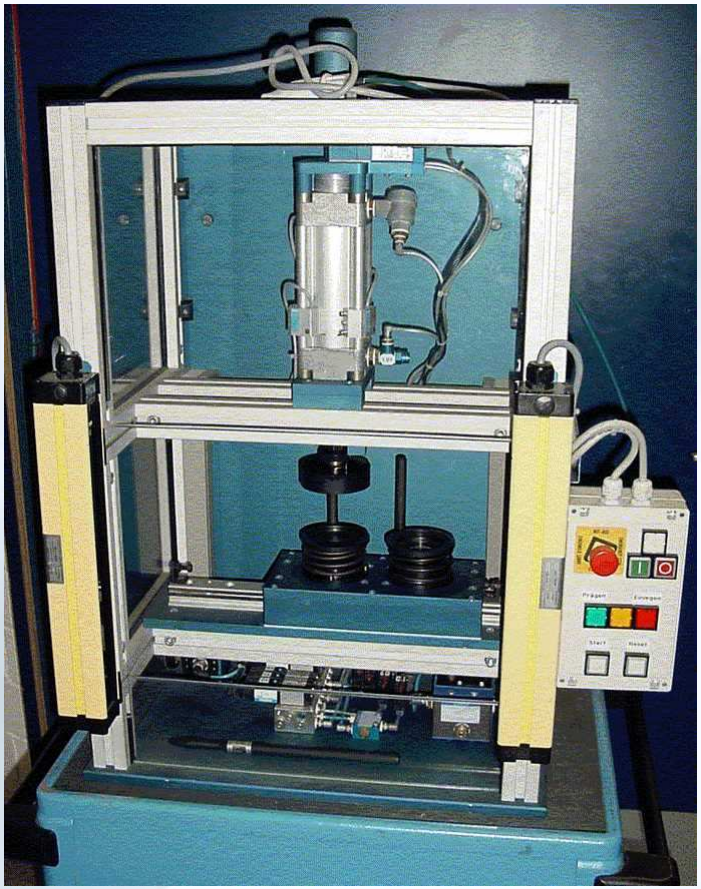
☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area - Safety measures required
Grey arey - Safety measures recommended

Consequences	Severity Se	Class Cl 3-4	5-7	8-10	11-13	14-15	Frequency, Fr (duration > 10min)		Probability of hzrd. Event, Pr		Avoidance, Av	
Death, losing an eye or an arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 hour	5	Common	5		
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1hr - ≤ 1day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	> 1day - ≤ 2wks	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	> 2wks - ≤ 1yr	3	Rarely	2	Possible	3
							> 1 year	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	RR
		Avvicinamento del battente	**3**	**5**	**3**	**3**	**11**	**Stop del cilindro**	

Funzione di controllo relativa alla sicurezza

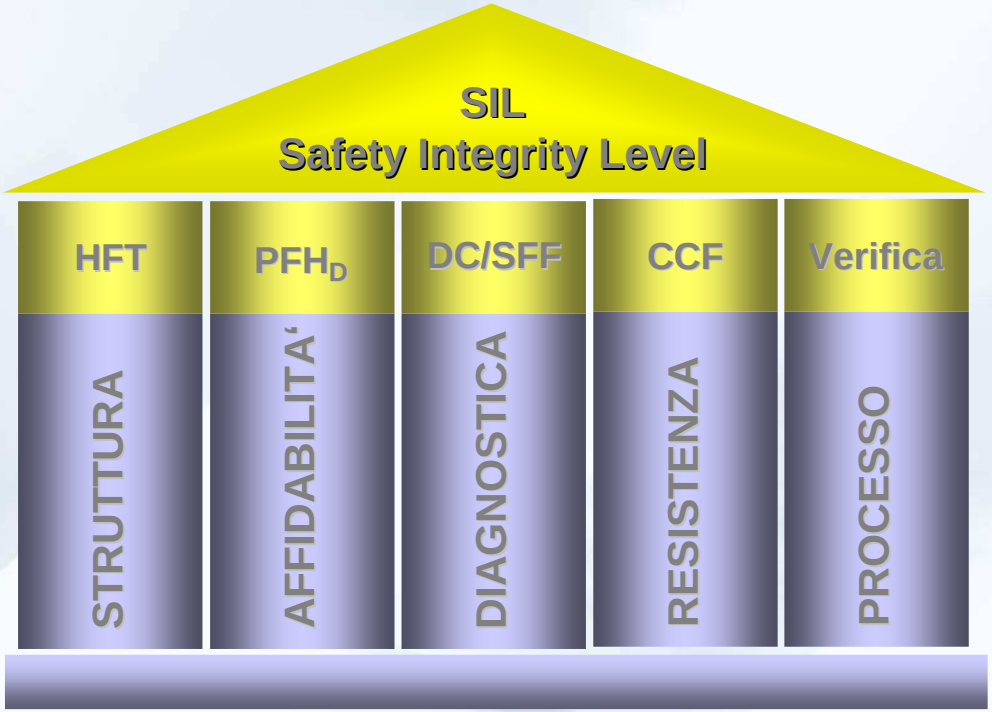


SRCF:

Il movimento del cilidro deve essere fermato quando il campo protetto della barriera viene infranto

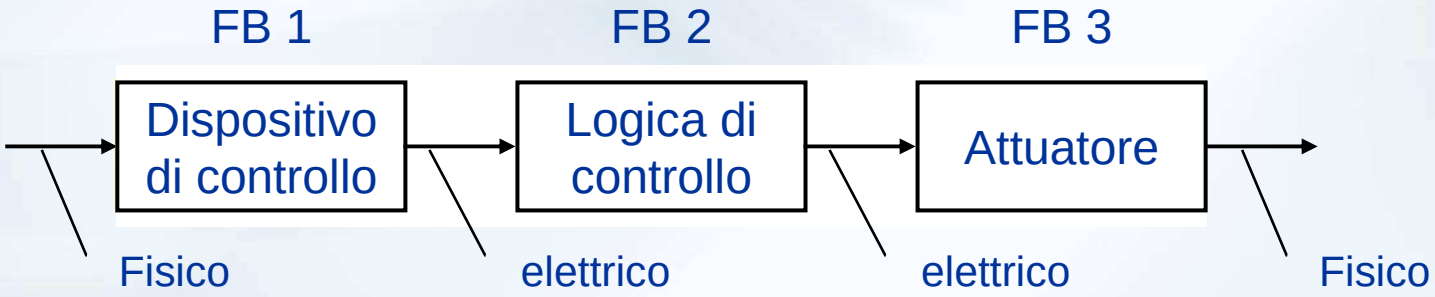
Livello di sicurezza richiesto: SIL 2

Determinare il SIL per lo SRECS



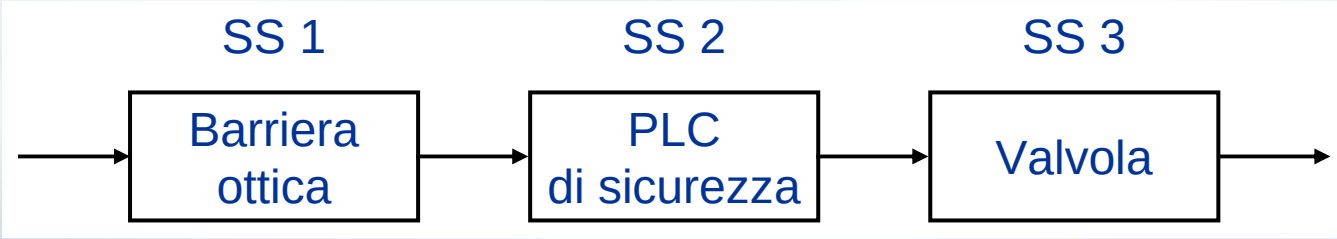
Aspetti strutturali

Divisione in blocchi funzione



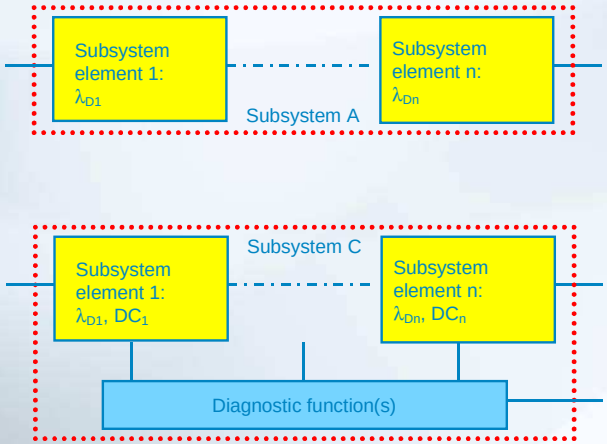
„Il più piccolo elemento di un SRCF, dove un guasto può causare la perdita della funzione di sicurezza“

Definire i sottosistemi

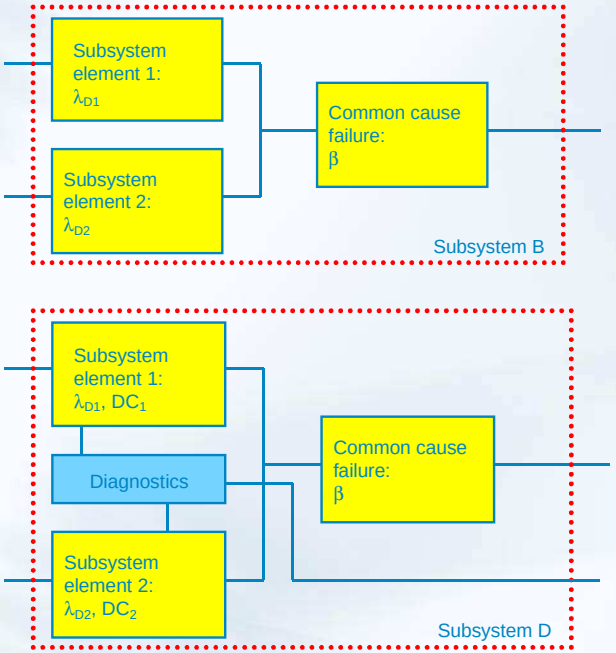


Elementi dei sottosistemi

HFT = 0

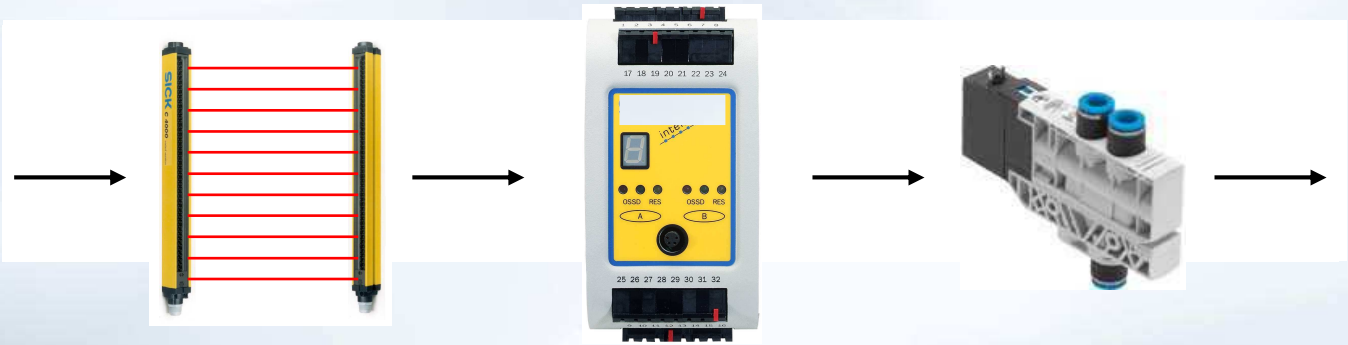


HFT = 1



„Parte di un sottosistema, comprensivo di un singolo componente o ogni gruppo di componenti“

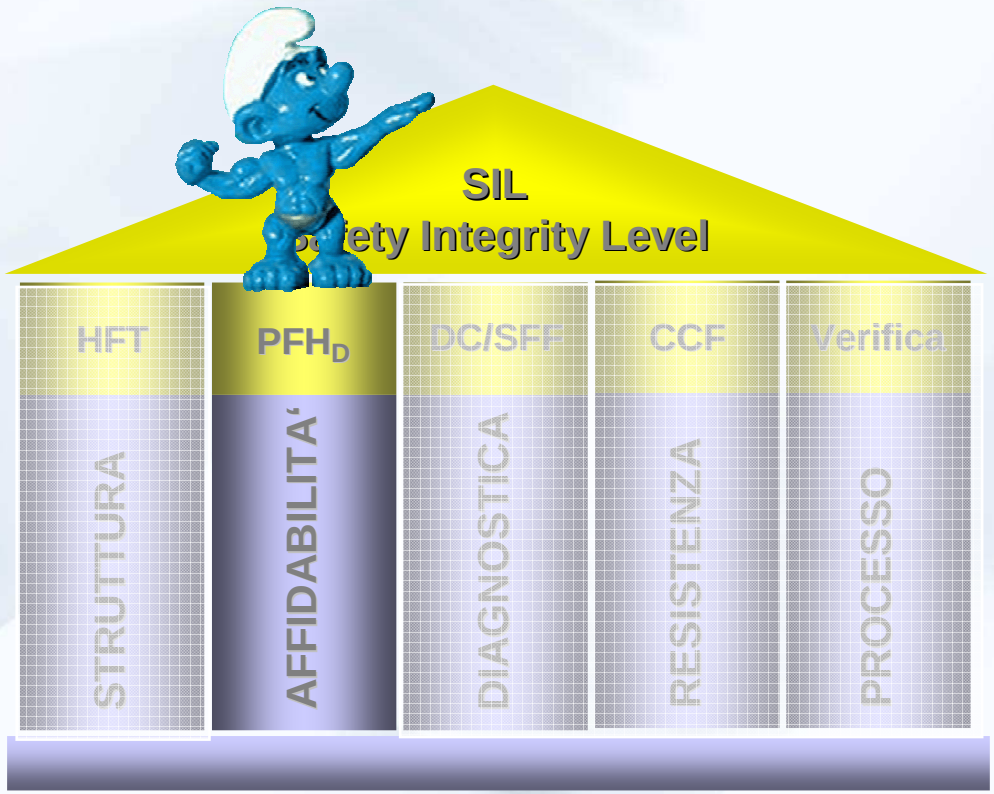
Architectural requirements



SIL richiesto ≥ 2 SIL richiesto ≥ 2 SIL richiesto ≥ 2

„Ogni sottosistema deve essere conforme al SIL dichiarato per il completo SRCF“

Aspetti di affidabilità



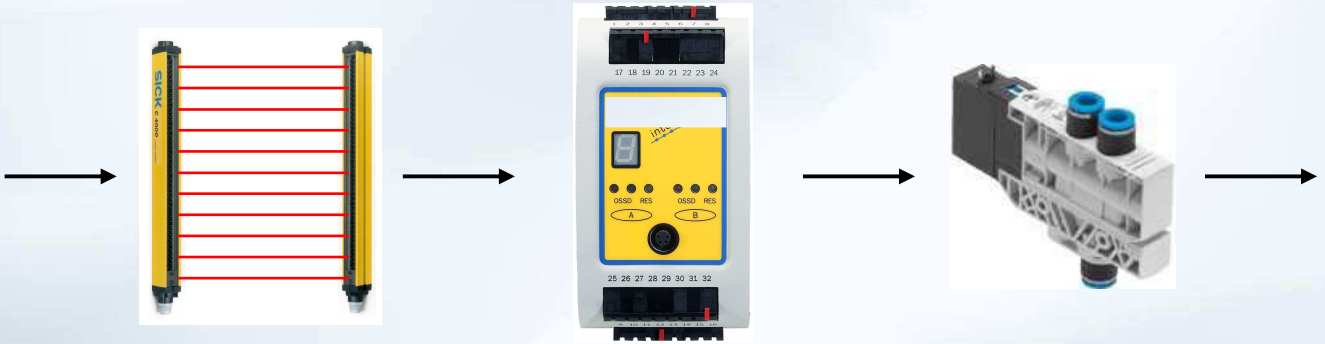
Probabilità di guasti „casuali“ pericolosi

SIL	Probabilità di guasti pericolosi per ora [1/h]
1	$10^{-6} \leq PFH_D < 10^{-5}$
2	$10^{-7} \leq PFH_D < 10^{-6}$
3	$10^{-8} \leq PFH_D < 10^{-7}$

$$PFH_D = PFH_{D1} + \ldots + PFH_{D2} + PFH_{TE}$$

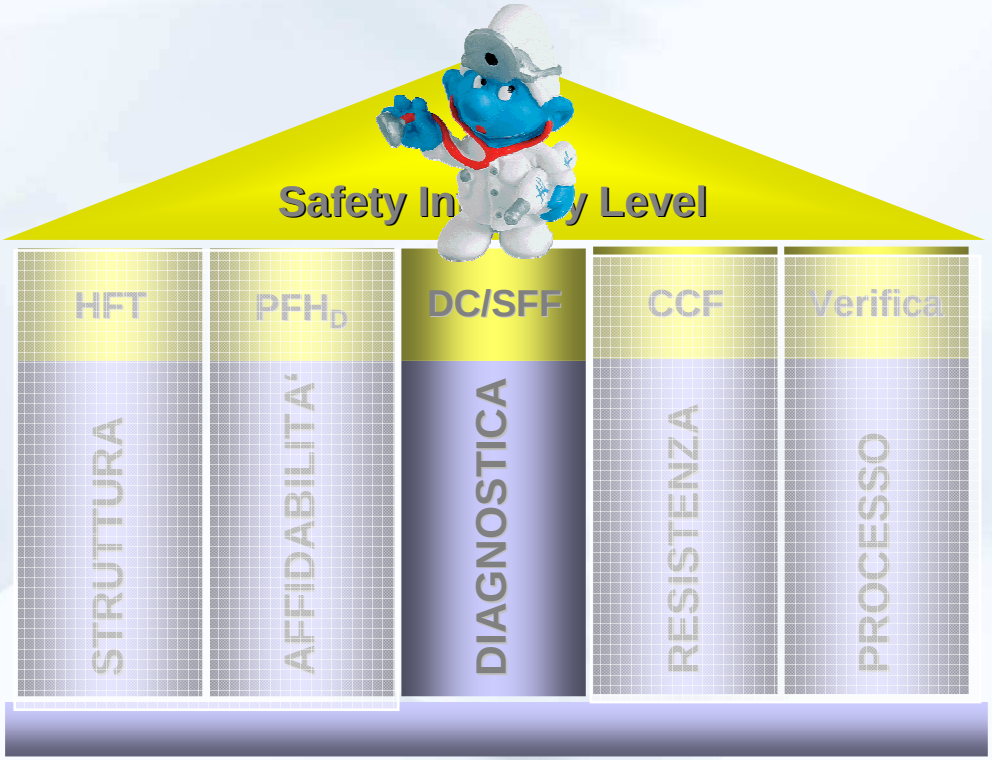
HW safety integrity requirements

PFH_{D1} PFH_{D2} PFH_{D3}



$$PFH_{D1} + PFH_{D2} + PFH_{D3} < 10^{-6}$$

Aspetti di diagnostica



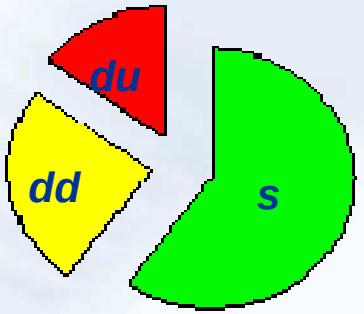
Diagnostic coverage

λ_{DU} Percentuale di guasti pericolosi non rilevati

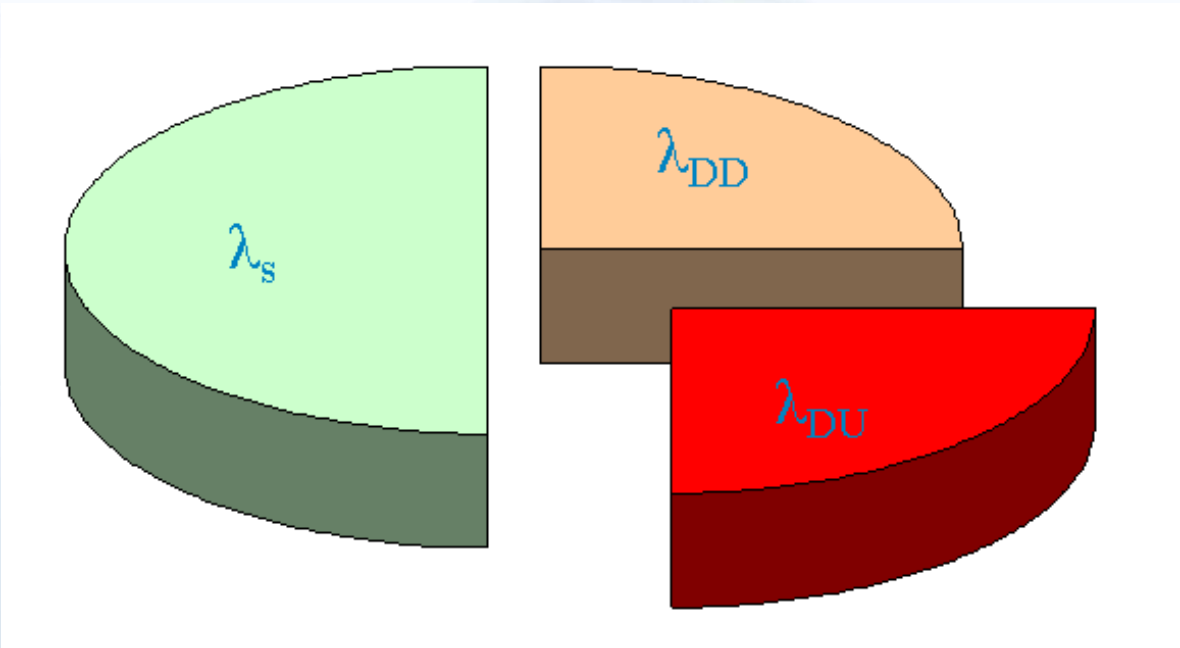
λ_D Percentuale di guasti pericolosi

λ_{DD} Percentuale di guasti pericolosi rilevati

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \lambda_{du}}$$

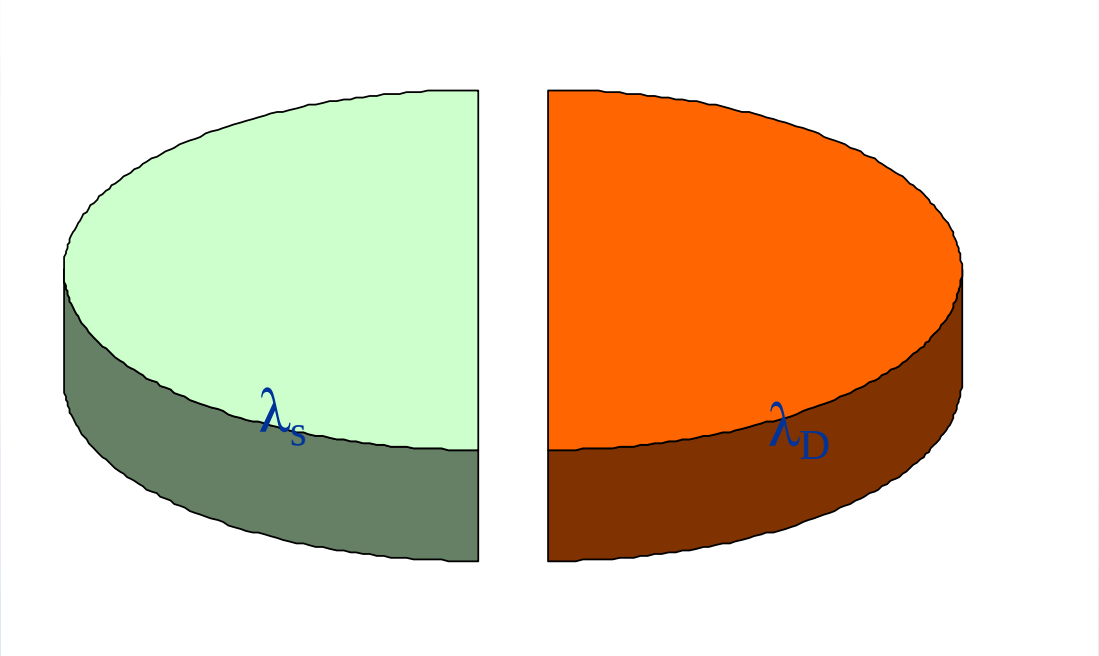


Safe failure fraction



$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$$

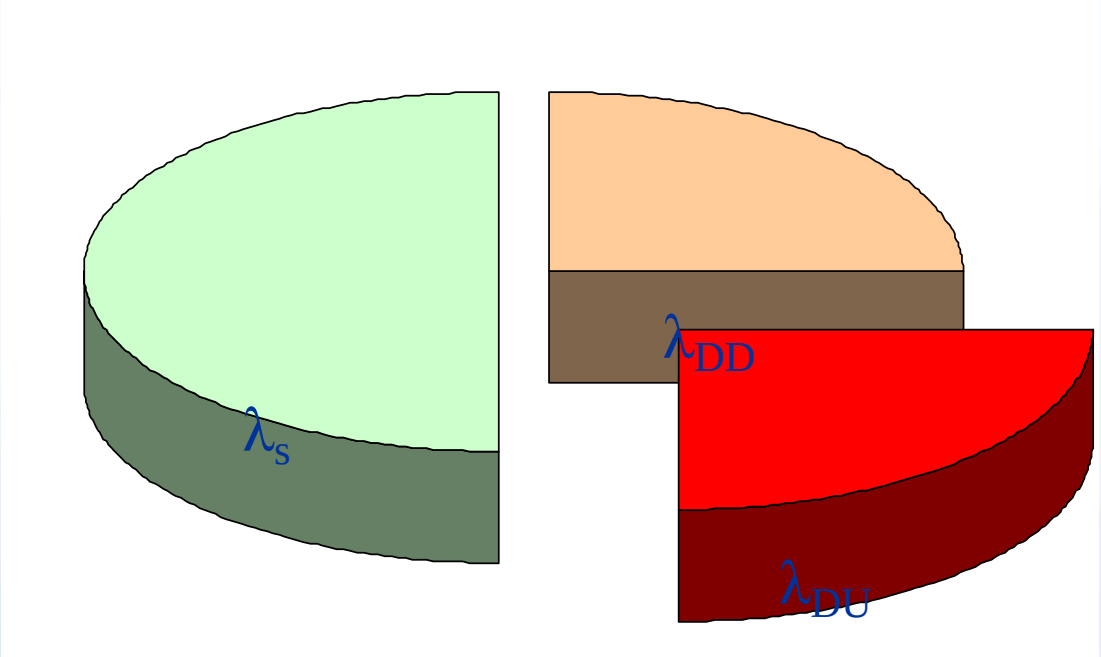
Differenza di calcolo DC e SFF 1/3



DC = 0%

SFF = 50%

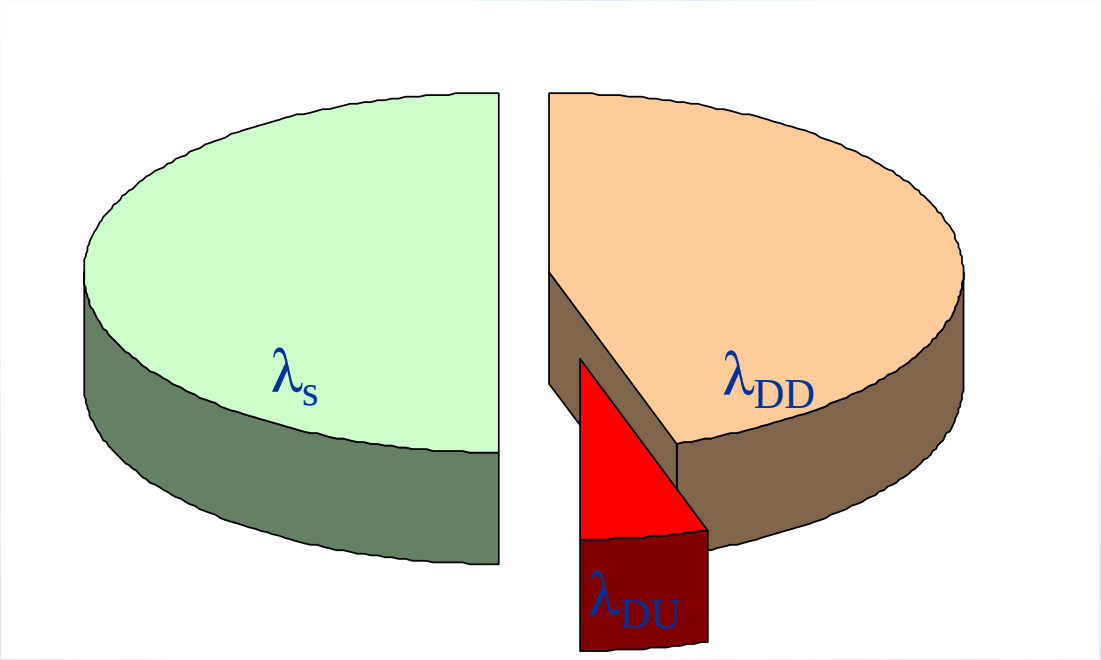
Differenza di calcolo DC e SFF 2/3



DC = 50%

SFF = 75%

Differenza di calcolo DC e SFF 3/3



DC = 90%

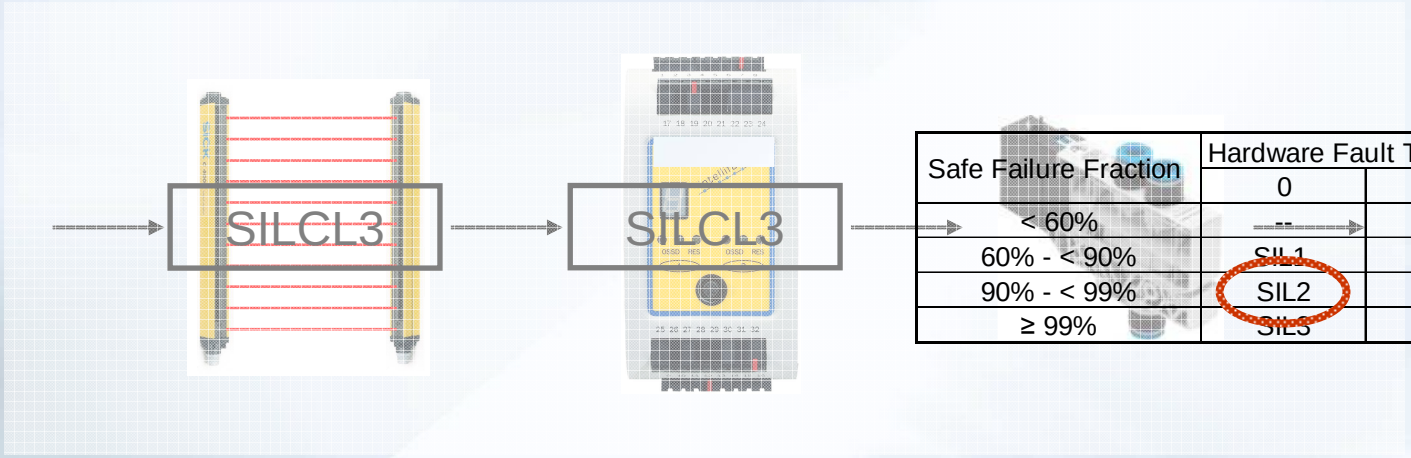
SFF = 95%

Restrizioni dell‘architettura

Safe Failure Fraction	Hardware Fault Tolerance	
	0	1
< 60%	--	SIL1
60% - < 90%	SIL1	SIL2
90% - < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

„Il SIL Raggiunto dallo SRECS in accordo con le restrizioni dell‘architettura, è minore od uguale al SILCL di ogni sottosistema coinvolto nelle performance del SRCF“

Hardware safety integrity - Target



Safe Failure Fraction	Hardware Fault Tolerance	
	0	1
< 60%	--	SIL1
60% - < 90%	SIL1	SIL2
90% - < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

SILCL 2 SILCL 2 SILCL 2

I modi di guasto della valvola

Table D.1 – Examples of the failure mode ratios for electrical/electronic components

Component	Failure mode	Typical failure mode ratios %
Solenoid valve	Does not energize	5
	Does not de-energize	15
	Change of switching times	5
	Leakage	65
	Other failure modes (see Note 4)	10

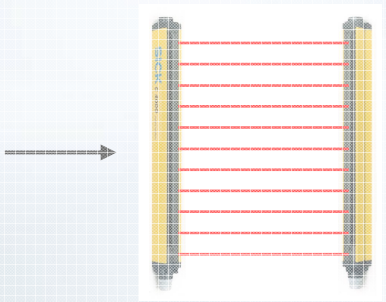
NOTE 4 Other failure modes that apply to a solenoid valve include:

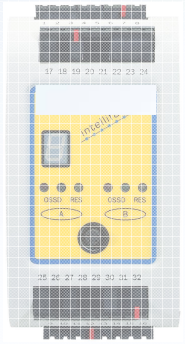
- non-switching (sticking in the end or zero position) or incomplete switching (sticking in a random intermediate position);
- spontaneous change of the init
- change in the leakage flow rate
- bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws;
- pneumatic/hydraulic faults which cause uncontrolled behaviour for servo and proportional valves.

Failure mode/mechanism distributions FMD-91, RAC 1991

SFF = 70%

Hardware safety integrity - Risultato





SFF	HFT		
	0	1	2
<60%	÷	SIL1	SIL2
60% to < 90%	SIL1	SIL2	SIL3
90% to <99%	SIL2	SIL3	SIL3
≥ 99%	SIL3	SIL3	SIL3

✓ ✓ ☹

SILCL 2 SILCL 2 SILCL 2

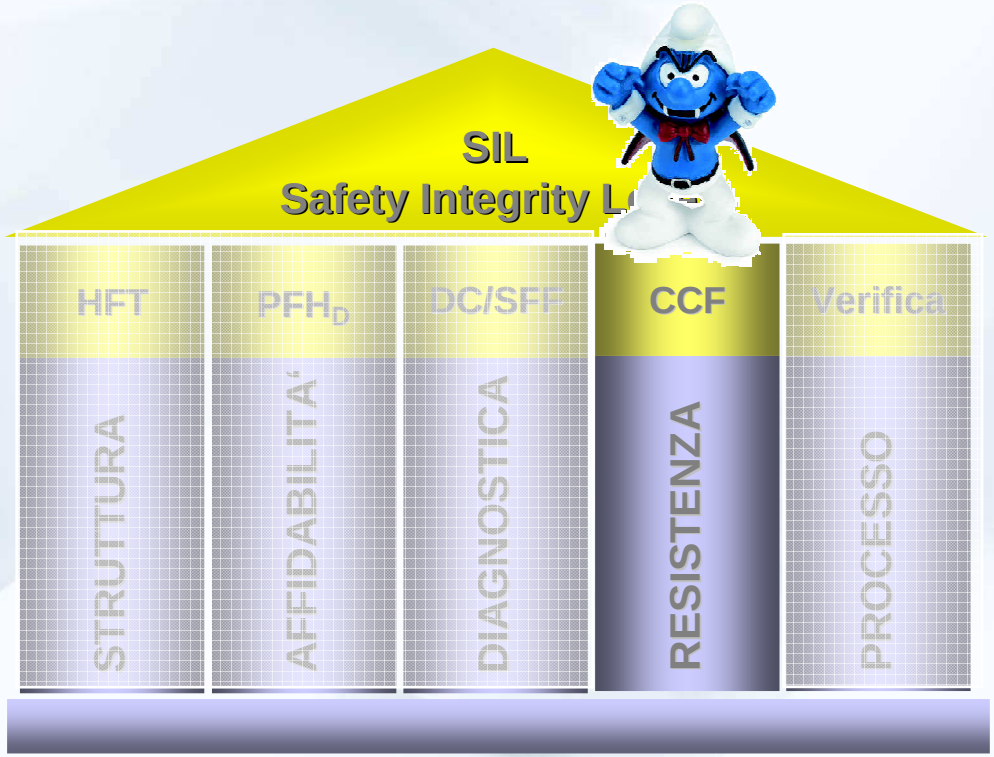
Sottosistemi a bassa complessità

?

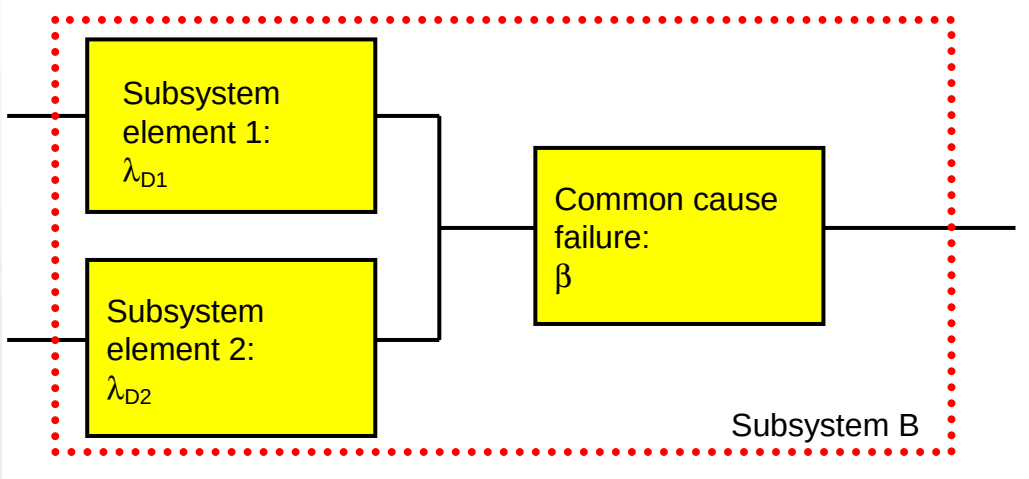
Safe Failure Fraction	Hardware Fault Tolerance	
	0	1
< 60%	--	SIL1
60% - < 90%	SIL1	SIL2
90% - < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

„Collegare in parallelo due sottosistemi a bassa complessità, entrambi rispondenti alle richieste dell'architettura per SIL1 "

Aspetti di resistenza



Causa di guasto comune



„Guasto che causa guasti contemporanei su due o più canali in un sottoinsieme multicanale“

Misure contro CCF

Table F.1 - Criteria for estimation of CCF

Item	Max. Score
Separation / segregation	25
Diversity / redundancy	38
Complexity / design / application	2
Assessment / analysis	18
Competence / training	4
Environmental control	18

Table F.2 - Estimation of CCF factor (ß)

Overall score	CCF factor (ß)
< 35	10%
35 ÷ 65	5%
65 ÷ 85	2%
85 ÷ 100	1%

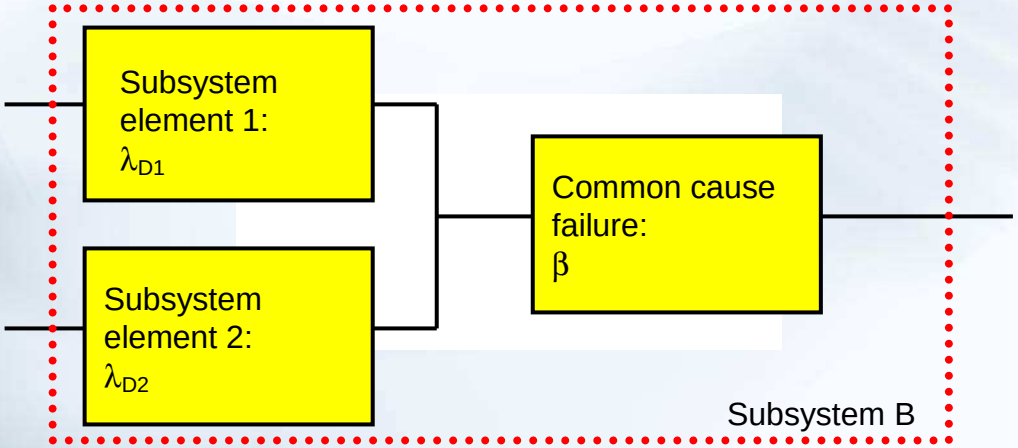
„L'allegato F fornisce un approccio semplice per il calcolo del CCF"

Tabella CCF

Table F.1 – Criteria for estimation of CCF

Item	Reference	Score
Separation/segregation		
Are SRECS signal cables for the individual channels routed separately from other channels at all positions or sufficiently shielded?		5
Where information encoding/decoding is used, is it sufficient for the detection of signal transmission errors?		10
Are SRECS signal and electrical energy power cables separate at all positions or sufficiently shielded?		5
If subsystem elements can contribute to a CCF, are they provided as physically separate devices in their local enclosures?		5
Diversity/redundancy		
Does the subsystem employ different electrical technologies for example, one electronic or programmable electronic and the other an electromechanical relay?		8
Does the subsystem employ elements that use different physical principles (e.g. sensing elements at a guard door that use mechanical and magnetic sensing techniques)?		10
Does the subsystem employ elements with temporal differences in functional operation and/or failure modes?		10
Do the subsystem elements have a diagnostic test interval of ≤1 min?		10
Complexity/design/application		
Is cross-connection between channels of the subsystem prevented with the exception of that used for diagnostic testing purposes?		2
Assessment/analysis		
Have the results of the failure modes and effects analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		9
Are field failures analysed with feedback into the design?		9
Competence/training		
Do subsystem designers understand the causes and consequences of common cause failures?		4
Environmental control		
Are the subsystem elements likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc. over which it has been tested, without the use of external environmental control?		9
Is the subsystem immune to adverse influences from electromagnetic interference up to and including the limits specified in Annex E?		9
NOTE An alternative item (e.g. references 1a and 1b) is given in Table F.1 where it is intended that a claim can be made for a contribution towards avoidance of CCF from only the most relevant item.		

Calcolo del PFH_D



$$PFH_d \approx \beta \cdot (\lambda_{D1} + \lambda_{D2})/2 \cdot 1/h$$
$$= \beta \cdot \lambda_D / \lambda \cdot \lambda_{Valve} \cdot 1/h$$
$$= 5\% \cdot 30\% \cdot 0{,}1 \cdot C/B10 \cdot 1h$$
$$= 5\% \cdot 30\% \cdot 0{,}1 \cdot 2C/B10_D \cdot 1h$$
$$= \frac{0{,}05 \cdot 0{,}3 \cdot 0{,}1 \cdot 2 \cdot 60/h}{20.000.000} \cdot 1h$$

$PFH_D = 9{,}0 \cdot 10^{-9}$

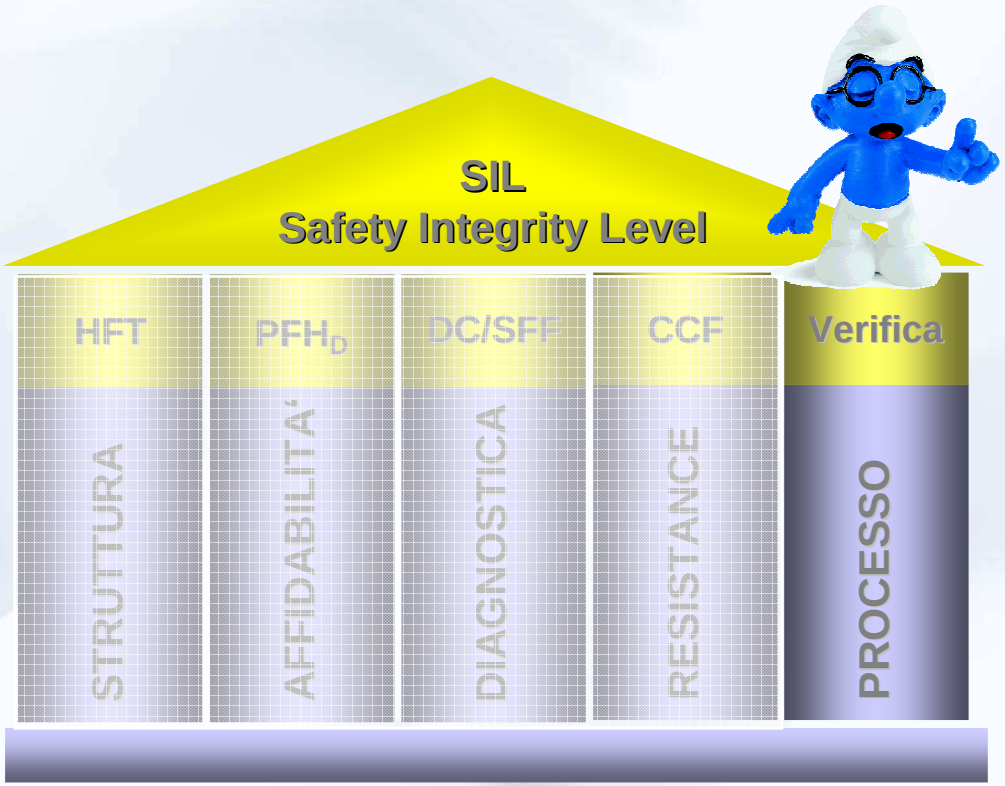
Table F.2 - Estimation of CCF factor (β)

Overall score	CCF factor (β)
< 35	10%
35 ÷ 65	5%
65 ÷ 85	2%
85 ÷ 100	1%

ISO 13849:
$B10_D$ = 20.000.000 Switching cycles

Assumption:
C = 60 /h

Aspetti di processo

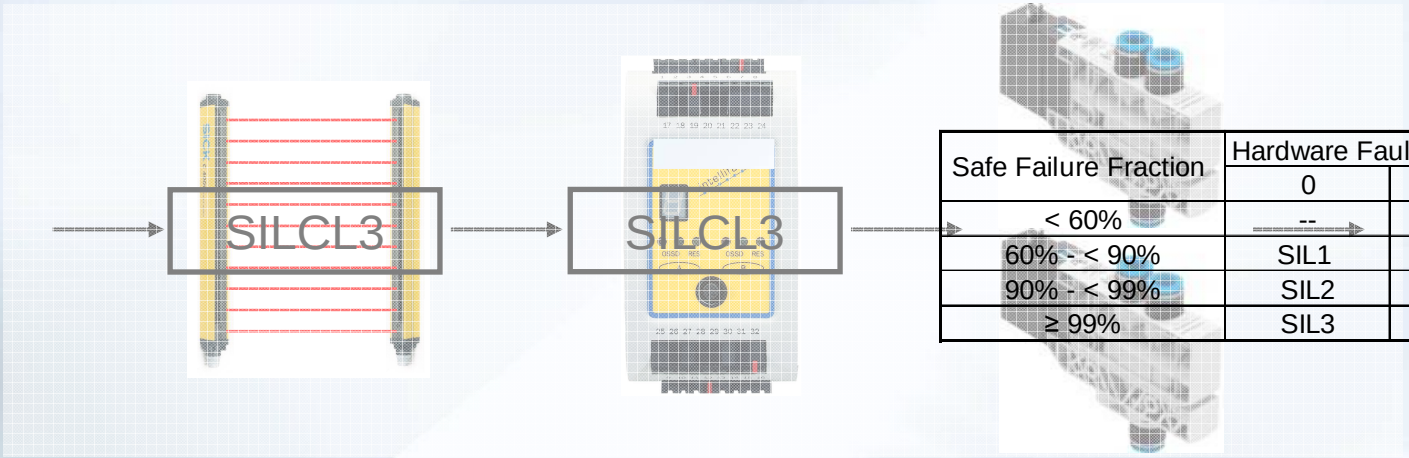


Safety related control function

$PFH_D = 2{,}5 \cdot 10^{-8}$ $PFH_D = 8{,}0 \cdot 10^{-9}$ $PFH_D = 9{,}0 \cdot 10^{-9}$

$$\Sigma\ PFH_D = 4{,}2 \cdot 10^{-8} < 10^{-6}$$

Hardware safety integrity



Safe Failure Fraction	Hardware Fault Tolerance	
	0	1
< 60%	--	SIL1
60% - < 90%	SIL1	SIL2
90% - < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

$$\Sigma\ PFH_D = 4{,}2 \cdot 10^{-8} < 10^{-6}$$

SIL 2

Misure contro i guasti sistematici

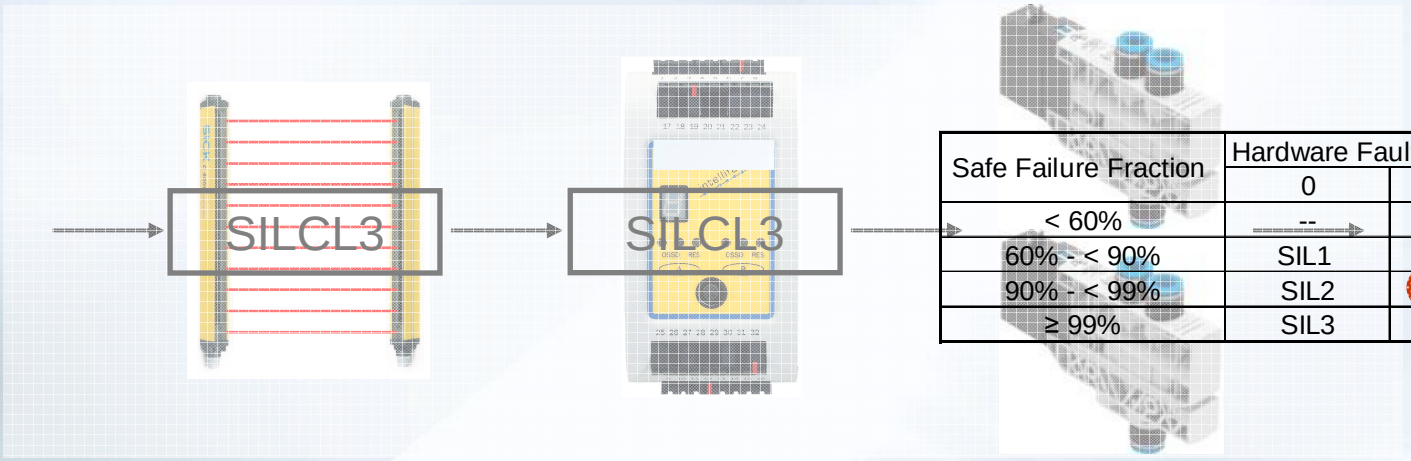
Misure contro i guasti sistematici

Per il controllo dei guasti sistematici, le seguenti misure devo essere applicate:

- individuazione dei guasti con monitoraggio on-line;
- test, tramite comparazione, dell‘ hardware ridondante;
- hardware diversi;
- operare in logica positiva (es. Un interruttore di posizione è premuto con protezione aperta);
- sovradimensionare con un fattore adatto, quando il produttore può dimostrare che questo aumenta l‘affidabilità.

Hardware safety integrity

Con la diagnostica !



Safe Failure Fraction	Hardware Fault Tolerance	
	0	1
< 60%	--	SIL1
60% - < 90%	SIL1	SIL2
90% - < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

$$\Sigma\ PFH_D = 4{,}2 \cdot 10^{-8} < 10^{-7}$$

SIL 3

L‘importanza dell‘informazione