FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE

CONFINDUSTRIA

DAL 1945 IL VALORE DELL'INNOVAZIONE

# Le nuove norme armonizzate

# EN ISO 13849-1 e EN 62061

**La norma EN 954-1 verrà ritirata il 28.12.2009, il giorno prima dell'entrata in vigore della nuova D.M 2006/42/CE.**

## EN 954-1 Sicurezza del macchinario – Parti dei sistemi di comando legate alla sicurezza - Principi generali per la progettazione.

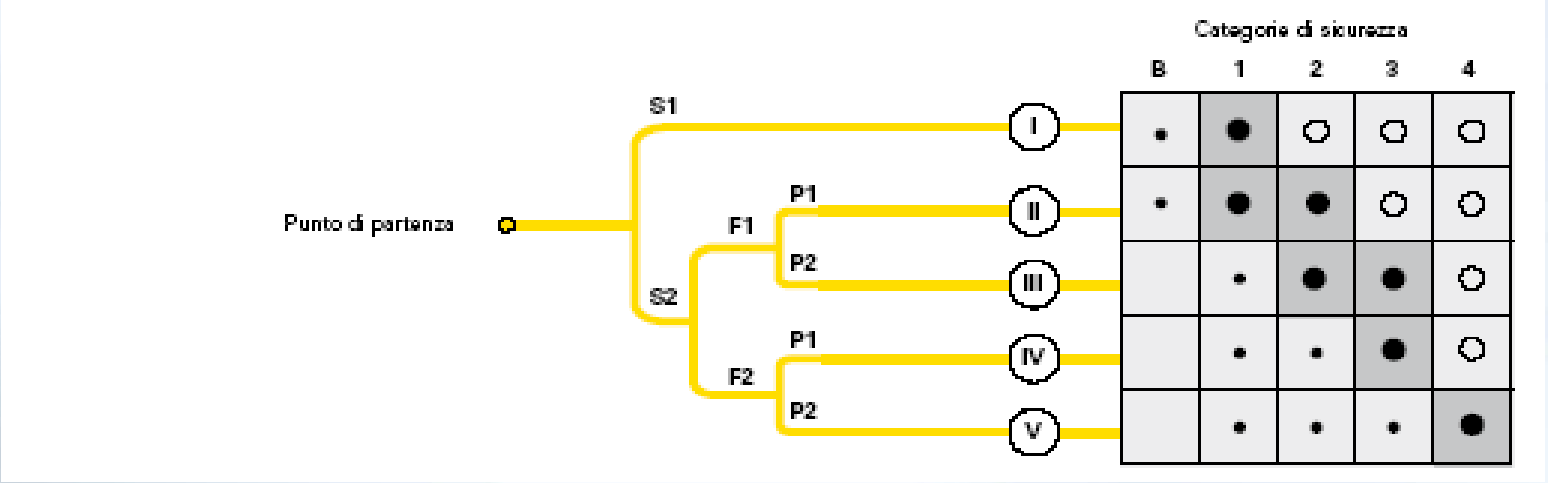
**E’ norma armonizzata dal 1996.**

**Stabilisce i criteri da adottare nella progettazione dei sistemi di controllo di sicurezza delle macchine.**

# Non rappresenta più lo stato dell’arte

# EN 954-1: Tre grossi difetti

**1** **La selezione della categoria di sicurezza tramite l'uso del cosiddetto grafico dei rischi non è oggettiva.**




● **Preferite**

**Si vede che all'aumentare della frequenza di esposizione al rischio e del grado di severità del danno sono da preferire le categorie che forniscono una capacità di rilevamento dei guasti più alta.**

# Categorie

**La resistenza ai guasti delle Cat. B e Cat.1 trae origine dalla affidabilità dei componenti ( si cerca di evitare il guasto).**

**La resistenza ai guasti delle categorie 2,3,4 trae origine dalla struttura del sistema (si cerca di controllare il guasto)**
**In particolare si controlla il guasto tramite monitoraggio ciclico per la Cat.2, ridondanza per la Cat.3 , ridondanza e monitoraggio per la Cat.4.**

**Tuttavia il comportamento ai guasti non può essere il solo metodo per stabilire il grado di sicurezza di un sistema**

Occorre considerare altri fattori, come ad esempio l'affidabilità dei componenti, che possono svolgere un ruolo importante, forse determinante nel stabilire il grado di sicurezza di un sistema.

Questo concetto in verità è stato riconosciuto nella norma EN 954-1 in cui si afferma (allegato B) che "l'affidabilità dei componenti e la tecnologia utilizzata nella particolare applicazione possono portare ad una deviazione dalla categoria prevista"

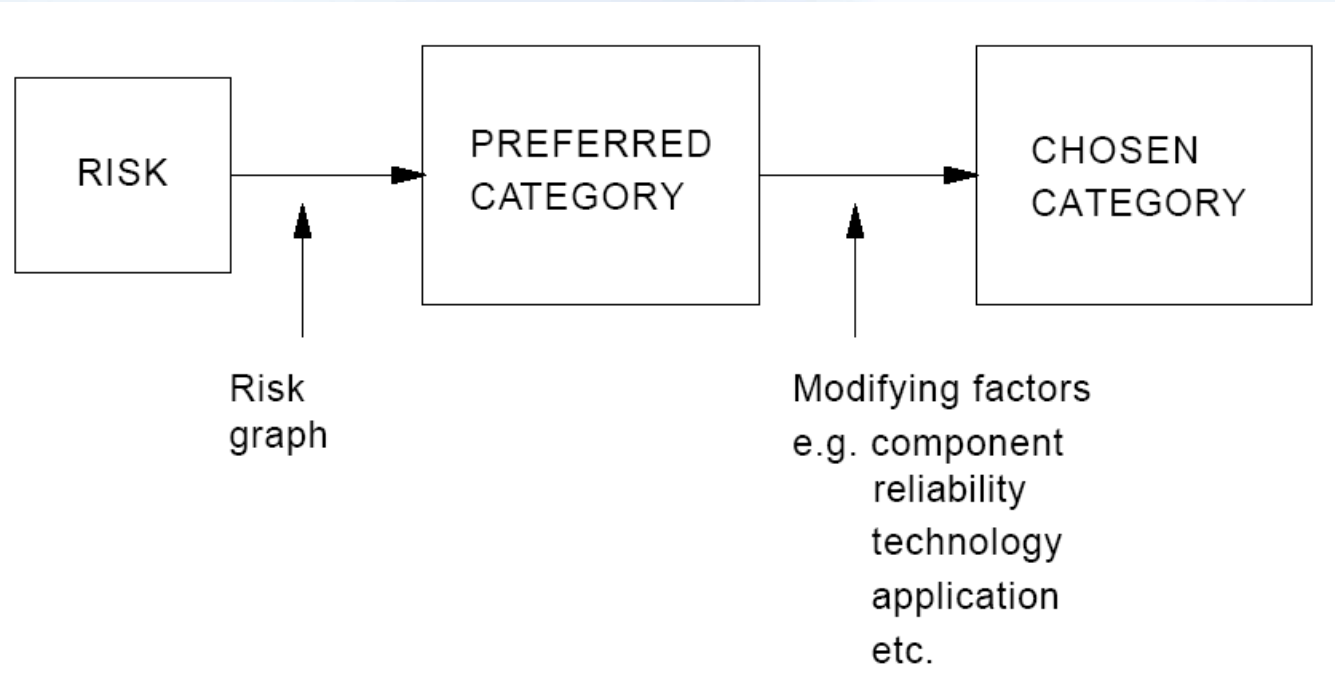
Quindi, mentre la scelta della categoria teorica è correlata al rischio, la categoria che dovrebbe essere adottata, considerando tutti i fattori, potrebbe essere diversa.

E' per questo motivo che nel grafico dei rischi sono elencate più scelte (oltre a quelle preferite).

## Il processo di selezione dovrebbe essere quindi il seguente:

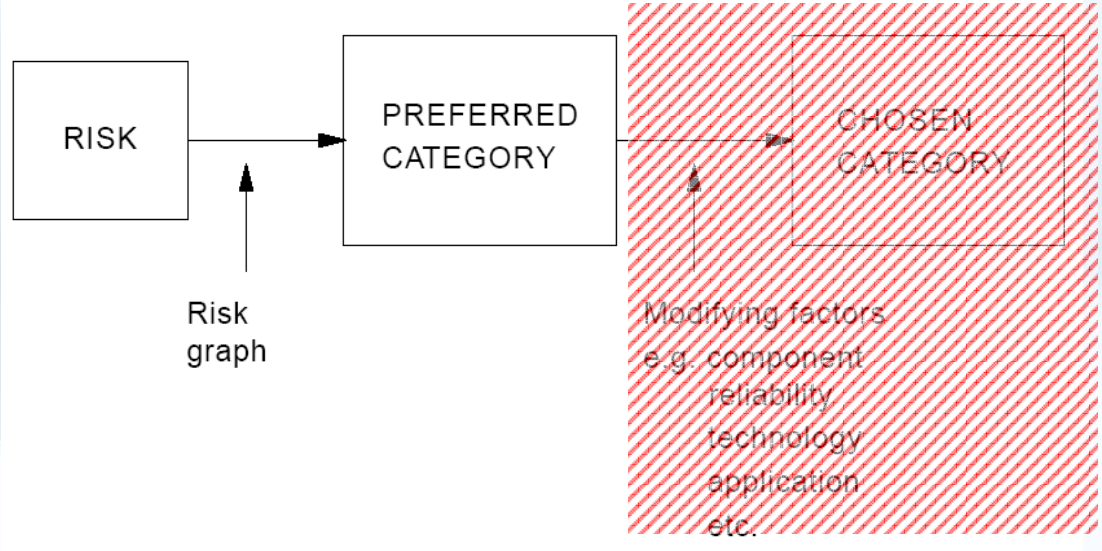
**si individua prima la Categoria teorica, o di "Riferimento" sulla base dell'analisi del rischio(tramite il grafico dei rischi)**

**quindi si modifica la scelta della categoria in base alla affidabilità dei componenti, alla tecnologia utilizzata, ecc.**



**Purtroppo la seconda fase di questo processo è in gran parte empirica, e poche indicazioni vengono fornite all'interno della norma.**

**Di conseguenza la selezione della categoria viene quasi sempre fatta riferendosi solo al grafico dei rischi senza considerare le modifiche dovute ad altri fattori oppure le modifiche apportate sono di natura così soggettiva che poi diventa difficile comprovare la sicurezza del sistema.**



**2** La strategia di rilevamento dei guasti pericolosi è puramente deterministica. Non è quindi adeguata nel caso di sistemi di automazione complessi.

***Es. Non è possibile analizzare gli effetti di tutti i guasti che possono capitare nei circuiti interni di un microcontrollore o di un PLC.***

**3** Non prevede l'uso di Software e di linee seriali di comunicazione di sicurezza fra sensori, sistema di controllo e azionamenti.

## Come fare per trovare una soluzione agli inconvenienti elencati?

**Occorre ri-definire il “grafico dei rischi” in modo che i requisiti di sicurezza in funzione del rischio individuato siano  univoci.**

**Occorre svincolarsi dall’approccio deterministico (impraticabile per sistemi complessi).**

**Occorre tener conto della affidabilità dei componenti**

**Un metodo che si può usare per valutare la prestazione di sicurezza di un sistema complesso è quello di calcolare la probabilità che possa capitare un guasto pericoloso in un determinato periodo di tempo tenendo conto dell'affidabilità dei suoi componenti.**

**Più il sistema è sicuro più è improbabile che capiti un guasto pericoloso.**

# Affidabilità dei sistemi

**L'affidabilità vera di un sistema non è mai nota esattamente, però la statistica e il calcolo delle probabilità ci offrono lo strumento per stimarla.**

**La probabilità di un sistema di non guastarsi durante il suo funzionamento è misurata dal suo tasso di guasto λ (numero di guasti per ora).**

**Il suo inverso, detto tempo medio fra i guasti, è misurato in ore ed è comunemente indicato con la sigla MTBF (mean time between failures) oppure MTTF (mean time to failure) nel caso di sistemi non riparabili.**

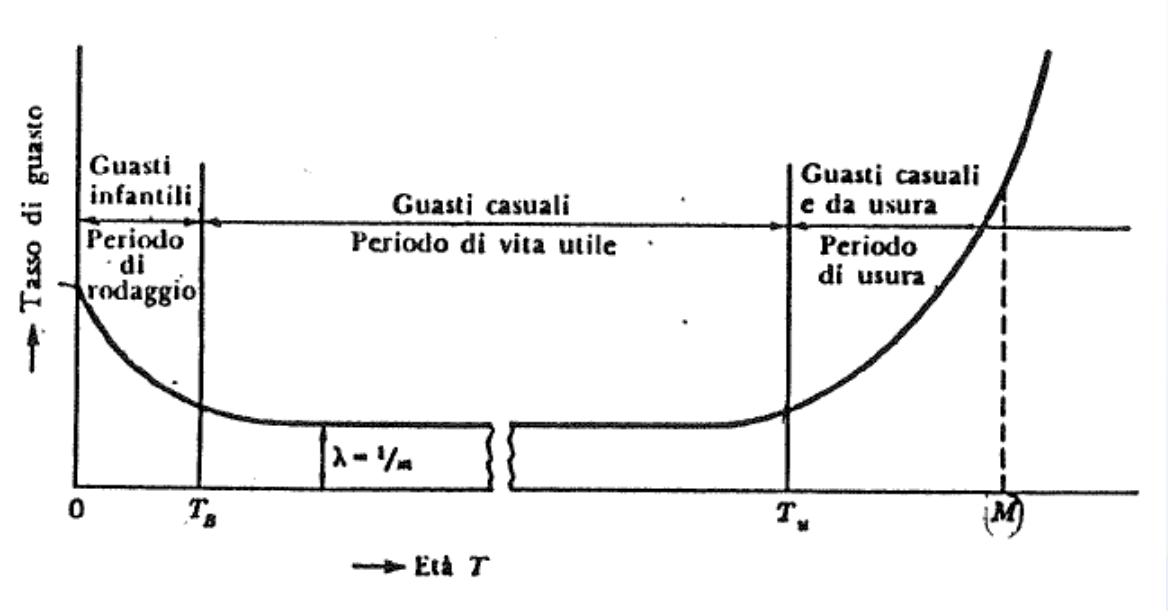
**Per calcolare l'affidabilità di un sistema conviene suddividere i guasti in:**

**infantili** **casuali** **per usura**

⇨ **perchè seguono distribuzioni statistiche diverse , quindi richiedono trattazioni matematiche diverse per la valutazione dei loro effetti.**

⇨ **perchè occorre ricorrere a metodi diversi per poterli eliminare**

## Andamento del tasso di guasto dei componenti in funzione dell'età




**Dopo il rodaggio il valore di tasso di guasto rimane approssimativamente costante per un certo periodo di tempo (T*u* – T*a*) cui si dà il nome di vita utile.**

**Nell'intervallo di tempo che va da T*u* a M circa la metà dei componenti sopravissuti subirà guasti. Il tempo M è la vita media per usura (la vita media va distinta dal tempo medio tra i guasti relativo al periodo di vita utile).**

**Guasti infantili** – sono in gran parte dovuti a inadeguatezza delle tecniche di costruzione e di controllo della qualità durante il processo di fabbricazione

Si possono eliminare mediante il processo di "rodaggio"

**Guasti per usura** – Si verificano soltanto se l'apparato non è sottoposto a perfetta manutenzione.

Nota la distribuzione statistica dei guasti per usura è possibile calcolare per via matematica la probabilità di guasto per usura a qualsiasi età del componente.

E' possibile quindi stabilire i periodi di revisione o di sostituzione preventiva.

**Guasti casuali** – tipo di guasti che nessun rodaggio, per quanto accurato, né alcuna manutenzione possono eliminare

Sono provocati da improvvisi accumuli di sollecitazioni oltre la resistenza massima di progetto del componente.

Si verificano ad intervalli casuali in maniera improvvisa del tutto inaspettata

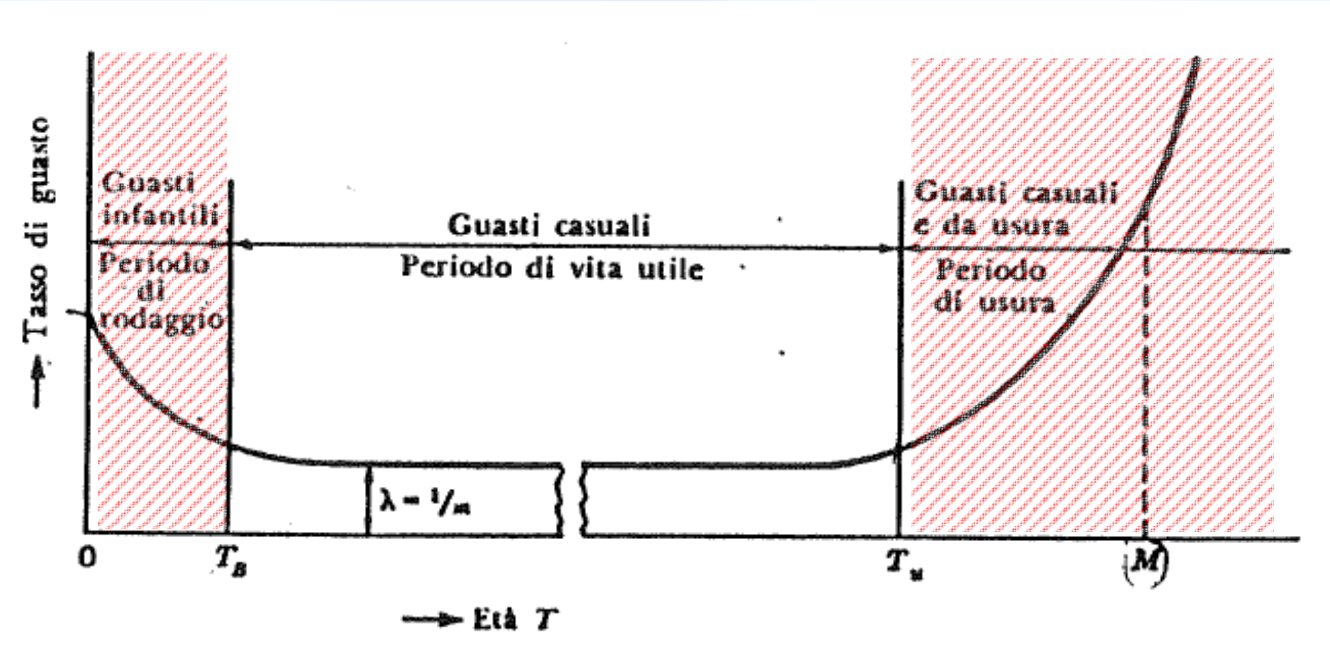
La frequenza di guasto presa su tempi sufficientemente lunghi è pressochè costante

Benché non sia in alcun modo possibile, per definizione, determinare il tempo in cui si verifica un guasto casuale, la teoria consente di calcolare la probabilità che questi guasti possano capitare entro un determinato periodo di funzionamento.

**I metodi descritti nelle due norme si riferiscono solo alla stima dei guasti casuali.**

**I guasti infantili vanno eliminati tramite adeguato rodaggio**

**I guasti per usura vanno eliminati adottando adeguate procedure di manutenzione preventiva.**



**Al contrario, non c'è tecnica di sostituzione che possa eliminare i guasti casuali, in ragione del tasso di guasto costante durante il periodo di vita utile.**

**La miglior cosa che si può fare durante il periodo di vita utile è sostituire i componenti appena si guastano.**

**Tuttavia, nessun componente deve essere mantenuto in servizio dopo il tempo T*u*, in caso contrario l'affidabilità del sistema scenderebbe a valori ridicoli.**

***Regola aurea dell'affidabilità:***

***Nel periodo di vita utile sostituire i componenti appena si guastano; un po' prima della fine del periodo di vita utile effettuare una sostituzione preventiva di tutti i componenti, benché non guasti.***

# ISO EN 13849-1 Sicurezza del macchinario –

# Parti dei sistemi di comando legate alla sicurezza - Principi generali per la progettazione.

**Può essere utilizzata indipendentemente dal tipo di tecnologia e di energia utilizzata (meccanica, idraulica, pneumatica, elettrica).**

**E' valida solo per le cinque architetture specificate.**

**Non è adatta per sistemi complessi.**

**La ISO EN 13849-1 nasce come revisione della EN 954-1**

**Obiettivo: sviluppare metodi semplici per calcolare la probabilità che possa capitare un guasto pericoloso in un determinato periodo di tempo.**

**Le complesse formule matematiche proprie della teoria della affidabilità dei sistemi  sono state sostituite da tabelle pre-calcolate.**

**Alcuni concetti della EN 954 sono stati mantenuti: funzione di sicurezza, categorie, ridondanza, monitoraggio.**

**Alcuni sono stati modificati: grafico dei rischi, scelta delle categorie**

**Il ruolo delle categorie non è più centrale come nella EN 954-1.**

**Al posto delle categorie, per valutare il grado di resistenza ai guasti, viene introdotto il concetto di "Livello di prestazione" (PL).**

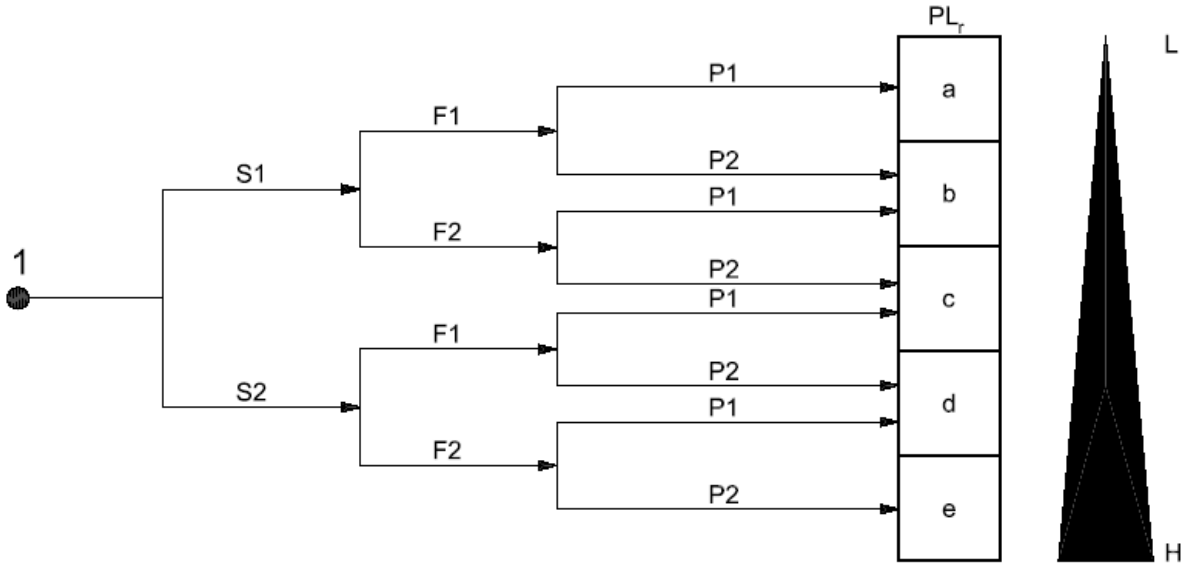
**La capacità da parte di un SRP/CS di svolgere una funzione di sicurezza è espressa attraverso il valore del PL definito come probabilità media di guasto pericoloso/ora ($PFHd_{avg}$).**

**Sono previsti 5 livelli, da PLa a PLe (Tabella 3 di ISO 13849-1).**

| PL | Average probability of dangerous failure per hour<br>1/h |
|---|---|
| a | $\geqslant 10^{-5}$ to $< 10^{-4}$ |
| b | $\geqslant 3 \times 10^{-6}$ to $< 10^{-5}$ |
| c | $\geqslant 10^{-6}$ to $< 3 \times 10^{-6}$ |
| d | $\geqslant 10^{-7}$ to $< 10^{-6}$ |
| e | $\geqslant 10^{-8}$ to $< 10^{-7}$ |

# Valutazione del Performance Level richiesto - $PL_r$

**Nuovo grafico dei rischi.**




**Key**

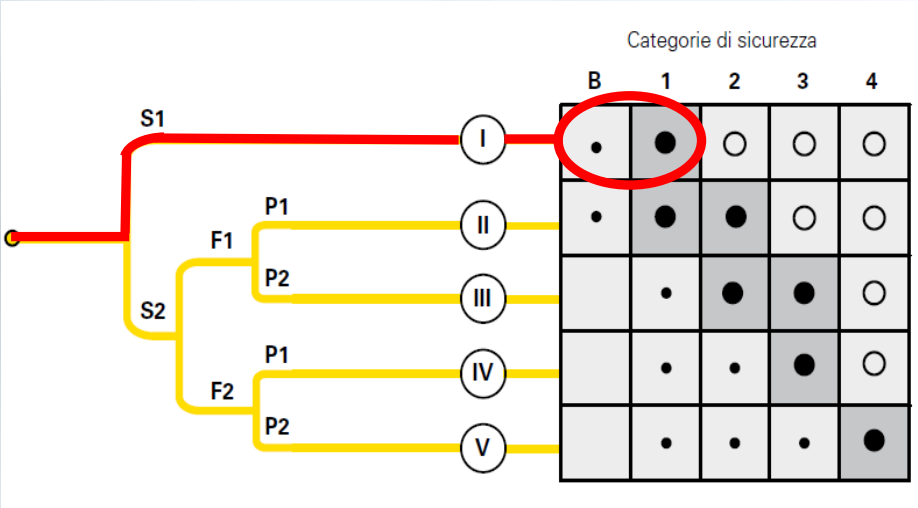
1 starting point for evaluation of safety function's contribution to risk reduction
L low contribution to risk reduction
H high contribution to risk reduction
$PL_r$ required performance level

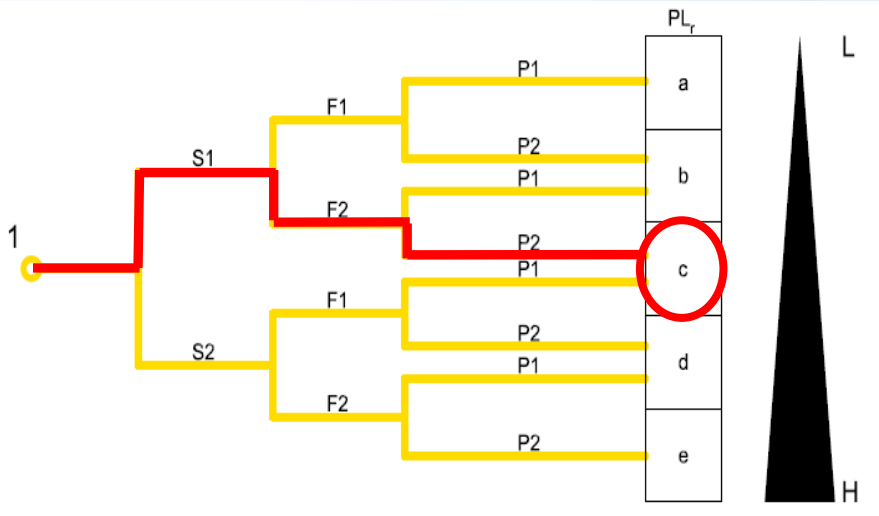
**Risk parameters:**

S severity of injury
S1 slight (normally reversible injury)
S2 serious (normally irreversible injury or death)
F frequency and/or exposure to hazard
F1 seldom-to-less-often and/or exposure time is short
F2 frequent-to-continuous and/or exposure time is long
P possibility of avoiding hazard or limiting harm
P1 possible under specific conditions
P2 scarcely possible

## Differenza importante rispetto alla EN 954-1:

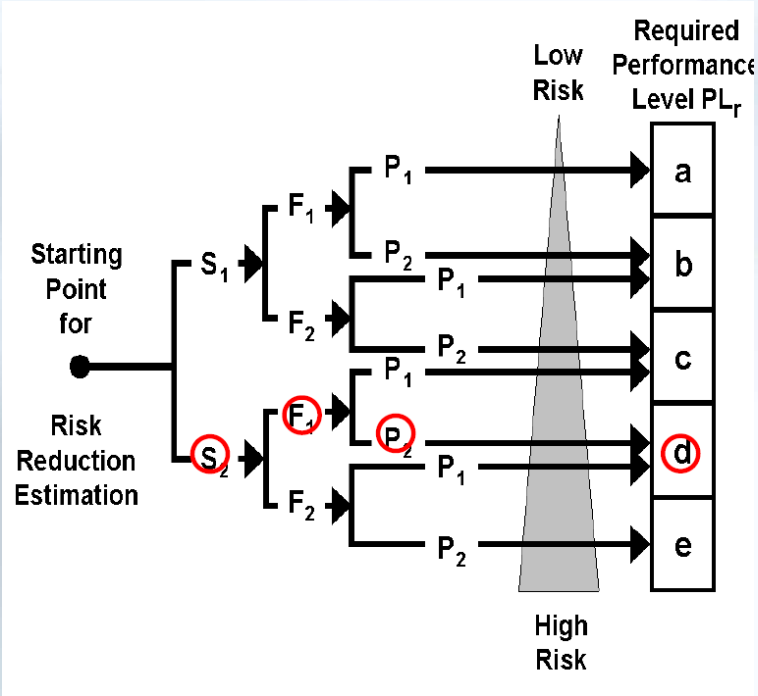
**Un rischio di infortunio leggero (danno non permanente) non porta più necessariamente ad un basso livello di sicurezza (categoria B o 1).**
**Se l'esposizione al rischio è frequente e difficilmente evitabile viene considerato pari ad un rischio di infortunio serio assai infrequente ed evitabile (PLr = c  nell'esempio).**



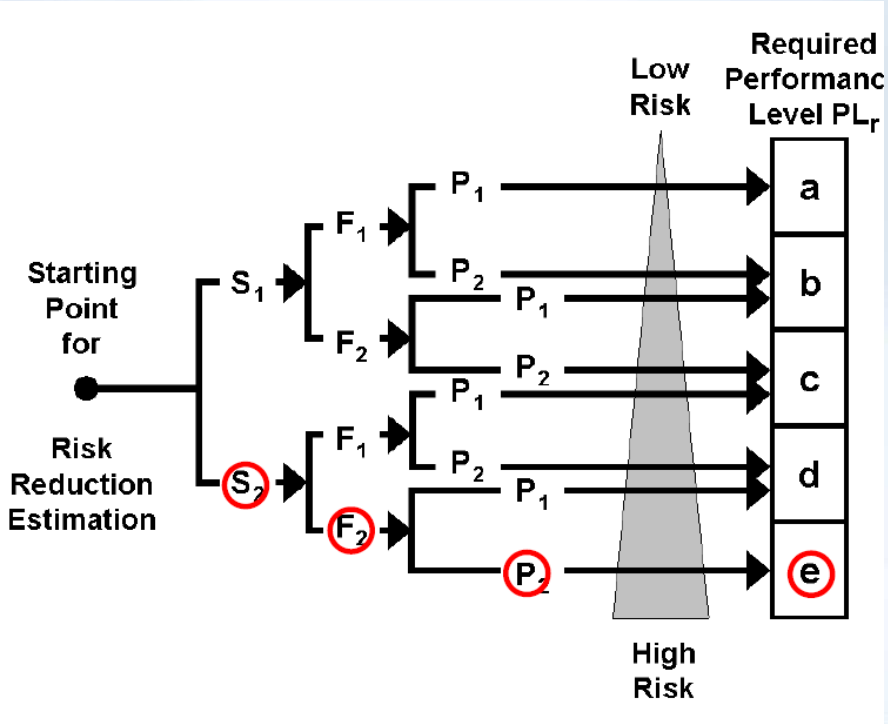
# Esempio di scelta del PLr

## Macchine automatiche




PLr = d

## Macchine semiautomatiche




PLr = e

# Il valore del PL è funzione di

**Aspetti quantitativi (PFHd)**

- **$MTTF_d$ per i singoli componenti (affidabilità)**
- **$DC_{avg}$ (diagnostica)**
- **CFF (resistenza)**
- **Categorie (struttura)**

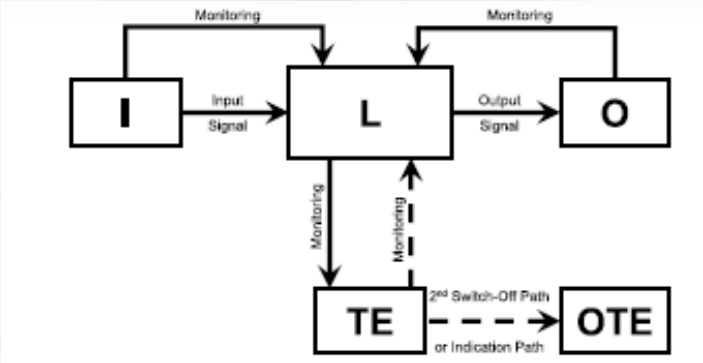
**Aspetti qualitativi**

- **Comportamento del sistema di sicurezza in condizioni di guasto**
- **Controllo dei guasti sistematici**
- **Software di sicurezza**
- **Possibilità di adempiere alla funzione di sicurezza in determinate condizioni ambientali**

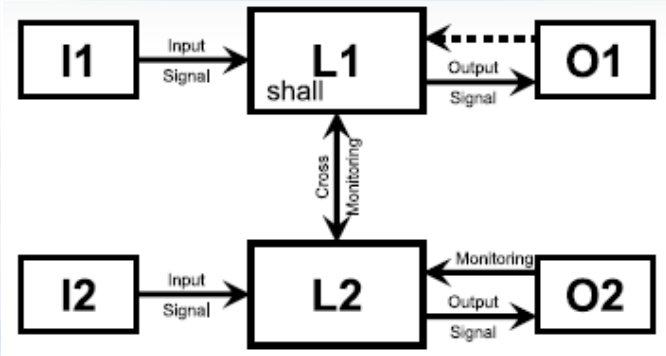
**La Norma può essere usata solo se per il progetto del sistema di controllo ci si avvale di una delle cinque architetture prefissate.**

**Cat. B (PLmax = b) e Cat. 1 (PLmax = c)**


**Cat. 2 (PLmax = d)**




**Cat. 3 (PLmax = d) e Cat. 4 (PL = e)**



**Scelta la Categoria in funzione del PLr richiesto dall'analisi di rischio, si progetta il circuito di controllo per la funzione di sicurezza individuata, si ricava il corrispondente valore di PL e si paragona al PLr.**

**Per ricavare il valore di PL risultante occorre calcolare il valore di $PFHd_{avg}$ (tabella 3).**

**Esistono diversi metodi per effettuare una stima della probabilità di guasto pericoloso/ora di un sistema complesso.**

**L'uso di questi metodi presuppone che per ogni componente si conosca il tasso di guasto, la percentuale di ripartizione del tasso di guasto per tutte le modalità di guasto del componente e l'effetto di ogni guasto sul comportamento del sistema.**

**La ISO 13849-1 semplifica il calcolo fornendo una tabella basata sulla modellazione di Markov dove il valore di PFHd è già precalcolato per diverse combinazioni di Categorie, e di valori di massima di MTTFd e di DCavg che vanno scelti anch'essi tramite tabelle.**

| Denotation | Range of $MTTF_d$ |
|---|---|
| low | 3 years ≤ $MTTF_d$ < 10 years |
| medium | 10 years ≤ $MTTF_d$ < 30 years |
| high | 30 years ≤ $MTTF_d$ ≤ 100 years |

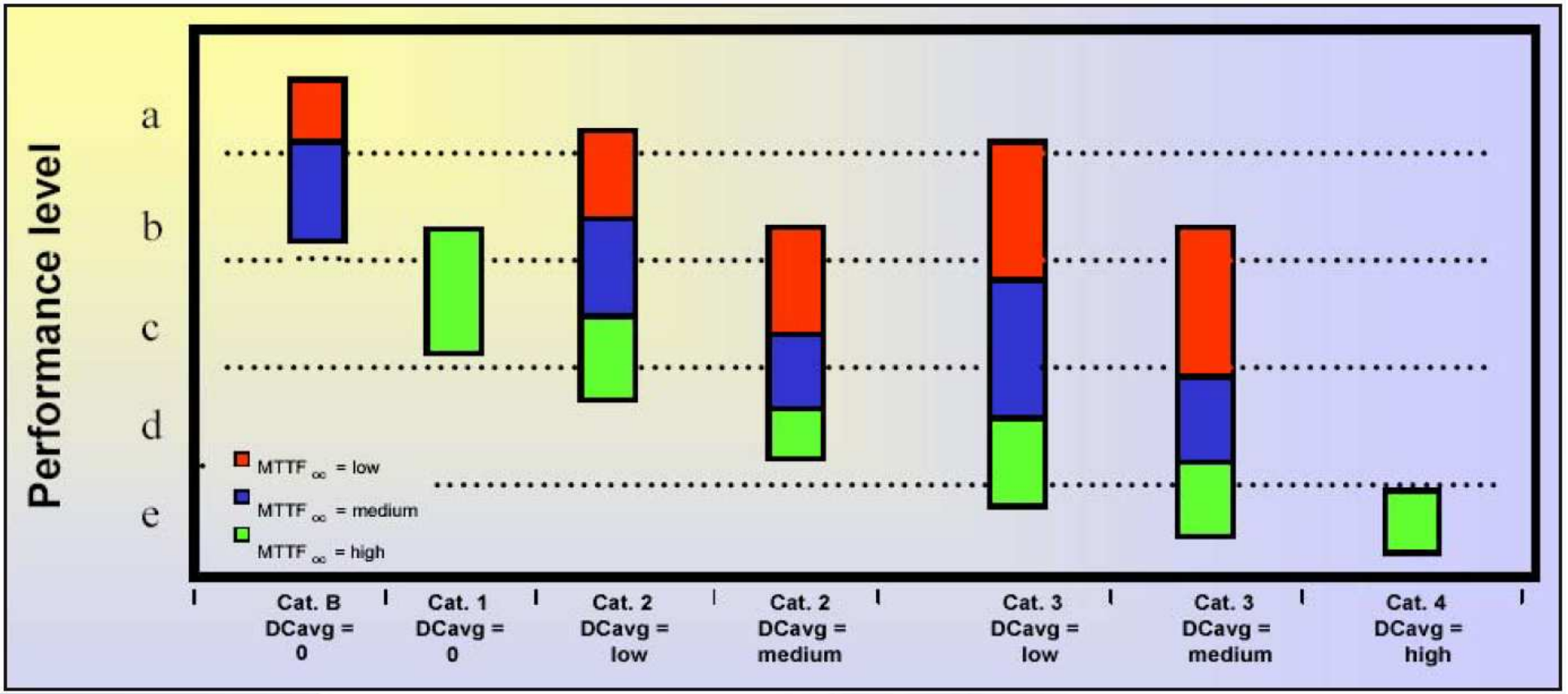
**MTTFd**

| Denomination | Range of values |
|---|---|
| none | DC < 60% |
| low | 60% ≤ DC < 90% |
| medium | 90% ≤ DC < 99% |
| high | 99% ≤ DC |

**DCavg**

**Il problema si riconduce quindi al calcolo semplificato di MTTFd e di DCavg e alla verifica che siano rispettate le condizioni di indipendenza di funzionamento dei canali nel caso di architetture ridondanti (Cat. 2,3 e 4)**

# Tabella 5




**Verifica del CCF**

# Calcolo semplificato dei parametri

**MTTFd  DC  CCF**

**MTTFd** = Stabilisce la durata media di funzionamento, espressa in anni, di un singolo canale del sistema di controllo di sicurezza prima che capiti un guasto casuale potenzialmente pericoloso (e non un guasto generico).

## Procedura semplificata per il calcolo del MTTFd

Poiché per il calcolo del MTTFd occorre conoscere il tasso di guasti pericolosi, bisognerebbe condurre una analisi FMECA (analisi delle modalità di guasto e effetti del guasto sul comportamento del circuito) determinando quindi per ogni componente, nel contesto dell'applicazione in esame, l'effettivo tasso di guasti pericolosi rispetto a tutti i guasti possibili.
Per semplicità di calcolo la norma consente di valutare , per ogni componente, come pericolosi il 50% dei guasti possibili (worst case), quindi

$$MTTFd = 2 \times MTTF$$

**Nell'ipotesi di tassi di guasto casuali costanti per tutto il tempo di vita utile del SRP/CS, e sufficientemente bassi, allora**

$$\lambda = 1/MTTF$$

**Per la determinazione dei valori di $\lambda$ la norma richiede di adottare la seguente procedura nell'ordine:**

**Si usano i dati forniti dai costruttori dei dispositivi**
**Si usano i dati riportati nell'allegato C della norma**
**Si fissa un MTTFd = 10 anni**

**Noto $\lambda$ si ricava quindi facilmente l'MTTFd di ogni componente.**

## Calcolo del MTTFd complessivo del sistema

**Nel caso di sisemi a singolo canale (Cat.1 e Ct.2) e nel caso di sistemi a doppio canale (Cat.3 e Cat.4) realizzati con due canali omogenei:**

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}}$$

**Dove $MTTF_{di}$ è il valore di $MTTF_d$ di ogni singolo componente che partecipa alla funzione di sicurezza**

**Il calcolo va fatto per un canale solo**

**Per sistemi a doppio canale (Cat.3 e Cat.4) nel caso che i due canali siano disomogenei :**

1 - **Si considera il valore più basso dei due (worst case)**

2 - **Si usa la seguente formula che agli effetti del calcolo ri-simmetrizza i due canali**

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right]$$

**$MTTF_{dC1}$ e $MTTF_{dC2}$ sono i valori dei due canali**

**Esempio: $MTTFd_{(canale\ 1)}$= 3 anni $MTTFd_{(canale\ 2)}$ = 100 anni**

**Dalla formula si trova $MTTFd_{simmetrizzato}$ = 66 anni**

## MTTFd di relè ed elettrovalvole

**Per tutti i componenti elettromeccanici, idraulici e meccanici soggetti a usura (es. relè ed elettrovalvole) il tasso di guasto aumenta con il numero di cicli lavorati, pertanto la loro affidabilità non viene riferita al tempo per cui hanno lavorato bensì al numero di cicli effettuati.**

**Il parametro utilizzato è il valore B10 espresso in numeri di manovre dopo il quale si verificano guasti nel 10 % dei componenti esaminati durante una prova della durata di esercizio sotto carico specificato.**

**In assenza di informazioni dettagliate la norma consiglia di considerare come pericolosi il 50% dei guasti, quindi $B10_d = 2 \times B10$.**

**Conoscendo il B10d e il numero medio di operazioni in un anno (Nop) si può ricavare il valore di MTTFd nel seguente modo:**

$$MTTFd = B10d / (0{,}1 \times Nop)$$

## Completato il calcolo, si sceglie la classe di MTTFd tramite la seguente tabella

| Denotation | Range of $MTTF_d$ |
|---|---|
| low | 3 years $\leq MTTF_d <$ 10 years |
| medium | 10 years $\leq MTTF_d <$ 30 years |
| high | 30 years $\leq MTTF_d \leq$ 100 years |

**DC** = copertura diagnostica *(indica quanto il sistema sia efficiente nel rilevare un proprio eventuale malfunzionamento per tempo).*

Rappresenta il rapporto fra il tasso di guasti pericolosi rilevati $\lambda dd$ *(dd = dangerous detected),* e il tasso di tutti i guasti pericolosi possibili $\lambda d$ (*d=dangerous*) rilevati e non rilevati.

## Metodo semplificato per il calcolo del DC

Per il calcolo viene fornita una lista (Tabella E:1) di 34 diverse tecniche di diagnosi suddivisa in tre famiglie (circuiti di ingresso, logica di elaborazione dei segnali, circuiti di uscita).
Per ogni tecnica è assegnato un punteggio percentuale variabile fra 0% e 99%.

0% = nessun guasto pericoloso viene rilevato
99% = altissima copertura di guasti pericolosi

**Il progettista dovrà scegliere dall'elenco la tecnica che ritiene più adatta alla sua applicazione per ogni parte (per i circuiti di ingresso , per la logica di elaborazione e per i circuiti di uscita) e che nel contempo garantisca il livello DC necessario.**

**Può capitare che per le singole parti vengano usate tecniche di diagnosi con livelli DC diversi. In questo caso la norma fornisce una formula che consente di calcolare il DC totale dell'intero sistema (DCavg).**

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}}$$

***Si può vedere che se una parte ha valori di valori di DC e di MTTFd bassi ha molto peso e porta ad un valore di DCavg basso (e viceversa).***

***Le parti che non sono testate hanno DC = 0 e contribuiscono solo per il denominatore***

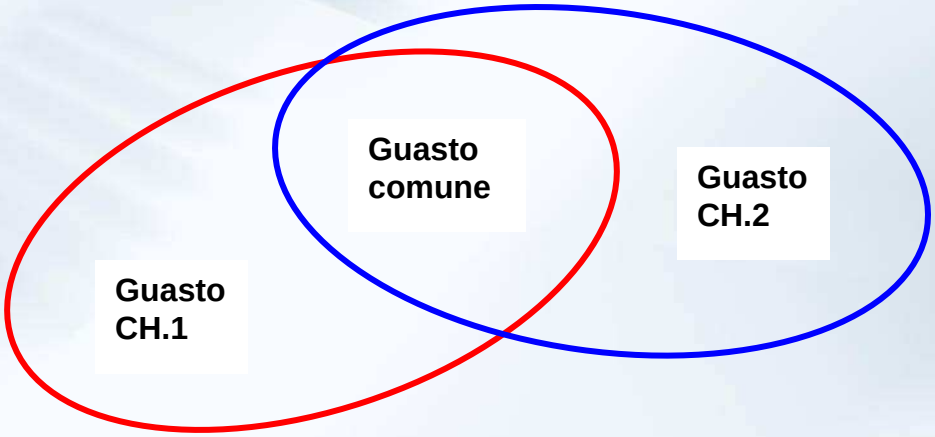
## Completato il calcolo, si sceglie la classe di DC tramite la seguente tabella

**Table 4 — Diagnostic coverage (DC)**

| denotation of diagnostic coverage | range of DC |
|---|---|
| none | DC < 60% |
| low | 60% ≤ DC < 90% |
| medium | 90% ≤ DC < 99% |
| high | 99% ≤ DC |

**CCF** = Guasti dovuti a cause comuni *(grado di indipendenza di funzionamento dei canali di un sistema ridondante)*

**Un CCF è guasto che procura un funzionamento critico contemporaneamente su entrambi i canali in una architettura a doppio canale.**




**Da considerare solo se si usano le architetture di Cat.2, Cat.3, Cat.4.**

**I metodi di progetto per combattere i guasti dovuti a cause comuni vanno scelti fra quelli elencati nella tabella F.1.**
**Ad ogni metodo è assegnato un punteggio. La somma totale dei punti vale 100.**
**Per poter garantire una resistenza sufficiente ai CCF occorre adottare un numero di metodi sufficienti per totalizzare almeno 65 punti.**

# IEC 62061 Sicurezza del macchinario –

# Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per il controllo delle macchine.

**E’ adatta solo per sistemi di comando che usano energia elettrica.**

**Vengono fornite formule per il calcolo dell’affidabilità dei sottosistemi solo per le quattro architetture tipiche del macchinario industriale.**

**Consente di integrare sottosistemi progettati in conformità con la ISO 13849-1**

**E’ la IEC 61508 adattata al settore del Macchinario industriale**

**La capacità da parte di un SRECS di svolgere una funzione di sicurezza è espressa attraverso il valore del SIL (Safety Integrity Level) definito come probabilità di guasto pericoloso/ora (PFHd).**

**Sono assegnati tre livelli: SIL 1, SIL2, SIL3.**

## Tabella 3 della norma

| Safety integrity level | Probability of a dangerous failure per hour ($PFH_D$) |
|---|---|
| 3 | $\geq 10^{-8}$ to $< 10^{-7}$ |
| 2 | $\geq 10^{-7}$ to $< 10^{-6}$ |
| 1 | $\geq 10^{-6}$ to $< 10^{-5}$ |

**Maggiore è il SIL, minore è la probabilità che lo SRECS non esegua la funzione di sicurezza richiesta.**

# Scelta del SIL

**Per ogni funzione di sicurezza individuata dall'analisi di rischio deve essere definito il SIL**

| Consequences | Severity (Se) | Class (Cl) | | | | | Frequency and duration (Fr) | | Probability of hazardous event (Pr) | | Avoidance (Av) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 3–4 | 5–7 | 8–10 | 11–13 | 14–15 | | | | | | |
| Death, losing an eye or arm | 4 | SIL 2 | SIL 2 | SIL 2 | SIL 3 | SIL 3 | ≤ 1 hour | 5 | Very high | 5 | | |
| Permanent, losing fingers | 3 | | OM | SIL 1 | SIL 2 | SIL 3 | > 1 hour – ≤ 1 day | 5 | Likely | 4 | | |
| Reversible, medical attention | 2 | | | OM | SIL 1 | SIL 2 | > 1 day – ≤ 2 weeks | 4 | Possible | 3 | Im-possible | 5 |
| Reversible, first aid | 1 | | | | OM | SIL 1 | > 2 weeks – ≤ 1 year | 3 | Rarely | 2 | Possible | 3 |
| | | | | | | | > 1 year | 2 | Negligible | 1 | Likely | 1 |

**Classe Cl = Fr + Pr + Av**

**OM = Raccomandato l'uso di altre misure**

# Il SIL è funzione di:

**Sicurezza dell'HW (PFHd)**

- **Probabilità di guasto pericoloso per ora**
- **Vincoli dell'architettura**

**Comportamento dello SRECS in condizioni di guasto**

**Software di sicurezza**

**Guasti sistematici**

- **Controllo dei guasti sistematici**
- **Possibilità di evitare i guasti**

## Sviluppo del sistema di sicurezza

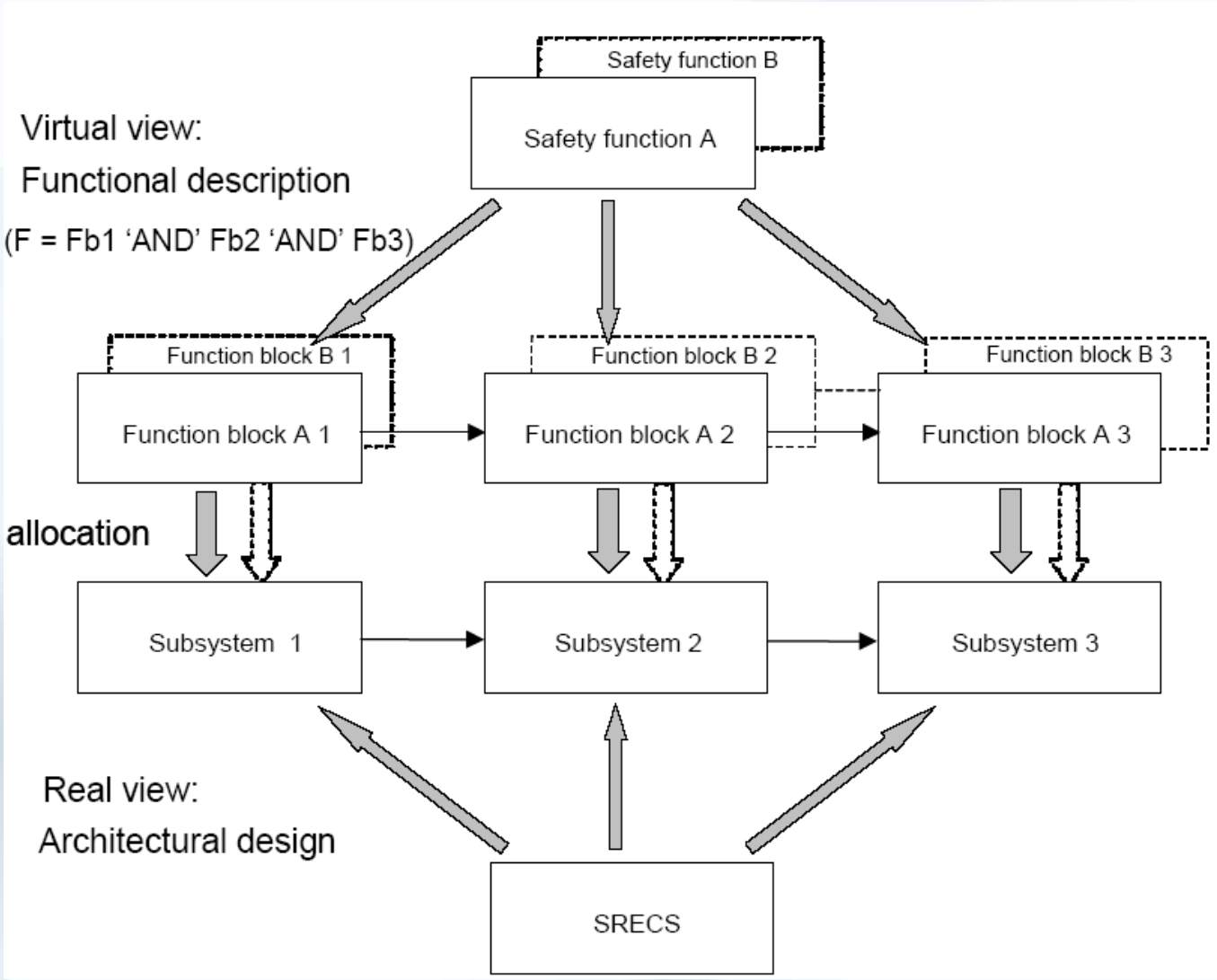
**Ogni funzione di sicurezza individuata dalla analisi di rischio viene scomposta in blocchi funzionali.**

**Ogni blocco funzionale viene specificato in termini di**

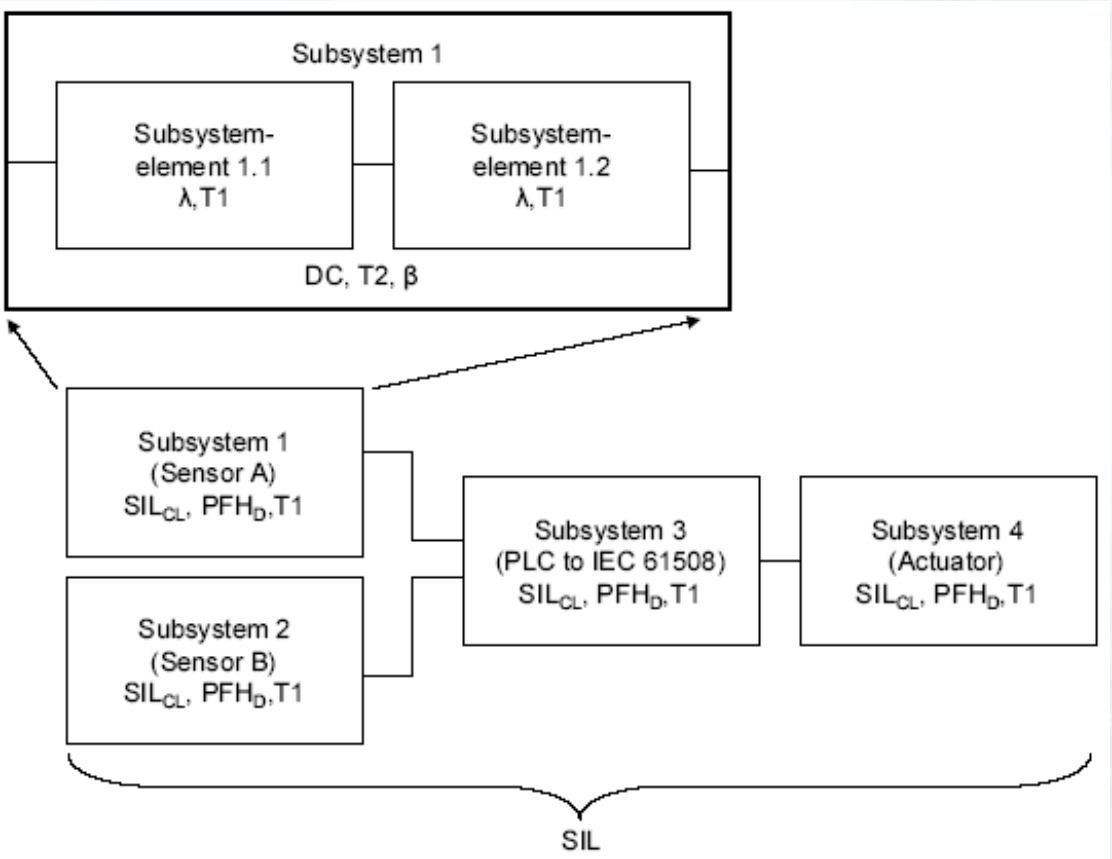
**-requisiti funzionali (informazioni in ingresso, elaborazioni logiche interne, tipo di uscita).**

**-requisiti di sicurezza**

**Ai blocchi funzionali sono quindi assegnati circuiti elettrici adatti ad implementare i requisiti individuati. Questi circuiti sono denominati sottosistemi.**


Virtual view:
Functional description
(F = Fb1 'AND' Fb2 'AND' Fb3)
Safety function B
Safety function A
Function block B 1
Function block B 2
Function block B 3
Function block A 1
Function block A 2
Function block A 3
allocation
Subsystem 1
Subsystem 2
Subsystem 3
Real view:
Architectural design
SRECS

**I sottosistemi saranno a loro volta composti da componenti elettrici interconnessi fra di loro. I componenti elettrici sono denominati elementi del sottosistema**




**Per ogni sottosistema occorre calcolare il PFHd.**

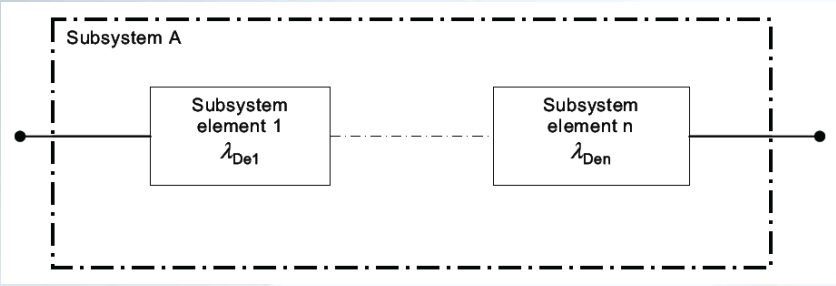
**Noto il PFHd, dalla tabella 3 si ricava il SILCL del sottosistema.**

# Calcolo del PFHd

**La norma suggerisce quattro schemi predefiniti per i sottosistemi e per ognuno di essi fornisce la formula per il calcolo di λd.**

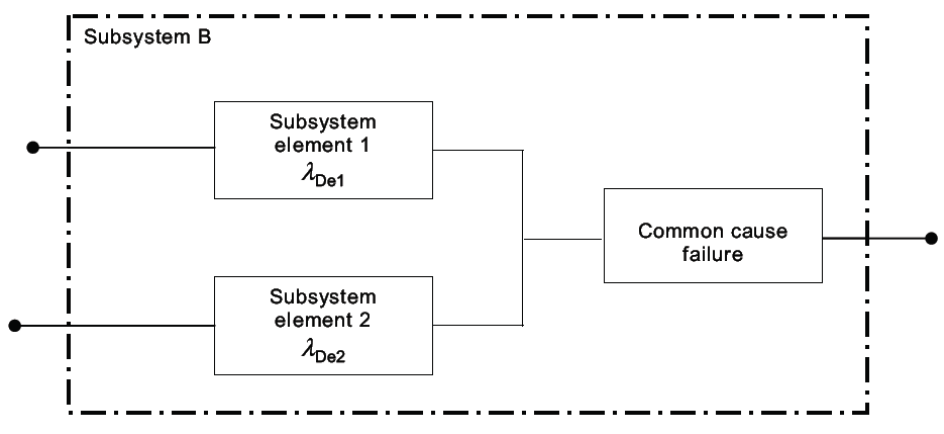
**Noto λd, il PFHd del sottosistema si ottiene**

**PFHd = λ x 1h**




**Sottosistema A :**
**Hardware fault tolerance = 0**

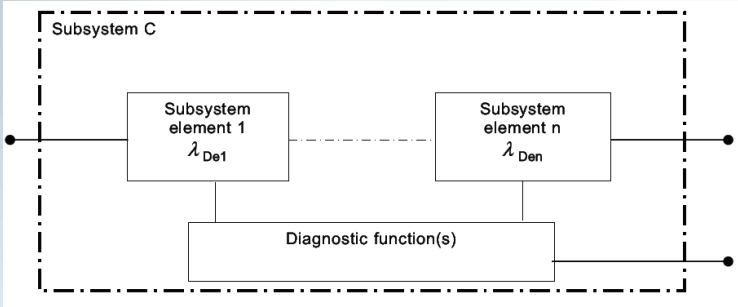
$$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$$




## Sottosistema B:

## Hardware fault tolerance = 1

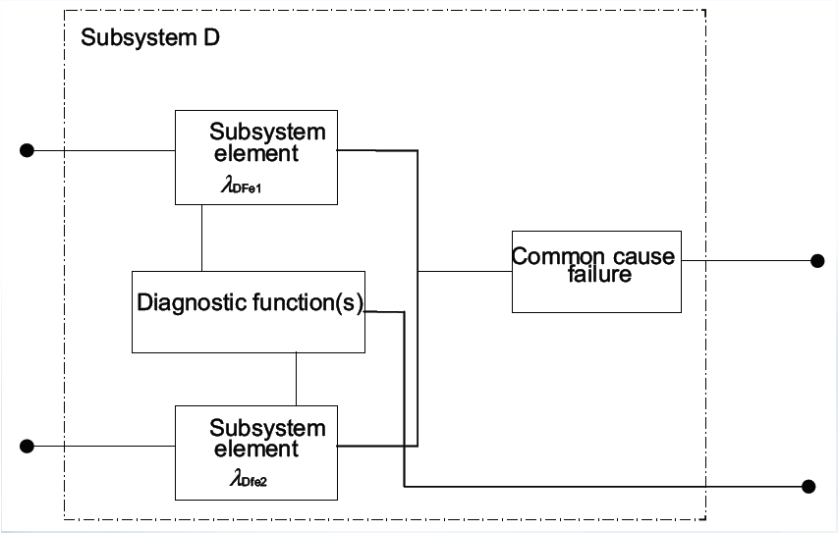
$$\lambda_{DssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$




## Sottosistema C:

## Hardware fault tolerance = 0

$$\lambda_{DssC} = \lambda_{De1}(1 - DC_1) + \ldots + \lambda_{Den}(1 - DC_n)$$




## Sottosistema D:

## Hardware fault tolerance = 1

**Nel caso di elementi di sottosistema omogenei**

$$\lambda_{DssD} = (1-\beta)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1-DC)] \times T_1\} + \beta \times \lambda_{De}$$

**con** $\lambda_D = \lambda_{DD} + \lambda_{DU}$ $\lambda_{DD} = \lambda_D \times DC$ $\lambda_{DU} = \lambda_D \times (1\text{-}DC)$

**Dove** $\lambda_{DD}$ **è il tasso di guasti pericolosi rilevabili**

$\lambda_{DU}$ **è il tasso di guasti pericolosi non rilevabili**

**T1 = (Proof Test) Intervallo di test di prova**
**Normalmente per le macchine viene fatto coincidere con la durata di vita (20 anni).**

**T2 = Intervallo di test diagnostico**

**Per calcolare il PFHd di ogni sottosistema devono quindi essere noti i valori: λd, λdd, λdu, β, DC, T1 e T2.**

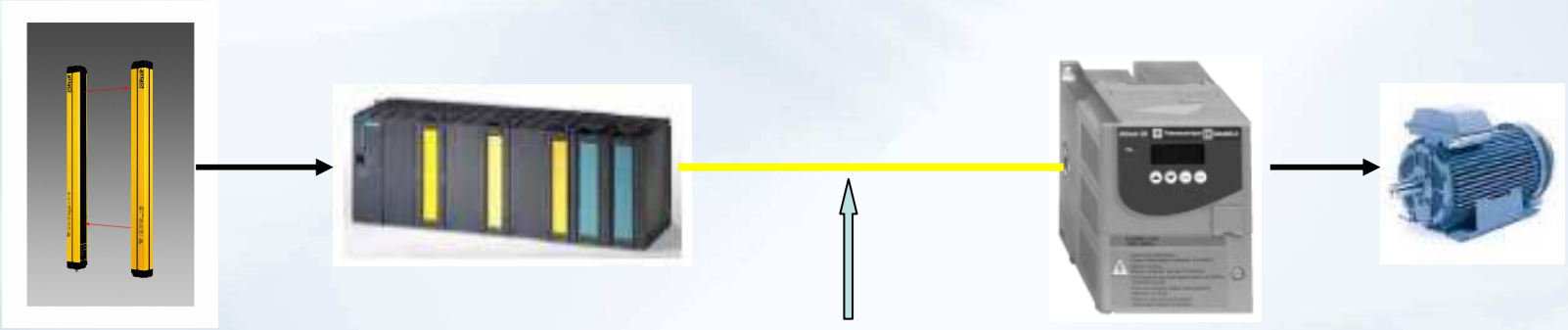
**Noto il PFHd, dalla Tabella 3 si ricava il SILCL del sottosistema**

**e si verifica che sia compatibile con i vincoli imposti dall'architettura scelta nel senso che il SILCL che può raggiungere un determinato sottosistema è limitato dalla tolleranza ai guasti dell'hardware e dal valore di SFF (tabella 5).**

| Safe failure fraction | Hardware fault tolerance (see Note 1) | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60 % | Not allowed (see Note 3) | SIL1 | SIL2 |
| 60 % – < 90 % | SIL1 | SIL2 | SIL3 |
| 90 % – < 99 % | SIL2 | SIL3 | SIL3 (see Note 2) |
| ≥ 99 % | SIL3 | SIL3 (see Note 2) | SIL3 (see Note 2) |

**Il SIL è quindi funzione di: Affidabilità, struttura e qualità del progetto.**

**La probabilità di guasto pericoloso/ora totale della funzione di sicurezza sarà uguale alla somma delle probabilità di guasto pericoloso/ora dei sottosistemi che concorrono alla sua realizzazione e dovrà includere, se necessario, anche la probabilità di guasto pericoloso per ora delle eventuali linee di comunicazione di sicurezza.**



PFH1 = $2*10^{-8}$/h PFH2 = $1*10^{-9}$/h PFH3 = $1*10^{-9}$/h PFH4 = $5*10^{-7}$/h

$$PFH_D = PFH1 + PFH2 + PFH3 + PFH4 = 5.22*10^{-7}/h$$

| Safety integrity level | Probability of a dangerous failure per hour ($PFH_D$) |
|---|---|
| 3 | $\geq 10^{-8}$ to $< 10^{-7}$ |
| 2 | $\geq 10^{-7}$ to $< 10^{-6}$ |
| 1 | $\geq 10^{-6}$ to $< 10^{-5}$ |

# Calcolo dei parametri

**λd** **DC** **SFF** **β**

**$\lambda$ (oppure B10 per i relè) = tasso di guasto di ogni componente elettrico o elettromeccanico.**
**Si desume da appositi database (es. SN 29500), oppure tramite l'annesso D della norma oppure da altre fonti ( es. Birolini)**

**Analizzando lo schema elettrico del sottosistema si stabiliscono per ogni componente le modalità di guasto e si separano quelle pericolose da quelle non pericolose (analisi FMECA)**

**senza considerare gli effetti di eventuali metodi di diagnosi implementati !**

**assegnando a ciascuna di esse la relativa probabilità.**
**Quindi per ogni componente si ricava:**

**$\lambda$ = $\lambda$d (dangerous) + $\lambda$s (safe).**

**DC = Copertura diagnostica**

**Se sono state adottate misure diagnostiche per rilevare i guasti pericolosi, allora in funzione della efficacia del metodo adottato si ricavano i valori**

**λdd (dangerous detected) e λdu (dangerous undetected).**

**Dove λd = λdd + λdu**

**Conoscendo λdd e λdu per ogni componente è ora possibile calcolare la copertura diagnostica totale per il sottosistema:**

$$DC = \Sigma\lambda dd / (\Sigma\lambda dd + \Sigma\lambda du).$$

**SFF** = Frazione del guasto in sicurezza (frazione del tasso di guasto globale di un sottosistema che non comporta un guasto pericoloso).

Conoscendo $\lambda s, \lambda d, \lambda dd$ per ogni componente è possibile calcolare la frazione di guasto in sicurezza del sottosistema:

$$SFF = (\Sigma\lambda s + \Sigma\lambda dd) / (\Sigma\lambda s + \Sigma\lambda d).$$

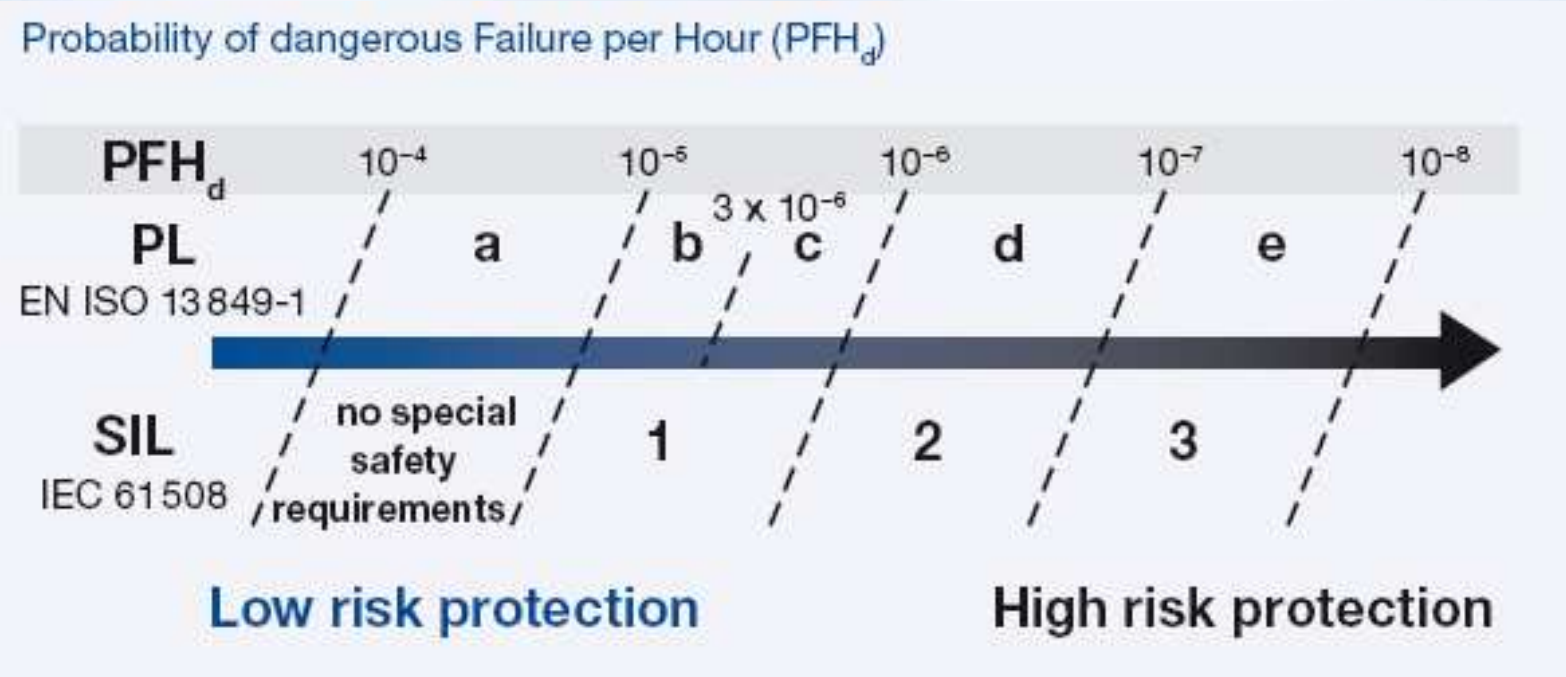
**β** = Suscettibilità ai guasti per cause comuni (= CCF)

I metodi di progetto per combattere i guasti dovuti a cause comuni vanno scelti fra quelli elencati nella tabella F.1.
Ad ogni metodo è assegnato un punteggio.
Tale punteggio viene utilizzato per determinare un fattore di guasto per cause comuni β utilizzando la tabella F.2

# Conclusioni

**Poiché ISO 13849-1 e EN 62061 usano lo stesso parametro, PFH, per definire il grado di resistenza ai guasti, è possibile paragonare PL e SIL**

## Relazione fra PL, probabilità di guasto pericoloso per ora e SIL



**I metodi proposti nella ISO 13849-1 riducono le difficoltà di calcolo della probabilità di guasto pericoloso rispetto a quanto richiesto dalla IEC 61508 fornendo un approccio pragmatico che meglio si adatta alle esigenze del settore dei macchinario.**

**Mantenendo le categorie e altri concetti fondamentali, come la funzione di sicurezza e il grafico del rischio, viene assicurata una continuità con la precedente versione del 1996.**

**L'aver voluto mantenere l'approccio quanto più lineare possibile per sistemi di controllo dotati di semplici funzioni di sicurezza fa si che la norma abbia dei limiti. Ad esempio per PL = e la ISO 13849-1 è applicabile solo se i sistemi di controllo sono realizzati con tecnologia elettrica oppure elettromeccanica semplice (relè).**

**Se si prevede l'impiego di tecnologie complesse, (ad esempio elettronica programmabile, bus di sicurezza, architetture diverse da quelle stabilite ecc.) è più appropriato progettare mediante la IEC 62061.**

**Se si usano dispositivi e/o sottosistemi che già rispondono alle norme IEC 61508 oppure ISO EN 13849-1, la norma EN 62061 specifica come incorporarli nello SRECS (tabelle 6 e 7).**

**PLC di sicurezza, barriere fotoelettriche di sicurezza, e in genere tutti i dispositivi di sicurezza complessi che integrano logica programmabile e che fanno uso di software enbedded, devono essere conformi alle rispettive norme di prodotto, se esistono, e alla IEC 61508 per gli aspetti che riguardano la sicurezza funzionale.**

# Considerazioni sul Proof Test – Prefazione alla EN 62061

INTERVALLO DI VERIFICA PERIODICA (PROOF TEST) E CICLO DI VITA

La seguente importante informazione deve essere notata in relazione ai requisiti di questa norma:

Dove la probabilità di guasti per ora ($PFH_D$) è altamente dipendente dalla verifica periodica (cioè la prova intesa a rivelare i guasti non rivelati dalla funzione diagnostica) allora l'intervallo della prova periodica è necessario che sia mostrato come realistico e praticabile nel contesto dell'uso previsto relativo alla sicurezza del sistema elettrico di controllo (SRECS) (per esempio un intervallo di verifica periodica inferiore a 10 anni può essere irragionevolmente corto per molte applicazioni del macchinario).

Il CEN/TC114/WG6 ha utilizzato un intervallo per la verifica periodica (tempo di missione) di 20 anni a supporto della stima del tempo medio al guasto pericoloso ($MTTF_D$) per la realizzazione dell'architettura riportata nell'Allegato B del prEN ISO 13849-1. Pertanto, si suggerisce che nell'attività di progettazione di uno SRECS si usi un intervallo della verifica periodica di 20 anni.

É riconosciuto che alcuni sottosistemi e/o elementi di sottosistema (per esempio componenti elettromeccanici con altri cicli di utilizzo) richiederanno la sostituzione all'interno dell'intervallo della verifica periodica.