

Machines 2010

Nuova legge in Europa



Nuove norme

SAFETY

Quasi-macchine

MTTFd

Documenti

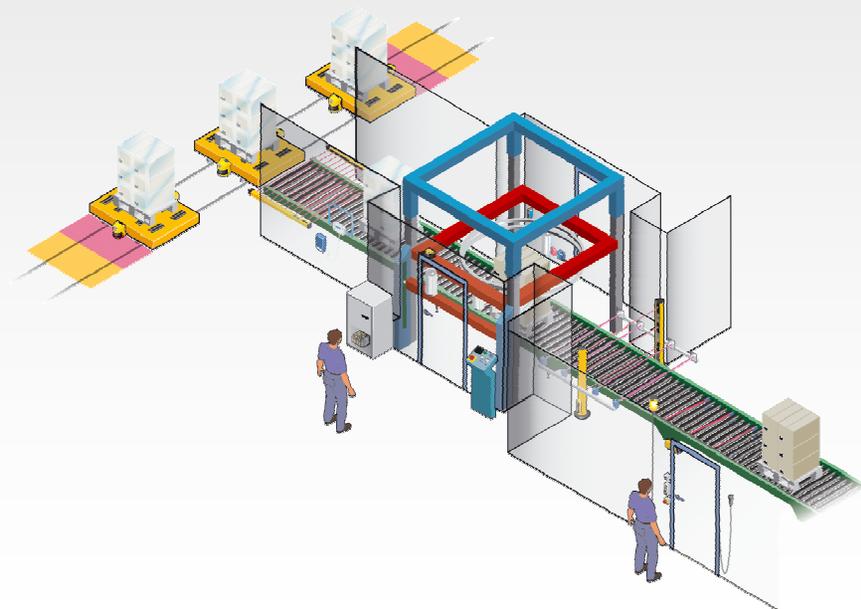
B10d

DC

CCF

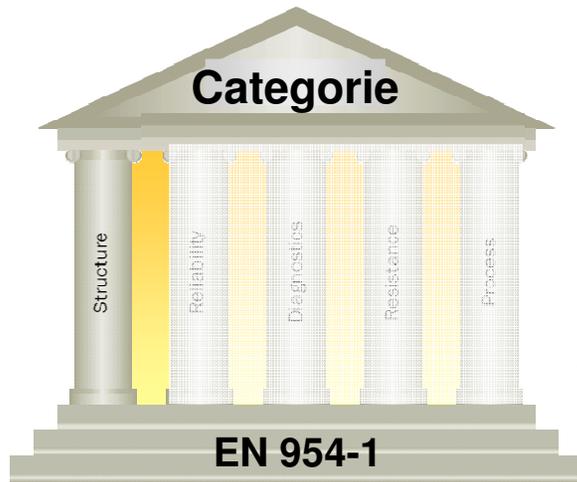
SIL

PL



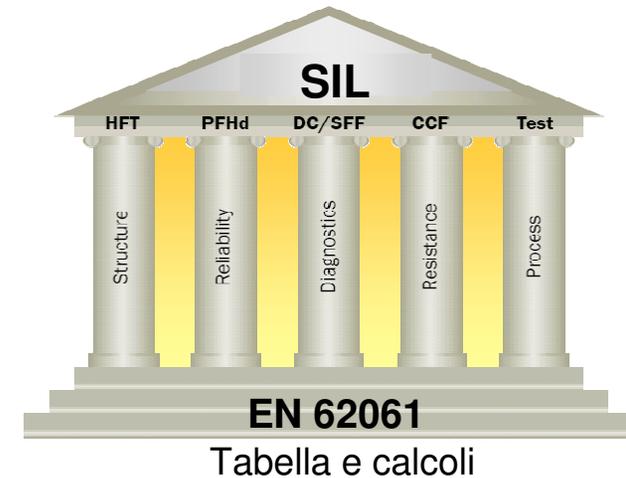
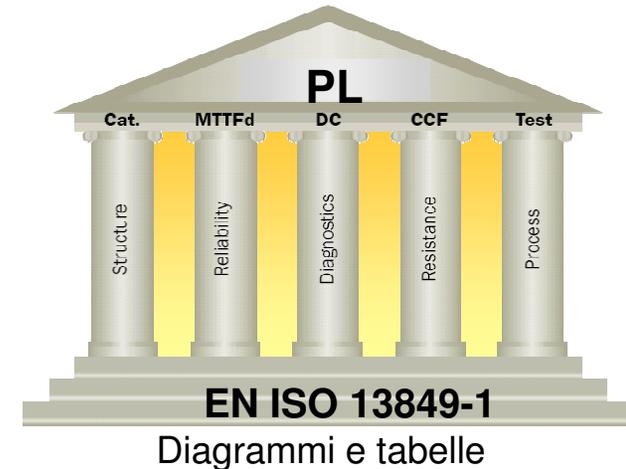
Nuove norme per la sicurezza delle macchine

Comparazione tra le richieste



Determinazione:

- : **Struttura**
- : **Affidabilità**
- : **Diagnostica**
- : **Resistenza**
- : **Processo (QM)**



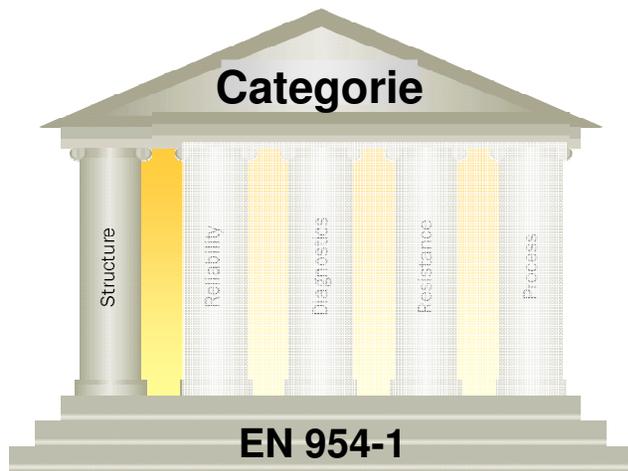
Nuove norme per la sicurezza delle macchine

Comparazione della copertura

EN ISO 13849-1: PL	Applicabile per	EN 62061: SIL
✓	Idraulica	-
✓	Pneumatica	-
✓	Meccanica	-
✓	Elettrica	✓
✓	Elettronica	✓
✓	Elettronica programmabile	✓
-	Elettronica programmabile complessa	✓
+	Semplice comprensione/utilizzo	

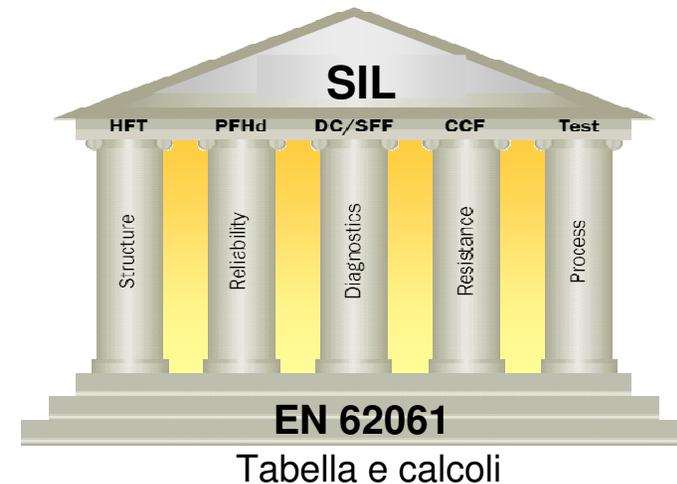
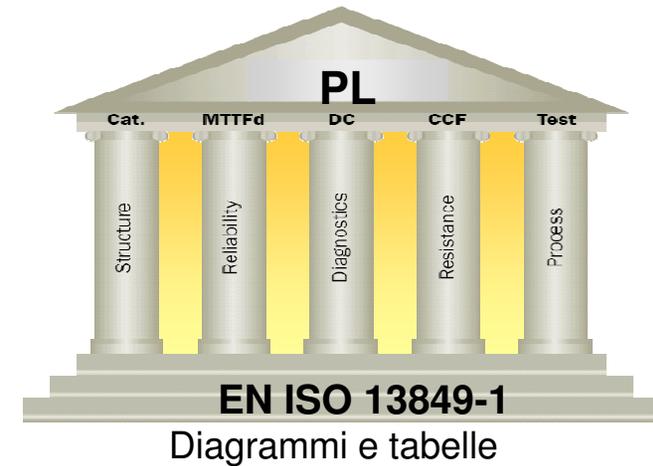
Nuove norme per la sicurezza delle macchine

Comparazione tra le richieste



Determinazione:

: **Struttura**



Le nuove norme armonizzate

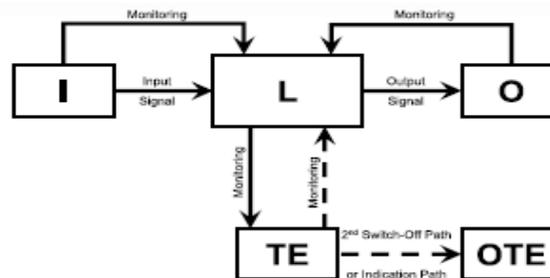
EN 13849

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

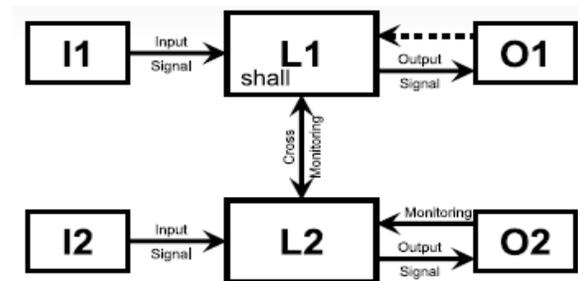
Cat. B (PLmax = b) e **Cat. 1** (PLmax = c)



Cat. 2 (PLmax = d)

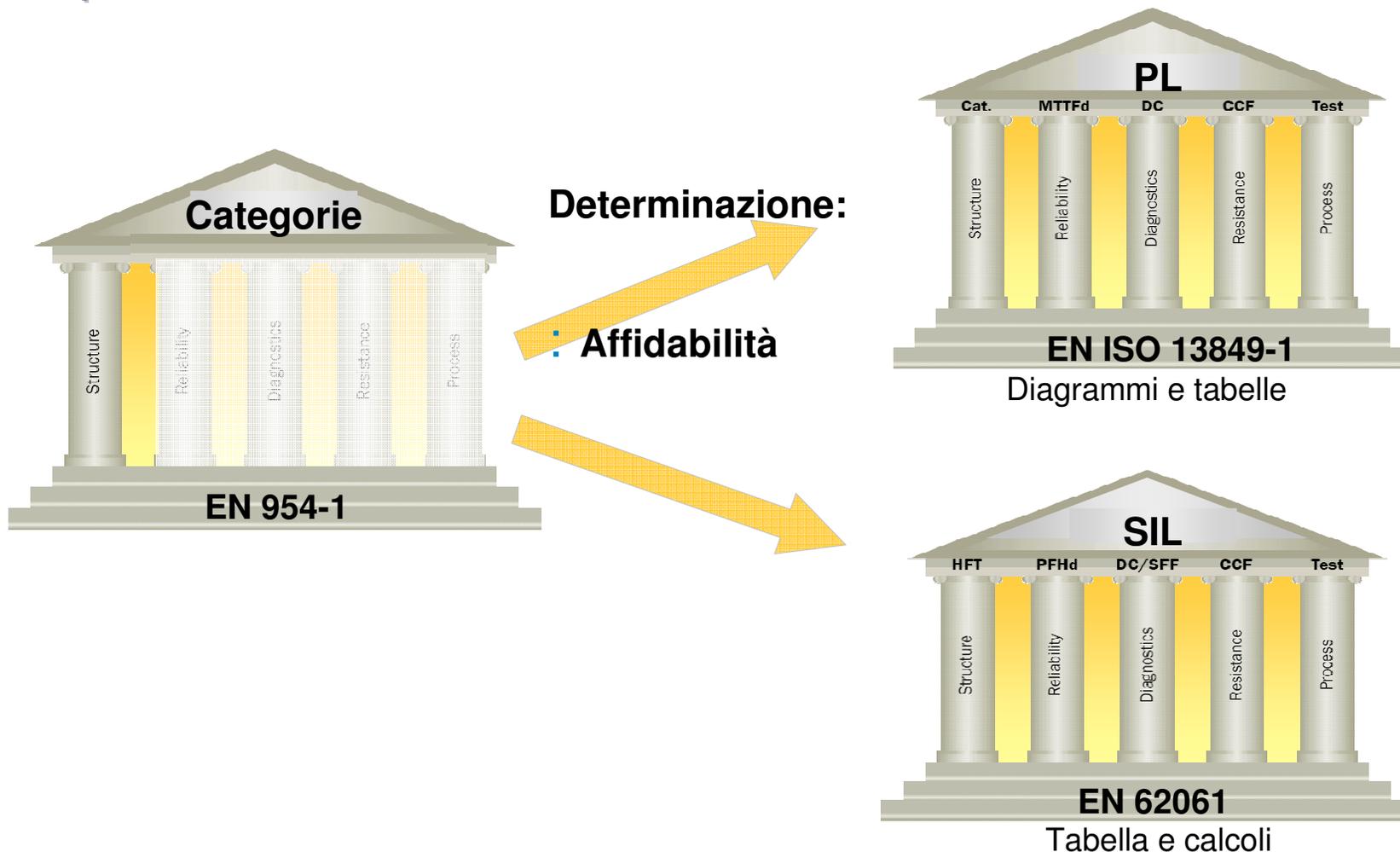


Cat. 3 (PLmax = d) e **Cat. 4** (PL = e)



Nuove norme per la sicurezza delle macchine

Comparazione tra le richieste



Le nuove norme armonizzate

EN 13849

Denotation	Range of $MTTF_d$
low	$3 \text{ years} \leq MTTF_d < 10 \text{ years}$
medium	$10 \text{ years} \leq MTTF_d < 30 \text{ years}$
high	$30 \text{ years} \leq MTTF_d \leq 100 \text{ years}$

$MTTF_d$

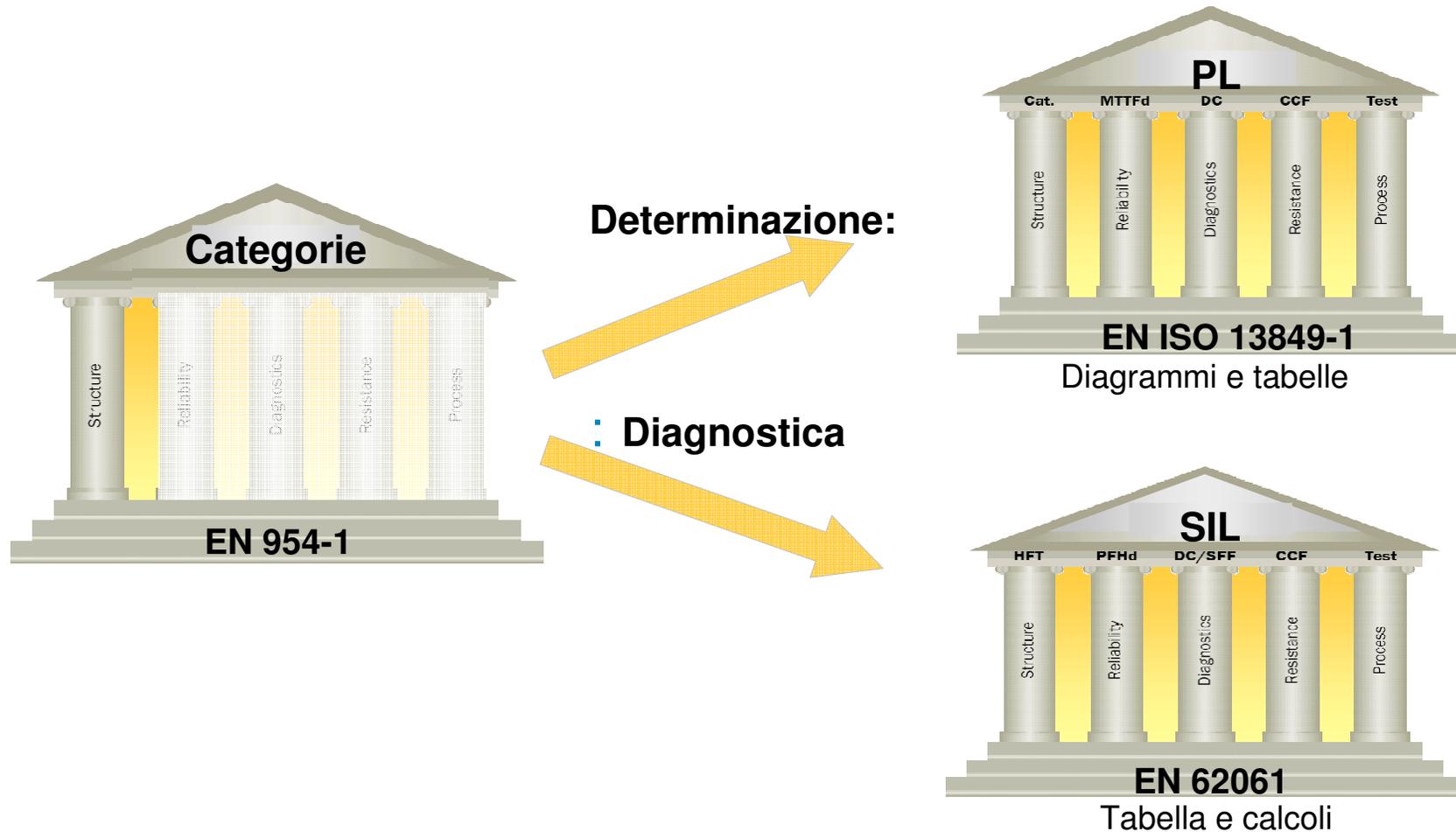


AssoAutomazione
Associazione Italiana
Automazione e Misura

“Dispositivi di sicurezza per l'adeguamento di macchine ed attrezzature industriali”

Nuove norme per la sicurezza delle macchine

Comparazione tra le richieste



Le nuove norme armonizzate

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 λ_{dd} (*dd = dangerous detected*), e il tasso di tutti i guasti pericolosi possibili λ_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



AssoAutomazione
Associazione Italiana
Automazione e Misura

“Dispositivi di sicurezza per l’adeguamento di macchine ed attrezzature industriali”

Le nuove norme armonizzate

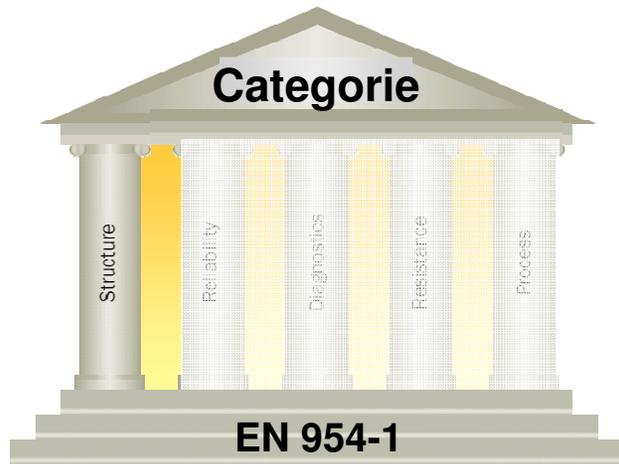
Completato il calcolo, si sceglie la classe di DC tramite la seguente tabella

Table 4 — Diagnostic coverage (DC)

denotation of diagnostic coverage	range of DC
none	$DC < 60\%$
low	$60\% \leq DC < 90\%$
medium	$90\% \leq DC < 99\%$
high	$99\% \leq DC$

Nuove norme per la sicurezza delle macchine

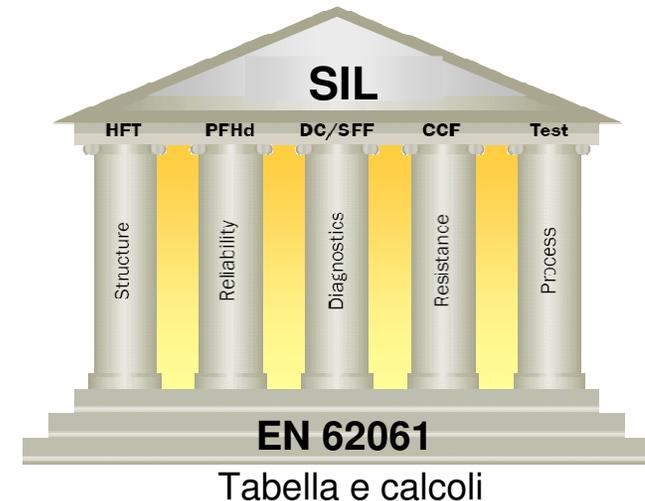
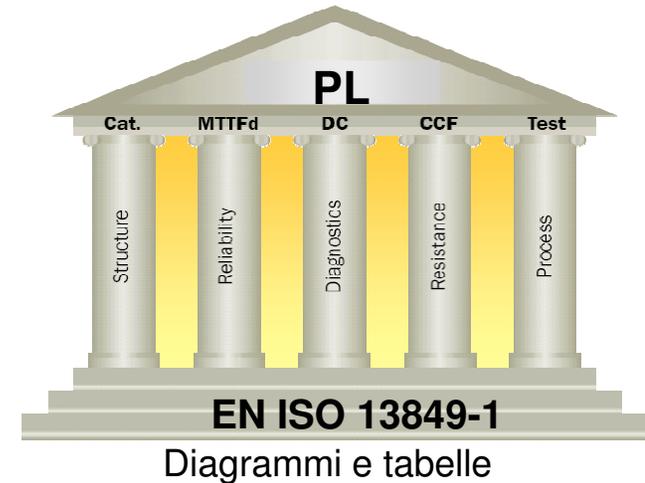
Comparazione tra le richieste



Determinazione:



: Resistenza

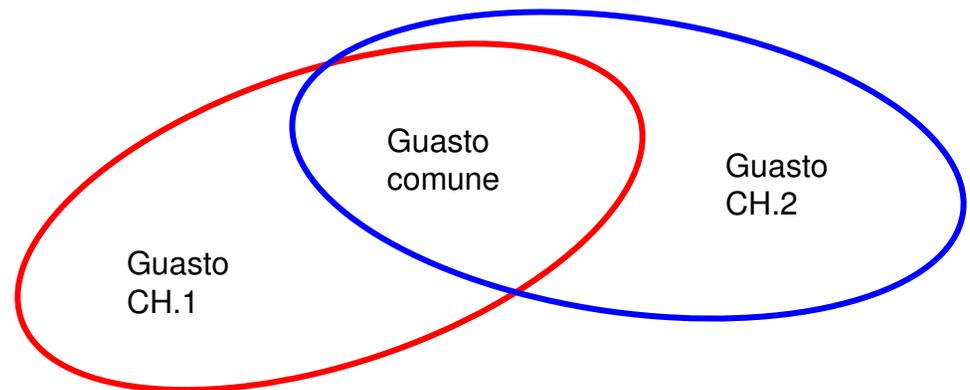


Le nuove norme armonizzate

EN 13849

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.

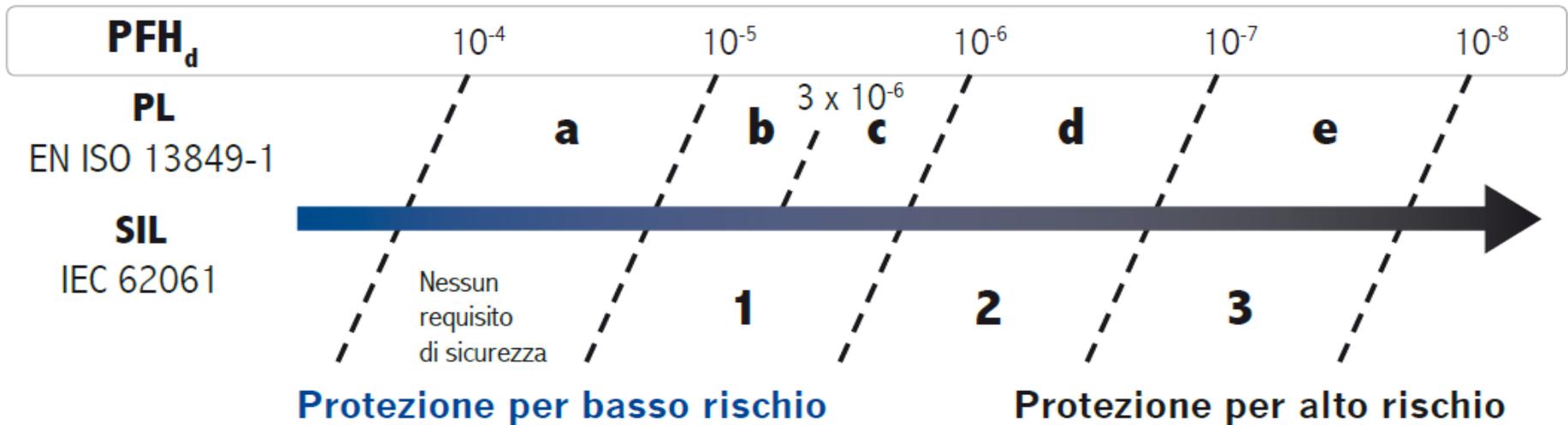


Da considerare solo se si usano le architetture di Cat.3, Cat.4.

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.

Confronto fra PL e SIL



Non è possibile individuare una perfetta corrispondenza biunivoca fra PL e SIL. E' però possibile confrontare la parte probabilistica di PL e SIL perché usano lo stesso concetto, PFH_d, per definire il grado di resistenza ai guasti.

E' importante avvertire tuttavia che, anche se il concetto probabilistico usato nelle due norme è lo stesso, il valore che si ottiene può essere diverso perché i metodi di calcolo non hanno lo stesso rigore in entrambe le norme.

E' possibile quindi confrontare i range ma non i valori puntuali.

Considerazioni conclusive

Il valore della Probabilità media di guasto pericoloso/ora è solo uno dei parametri che contribuiscono all'assegnazione del SIL o del PL.

Per poter rivendicare un valore di SIL o PL bisogna altresì dimostrare e documentare di

- aver preso in considerazione e rispettato tutti i requisiti relativi al controllo dei guasti sistematici
- di aver tenuto conto delle condizioni ambientali in cui dovrà operare il sistema di controllo di sicurezza
- nel caso sia stato necessario scrivere software, di aver adottato tutti gli aspetti di organizzazione e di progetto esemplificati nella IEC 61508-3 (per quanto riguarda i SIL) o nel modello di sviluppo a V di Fig. 6 della EN ISO 13849-1 (per quanto riguarda i PL)



AssoAutomazione
Associazione Italiana
Automazione e Misura

“Dispositivi di sicurezza per l'adeguamento di macchine ed attrezzature industriali”