ISPESL - Politecnico di Bari - ARPA Puglia

"La sicurezza delle macchine tra nuova Direttiva Macchine e Testo Unico"

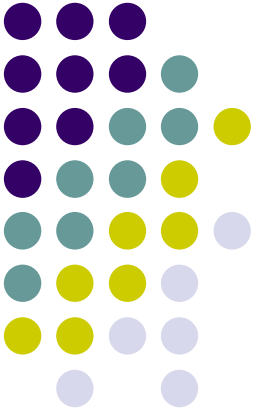
Bari, 23 ottobre 2009

POLITECNICO DI BARI

Aspetti metodologici innovativi per la valutazione dei rischi nell'ambito della Nuova Direttiva Macchine

Francesco Boenzi, Salvatore Digiesi,

Giorgio Mossa, Giovanni Mummolo



Evoluzione legislativa e tecnico-normativa

"Vecchia"
Direttiva Macchine
(89/392/CE, 91/368/CE, 93/44/CE, 93/68/CEE riunite nella 98/37/CE)
[in Italia DPR 459/96]

entro
29 giugno 2008:
recepimento

"Nuova"
Direttiva Macchine
(2006/42/CE)

29 dicembre 2009:
termine di attuazione

Norma tecnica
UNI EN 954-1:1996 "Sicurezza del macchinario – Parti dei sistemi di comando legate alla sicurezza, Parte 1: Principi generali per la progettazione"

ritirata ufficialmente dall'UNI il 22 febbraio 2007

può essere utilizzata ancora fino al 28 dicembre 2009
(proroga della cessazione di *)

UNI EN ISO
13849-1:2008

CEI EN 62061:2005
"Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza"

*** PRESUNZIONE DI CONFORMITA' AI RES**
1.2.1. *Sicurezza ed affidabilità dei sistemi di comando*
1.2.7. *Avaria del circuito di comando*
CONFLUITI IN
1.2.1. Sicurezza ed affidabilità dei sistemi di comando

Safety Related Parts of Control Systems - SRP/CS

Definizione

- parti dei sistemi di comando delle macchine a cui sono assegnate funzioni di sicurezza, indipendentemente dal tipo di energia utilizzata (elettrica, idraulica, pneumatica, meccanica)
- possono essere costituite da circuiti cablati e circuiti logici
- possono essere parti separate o integranti del sistema di comando

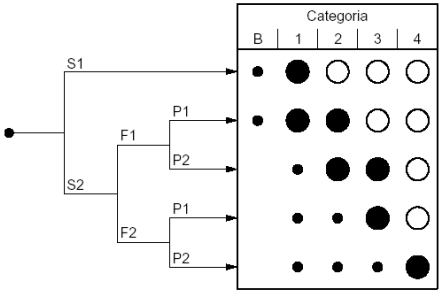
Limiti di sistema

- dai punti in cui i segnali legati alla sicurezza vengono generati (camme di attuatori, interruttori di posizione, sensori opto-elettronici, ecc.) fino all'uscita degli elementi di comando di potenza (es. contatti di un sezionatore), includendo anche i sistemi di monitoraggio del funzionamento (diagnostica del sistema)

Esempi di funzioni di sicurezza svolte:

- arresto attivato dall'intervento di un dispositivo di protezione elettrosensibile su una pressa
- blocco di un riparo nel momento in cui un'operazione pericolosa è stata avviata

UNI EN 954-1 – Determinazione della categoria di sicurezza



Categorie di Sicurezza ai sensi della EN 954-1				
B	1	2	3	4

Affidabilità e capacità di “fault-tolerance” (ridondanza, diagnostica, ecc.)

I parametri legati al Rischio possono essere combinati per fornire una scala qualitativa ⇒ categoria del rischio ⇒ deve corrispondere una categoria del sistema SRP/CS

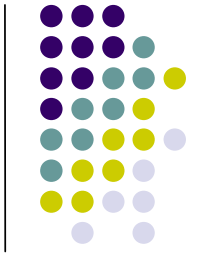
Elementi che determinano la categoria:

- ✓ AFFIDABILITA’ DEI COMPONENTI
- ✓ STRUTTURA DEL SISTEMA (ARCHITETTURA)
- ✓ ASPETTI QUALITATIVI non quantificabili

  es. qualità della documentazione legata alla sicurezza; completezza delle specifiche; qualità e precisione del software; completezza delle prove funzionali,ecc.

..... nessuna indicazione specifica

UNI EN 954-1
Principali limiti applicativi



- natura qualitatativa delle prestazioni di carattere affidabilistico e di resistenza ai guasti richieste ai sistemi
  - nessuna indicazione numerica o configurazionale del sistema
- approccio metodologico
  - non è illustrato alcun metodo per valutare le prestazioni raggiunte da un insieme di dispositivi: in altri termini non è chiaro in che modo possa essere classificato un insieme a partire dalla conoscenza di affidabilità e comportamento al guasto delle parti costituenti (es. sensori, logica, attuatori) ai fini di una valutazione oggettiva da parte del fabbricante o di una parte terza
- eccessiva semplicità nel caso di soluzioni di SRP/CS complesse
- obsolescenza tecnica
  - non è presente alcun elemento utile in merito alla valutazione dei sistemi elettronici programmabili o del software utilizzati per funzioni di sicurezza

UNI EN ISO 13849-1:2008
Elementi innovativi

- introduzione di un parametro oggettivo di valutazione

  PL – Performance Level (a,b,c,d,e)

  rappresenta la discretizzazione (5 livelli contigui) della prob. oraria di guasto pericoloso del sistema SRP/CS

  PFHd: Probability of (dangerous) Failure per Hour

- dipendenza da prestazioni affidabilistiche del sistema SRP/CS

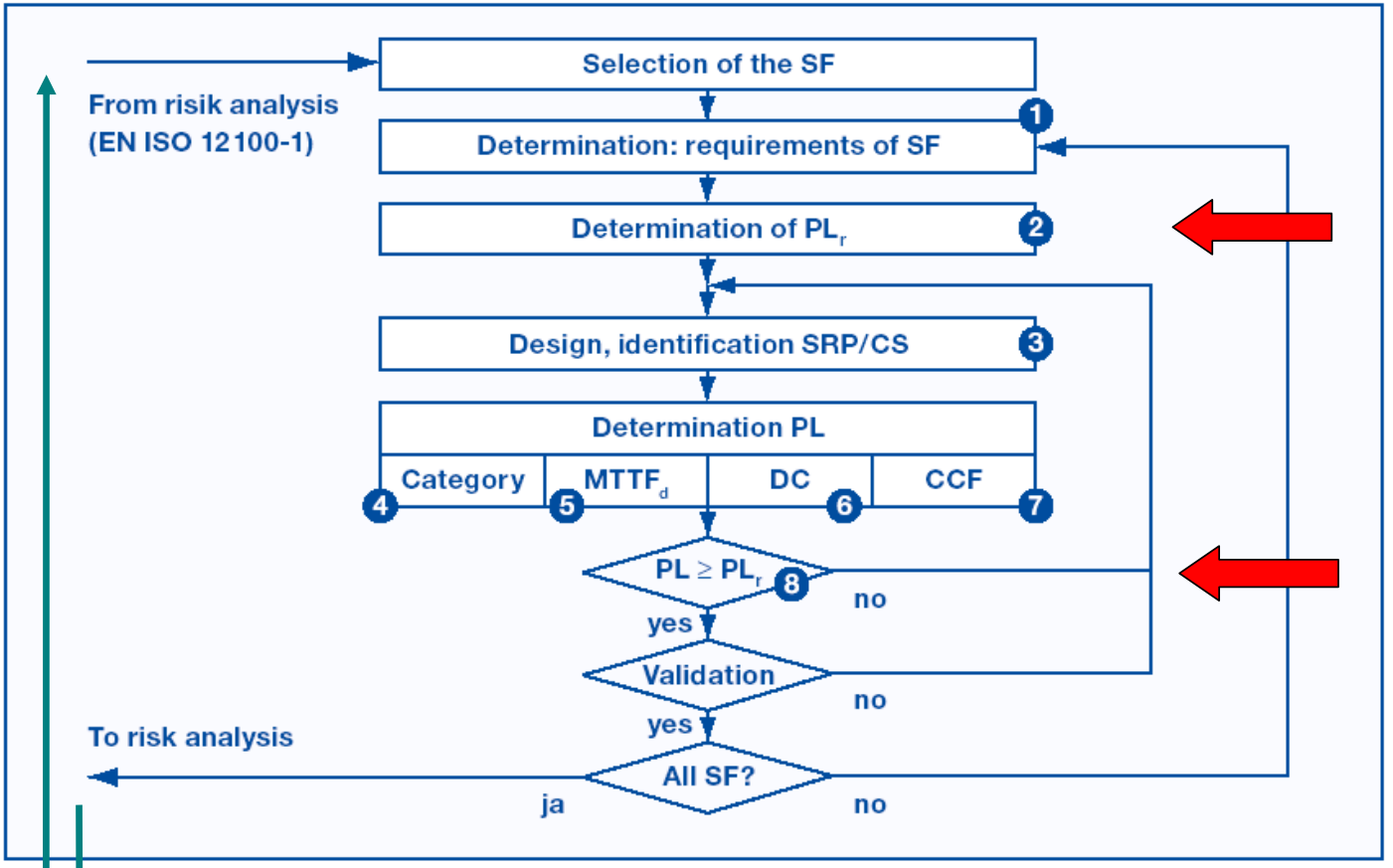
  1. **Architettura del sistema** (5 architetture predefinite tra le quali scegliere)
     Parametri numerici (da quantificare) al suo interrno:
  2. **MTTFd**: Mean Time To (dangerous) Failure oppure **B_{10}d** (cicli)
  3. **DC**: Diagnostic Coverage (frazione di guasti auto-rilevati)

- sistemi ridondanti

  metodo a punteggio per valutaz. misure contro i guasti per cause comune (CCF)

- valutazione del software impiegato con funzioni di sicurezza

UNI EN ISO 13849-1:2008
Procedura iterativa



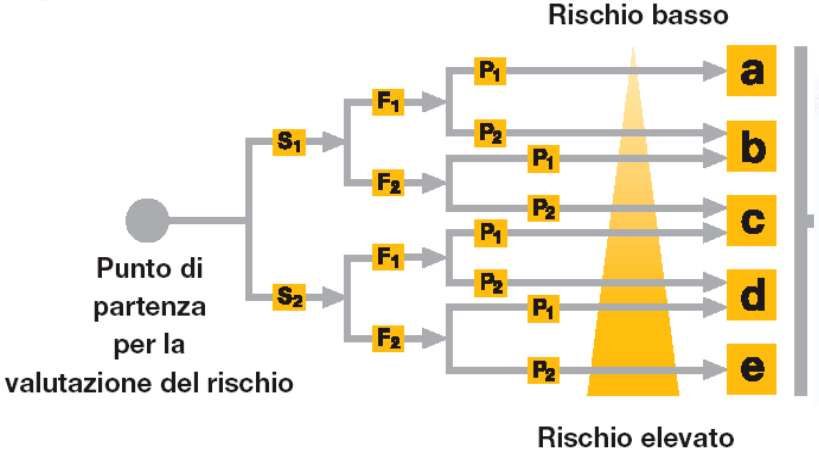
Determinaz. del PL richiesto (PLr)

Verifica del Livello di prestazione e successiva Convalida

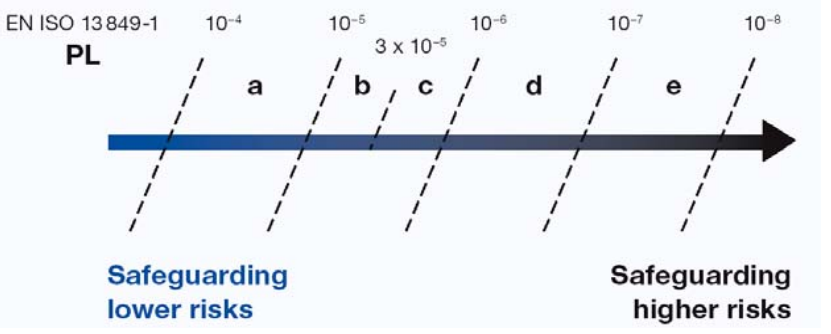
Procedura generale in accordo alla norma UNI EN ISO 14121-1:2007
"Sicurezza del macchinario, Valutazione del rischio - Parte 1: Principi"

UNI EN ISO 13849-1:2008
Determinazione del PLr (Risk-Graph)

- **S – Gravità delle lesioni**
  - S_1 = lesioni leggere (solitamente reversibili)
  - S_2 = lesioni serie, morte inclusa (solitamente irreversibili)
- **F – Frequenza e/o durata dell'esposizione al pericolo**
  - F_1 = da rara a poco frequente e/o breve durata
  - F_2 = da frequente a continua e/o prolungata esposizione
- **P – Possibilità di evitare il pericolo**
  - P_1 = possibile in alcune circostanze
  - P_2 = quasi impossibile



Corrispondenza numerica con PFHd



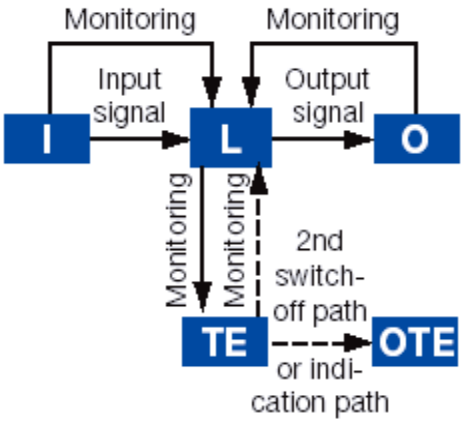
UNI EN ISO 13849-1:2008
Categorie (Architetture predefinite)

Categories B and 1:

Differenze tra cat. B e cat. 1:
il valore di MTTFd del canale deve essere di tipo HIGH per la cat. 1

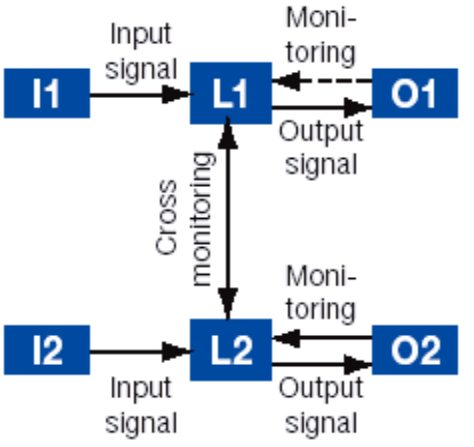
N.B. non è presente la diagnostica (DCavg=none) e non esistono CCF (un solo canale)

Category 2:



Differenza tra cat. 2 e cat. B-1:
è presente una funzione auto-diagnostica

Categories 3 and 4:

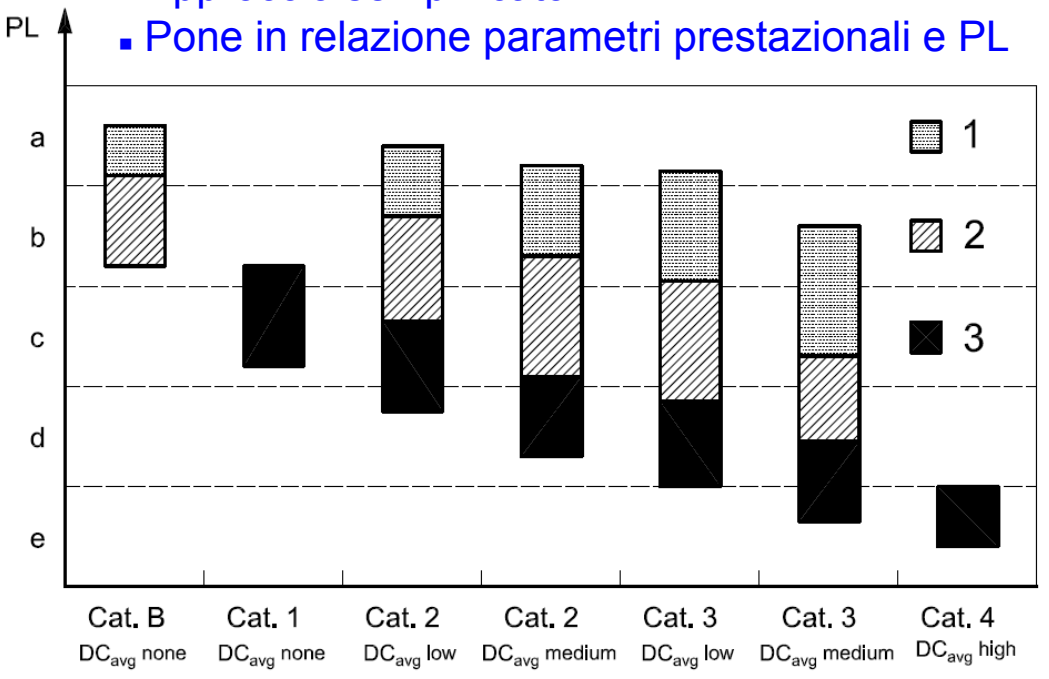


Differenze tra cat. 3 e cat. 4:
il valore di MTTFd dei canali (due in parallelo) è di tipo HIGH per la cat. 4

DCavg = HIGH per la cat. 4

UNI EN ISO 13849-1:2008
Scelta di una configurazione architetturale

- Approccio semplificato
- Pone in relazione parametri prestazionali e PL



1 $MTTF_d$ of each channel = low
2 $MTTF_d$ of each channel = medium
3 $MTTF_d$ of each channel = high

Nella nuova norma le “Categorie” rappresentano delle definite configurazioni di architettura del sistema e non sono il punto di arrivo della valutazione, ma uno degli elementi che concorrono alla determinazione del PL raggiunto

CEI EN 62061:2005 - Determinazione del Safety Integrity Level (SIL) richiesto

1. Determinazione del SIL richiesto

Frequenza e durata	F > 10 Min	F ≤ 10 Min
≤ 1 ora	5	5
> 1 ora – ≤ 1 g.	5	4
> 1 g. – ≤ 2 sett.	4	3
> 2 sett. – ≤ 1 a.	3	2
> 1 anno	2	1

Probabilità evento pericoloso	P
molto alta	5
probabile	4
possibile	3
scarsa	2
trascurabile	1

Evitabilità	E
impossibile	5
possibile	3
probabile	1

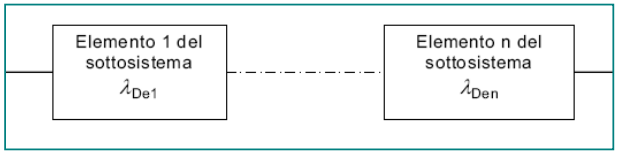
Conseguenze e gravità	S	Classe C = F+W+P				
		3 - 4	5 - 7	8 - 10	11 - 13	14 - 15
morte, perdita di occhio o braccio	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
permanente, perdita di dita	3		AM	SIL 1	SIL 2	SIL 3
reversibile, intervento medico	2			AM	SIL 1	SIL 2
reversibile, pronto soccorso	1				AM	SIL 1
						AM = altre misure

Safety integrity level SIL	Probability of a dangerous Failure per Hour, PFH_D
3	$>10^{-8}$ to $<10^{-7}$
2	$>10^{-7}$ to $<10^{-6}$
1	$>10^{-6}$ to $<10^{-5}$

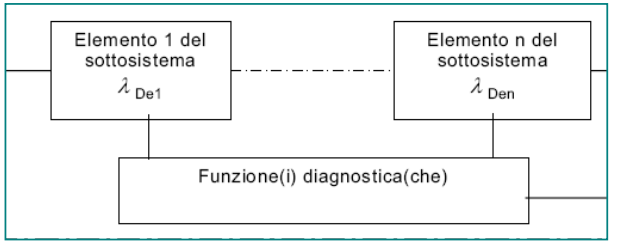
CEI EN 62061:2005 – Safety Related Electrical Control System (SRECS)

Architetture di base (formule di calcolo affidabilistico)

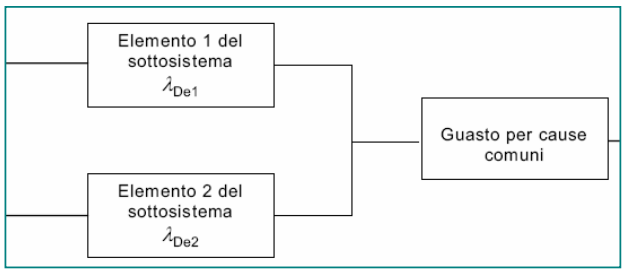
Sottosistema A



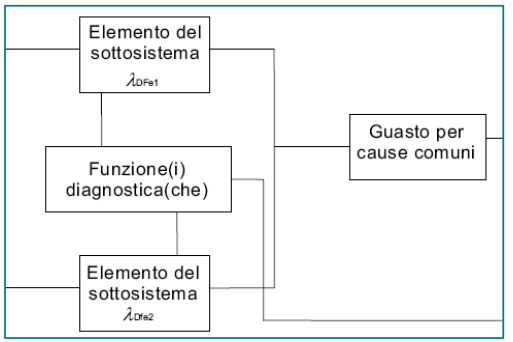
Sottosistema C



Sottosistema B



Sottosistema D



2. Progettazione del sistema (con n sottosistemi)

3. Verifica: $PFH_{DSRECS} = PFH_{D1} + ... + PFH_{Dn} + P_{TE}$ —> SIL ≥ SIL richiesto

4. Convalida

Rapporto tra le norme UNI EN ISO 13849-1:2008 e CEI EN 62061:2005

	Tecnologia che realizza la(e) funzione(i) di controllo relativa(e) alla sicurezza	ISO 13849-1	IEC 62061
A	Non elettrica, es. idraulica	X	Non contemplata
B	Elettromeccanica, es. relè, o elettronica non complessa	Limitata ad architetture designate (vedere Nota 1) e fino a PL=e	Tutte le architetture e fino a SIL 3
C	Elettronica complessa, es. programmabile	Limitata ad architetture designate (vedere Nota 1) e fino a PL=d	Tutte le architetture e fino a SIL 3
D	A in combinazione con B	Limitata ad architetture designate (vedere Nota 1) e fino a PL=e	X vedere Nota 3
E	C in combinazione con B	Limitata ad architetture designate (vedere Nota 1) e fino a PL=d	Tutte le architetture e fino a SIL 3
F	C in combinazione con A, o C in combinazione con A e B	X vedere Nota 2	X vedere Nota 3

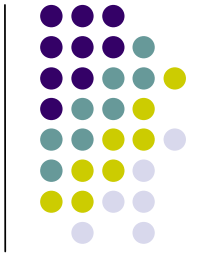
"X" indica che questa voce è trattata nella Norma indicata nell'intestazione di colonna.

NOTA 1 Le architetture designate sono definite nell'Allegato B della EN ISO 13849-1(rev.) per fornire un approccio semplificato alla quantificazione dei livelli di prestazione.

NOTA 2 Per l'elettronica complessa: Utilizzare architetture designate in conformità alla EN ISO 13849-1(rev.) fino a PL=d o qualsiasi architettura conforme alla IEC 62061.

NOTA 3 Per la tecnologia non elettrica, utilizzare come sottosistemi parti conformi alla EN ISO 13849-1(rev.).

Caso applicativo - Sistema elettronico di spegnimento di un motore elettrico all'apertura di un riparo mobile (*Safety-related stop function*)



Definizione della funzione di controllo relativa alla sicurezza (SRCF)

Specifica funzionale:

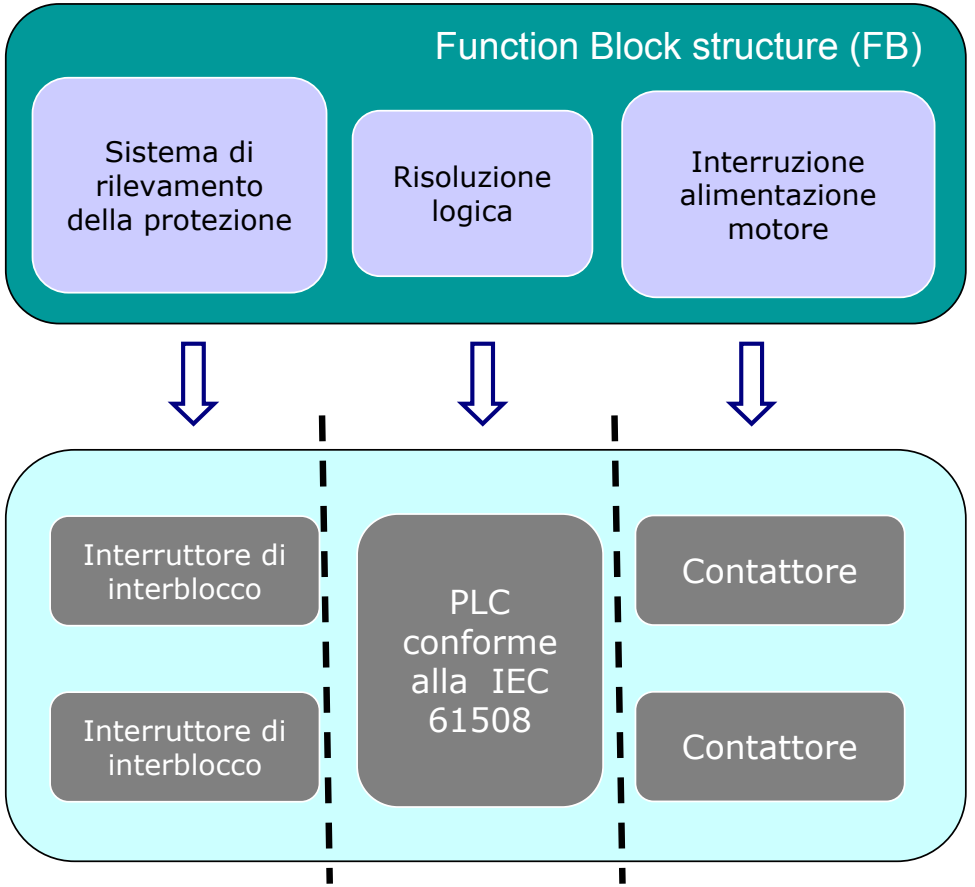
- Se il riparo viene aperto, il motore elettrico deve essere disalimentato

Specifica di integrità:

- da valutare sulla base delle informazioni disponibili:
  - Lesioni irreversibili
  - Elevata frequenza di esposizione al pericolo
  - Elevata probabilità di accadimento dell'evento pericoloso
  - Bassa possibilità di evitare il pericolo o di evitare il danno

Caso applicativo

Componenti del sistema elettronico di controllo relativo alla sicurezza (SRECS)



N.B.

- Le funzioni diagnostiche relative agli interruttori di interblocco sono incorporate all'interno del PLC
- Non è prevista alcuna funzione diagnostica per i contattori

UNI EN ISO 13849-1: Determinazione del Performance Level richiesto (PLr)

Gravità delle lesioni

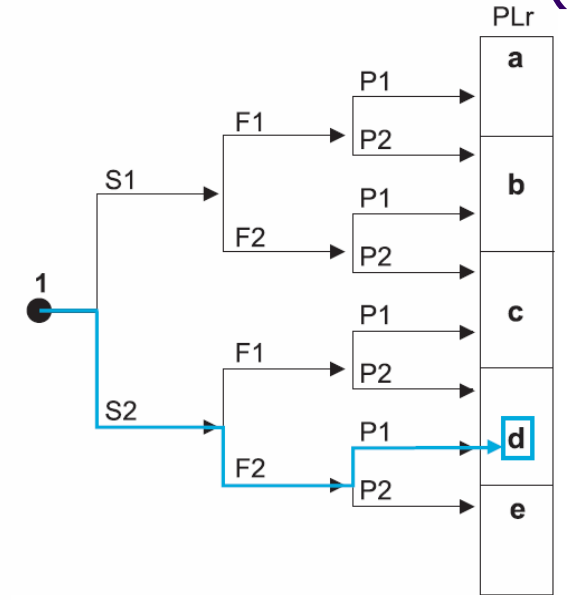
S2 = lesioni gravi (solitamente irreversibili, incluso il decesso)

Frequenza e/o durata dell'esposizione al pericolo

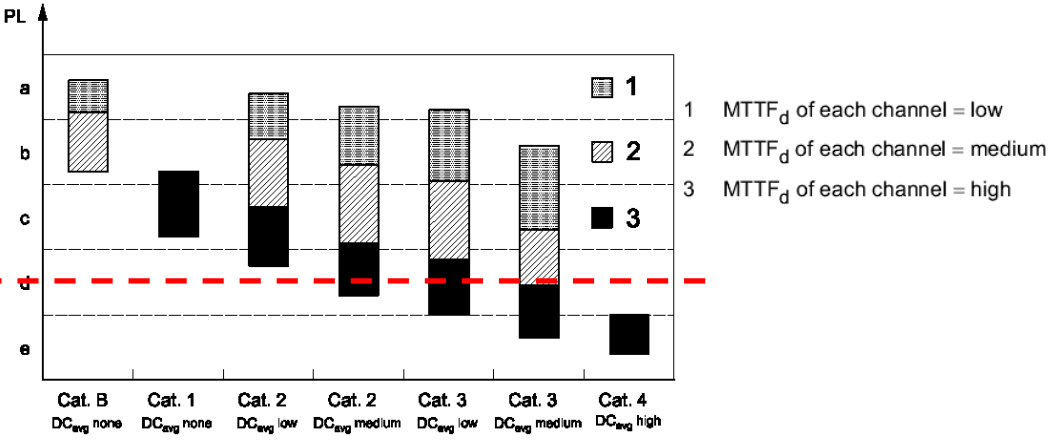
F2 = da frequente a continua e/o prolungata esposizione

Possibilità di evitare il pericolo o di limitare il danno

P1 = possibile in alcune circostanze



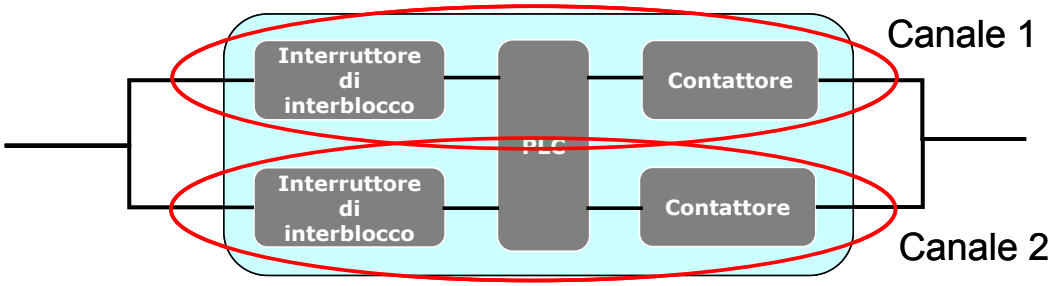
PLr = d

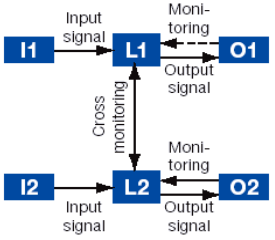


UNI EN ISO 13849-1: Progettazione del sistema di controllo

1. Individuazione delle parti costituenti il sistema di controllo (SRP/CS) e definizione della categoria del sistema
2. Scelta dei componenti e determinazione delle prestazioni di sicurezza (PL) di ciascun SRP/CS
3. Verifica della prestazione di sicurezza raggiunta dal sistema di controllo

UNI EN ISO 13849-1: Progettazione del sistema di controllo





Categoria SRP/CS = 3

Interruttore di interblocco
$MTTF_D$ = 1420.0 [anni]
PLC
$MTTF_D$ = 72.2 [anni]
Contattore
$MTTF_D$ = 142.0 [anni]

Per ciascun canale

$[MTTF_D]_{Canale}$ = 46.3 [anni]

Index	MTTFd range
Low	>3 years to <10 years
Medium	>10 years to <30 years
High	>30 years to <100 years

Copertura Diagnostica media

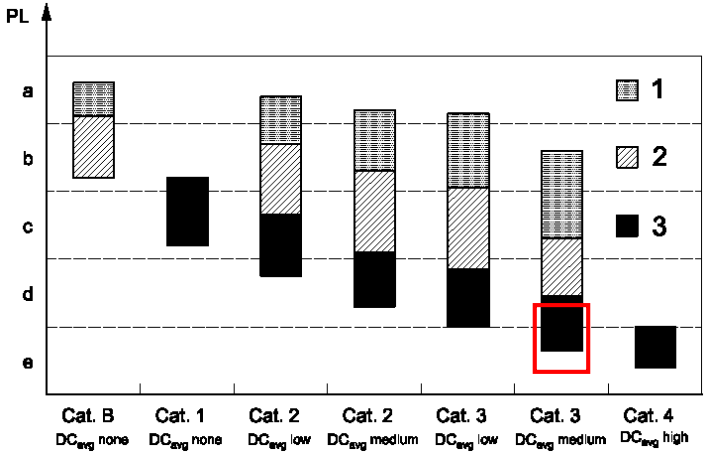
DC_{avg} = 98%

Index	Diagnostic coverage
Nil	<60%
Low	>60% to <90%
Medium	>90% to <99%
High	>99%

UNI EN ISO 13849-1: Progettazione del sistema di controllo

Category	B	1	2	2	3	3	4
DC_{avg}	none	none	low	medium	low	medium	high
$MTTF_d$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

PL del sistema = PL richiesto



CEI EN 62061: Determinazione del Safety Integrity Level (SIL) richiesto

1. SIL =f(Severità del danno; Probabilità di occorrenza del danno)

Frequenza e durata	F > 10 Min	F ≤ 10 Min
≤ 1 ora	5	5
> 1 ora – ≤ 1 g.	5	4
> 1 g. – ≤ 2 sett.	4	3
> 2 sett. – ≤ 1 a.	3	2
> 1 anno	2	1

Probabilità evento pericoloso	P
molto alta	5
probabile	4
possibile	3
scarsa	2
trascurabile	1

Evitabilità	E
impossibile	5
possibile	3
probabile	1

Conseguenze e gravità		Classe C = F+W+P				
	S	3 - 4	5 - 7	8 - 10	11 - 13	14 - 15
morte, perdita di occhio o braccio	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
permanente, perdita di dita	3		AM	SIL 1	SIL 2	SIL 3
reversibile, intervento medico	2			AM	SIL 1	SIL 2
reversibile, pronto soccorso	1				AM	SIL 1

AM = altre misure

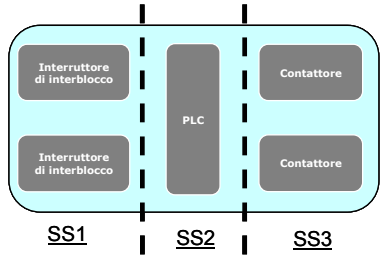
CEI EN 62061:
Progettazione del dispositivo

1. Individuazione dei sottosistemi e definizione della loro architettura (A, B, C, D)

   Architettura = f(tolleranza all'avaria; diagnostica)

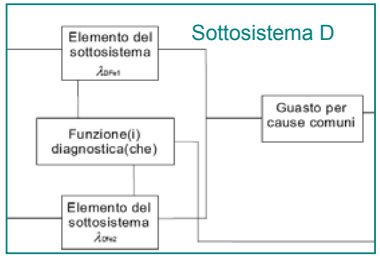
2. Scelta dei componenti e determinazione delle prestazioni di sicurezza dei sottosistemi
3. Verifica della prestazione di sicurezza raggiunta dal dispositivo

CEI EN 62061:
Progettazione del dispositivo



Sottosistema 1 (SS1)

- Architettura tipo D (funzione diagnostica svolta dal PLC ad ogni intervento degli interruttori)



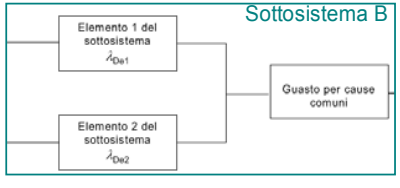
- B_{10} = 10 Milioni [cicli]
- Frazione di guasti pericolosi = 20%
- Vita attesa o intervallo di test = 10 [anni]
- Guasti comuni = 10%

$(PHF_D)_{SS1} = 1.60\ 10^{-9}$

Sottosistema 2 (SS2) *dato noto* $(PHF_D)_{SS2} = 5.96\ 10^{-9}$

Sottosistema 3 (SS3)

- Architettura tipo B (nessuna funzione diagnostica prevista)



- B_{10} = 1 Milione [cicli]
- Frazione di guasti pericolosi = 73%
- Vita attesa o intervallo di test = 20 [anni]
- Guasti comuni = 10%

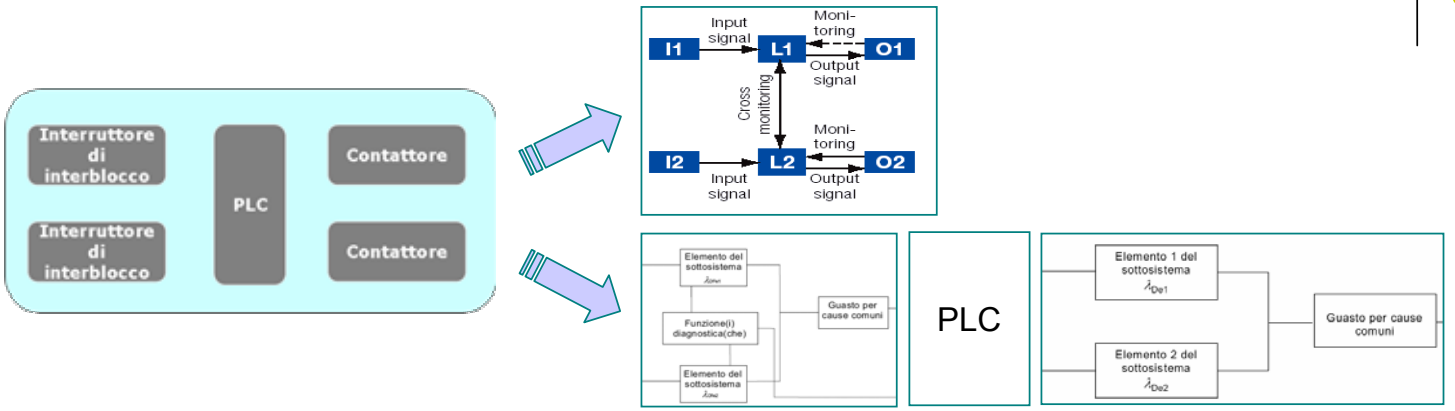
$(PHF_D)_{SS3} = 9.32\ 10^{-8}$

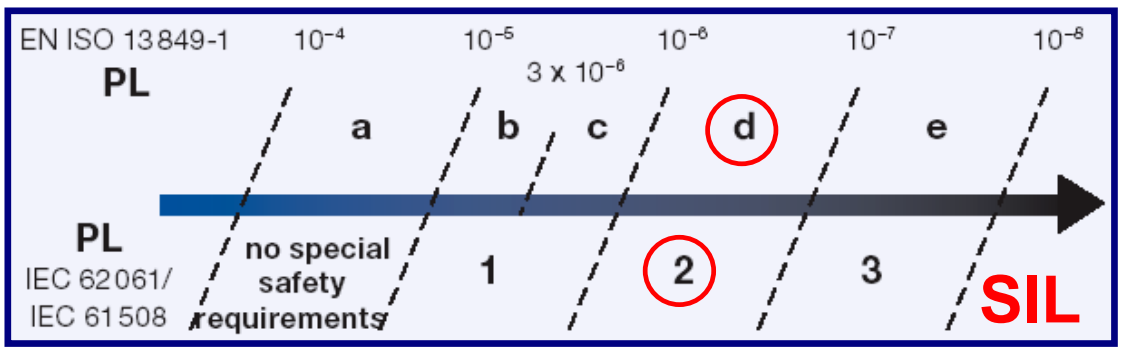
$[PFH_D]_{SRECS} = [PFH_D]_1 + [PFH_D]_2 + [PFH_D]_3 = 1.0076\ 10^{-7}$

Livello di integrità della sicurezza	Probabilità di un guasto pericoloso per ora (PFH_D)
3	$\geq 10^{-8}$ a $< 10^{-7}$
2	$\geq 10^{-7}$ a $< 10^{-6}$
1	$\geq 10^{-6}$ a $< 10^{-5}$

SIL sistema >= SIL richiesto

Corrispondenza tra PL (UNI EN 13849-1) e SIL (CEI EN 62061)





Le metodologie di calcolo delle due norme portano a classificare il dispositivo con lo stesso livello di prestazione (valore di **PFHd**)

Conclusioni

- La procedura di valutazione del rischio nelle due norme conduce a stabilire identiche necessità di prestazioni da parte del sistema (PL d ⇔ SIL 2)
- Le metodologie di calcolo delle due norme classificano il dispositivo in categorie prestazionali equivalenti
- La norma EN IEC 62061 presenta metodi di calcolo molto più generali rispetto alla ISO 13849-1
  - è applicabile a qualsiasi configurazione del sistema
- Il limite sostanziale della norma ISO 13849-1 risiede nell'impostazione prescrittiva riguardo alle architetture (configurazioni) possibili del sistema (maggiore immediatezza)
  - le relazioni tra parametri affidabilistici e prestazione del sistema (PL) sono ricavate attraverso modelli markoviani ristretti a quelle sole configurazioni
- Nella norma ISO 13849-1 gli aspetti legati alla manutenzione (test periodici, ecc.) appaiono poco approfonditi

POLITECNICO
DI BARI

Grazie per l'attenzione