ZVEI:
Die Elektroindustrie

Sicurezza delle Macchine

Indicazioni per l'applicazione delle norme EN 62061 ed EN ISO 13849-1

2° Edizione

Fachverband Automation

SIGLA EDITORIALE

Sicurezza delle Macchine

Indicazioni per l'applicazione delle Norme EN 62061 ed EN ISO 13849-1

ZVEI - Zentralverband Elektrotechnik und Elektronikindustrie e. V.
Lyoner Straße 9
60528 Francoforte

Associazione di Categoria - Automazione
Settore Quadri elettrici,
Quadri, Sistemi di comando industriali
Comitato Tecnico
Sistemi di sicurezza nell'automazione

Autore: Dr. Markus Winzenick

Tel: +49 69 6302-426
Fax: +49 69 6302-319
Mail: winzenick@zvei.org
www.zvei.org/automation

Luglio 2012

Sicurezza delle macchine

Siete costruttori di macchine, system integrator oppure vi occupate del revamping di macchine?

Ecco ciò che è necessario considerare in futuro in termini di sicurezza funzionale!

Indicazioni per l'applicazione delle Norme EN 62061 ed EN ISO 13849-1

1. Procedure base per soddisfare i requisiti della Direttiva Macchine

Cosa è necessario fare per mettere in commercio una macchina che sia conforme alle Direttive in vigore?

La Direttiva Macchine CE stabilisce che le macchine non debbano essere fonte di pericolo (Valutazione dei Rischi secondo EN ISO 12100).

Dato che la tecnologia non garantisce la totale assenza di rischio, l'obbiettivo è di raggiungere un livello di rischio residuo accettabile. Se la sicurezza dipende dai sistemi di comando e controllo, questi devono essere costruiti in modo che la probabilità di guasti funzionali sia sufficientemente bassa. Quando questo non è possibile, è necessario garantire che gli eventuali guasti non portino alla perdita della funzione di sicurezza.

Per soddisfare questo requisito è opportuno seguire le indicazioni fornite delle norme armonizzate, realizzate secondo il mandato della Commissione Europea e pubblicate nella Gazzetta Ufficiale della Comunità Europea (Presunzione di Conformità).

Questo è l'unico modo per evitare ulteriori costi, in termini di sforzo e tempo, per dimostrare la conformità. Di seguito si fornisce una comparazione tra la norma EN 62061 e la norma EN ISO 13849-1 e viene fornita una guida all'utilizzo.

2. Perché la EN 954-1 non è più applicabile?

In passato, le parti dei sistemi di comando di una macchina legate alla sicurezza, venivano progettate secondo la EN 954-1.

Questa era basata sul rischio calcolato (classificato in categorie). Lo scopo era assegnare a ciascuna categoria identificata un adeguato comportamento del sistema (approccio deterministico). In seguito all'introduzione dell'elettronica e soprattutto dell'elettronica programmabile nella tecnica della sicurezza, non era più possibile garantire la sicurezza unicamente tramite il semplice sistema di categorie previsto dalla EN 954-1. Inoltre, non era possibile fornire alcun tipo di indicazione relativa alla probabilità di guasto (approccio probabilistico).

La soluzione è arrivata con l'introduzione delle norme EN 62061 ed EN ISO 13849-1, che sostituiscono la EN 954-1.

3. Campo applicativo delle due norme

EN ISO 13849-1: *Parti del sistema di comando legate alla sicurezza - Parte 1: Principi generali per la progettazione.*

Questa norma può essere utilizzata per SRP/CS (Parti dei sistemi di comando legate alla sicurezza) e per tutti i tipi di macchine, indipendentemente dalla tecnologia e dall'energia utilizzate (elettrica, idraulica, pneumatica, meccanica, ecc.).

La EN ISO 13849-1 indica anche requisiti specifici per SRP/CS con sistemi elettronici programmabili.

EN 62061: *Sicurezza funzionale di sistemi di controllo elettrici, elettronici ed elettronici programmabili.*

Questa norma stabilisce i requisiti e fornisce indicazioni per la realizzazione, l'integrazione e la validazione di sistemi di comando e controllo di sicurezza elettrici, elettronici ed elettronici programmabili (SRECS) per le macchine.

La norma non indica alcun requisito relativo alle prestazioni di dispositivi di controllo comando di sicurezza non elettrici (ad es. idraulici, pneumatici, elettromeccanici) per le macchine.

4. Breve descrizione EN ISO 13849-1

La EN ISO 13849-1 si basa sulle categorie come già specificate nella EN 954-1:1996. La nuova norma riguarda le funzioni di sicurezza nella loro interezza, inclusi tutti i componenti utilizzati nella loro progettazione.

Oltre alle indicazioni della EN 954-1 (approccio qualitativo), la EN ISO 13849-1 prevede anche una valutazione quantitativa delle funzioni di sicurezza. A questo scopo vengono definiti, basandosi sulle categorie, i Performance Level (PL). I dispositivi, a seconda del tipo, richiedono i seguenti parametri caratteristici legati alla sicurezza:

- Categoria (requisito strutturale)
- PL : Performance Level
- $MTTF_d$: tempo medio prima di un guasto pericoloso (mean time to dangerous failure)
- B_{10d} : numero di cicli entro cui, in un controllo a campione, il 10% dei componenti soggetti ad usura presi in esame subisce guasti pericolosi

- DC : Copertura Diagnostica (Diagnostic Coverage)
- CCF : Guasti da causa comune (Common Cause Failure)
- T_M : Tempo di servizio (Mission Time)

La norma descrive come calcolare il Performance Level (PL) per le parti di dei sistemi di comando legate alla sicurezza, sulla base di architetture predefinite (designated architectures) per la durata d'utilizzo prevista TM (Mission Time).

In caso di eccezioni, per quanto riguarda i sistemi elettrici/elettronici, la EN ISO 13849-1 rimanda alla IEC 61508. Qualora più parti legate alla sicurezza vengano combinate in un unico sistema, la Norma descrive come calcolare il PL complessivo che può essere raggiunto.

Per ulteriori indicazioni relative alla validazione, la EN ISO 13849-1 rimanda alla Parte 2, Questa parte fornisce informazioni riguardanti , tra gli altri argomenti, valutazione di guasti manutenzione, documentazione tecnica e linee guida di utilizzo. Il periodo di transizione dalla EN 954-1 alla EN ISO 13849-1 è terminato il 31 Dicembre 2011.

5. *Breve descrizione EN 62061*

La EN 62061 rappresenta una norma specifica di settore all'interno della IEC 61508.

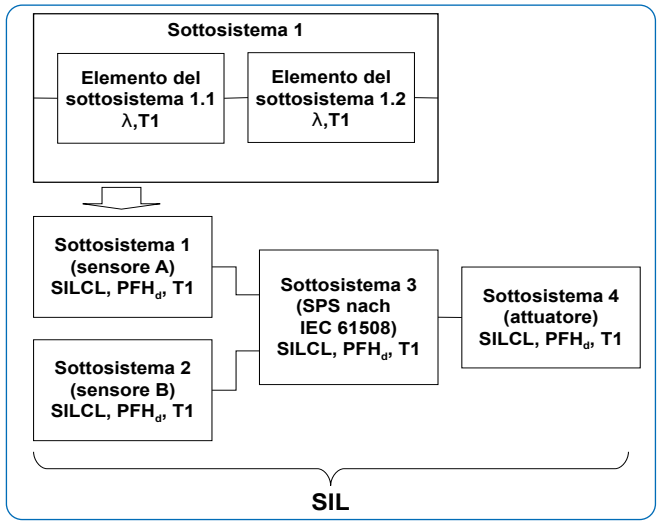
Descrive l'implementazione di sistemi di comando e controllo di sicurezza elettrici ed elettronici di macchine e impianti, e ne prende in considerazione l'intero ciclo di vita, dalla progettazione alla dismissione.

La norma si basa su valutazioni qualitative e quantitative delle funzioni di comando correlate alla sicurezza.

Le prestazioni di una funzione di sicurezza vengono indicate con il **Safety Integrity Level (SIL).**

Le funzioni di sicurezza identificate dall'analisi del rischi, vengono suddivise in sottofunzioni di sicurezza; queste sottofunzioni di sicurezza vengono quindi correlate a dispositivi reali, chiamati sottosistemi ed elementi del sottosistema. Questo include sia la parte hardware sia la parte software.

Le caratteristiche legate alla sicurezza di questi sottosistemi sono descritte da parametri caratteristici (limite di SIL richiesto e „PFH_d".



Parametri caratteristici legati alla sicurezza per i sottosistemi:

- SILCL : limite SIL richiesto (SIL claim limit)
- PFH_d : probabilità di guasti pericolosi per ora (probability of dangerous failure per hour)
- T_1 : ciclo di vita (lifetime)

Questi sottosistemi possono essere composti a loro volta da diversi elementi (dispositivi) di sottosistemi interconnessi, con i parametri caratteristici per calcolare il corrispondente valore PFHd del sottosistema.

Parametri caratteristici legati alla sicurezza per elementi di sottosistemi (dispositivi):

- λ : tasso di guasto (failure rate); per elementi soggetti ad usura: valore B_{10}
- SFF : frazione di guasto in sicurezza (Safe Failure Fraction)

Nel caso di dispositivi elettromeccanici, il costruttore indica il tasso di guasto tramite il valore B10, basato sul numero di cicli di commutazione. Il tasso di guasto, legato al tempo, ed il ciclo di vita devono essere determinati sulla base della frequenza di commutazione relativa all'applicazione specifica.

I parametri interni da definire durante la progettazione/realizzazione, devono includere tutti quelli specifici degli elementi del sottosistema:

- T_2 : intervallo di test diagnostico (diagnostic test interval)
- β : suscettibilità ai guasti da causa comune (susceptibility to common cause failure)
- DC : grado di copertura diagnostica (diagnostic coverage)

Il valore PFH_d del sistema di comando e controllo di sicurezza è dato dalla somma dei singoli valori PFH_d dei sottosistemi.

Nella progettazione di un sistema di comando e controllo di sicurezza, gli utilizzatori hanno le seguenti opzioni:

- utilizzare dispositivi e sottosistemi già conformi alla EN ISO 13849-1 ed IEC 61508 o EN 62061. La norma fornisce indicazioni su come integrare dispositivi certificati nella realizzazione delle funzioni di sicurezza.
- sviluppare sottosistemi propri.
  – sottosistemi elettronici programmabili, sottosistemi complessi: applicare la IEC 61508.
  – dispositivi e sottosistemi semplici: applicare la EN 62061.

La norma rappresenta un sistema completo per la realizzazione di sistemi di comando e controllo di sicurezza elettrici, elettronici ed elettronici programmabili. La EN 62061 è norma armonizzata dal dicembre 2005.

Per i sistemi non elettrici è necessario utilizzare la EN ISO 13849-1.

6. La sicurezza passo passo – Procedura base

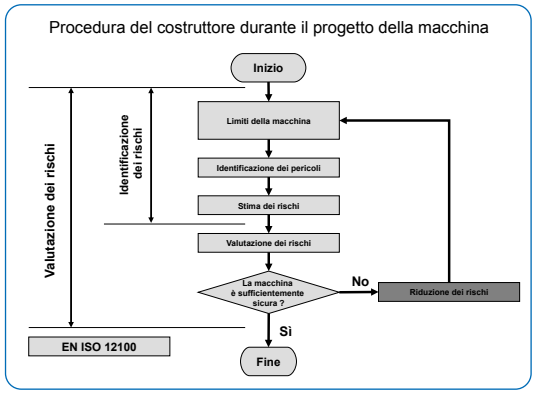
Fase 1 – Valutazione dei Rischi secondo EN ISO 12100

Se non si impiegano misure di sicurezza, è prevedibile che prima o poi un eventuale pericolo presente su una macchina porti a danni/incidenti.

Le misure di sicurezza sono una combinazione delle misure previste dal costruttore e quelle integrate dall'utilizzatore.

E' preferibile prevedere le misure di sicurezza già in fase di progettazione, piuttosto che integrarle successivamente (da parte dell'utilizzatore); generalmente le prime sono più efficaci delle seconde.

Il costruttore deve seguire la sequenza sotto riportata, tenendo in considerazione sia l'esperienza acquisita da utilizzatori finali di macchine simili, sia le informazioni emerse dalle discussioni con potenziali utilizzatori (quando questo è possibile).



– stabilire i limiti e l'utilizzo previsto della macchina;
– identificare i pericoli e ogni tipo di situazione pericolosa;
– stimare i rischi per ogni pericolo o situazione pericolosa identificati;
– valutare i rischi e decidere se sia necessario ridurli.

Fase 2 – Definizione delle misure per ridurre i rischi

L'obiettivo è ridurre i rischi quanto più possibile, tenendo in considerazione diversi fattori. Il processo è iterativo; pur utilizzando nel miglior modo possibile le tecnologie disponibili, può essere necessario ripetere il processo più volte fino a raggiungere un'adeguata riduzione dei rischi.

Nell'eseguire questo processo è necessario osservare le seguenti priorità:

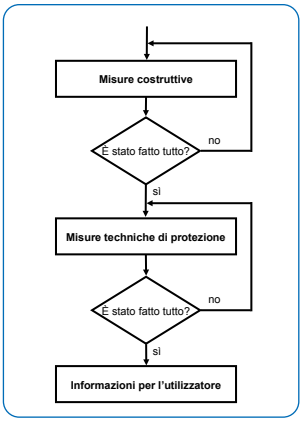
– sicurezza della macchina in ogni fase del ciclo di vita;

– potenzialità della macchina nello svolgere le funzioni a cui è destinata;

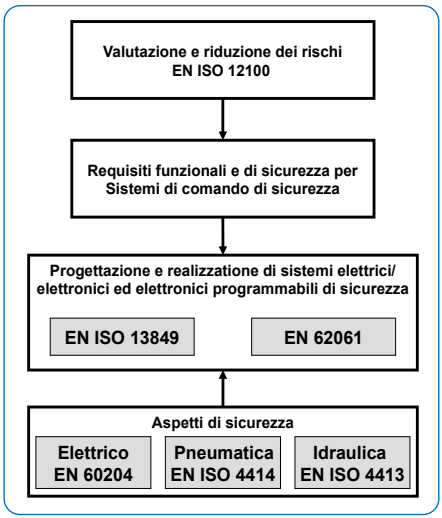
– Facilità d'uso della macchina.

Solo in seguito si valuteranno i costi di costruzione, funzionamento e dismissione della macchina.

L'Analisi dei rischi e il processo di riduzione dei rischi prevedono che i rischi vengano eliminati o ridotti mediante una serie di misure specifiche secondo l'ordine gerarchico seguente:



– eliminazione dei pericoli o riduzione dei rischi già in fase di progettazione
– riduzione dei rischi tramite dispositivi tecnici di protezione e potenziali misure protettive aggiuntive
– riduzione dei rischi grazie alla disponibilità di informazioni, per l'utilizzatore, in merito ai rischi residui.



Fase 3 – Riduzione dei rischi tramite misure di controllo

Se le parti di comando legate alla sicurezza vengono utilizzate per implementare misure di protezione ed ottenere una adeguata riduzione dei rischi, la progettazione di tali parti di comando, deve essere parte integrante dell'intera procedura di progettazione della macchina. Il sistema di comando e controllo di sicurezza fornisce le funzioni di sicurezza con valori di SIL o di PL, che realizzano la necessaria riduzione dei rischi.

Fase 4 – Implementazione di misure di controllo secondo EN ISO 13849-1 o EN 62061

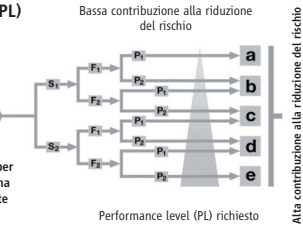
1) Determinazione del Performance Level richiesto (PL)

EN ISO 13849-1

Determinazione del performance level richiesto (PL)

- **S – Gravità della lesione**
  - S_1 = Lesione lieve (normalmente reversibile)
  - S_2 = Lesione grave (normalmente irreversibile inclusa la morte)
- **F – Frequenza e/o tempo di esposizione al pericolo**
  - F_1 = Da raramente ad abbastanza spesso e/o tempo di esposizione breve
  - F_2 = Da frequente a continuo e/o tempo di esposizione lungo
- **P – Possibilità di evitare il pericolo**
  - P_1 = Possibile in determinate condizioni
  - P_2 = Scarsamente possibile

Punto di partenza per la stima del rischio per le parti del sistema di comando legate alla sicurezza.



EN 62061

Valutazione del rischio e misure de sicurezza

Consequenze	Gravià Se	Fréquenza durata	Fr	Probabilita del-ievento pericoloso Pr		Evitabilità	Av	Classe C 3-4	5-7	8-10	11-13	14-15
Morte, perdita di occhio un braccio	4	≤1 h	5	Molto alta	5			SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanente: perdita di dita	3	>1 h a ≤ 1 giorno	5	Probabile	4				QM	SIL 1	SIL 2	SIL 3
Reversibile: intervento medico	2	> 1 giorno a ≤ 2 sett.	4	Possibile	3	Impossibile	5			QM	SIL 1	SIL 2
Reversibile: pronto soccorso		> 2 sett. a ≤ 1 anno	3	Scarsa	2	Possibile	3				QM	SIL 1
		> 1 anno	2	Trascurabile	1	Probabile	1					
				EN 62061				□				

2) Specifiche

Le specifiche dei requisiti funzionali devono descrivere ogni singola funzione di sicurezza da eseguire. E' necessario definire eventuali interfacce con altre funzioni di controllo, e stabilire le appropriate reazioni all'errore. E' inoltre necessario definire il SIL o il PL richiesti.

3) Progettazione dell'architettura

Parte del processo di riduzione dei rischi riguarda la definizione delle funzioni di sicurezza della macchina. Queste comprendono anche le funzioni di sicurezza del sistema di comando e controllo, ad esempio per impedire un avvio imprevisto.

Nella definizione delle funzioni di sicurezza è sempre importante ricordare il fatto che una macchina è dotata di diverse modalità operative (ad es. funzionamento automatico e modalità di set-up), e quindi che le misure di sicurezza possono essere totalmente diverse fra loro a seconda della modalità operativa (ad es. velocità di discesa lenta durante il funzionamento in modalità di set-up <-> bimanuale durante la modalità automatica). Una funzione di sicurezza può essere realizzata mediante uno o più dispositivi di comando e controllo di sicurezza, e più funzioni di sicurezza possono essere suddivise tra uno o più dispositivi di comando e controllo di sicurezza (ad es. moduli logici, elementi di trasmissione dell'energia).

4) Determinazione del Performance Level raggiunto

EN ISO 13849-1

E' necessario determinare il PL per ogni SRP/CS selezionata o per ogni combinazione di SRP/CS dedicate alla gestione di una funzione di sicurezza.

IL PL dell'SRP/CS deve essere determinato partendo dalla valutazione dei seguenti parametri:

- valore $MTTF_d$ o B_{10d} dei singoli componenti
- DC
- CCF
- Architettura (Categoria)
- Reazione in caso di guasto
- Software di sicurezza
- Guasti sistematici
- capacità di eseguire una funzione di sicurezza in condizioni ambientali previste.

EN 62061

La selezione o la progettazione dell' SRECS devono sempre soddisfare i requisiti minimi seguenti:

- Requisiti per l'integrità della sicurezza hardware, comprendenti
- Limiti architetturali per l'integrità di sicurezza hardware
- requisiti relativi alla probabilità di guasti casuali pericolosi dell'hardware

Requisiti aggiuntivi relativi all'integrità sistematica della sicurezza, comprendenti

- requisiti per evitare i guasti e
- requisiti per il controllo dei guasti sistematici.

La EN 62061 descrive anche i requisiti relativi alla realizzazione di programmi applicativi.

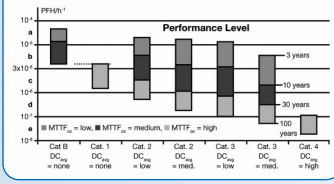
Parametri di sicurezza per sottosistemi:

- SILCL : limite SIL richiesto (SIL claim limit)
- PFH_d : probabilità di guasti pericolosi per ora
- T_1 : ciclo di vita

EN ISO 13849-1

Performance Level	Probabilità di guasti pericolosi [1/h]		
a	≥ 10^{-5}	PFH_d	< 10^{-4}
b	≥ $3x10^{-6}$	PFH_d	< 10^{-5}
c	≥ 10^{-6}	PFH_d	< $3x10^{-6}$
d	≥ 10^{-7}	PFH_d	< 10^{-6}
e	≥ 10^{-8}	PFH_d	< 10^{-7}

Relazione tra categorie, DC, MTTFd e PL



Nota Bene:
I valori di PFH_d rappresentano un requisito essenziale per la determinazione del Performance Level. Inoltre per una completa determinazione del PL devono essere considerati anche CCF, Categoria e DC.

EN IEC 62061

SIL (IEC 61508)	Probabilità di guasti pericolosi [1/h]		
1	≥ 10^{-6}	PFH_d	< 10^{-5}
2	≥ 10^{-7}	PFH_d	< 10^{-6}
3	≥ 10^{-8}	PFH_d	< 10^{-7}

Parametri di sicurezza per elementi dei sottosistemi (dispositivi):

- λ: tasso di guasto
- B_{10d} : per elementi soggetti ad usura
- T_1 : ciclo di vita
- T_2 : intervallo di test diagnostico
- β: suscettibilità ai guasti da causa comune
- DC : grado di copertura diagnostica
- SFF : frazione di guasto in sicurezza (Safe failure Fraction)
- HFT : tolleranza ai guasti hardware

SFF	HFT 0	HFT 1	HFT 2
< 60%	Nicht zulässig	SIL1	SIL2
≥ 60% bis < 90%	SIL1	SIL2	SIL3
≥ 90% bis < 99%	SIL2	SIL3	SIL3
≥ 99%	SIL3	SIL3	SIL3

EN ISO 13849-1	EN IEC 62061

Performance Level	SIL
a	-
b	1
c	
d	2
e	3

Nota Bene:
L'illustrazione descrive la relazione tra i due concetti delle norme (PL e SIL) basata sulla probabilità di guasto PFH_d.

5) Verifica

Per ogni singola funzione di sicurezza, il PL dello SRP/CS deve corrispondere al „Performance Level richiesto".

I PLs di più SRP/CS, che sono parte di una funzione di sicurezza, devono essere uguali o maggiori del Performance Level richiesto per questa funzione.

In caso di più SRP/CS collegati in serie, il PL definitivo può essere determinato utilizzando la Tabella 11 prevista dalla norma

La probabilità di guasti pericolosi di ogni funzione di controllo di sicurezza (SRCF) causata da guasti hardware casuali deve essere uguale o inferiore al valore limite stabilito nelle specifiche dei requisiti di sicurezza.

Il SIL raggiunto grazie allo SRECS sulla base dei limiti architetturali deve essere inferiore o uguale al SILCL più basso di qualsiasi sottosistema coinvolto nell'esecuzione della funzione di sicurezza.

6) Validazione

La progettazione di una funzione di comando e controllo di sicurezza deve essere validata. L'idoneità della funzione di comando e controllo di sicurezza viene esaminata per l'applicazione specifica. La validazione può essere effettuata mediante analisi o test (ad esempio simulazione di guasti singoli o multipli).

7. Glossario

Abbreviazione	Definizione in inglese	Descrizione in italiano
B_{10d}		Numero di cicli a cui il 10% dei componenti si guasta in modo pericoloso
λ	Failure Rate	Tasso di guasto
λ_s		Tasso di guasto – guasti non pericolosi
λ_d		Tasso di guasto – guasti pericolosi
CCF	Common Cause Failure	Guasti da causa comune
DC	Diagnostic Coverage	Copertura diagnostica
DC_{avg}	Average Diagnostic Coverage	Copertura diagnostica media
	Designated Architecture	Architettura prevista di un SRP/CS
HFT	Hardware Fault Tolerance	Tolleranza guasti hardware
MTBF	Mean Time	Tempo medio che intercorre tra due guasti
MTTF	Mean Time To Failure	Tempo medio al guasto
$MTTF_d$	Mean Time To Dangerous Failure	Tempo medio al guasto pericoloso
MTTR	Mean Time To Repair	Tempo medio al ripristino (sempre decisamente inferiore al MTTF)
PFH	Probability Of Failure Per Hour	Probabilità che si verifichi un guasto all'ora
PFH_D	Probability Of Dangerous Failure Per Hour	Probabilità che si verifichi un guasto pericoloso all'ora
PL	Performance Level	Capacità delle parti di comando di svolgere una funzione di sicurezza in condizioni prevedibili, per garantire la riduzione del rischio prevista
PL_r	Performance Level required	Performance Level richiesto
SIL	Safety Integrity Level	Livello di integrità della sicurezza
SILCL	Safety Integrity Claim Limit	Limite SIL richiesto
SRCF	Safety Related Control Function	Funzione di controllo relativa alla sicurezza
SRP/CS	Safety Related Parts of a Control System	Parti di un sistema di comando legate alla sicurezza
SRECS	Safety Related Electrical Control Systems	Sistema elettrico di controllo relativo alla sicurezza

Abbreviazione	Definizione in inglese	Descrizione in italiano
T_1	Lifetime	Ciclo di vita
T_2	Diagnostic Test Interval	Intervallo di test diagnostico
T_M	Mission Time	Durata dell'utilizzo
β	Susceptibility to Common Cause Failure	Suscettibilità ai guasti da causa comune
C	Duty Cycle	Ciclo di vita (all'ora) di un componente elettromeccanico
SFF	Safe Failure Fraction	Frazione guasti non pericolosi
Protezione		Termine comune per ripari di protezione. Il controllo consente di proteggere cose o persone.
Sicurezza		Termine comune per la sicurezza funzionale e la sicurezza delle macchine
Sicurezza Macchine		Stato raggiunto quando sono state realizzate misure di sicurezza per la riduzione dei rischi a rischi residui accettabili, a seguito dell' Analisi del Rischi.
Sicurezza funzionale		Parte di sicurezza di una macchina e del sistema di comando e controllo di una macchina che dipende dal corretto funzionamento dell'SRECS, dei sistemi di sicurezza e di dispositivi esterni per la riduzione del rischio

8. FAQ

Q: Le elettrovalvole / i contattori hanno una classificazione secondo i SIL o i PL?

R: No. I SIL e i PL non sono applicabili a componenti singoli.

Q: Qual è la differenza tra SIL e SILCL?

R: Il SIL si riferisce sempre a una funzione di sicurezza completa, mentre il SILCL si riferisce ad un sottosistema.

Q: Ci sono analogie tra PL e SIL?

R: Tramite il valore PFHd è possibile stabilire una relazione tra PL e SIL. (v. Fase 4: „Determinazione del Performance Level raggiunto").

Nota – la tabella non tiene conto delle indicazioni specifiche delle due norme in merito a: architettura, copertura diagnostica, requisiti sistematici.

Probabilità pericolose all di guasti pericolosi per ora [1/h]			Performance level (PL) EN ISO 13849-1	Livello SIL (IEC61508)
$\geq 10^{-5}$	PFH_d	$< 10^{-4}$	a	-
$\geq 3x10^{-6}$	PFH_d	$< 10^{-5}$	b	1
$\geq 10^{-6}$	PFH_d	$< 3x10^{-6}$	c	
$\geq 10^{-7}$	PFH_d	$< 10^{-6}$	d	2
$\geq 10^{-8}$	PFH_d	$< 10^{-7}$	e	3

Q: Quale grado di copertura diagnostica è possibile prevedere per relè e contattori con apertura guidata dei contatti?

R: In conformità a entrambe le norme, è possibile prevedere un DC del 99% in considerazione dei contatti ad apertura guidata, con contattori e relè ridondanti (Doppio canale).

Una funzione diagnostica con appropriata reazione al guasto rappresenta un prerequisito.

Q: E' possibile raggiungere una tolleranza al guasto pari a 1 con un singolo dispositivo di interblocco elettromeccanico (ripari mobili)?

R: No, una sola anomalia causerebbe il guasto del circuito. Per dispositivi magnetici o RFID, il costruttore può garantire una tolleranza al guasto pari a 1.

Q: E' previsto un valore PFHd per componenti soggetti ad usura?

R: No, l'utilizzatore può calcolare il valore di PFHd per componenti soggetti ad usura, sulla base dell'applicazione specifica, utilizzando il valore $B10_d$ in relazione al numero di cicli di lavoro.

Q: Qual è la differenza tra MTBF e MTTF?

R: L'MTBF descrive il tempo che intercorre tra 2 guasti, a differenza dell'MTTF che invece descrive il tempo medio prima che si verifichi il primo guasto.

Q: Cosa significa la lettera „d" in $MTTF_d$?

R: „d" sta per „dangerous" –> l'$MTTF_d$ descrive il tempo medio prima che si verifichi il primo guasto pericoloso.

Q: Posso applicare la EN ISO 13849-1 nell'integrazione di dispositivi elettronici programmabili complessi?

R: Sì. Tuttavia, per il software del sistema operativo e per le funzioni di sicurezza secondo il PL „e", è necessario tenere in considerazione i requisiti della IEC 61508-3.

Q: Cosa si può fare se il costruttore non fornisce alcun dato tecnico relativo ai componenti?

R: Gli Allegati della EN ISO 13849-1 e della EN 62061 includono entrambe valori di riferimento per i componenti di utilizzo comune. Dove possibile, è comunque preferibile utilizzare sempre i dati forniti dal costruttore dei componenti stessi.

Q: E' possibile applicare la EN ISO 13849-1 per calcolare l'MTTF per valvole di processo/armature utilizzate solo una o due volte all'-anno (Low Demand)?

R: No, la EN ISO 13849-1 prevede unicamente la modalità High Demand. E' quindi possibile effettuare una valutazione dell'MTTF solo mediante misure aggiuntive, quali ad es. la „dinamizzazione forzata".

Q: E' possibile applicare la EN 62061 per calcolare il tasso di anomalia/guasto per valvole di processo/armature utilizzate solo una o due volte all'anno (Low Demand)?

R: Vedi domanda precedente.

Q: I software applicativi devono essere certificati? Se „sì", secondo quale norma?

R: No. Non è obbligatoria nessuna certificazione secondo entrambe le Norme. Nell'ambito di verifica e validazione di funzioni di sicurezza, un test software può essere necessario.

Le informazioni su questo argomento si possono trovare in EN ISO 13849-1 capitolo 4.6 e EN 62061 capitoli 6,9 e 6,10 così come nella EN 61508-3.

Q: Può ogni componente con MTTF essere utilizzato per tecnologie di sicurezza?

R: No, in aggiunta ai dati caratteristici quali MTTF e B_{10d}, il componente deve essere funzionalmente adatto per la specifica funzione e deve soddisfare alcuni requisiti minimi, sia costruttivi che relativi alla sicurezza (attuazione e applicazione dei principi di sicurezza).

ZVEI – Zentralverband Elektrotechnik und
Elektronikindustrie e. V.

Lyoner Straße 9
60596 Francoforte

Associazione di Categoria - Automazione

Settore Quadri elettrici,
Quadri, Sistemi di comando industriali

Comitato Tecnico
Sistemi di sicurezza nell'automazione