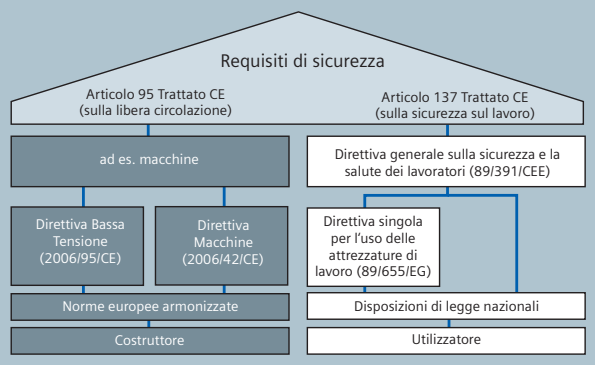
Requisiti fondamentali di sicurezza nell'industria manifatturiera



Norme armonizzate (presunzione di conformità)

Norme di base per le funzioni di comando legate alla sicurezza

Progettazione e analisi dei rischi della macchina

EN ISO 12100-1 Sicurezza del macchinario — Concetti di base, principi generali di progettazione

Requisiti funzionali e di sicurezza per controllori di sicurezza

Disegno e realizzazione di controllori di sicurezza

EN 62061 **Sicurezza del macchinario** Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza	**EN ISO 13849-1** **Sicurezza del macchinario** Parti dei sistemi di comando legate alla sicurezza, Parte 1: Principi generali di progettazione
Architetture qualsiasi **Livello di integrità della sicurezza (SIL)** SIL 1, SIL 2, SIL 3	**Architetture previste (categorie)** **Performance Level (PL)** PL a, PL b, PL c, PL d, PL e

Aspetti sulla sicurezza elettrica

EN 60204-1 Sicurezza del macchinario: Equipaggiamento elettrico delle macchine, Parte 1: Regole generali

Disegno e realizzazione di controllori di sicurezza

Strategia di riduzione dei rischi secondo la norma EN ISO 12100-1

Definizione di misure volte alla riduzione dei rischi attraverso un processo iterativo

1. Definizione dei limiti della macchina
2. Identificazione dei pericoli, stima dei rischi, valutazione dei rischi
3. Valutazione del rischio per ogni pericolo identificato
4. Valutazione del rischio e definizione di decisioni atte a ridurre i rischi
5. Eliminazione del pericolo o riduzione del rischio connesso attraverso misure opportune (metodo dei „3 passi": inerente a costruzione sicura, misure tecniche e informazione dell'utente)

Applicabile a sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza (SRECS) per le macchine

EN 62061 **(Norma settoriale all'interno della norma generale IEC 61508)**

Applicabile alle parti di sicurezza di controllori e a tutti i tipi di macchine, a prescindere dalla tecnologia e dall'energia utilizzate (elettrica, idraulica, pneumatica, meccanica ecc.).

EN ISO 13849-1

Piano di sicurezza

Strategia di realizzazione della funzione di sicurezza, responsabilità, manutenzione ecc.

Analisi dei rischi

Rischio riferito al pericolo identificato = Entità del danno **Se** e
- Frequenza e durata dell'esposizione al pericolo **Fr**
- Probabilità che si produca l'evento pericoloso **Pr**
- Possibilità di evitare il rischio **Av**

Determinazione del SIL necessario

(mediante assegnazione del SIL)

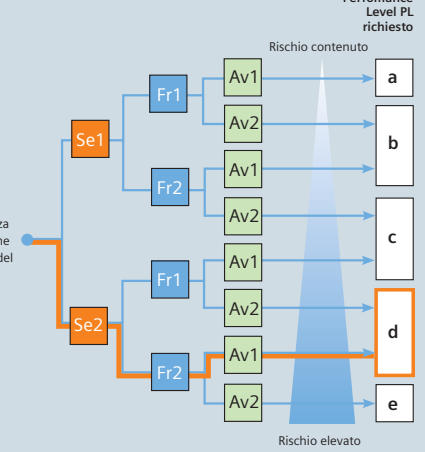
Frequenza e/o durata Fr		Probabilità che si produca l'evento pericoloso Pr		Possibilità di evitare il rischio Av	
≤ 1 ora	5	frequente	5		
Da > 1 ora a ≤ 1 giorno	5	probabile	4		
Da > 1 giorno a ≤ 2 sett.	4	possibile	3	impossibile	5
Da > 2 sett. a ≤ 1 anno	3	rara	2	possibile	3
> 1 anno	2	trascurabile	1	probabile	1

Effetti	Entità del danno Se	Classe Cl = Fr + Pr + Av				
		3–4	5–7	8–10	11–13	14–15
Morte, perdita di un occhio o di un braccio	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanente, perdita delle dita	3			SIL 1	SIL 2	SIL 3
Reversibile, cure mediche	2	altre misure			SIL 1	SIL 2
Reversibile, pronto soccorso	1					SIL 1

Procedimento
1. Determinazione dell'entità del danno Se
2. Determinazione dei punti per frequenza Fr, probabilità Pr e possibilità di evitare il rischio Av:
3. Totale dei punti per Fr + Pr + Av = classe Cl
4. Punto di intersezione tra riga per entità del danno Se e colonna Cl = SIL richiesto

Determinazione del PL necessario

(tramite grafo di rischio)



Parametri di rischio

Se = **entità della lesione**
- Se1 = lesione leggera (normalmente reversibile)
- Se2 = lesione grave (normalmente irreversibile), inclusa la morte

Fr = **frequenza e/o durata dell'esposizione al pericolo**
- Fr1 = da raro a frequente e/o il periodo di esposizione al rischio è breve
- Fr2 = da frequente a permanente e/o il periodo di esposizione al rischio è lungo

Av = **possibilità di evitare il pericolo o contenimento del danno**
- Av1 = possibile a determinate condizioni
- Av2 = quasi impossibile

a, b, c, d, e = **obiettivi del Performance Level di sicurezza**

Configurazione della funzione di sicurezza e determinazione dell'integrità della sicurezza ottenuta

SRECS

	Sistema parziale di rilevamento: Sensori		Sistema parziale di analisi: Unità di controllo	Sistema parziale di reazione: Attuatori	
	Disegno eseguito dall'utente certificati	Utilizzo di componenti certificati	Utilizzo di componenti certificati	Disegno eseguito dall'utente	Utilizzo di componenti certificati
Sistema parziale lambda	Scelta architettura Calcolo con			Scelta architettura Calcolo con	
Componenti elettromeccanici	• valore B10			• valore B10	
Ciclo di azionamento	• C (n. manovre/ora)			• C (n. manovre/ora)	
DC	0 ... 99 %			0 ... 99 %	
SIL CL oppure derivazione del SIL CL dal PL	SIL 1, 2 oppure 3	SIL 1, 2 oppure 3	SIL 1, 2 oppure 3	SIL 1, 2 oppure 3	SIL 1, 2 oppure 3
Probabilità di guasto o PFH	Calcolo secondo architetture di base sistema parziale	Indicazione produttore	Indicazione produttore	Calcolo secondo architetture di base sistema parziale	Indicazione produttore
	Risultato parziale Sensori		**Risultato parziale Unità di controllo**	**Risultato parziale Attuatori**	

Il SIL raggiungibile risulta dal SIL più basso dei risultati parziali e dalla somma delle probabilità di guasto PFH

Determinare il fattore CCF dal 1% al 10% secondo la tabella F.1 della norma.
Se necessario aggiungere la probabilità di guasto della comunicazione fail-safe.

Utente (ad es. costruttore di macchine) *Produttore (prodotti, componenti)* *Risultati*

SRP/CS

	SRP/CS di rilevamento: Sensori		SRP/CS di analisi: Unità di controllo	SRP/CS di reazione: Attuatori	
	Disegno eseguito dall'utente	Utilizzo di componenti certificati	Utilizzo di componenti certificati	Disegno eseguito dall'utente	Utilizzo di componenti certificati
Categoria MTTFd	*Scelta architettura Calcolo con*			*Scelta architettura Calcolo con*	
Componenti elettromeccanici	• valore B10			• valore B10	
Ciclo di azionamento	• C (n. manovre/ora)			• C (n. manovre/ora)	
DC	0 ... 99 %			0 ... 99 %	
PL oppure derivazione del PL da SIL CL	PL a, b, c, d oppure e	PL a, b, c, d oppure e	PL a, b, c, d oppure e	PL a, b, c, d oppure e	PL a, b, c, d oppure e
Probabilità di guasto o PFH	Assegnazione in tabella (Allegato K della norma)	Indicazione produttore	Indicazione produttore	Assegnazione in tabella (Allegato K della norma)	Indicazione produttore
	Risultato parziale Sensori		**Risultato parziale Unità di controllo**	**Risultato parziale Attuatori**	

Il PL raggiungibile risulta dal PL più basso dei risultati parziali e dalla somma delle probabilità di guasto PFH

Fattore CCF presunto del 2 % se sono soddisfatti determinati criteri (tabella F.1 della norma).
Se necessario aggiungere la probabilità di guasto della comunicazione fail-safe.

Utente (ad es. costruttore di macchine) *Produttore (prodotti, componenti)* *Risultati*

SIL e PL sono convertibili tra loro

Livello di integrità della sicurezza SIL	Probabilità di guasto potenzialmente pericoloso all'ora (1/h)	Performance Level PL
–	$\geq 10^{-5} \ldots < 10^{-4}$	a
SIL 1	$\geq 3 \times 10^{-6} \ldots < 10^{-5}$	b
SIL 1	$\geq 10^{-6} \ldots < 3 \times 10^{-6}$	c
SIL 2	$\geq 10^{-7} \ldots < 10^{-6}$	d
SIL 3	$\geq 10^{-8} \ldots < 10^{-7}$	e

Validazione sulla base del Piano di validazione

Controllo della realizzazione dei requisiti di sicurezza specificati
Pianificazione — Test/verifica — Documentazione

Marcatura CE (dichiarazione di conformità) CE

Guasto (failure)
Cessazione della capacità di un'unità di soddisfare la funzione richiesta.

β, beta:
Fattore di guasto in seguito a una causa comune Fattore CCF: common cause failure factor β (0,1 – 0,05 – 0,02 – 0,01)

B10
Il valore B10 per i componenti soggetti a usura viene espresso in numeri di manovre, ovvero il numero di manovre dopo il quale si verificano guasti nel 10 % dei componenti esaminati durante una prova della durata di esercizio.
Con il valore B10 e il ciclo di azionamento è possibile calcolare il tasso di guasto dei componenti elettromeccanici.

B10d
B10d = B10 / Percentuale dei guasti pericolosi

CCF (common cause failure)
Guasto in seguito a una causa comune (ad es. un cortocircuito).
È il guasto di diverse unità in seguito ad un unico evento, senza tuttavia che una delle unità abbia causato l'avaria dell'altra.

DC (diagnostic coverage), copertura diagnostica
Rilevamento della probabilità di guasti dell'hardware potenzialmente pericolosi risultante dall'esecuzione dei test di diagnostica automatici.

Tolleranza di errore
Capacità di un SRECS (sistema di controllo elettrico di sicurezza), di un sistema parziale o di un elemento del sistema parziale di continuare a eseguire la funzione richiesta anche in presenza di errori o guasti (resistenza rispetto agli errori).

Sicurezza funzionale
Parte della sicurezza complessiva riferita alla macchina e al sistema di comando della macchina che dipende dal funzionamento corretto dell'SRECS (sistema di controllo elettrico di sicurezza), di sistemi di sicurezza con altre tecnologie e dispositivi esterni per la riduzione dei rischi.

Guasto potenzialmente pericoloso (dangerous failure)
Ogni disfunzione della macchina o dell'alimentazione di energia che aumenta il rischio.

Categorie B, 1, 2, 3 o 4 (architetture previste)
Oltre ad aspetti qualitativi, queste categorie comprendono anche aspetti quantificabili (come ad es. $MTTF_d$, DC e CCF). Con un procedimento semplificato basato sulle categorie come „architetture previste" è possibile valutare il PL (Performance Level) ottenuto.

λ, Lambda
Tasso di guasto statistico che include i guasti sicuri (λ_s) ed i guasti potenzialmente pericolosi (λ_D). L'unità di lambda è FIT (Failure In Time).

$MTTF$ / $MTTF_d$
(Mean Time To Failure/Mean Time To Failure dangerous) Intervallo di tempo medio prima di un guasto o di un guasto potenzialmente pericoloso. L'MTTF può essere eseguito per i componenti analizzando i dati di campo o mediante previsioni. Con un tasso di guasto costante, il valore medio per il tempo di lavoro senza avarie è MTTF = 1 / λ (lambda λ indica il tasso di guasto dell'apparecchiatura). (Sul piano statistico è possibile supporre che al termine dell'MTTF il 63,2 % dei componenti interessati sia guasto.)

PL (Performance Level)
Livello discreto che specifica la capacità delle parti legate alla sicurezza di un controllore di eseguire una funzione di sicurezza a condizioni prevedibili: dal PL „a" (massima probabilità di guasto) al PL „e" (minima probabilità di guasto).

PFH_D (Probability of dangerous failure per hour)
Probabilità di guasto potenzialmente pericoloso all'ora.

Intervallo test di prova o durata utile (T1)
Controllo ricorrente in grado di riconoscere la presenza di errori o un peggioramento in un SRECS e nei suoi sistemi parziali in modo che, all'occorrenza, l'SRECS e i sistemi parziali possano essere riportati in uno stato „come nuovo" o in uno stato possibilmente analogo nei limiti della pratica.

SFF (safe failure fraction)
Percentuale di guasti sicuri nel tasso di guasto complessivo di un sistema parziale che non comporta un guasto potenzialmente pericoloso.

SIL (Safety Integrity Level) livello di integrità della sicurezza
Livello discreto (è possibile uno su tre) per stabilire i requisiti di integrità della sicurezza delle funzioni di comando di sicurezza che viene assegnato all'SRECS; il livello di integrità della sicurezza 3 è il più alto mentre il livello di integrità della sicurezza 1 è il più basso.

SIL CL (Claim Limit), Claim Limit SIL
SIL massimo che può essere richiesto da un sistema parziale SRECS per quanto riguarda le limitazioni strutturali e l'integrità della sicurezza del sistema.

Funzione di sicurezza
Funzione di una macchina il cui guasto può causare un immediato aumento del rischio/dei rischi.

SRCF (Safety-Related Control Function), funzione di comando
Funzione di comando legata alla sicurezza ed eseguita dall'SRECS con un livello di integrità definito il cui obiettivo è di mantenere lo stato di sicurezza della macchina o di evitare un aumento diretto dei rischi.

SRECS (Safety-Related Electrical Control System)
Sistema di controllo elettrico di sicurezza di una macchina il cui guasto comporta un diretto aumento dei rischi.

SRP/CS (Safety-Related Parts of Control System)
Parte di un controllore preposta alla sicurezza che reagisce a segnali di ingresso relativi alla sicurezza e genera segnali di uscita relativi alla sicurezza.

Sistema parziale
Unità del disegno dell'architettura dell'SRECS sul massimo livello; il guasto di un qualunque sistema parziale comporta il guasto della funzione di comando di sicurezza.

Elemento del sistema parziale
Parte di un sistema parziale costituito da un singolo componente o che comprende un gruppo di componenti.

Sicurezza funzionale delle macchine

Applicazione della Direttiva Europea sulle macchine con le norme armonizzate
siemens.com/safety-integrated

SIEMENS