Sicurezza funzionale di macchine e impianti

Applicazione della Direttiva Europea sulle Macchine

EN ISO 13849-1

EN 62061

Safety Integrated

www.siemens.it/safety

SIEMENS

Nuove norme: un ausilio ai costruttori di macchine

Standard internazionali, direttive ad ampio raggio

Contenuto

In qualità di partner per tutti i requisiti legati alla sicurezza, assistiamo i nostri clienti non solo con prodotti e sistemi fail-safe adatti, ma con conoscenze sempre aggiornate sulle norme e le prescrizioni internazionali. Ai costruttori di macchine e ai gestori di impianti offriamo un'ampia gamma di corsi di formazione e di servizi per l'intero ciclo di vita di impianti e macchine realizzati secondo la tecnica di sicurezza.

Per contenere il rischio residuo entro limiti tollerabili nella costruzione di una macchina, sono di fondamentale importanza un'analisi dei rischi ed eventualmente una riduzione degli stessi. Se da un lato l'analisi dei rischi consente di ottimizzare la sicurezza tecnica della macchina „step by step", dall'altro essa costituisce „materiale di prova" in caso di guasto. La documentazione descrive il percorso dell'analisi e i risultati ottenuti per ridurre i rischi al minimo. Essa costituisce la base per un utilizzo sicuro della macchina, senza dimenticare che la sicurezza sul lavoro richiede un training completo dei dipendenti da parte del gestore. Un gestore che assembli macchine esistenti per formare un unico impianto, o che apporti determinate modifiche e ampliamenti a una macchina, può essere considerato a sua volta un costruttore.

L'ottemperanza alla Direttiva Macchine può essere garantita in diversi modi: tramite collaudo della macchina presso un Centro preposto, tramite rispondenza alle Norme armonizzate oppure soltanto mediante la certificazione di sicurezza che richiede un elevato onere di documentazione e verifiche. In ogni caso, la prova tangibile dell'ottemperanza alla Direttiva Macchine è la marcatura CE con la rispettiva certificazione di sicurezza. La marcatura CE è prescritta dalla direttiva generale europea in materia di sicurezza sul lavoro ed è obbligatoria.

Evitare gli incidenti per impedire conseguenze pericolose

Rispetto alle conseguenze fisiche o psichiche che può subire una persona in seguito ad un infortunio causato da una macchina o da un impianto, i danni tecnici sono più tollerabili, anche se un eventuale guasto della macchina o un arresto della produzione possono significare considerevoli perdite economiche. Se davvero si dovesse verificare uno „scenario caso peggiore", sarebbe necessario chiarire la questione della responsabilità con un'indagine e, qualora risultasse che non tutte le Direttive rilevanti sono state rispettate, le richieste di risarcimento dei danni potrebbero essere ingenti. Inoltre, una tale eventualità potrebbe danneggiare l'immagine dell'azienda con notevoli conseguenze. Applicando tutte le norme del caso, invece, è possibile partire dal presupposto che anche tutti i requisiti delle rispettive Direttive (presunzione di conformità) siano automaticamente soddisfatti.

Qui di seguito vi mostriamo passo dopo passo in che modo ottenere sempre la massima sicurezza nell'impiego delle macchine.

Safety Evaluation Tool

Il Safety Evaluation Tool per le norme IEC 62061 e ISO 13849-1 vi guida direttamente allo scopo. Questo tool online testato dal TÜV e facente parte del programma Safety Integrated di Siemens vi aiuta a valutare in modo rapido e sicuro le funzioni di sicurezza della vostra macchina. Come risultato ottenete un report conforme alle norme, che può essere integrato nella documentazione come attestato di sicurezza.

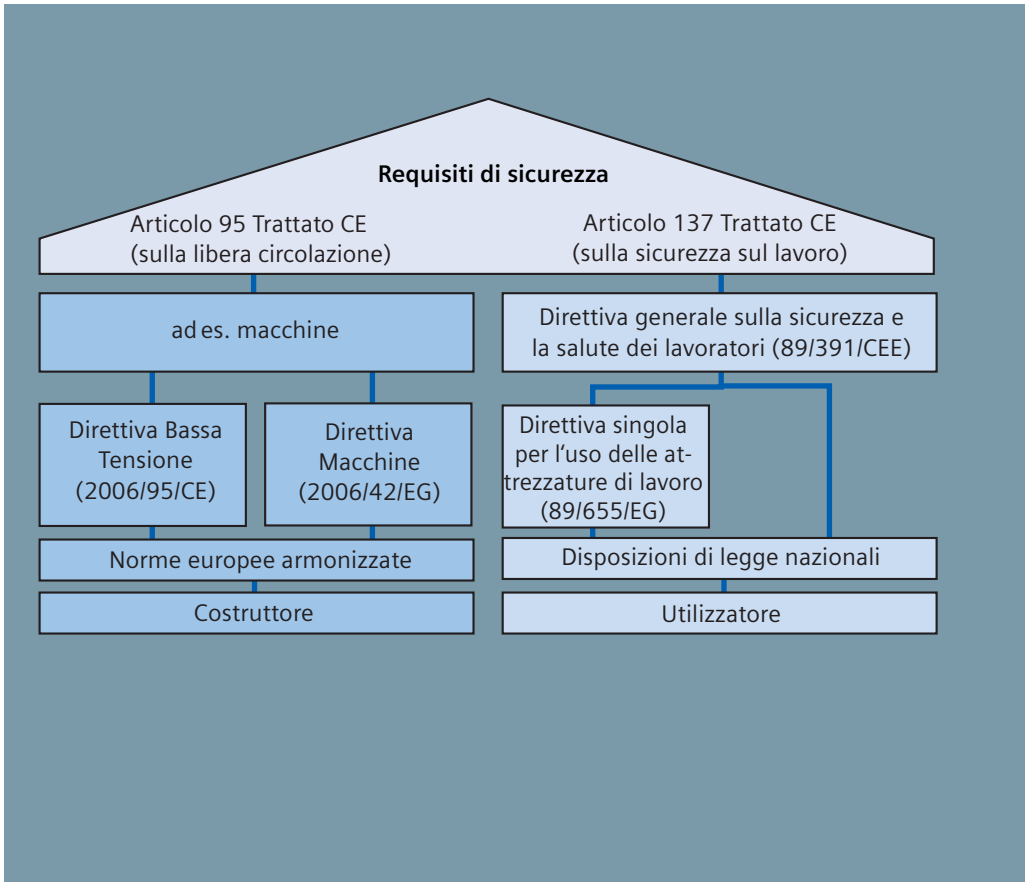
www.siemens.com/safety-evalution-tool

Requisiti fondamentali di sicurezza nell'industria manifatturiera

Obiettivo:
Protezione del personale, della macchina e dell'ambiente

Risultato:
Marcatura CE quale certificazione di una „macchina sicura".

CE



Con l'introduzione del mercato comune europeo, le norme e le disposizioni di legge nazionali che regolano la realizzazione tecnica delle macchine sono state uniformate e armonizzate tra loro.

- Nell'ambito della sicurezza, perciò, sono stati stabiliti requisiti di base che in parte si rivolgono al costruttore, e sono definiti nell'articolo 95 sulla libera circolazione delle merci, e in parte all'utilizzatore, ovvero il gestore, e sono definiti nell'articolo 137 sulla sicurezza sul lavoro.
- Di conseguenza, i singoli Stati membri hanno dovuto convertire in leggi nazionali i contenuti della Direttiva Macchine in quanto direttiva europea basata sui trattati CE.
  In Germania, ad esempio, questa direttiva è stata integrata nella legge sulla sicurezza delle apparecchiature (GSG).

Per garantire la conformità con una direttiva si raccomanda di applicare le rispettive norme europee armonizzate che, grazie alla cosiddetta „presunzione di conformità", assicurano a gestore e costruttore una certezza di diritto sia per quanto riguarda il rispetto delle norme nazionali che della direttiva CE.

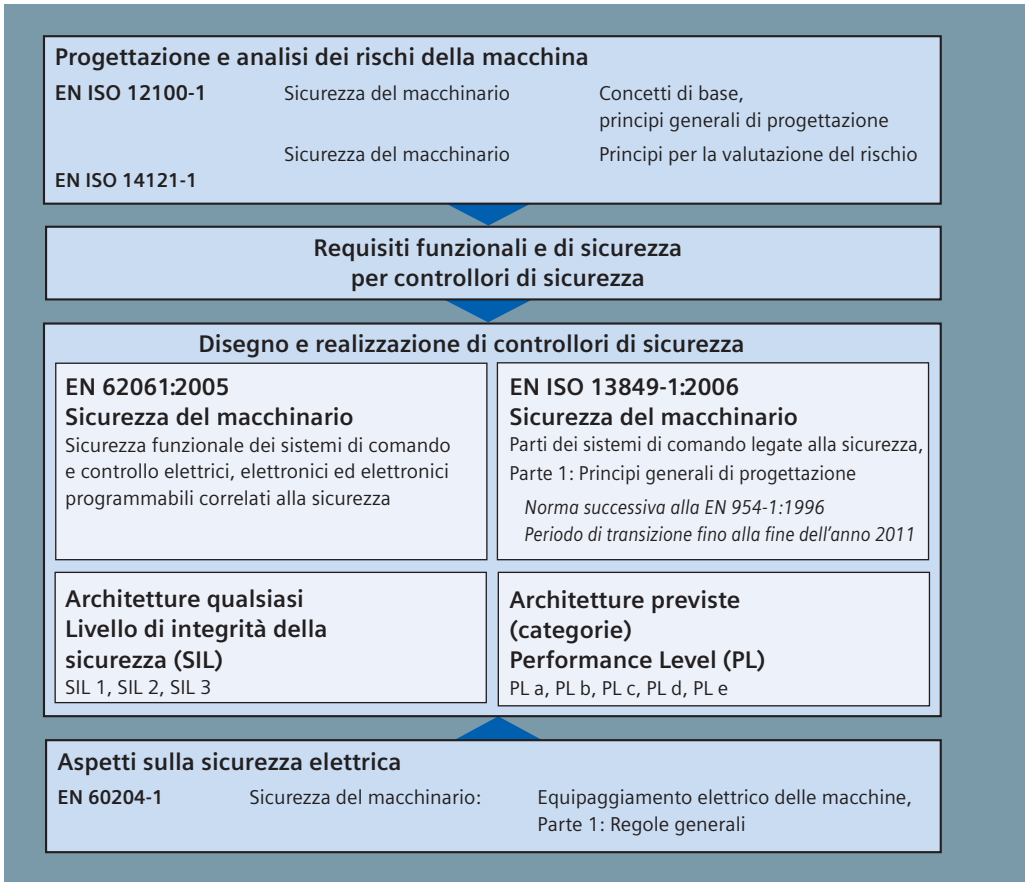
Con la marcatura CE il costruttore di una macchina certifica l'adempimento di tutte le direttive e le norme valide per la libera circolazione delle merci. Poiché le direttive CE sono riconosciute in tutto il mondo, la loro applicazione agevola anche le esportazioni verso i Paesi dello Spazio Economico Europeo.

Tutte le spiegazioni fornite qui di seguito sono rivolte al costruttore di una macchina o al suo gestore qualora quest'ultimo dovesse apportare o far apportare alla macchina modifiche rilevanti per la sicurezza.

Norme di base per il disegno delle funzioni di comando

Obiettivo:
rispetto di tutti i requisiti di sicurezza del caso grazie a una sufficiente riduzione dei rischi, al fine di garantire l'assunzione della responsabilità e le capacità di esportazione.

Risultato:
adozione di misure di riduzione dei rischi al minimo mediante l'applicazione di norme armonizzate, quindi raggiungimento della conformità con i requisiti di sicurezza della Direttiva Macchine sulla base della cosiddetta „presunzione di conformità".

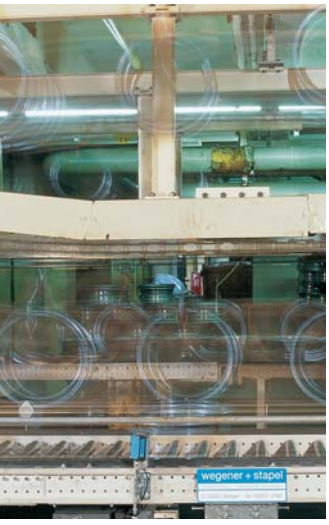


La sicurezza richiede una protezione da svariati pericoli, che possono essere evitati con le misure seguenti:

- Costruzione conforme a principi di progettazione volti alla riduzione dei rischi e valutazione del rischio della macchina (EN ISO 12100-1, EN ISO 14121-1)
- Misure tecniche di sicurezza, eventualmente mediante utilizzo di sistemi di comando e controllo per applicazioni di sicurezza (sicurezza funzionale secondo EN 62061 o EN ISO 13849-1)
- Sicurezza elettrica (EN 60204-1)

Qui di seguito viene trattata la **sicurezza funzionale**, ovvero quella parte della sicurezza di una macchina o di un impianto che dipende dal corretto funzionamento dei dispositivi di comando o di protezione. L'utente può fare riferimento a due norme:

- EN 62061:2005, come norma settoriale europea della norma di base IEC 61508.
- EN ISO 13849-1:2006, come modifica che va a sostituire la EN 954-1, ormai insufficiente per quanto riguarda le categorie.



Passo dopo passo:

Disegno e realizzazione di controllori di sicurezza

Norma EN 62061

La norma EN 62061 „Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza“ definisce numerosi requisiti. Inoltre essa comprende raccomandazioni per il disegno, l'integrazione e la validazione sia di sistemi elettrici ed elettronici che di controllori programmabili per applicazioni di sicurezza (SRECS) per le macchine. La norma contempla per la prima volta l'intero processo di sicurezza, dal sensore all'attuatore. Per raggiungere un livello di integrità della sicurezza come ad esempio il SIL 3 non è più sufficiente la corrispondente certificazione dei singoli componenti ma è necessario che la funzione di sicurezza complessiva risponda alle aspettative previste.

La norma non definisce requisiti sulle prestazioni degli elementi di comando non elettrici (bensì, ad es., idraulici, pneumatici o elettromeccanici) preposti alla sicurezza delle macchine.

Nota:
Se gli elementi di comando di sicurezza non elettrici sono sorvegliati da un'adeguata informazione di lettura in ritorno elettrica, essi possono essere trascurati nell'esame della sicurezza qualora vengano soddisfatti i requisiti previsti.

Norma EN ISO 13849-1

La norma EN ISO 13849-1 „Sicurezza del macchinario – Parti dei sistemi di comando legate alla sicurezza, Parte 1: Principi generali di progettazione“ si basa sulle note categorie della EN 954-1, versione 1996. Essa contempla le funzioni di sicurezza complete con tutte le apparecchiature interessate.

Oltre all'approccio qualitativo della EN 954-1, la norma EN ISO 13849-1 introduce un approccio quantitativo delle funzioni di sicurezza che si avvale di Performance Level (PL) basati sulle categorie. Questa norma descrive la determinazione del PL per le parti rilevanti per la sicurezza dei controllori sulla base di architetture previste („designated architecture“) per la durata di utilizzo prevista. In caso di differenze, la norma EN ISO 13849-1 rimanda alla IEC 61508. Per la combinazione di diverse parti rilevanti per la sicurezza in un sistema complessivo, la norma fornisce i dati per la determinazione del PL.

Essa può essere applicata alle parti di sicurezza di controllori (SRP/CS) e a tutti i tipi di macchine, a prescindere dalla tecnologia e dall'energia utilizzate (elettrica, idraulica, pneumatica, meccanica ecc.).

Il periodo di transizione dalla EN 954-1 alla EN ISO 13849-1 scade nel 2011. Durante questo periodo è possibile utilizzare entrambe le norme alternativamente.

Piano di sicurezza secondo la norma EN 62061 – il filo conduttore nella realizzazione di macchine sicure

Con un procedimento sistematico attraverso l'intero ciclo di vita del prodotto è possibile determinare e realizzare tutti gli aspetti rilevanti per la sicurezza e le regole per la costruzione e il funzionamento di una macchina in condizioni di sicurezza.
Il Piano di sicurezza (Safety Plan) supporta l'utente in tutte le fasi, fino all'ammodernamento e all'upgrade. Struttura e obblighi di applicazione del Piano di sicurezza sono definiti nella norma EN 62061.

In questo ambito la norma richiede un procedimento sistematico nella realizzazione di un sistema di sicurezza (SRECS), come la documentazione di tutte le attività nel Piano di sicurezza. In tutte le fasi operative (valutazione dei pericoli, analisi dei rischi della macchina, disegno, realizzazione dell'SRECS e validazione), il Piano di sicurezza deve sempre essere aggiornato parallelamente alla realizzazione dell'SRECS.

Nel Piano di sicurezza sono documentati gli argomenti e le attività seguenti:

- **Pianificazione e procedimento di tutte le attività necessarie per realizzare un SRECS.**
  Ad esempio:
  - Sviluppo della specifica della funzione di comando di sicurezza (SRCF)
  - Disegno e integrazione dell'SRECS
  - Validazione dell'SRECS
  - Creazione della documentazione utente per l'SRECS
  - Documentazione di tutte le informazioni rilevanti per la realizzazione dell'SRECS (documentazione di progetto)
- **Strategia per il raggiungimento della sicurezza funzionale**
- **Responsabilità per l'esecuzione ed il controllo di tutte le attività**

Le operazioni qui specificate non sono descritte esplicitamente in EN ISO 13849-1:2006, ma sono tuttavia indispensabili per la corretta attuazione della Direttiva Macchine.

Passo 1:
Strategia di riduzione dei rischi secondo la norma EN ISO 12100-1, paragrafo 1

Obiettivo:
Riduzione dei rischi

Risultato:
Definizione e determinazione delle misure di sicurezza

Il compito principale nell'ambito della riduzione dei rischi è quello di riconoscere i pericoli, saperli valutare e gestirli con l'aiuto di misure di sicurezza in modo da prevenire qualunque danno che potrebbe derivarne.

Pertanto la norma EN ISO 12100-1 propone il seguente procedimento:

1. Definizione dei limiti fisici e temporali della macchina
2. Identificazione dei pericoli e stima/valutazione dei rischi
3. Valutazione del rischio per ogni pericolo identificato e ogni situazione pericolosa
4. Valutazione del rischio e definizione di decisioni atte a ridurre i rischi
5. Eliminazione del pericolo o riduzione del rischio connesso attraverso il metodo dei „3 passi" inerente a costruzione sicura, misure tecniche di sicurezza e informazione dell'utilizzatore.

La norma EN ISO 14121-1 contiene informazioni dettagliate sui passi 1 a 4.

Dai rischi calcolati risultano i requisiti di sicurezza che devono essere soddisfatti. Con il Piano di sicurezza, la norma EN 62061 offre la possibilità di seguire un procedimento chiaramente strutturato: per ogni pericolo che viene rilevato, è necessario specificare una funzione di sicurezza.
Tra queste rientra anche la specifica del test (vedere „Validazione").

Passo 2:
Analisi dei rischi

Obiettivo:
Determinazione e valutazione degli elementi di rischio per una funzione di sicurezza

Risultato:
Definizione dell'integrità della sicurezza richiesta

Gli elementi di rischio (Se, Fr, Pr e Av) fungono da grandezza iniziale per entrambe le norme. La valutazione di questi elementi di rischio avviene in modo diverso. In base alla norma EN 62061 si determina il livello di integrità della sicurezza richiesto (SIL) mentre sulla base della EN ISO 13849-1 si calcola il Performance Level (PL).

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**

Prendendo come esempio l'arresto di sicurezza di un mandrino rotante all'apertura di una calotta di protezione, lo scopo è ridurre il rischio applicando entrambe le norme.

Determinazione del SIL necessario (mediante assegnazione del SIL)

Frequenza e/o durata **Fr**	
≤ 1 ora	5
Da > 1 ora a ≤ 1 giorno	5
Da > 1 giorno a ≤ 2 sett.	4
Da > 2 sett. a ≤ 1 anno	3
> 1 anno	2

Probabilità che si produca l'evento pericoloso **Pr**	
frequente	5
probabile	4
possibile	3
rara	2
trascurabile	1

Possibilità di evitare il rischio **Av**	
impossibile	5
possibile	3
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	altere misure		SIL 1	SIL 2	SIL 3
Reversibile, cure mediche	2				SIL 1	SIL 2
Reversibile, pronto soccorso	1					SIL 1

Esempio

Pericolo	Se	Fr	Pr	Av		Cl	Misure di sicurezza	Sicuro
Mandrino rotante	3	5	4	3	=	**12**	Sorveglianza calotta di protezione con **SIL 2** richiesto	Sì, con SIL 2

Procedimento

1. Determinazione dell'entità del danno Se:	permanente, perdita delle dita, Se = 3
2. Determinazione dei punti per frequenza Fr, probabilità Pr e possibilità di evitare il rischio Av:	– Permanenza nell'area a rischio: una volta al giorno, Fr = 5 – Probabilità che si produca l'evento pericoloso: probabile, Pr = 4 – Possibilità di evitare il rischio: possibile, Av = 3
3. Totale dei punti per Fr + Pr + Av = classe Cl	Cl = 5 + 4 + 3 = 12
4. Punto di intersezione tra riga per entità del danno Se e colonna Cl = SIL richiesto	SIL 2

Il SIL richiesto quindi è SIL 2

Determinazione del PL necessario (tramite grafo di rischio)

La valutazione dei rischi viene eseguita in base agli stessi parametri di rischio:

Parametri di rischio

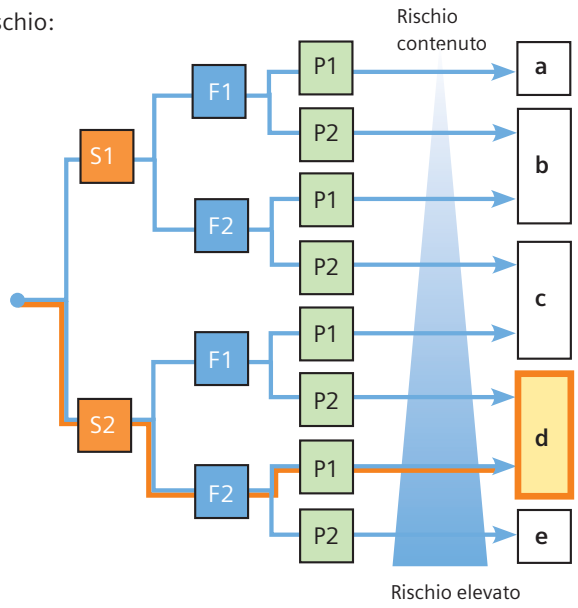
S = entità della lesione
- S1 = lesione leggera (normalmente reversibile)
- S2 = lesione grave (normalmente irreversibile), inclusa la morte

F = frequenza e/o durata dell'esposizione al pericolo
- F1 = da raro a frequente e/o il periodo di esposizione al rischio è breve
- F2 = da frequente a permanente e/o il periodo di esposizione al rischio è lungo

P = possibilità di evitare il pericolo o contenimento del danno
- P1 = possibile a determinate condizioni
- P2 = quasi impossibile

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

Perfomance Level PL richiesto



Procedimento		
	1. Determinazione dell'entità del danno :	S2 = lesione grave (normalmente irreversibile), inclusa la morte
	2. Definizione della frequenza e/o durata dell'esposizione al pericolo F	F2 = da frequente a permanente e/o il periodo di esposizione al rischio è lungo
	3. Definizione della possibilità di evitare il pericolo o contenimento del danno P:	P1 = possibile a determinate condizioni
	Il Performance Level richiesto quindi è PL d.	

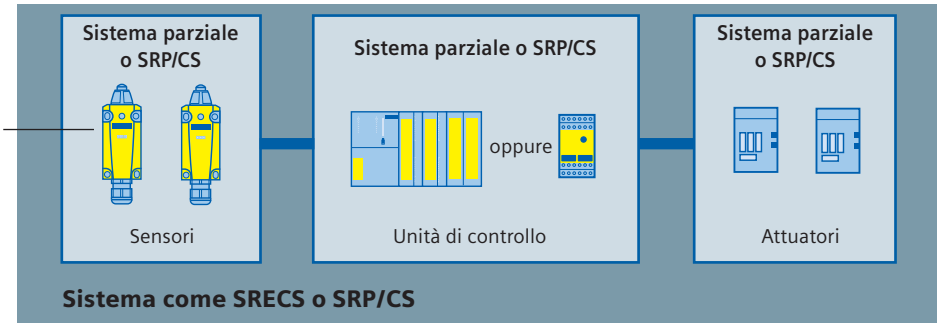
Passo 3:
Configurazione della funzione di sicurezza e determinazione dell'integrità della sicurezza

Obiettivo:
Funzione di comando e determinazione dell'integrità della sicurezza

Risultato:
Qualità della funzione di comando scelta

Benché nell'ambito delle due norme venga applicato un metodo diverso per la valutazione di una funzione di sicurezza, i risultati sono analoghi. Entrambe le norme adottano concetti e definizioni simili.
Entrambe le norme contemplano l'intero processo di sicurezza in modo simile: una funzione di sicurezza viene definita „sistema".

Struttura di una funzione di sicurezza



SRP/CS: parti di sicurezza di un controllore ai sensi della norma EN ISO 13849-1
SRECS: sistema di controllo elettrico di sicurezza ai sensi della norma EN 62061

Esempio:

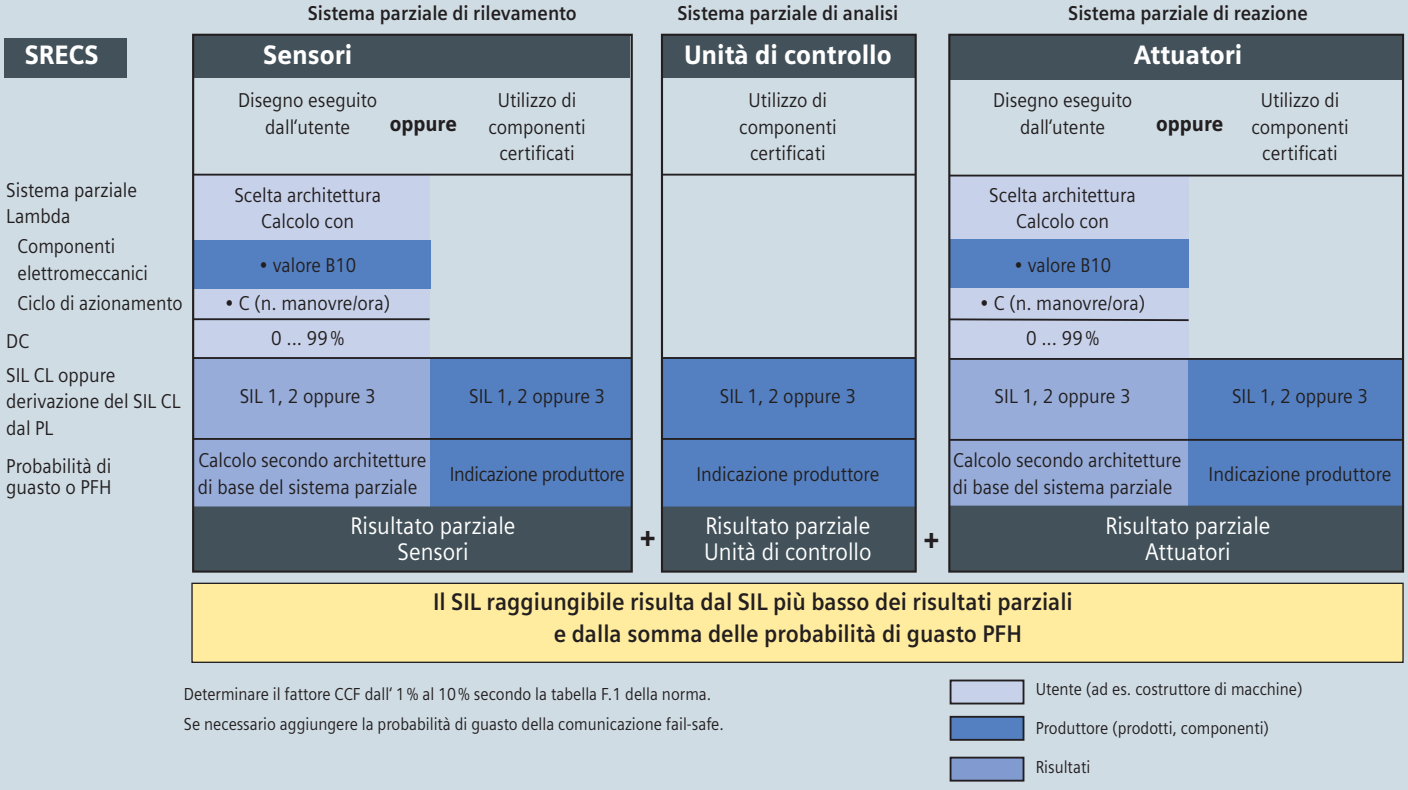
- Obiettivo: arresto di sicurezza di un mandrino rotante nel momento in cui viene aperta la calotta di protezione.
- Soluzione: la sorveglianza della calotta di protezione è affidata a due interruttori di posizione (sensori). Il mandrino rotante viene disattivato da due contattori (attuatori). L'unità di controllo può essere un controllore fail-safe (CPU, F-DI, F-DO) oppure un apparecchio di manovra di sicurezza.

Inoltre va tenuta in considerazione la tecnica di collegamento tra i sistemi parziali.

Procedimento comune semplificato:

1. Analizzare ogni sistema parziale o SRP/CS per ricavarne „risultati parziali". Esistono due possibilità:
   a. utilizzo di componenti certificati con dati del produttore (ad es. SIL CL, PFH o PL)
   b. calcolo dei tassi di guasto degli elementi o componenti del sistema parziale in base all'architettura scelta (a uno o due canali). Quindi calcolo della probabilità di guasto del sistema parziale o dell'SRP/CS.
2. Valutare i risultati parziali riguardo ai requisiti strutturali (SIL CL o PL) e aggiungere le probabilità di guasto/PFH.

Metodo secondo la norma EN 62061



Annotazioni: 1. Una descrizione dettagliata su come si determina il livello di integrità di sicurezza, è riportata nell'esempio di funzione a EN 62061.
Vedere anche: http://support.automation.siemens.com/WW/view/de/2399647
2. A pagina 19 di questa brochure troverete delle spiegazioni relative alle abbreviazioni utilizzate.

Sistema parziale di rilevamento (sensori)

Con i componenti certificati, il produttore fornisce i valori necessari (SIL CL e PFH). Utilizzando componenti elettromeccanici nel disegno dell'utente è possibile determinare il SIL CL e il valore PFH nel modo seguente.

Determinazione del SIL CL
Per l'esempio è possibile prendere il SIL CL 3, poiché l'architettura utilizzata corrisponde alla categoria 4 secondo EN 954-1 ed è disponibile la diagnostica del caso.

Calcolo dei tassi di guasto l degli elementi del sistema parziale „interruttore di posizione"
Con il valore B10 e il numero di manovre C è possibile calcolare l'intero tasso di guasto λ di un componente elettromeccanico secondo EN 62061, paragrafo 6.7.8.2.1:

$\lambda = (0{,}1 * C)/B10 = (0{,}1 * 1)/10.000.000 = 10^{-8}$
C = indicazione dell'utente riguardo ai cicli di azionamento all'ora (duty cycle)
Valore B10 = indicazione produttore (vedere Appendice, pag. 18, tabella Valori B10)

Il tasso di guasto λ è costituito da parti non pericolose (λ_S) e potenzialmente pericolose (λ_D):

$\lambda = \lambda_S + \lambda_D$
$\lambda_D = \lambda$* guasti potenzialmente pericolosi in %
$= 10^{-8} * 0{,}2 = 2 * 10^{-9}$
(vedere Appendice, pag. 18, tabella Valori B10)

Calcolo della probabilità di guasti potenzialmente pericolosi PFH_D in base all'architettura utilizzata
La norma EN 62061 definisce 4 architetture per i sistemi parziali (architettura di base del sistema parziale da A a D). Per il rilevamento della probabilità di guasto PFH_D la norma fornisce formule di calcolo per ogni architettura.

Per un sistema parziale a due canali con diagnostica (architettura di base del sistema parziale D) e con elementi uguali, per ogni sistema parziale si calcola il seguente tasso di guasto potenzialmente pericoloso λ_D:

$\lambda_D = (1 - \beta)^2 * \{[\lambda_{De}^2 * DC * T2] + [\lambda_{De}^2 * (1 - DC) * T1]\} + \beta * \lambda_{De}, = \approx 2*10^{-10}$
$PFH_D = \lambda_D * 1$ ora $\approx 2*10^{-10}$
λ_{De} = tasso di guasto potenzialmente pericoloso per un elemento del sistema parziale

Il calcolo dell'esempio si basa sulle supposizioni seguenti:

ß = 0,1	supposizione conservativa, poiché il valore max. è fuori dalla norma
DC = 0,99	tramite sorveglianza di discrepanza e cortocircuito
T2 = 1/C	mediante analisi nel programma di sicurezza
T1 = 87.600 ore (10 anni)	durata di utilizzo del componente

Sistema parziale di analisi (unità di controllo):

Con i componenti certificati, il produttore fornisce i valori necessari.

Esempi di valori:
SIL CL = SIL 3
$PFH_D = < 10^{-9}$

Sistema parziale di reazione (attuatori):

Con i componenti certificati, il produttore fornisce i valori necessari.

Esempi di valori:
SIL CL = SIL 2
$PFH_D = 1,29*10^{-7}$

Se il disegno è stato realizzato dall'utente, il procedimento per il sistema parziale di reazione è lo stesso del sistema parziale di rilevamento.

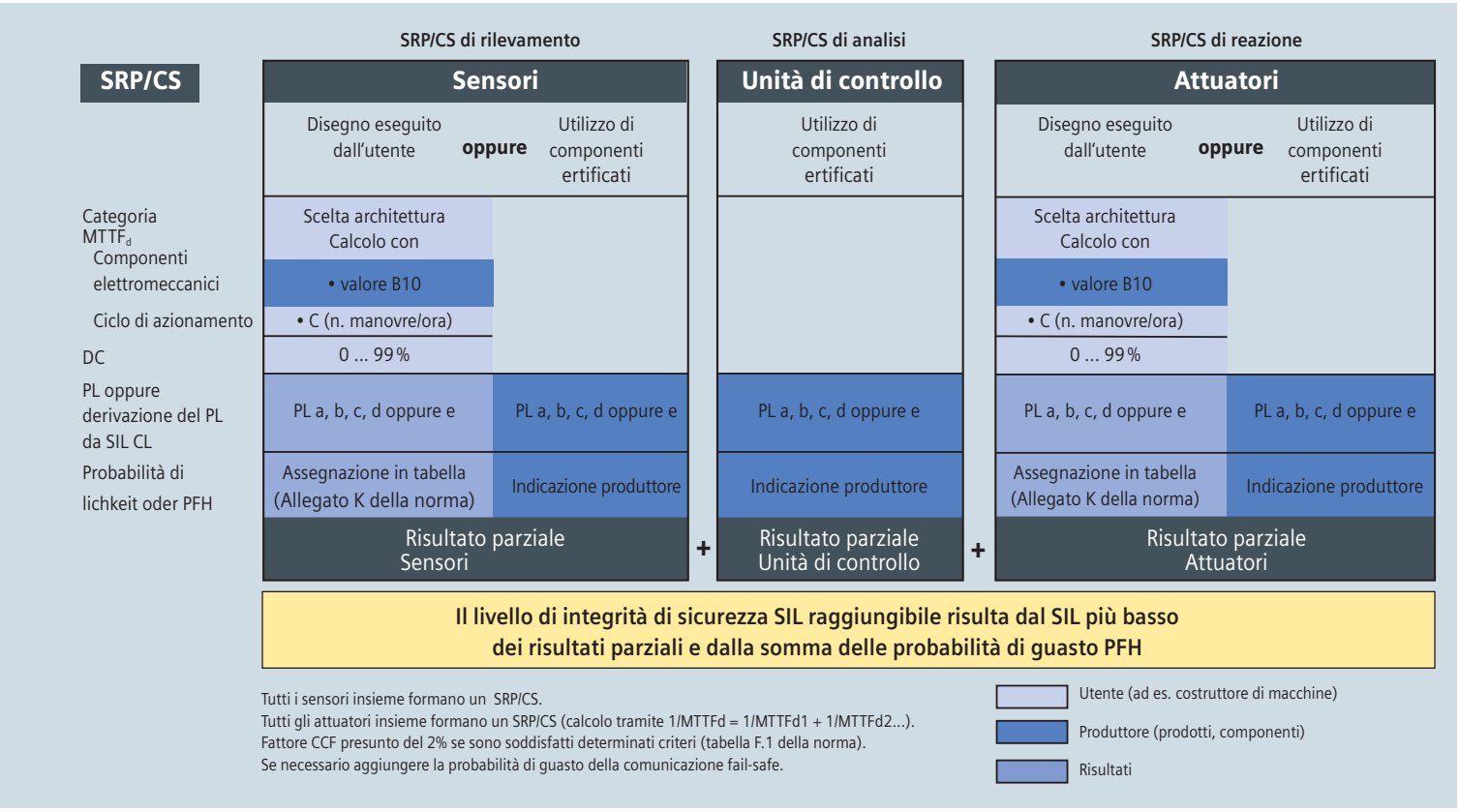
Determinazione dell'integrità della sicurezza della funzione di sicurezza
È necessario determinare il Claim Limit SIL (SIL CL) minimo di tutti i sistemi parziali della funzione di comando di sicurezza (SRCF):

SIL CL Min = min. (SIL CL (sistema parziale1)) .....SIL CL (sistema parziale n)
= SIL CL 2

Somma delle probabilità di guasti potenzialmente pericolosi (PFHD) dei sistemi parziali
$PFH_D = PFH_D$ (sistema parziale1) + ... + PFH_D (sistema parziale n) = $1,30*10^{-7}$
$= <10^{-6}$ equivale a SIL 2

Risultato: la funzione di sicurezza soddisfa i requisiti per SIL 2

Metodo secondo la norma EN ISO 13849-1



SRP/CS di rilevamento (sensori)

Con i componenti certificati, il produttore fornisce i valori necessari (PL ,SIL CL o PFHD).
SIL CL e PL sono assimilabili in base alle probabilità di guasto (vedere il punto sulla conversione di SIL e PL).
Utilizzando componenti elettromeccanici nel disegno dell'utente è possibile determinare il PL e il valore PFH_D nel modo seguente.

Calcolo dei tassi di guasto degli elementi SRP/CS „interruttori di posizione"
Con il valore B10 e il numero di manovre nop l'utente può calcolare il tasso di guasto $MTTF_d$ dei componenti elettromeccanici:

$MTTF_d = B10_d / (0{,}1 * n_{op}) = 0{,}2 * 10^8$ ore = 2.300 anni corrisponde a $MTTF_d$ = alto

con n_{op} = azionamenti annui (numero di operazioni: indicazione dell'utente)

$n_{op} = (d_{op} * h_{op} * 3.600\ s/h) / t_{ciclo}$

Con le seguenti supposizioni, derivanti dall'applicazione del componente:

- h_{op} è il tempo di funzionamento medio in ore al giorno;
- d_{op} è il tempo di funzionamento medio in giorni all'anno;
- t_{ciclo} è il tempo medio tra l'inizio di due cicli consecutivi del componente (ad es. attivazione di una valvola) in secondi per ogni ciclo.

Il calcolo dell'esempio si basa sulle supposizioni seguenti:

DC „alto" tramite sorveglianza di discrepanza e cortocircuito
Categoria 4

Risultato: si ottiene un Performance Level „PL e" con una probabilità di guasto di 2,47 10-8

(dall'Allegato K della norma EN ISO 13849-1: 2006)

SRP/CS di reazione (attuatori)

Con i componenti certificati, il produttore fornisce i valori necessari.

Esempi di valori:
SIL CL = SIL 3, equivale a PL e
PFH_D = < 10^{-9}

SRP/CS di reazione (attuatori)

Con i componenti certificati, il produttore fornisce i valori necessari.

Esempi di valori:
SIL CL = SIL 2, equivale a PL d
PFH_D = 1,29*10^{-7}

Se il disegno è stato realizzato dall'utente il procedimento per l'SRP/CS di reazione è lo stesso dell'SRP/CS di rilevamento.

Determinazione dell'integrità della sicurezza della funzione di sicurezza
È necessario determinare il PL più piccolo di tutti gli SRP/CS della funzione di comando di sicurezza (SRCF):

PL Min = min. (PL (SRP/CS 1)) .....PL (SRP/CS n) = PL d

Somma delle probabilità di guasti potenzialmente pericolosi (PFH_D) dell'SRP/CS
$PFH_D = PFH_D$ (SRP/CS 1) + ... + PFH_D (SRP/CS n) = 1,74*10^{-7} = <10^{-6} equivale a PL d

Risultato: la funzione di sicurezza soddisfa i requisiti per PL d

Determinazione del Performance Level in base a categoria, DC e $MTTF_d$

Benché nell'ambito delle due norme venga applicato un metodo diverso per la valutazione di una funzione di sicurezza, i risultati sono analoghi.
Procedimento semplificato per la valutazione del PL ottenuto tramite un SPR/CS:

Categoria	B	1	2	2	3	3	4
DC_{avg}	nessuno	nessuno	basso	medio	basso	medio	alto
$MTTF_d$ di ogni canale							
basso	a	non coperto	a	b	b	c	non coperto
medio	b	non coperto	b	c	c	d	non coperto
alto	non coperto	c	c	d	d	d	e

Conversione di SIL e PL

Come mostrato precedentemente, una funzione di sicurezza può essere valutata con due metodi diversi. SIL e PL possono essere confrontati tra loro sulla base delle probabilità di guasti potenzialmente pericolosi (vedere la tabella seguente).

SIL e PL sono riproducibili tra loro

Livello di integrità della sicurezza SIL	Probabilità di guasti potenzialmente pericolosi 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

Passo 4:
Validazione sulla base del Piano di sicurezza

Obiettivo:
Controllo della realizzazione dei requisiti di sicurezza specificati

Risultato:
Prova documentata relativa all'adempimento dei requisiti di sicurezza

Con la validazione si controlla che il sistema di sicurezza (SRECS) soddisfi i requisiti indicati nella specifica dell'SRCF. La base di questa operazione è il Piano di sicurezza.
La validazione richiede il seguente procedimento:

- Definire e documentare le responsabilità.
- Documentare anche tutti i test.
- Ogni SRCF deve essere convalidata da test e/o analisi.
- Deve essere convalidata anche l'integrità della sicurezza del sistema SRECS.

Pianificazione

Creare il Piano di sicurezza. La validazione viene eseguita sulla base di questo documento.

Test/verifica

È necessario verificare tutte le funzioni di sicurezza secondo la specifica (come descritto nel passo 1).

Documentazione

La documentazione è un elemento fondamentale della perizia in caso di sinistro.
Il contenuto dell'elenco della documentazione è predefinito dalla Direttiva Macchine. Sostanzialmente esso comprende:

- Analisi dei pericoli
- Valutazione dei pericoli
- Specifica delle funzioni di sicurezza
- Componenti hardware, certificati ecc.
- Schemi circuitali
- Risultati dei test
- Documentazione software comprensiva di firme, certificati ecc.
- Informazioni sull'utilizzo comprensive di avvertenze sulla sicurezza e limitazioni per il gestore

Al termine della validazione corretta è possibile creare la dichiarazione di conformità CE per quanto riguarda le misure di sicurezza volta alla riduzione dei rischi.

CE

Un vantaggio completo: sicurezza fornita da un unico partner

Sia che si tratti di rilevamento, comando, segnalazione, analisi oppure di reazioni, il nostro portafoglio di prodotti Safety Integrated copre tutte le aspettative di sicurezza nell'industria manifatturiera. Rivolgendovi ad un unico partner voi potete così usufruire di una sicurezza totale, integrata e omogenea, secondo il concetto di Totally Integrated Automation. Per voi, questo significa un funzionamento più economico, più sicuro e più affidabile.

Integrazione della tecnica di sicurezza, risparmio di costi

Safety Integrated rappresenta l'applicazione sistematica della tecnica di sicurezza secondo il concetto di Totally Integrated Automation: la nostra gamma di prodotti e sistemi per la realizzazione di soluzioni di automazione, unica per completezza e omogeneità. Le funzioni della tecnica di sicurezza vengono sistematicamente integrate nell'automazione standard, così da ottenere un sistema completo e omogeneo. I conseguenti vantaggi per costruttori di macchine e gestori di impianti si traducono in una considerevole riduzione dei costi nell'intero ciclo di vita.

Con i nostri prodotti, i sistemi, il service e il training per la tecnica standard e di sicurezza forniti da un unico partner, andate sul sicuro: Safety Integrated offre sempre una soluzione veloce e soprattutto economica.

Indipendentemente dal fatto:

- che abbiate optato per una soluzione convenzionale, basata su bus o basata su controllore/azionamento **(flessibilità)** e/o
- che si tratti di una semplice funzione di arresto d'emergenza, di una semplice concatenazione di circuiti di sicurezza o di processi altamente dinamici **(complessità)**.

SIRIUS – valori B10 standard dei componenti elettromeccanici con carico nominale

Nella tabella seguente sono elencati i valori B10 standard SIRIUS con la percentuale di guasti potenzialmente pericolosi derivati dalle norme ISO 13849-2 (Allegato D), ISO/FDIS 13849-1:2005 (Allegato C) e DIN EN 62061 (Allegato D sui tipi di guasto di componenti elettrici/elettronici). La norma Siemens SN 31920 contiene maggiori dettagli.

Gamma di prodotti Siemens SIRIUS (componenti elettromeccanici)	Valore B10 (Manovre)	Percentuale di guasti potenzialmente pericolosi
Apparecchi di comando per ARRESTO/OFF di EMERGENZA (con contatti ad apertura forzata) • con sblocco a trazione • con sblocco a rotazione (anche a chiave)	 30.000 100.000	 20 % 20 %
Interruttori a fune per funzione di ARRESTO/OFF di EMERGENZA (con contatti ad apertura forzata)	1.000.000	20 %
Interruttori di posizione standard (con contatti ad apertura forzata)	10.000.000	20 %
Interruttori di posizione con attuatore separato (con contatti ad apertura forzata)	1.000.000	20 %
Interruttori di posizione con blocco di ritenuta (con contatti ad apertura forzata)	1.000.000	20 %
Interruttori a cerniera (con contatti ad apertura forzata)	1.000.000	20 %
Interruttori di posizione con attuatore separato (con contatti ad apertura forzata)	1.000.000	20 %
Pulsanti (senza aggancio a scatto, con contatti ad apertura forzata)	10.000.000	20 %
Contattori/avviatori motore (con contatti a guida forzata per 3RH/3TH o contatti speculari per 3RT/3TF)	1.000.000	73 %

Glossario della sicurezza funzionale

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

β, **beta:**
Fattore di guasto in seguito ad 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 della sua 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 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.





Prodotti Omologazione (max.)	Interruttori di posizione SIRIUS con azionatore separato, senza e con blocco di ritenuta, interruttori a cerniera, interruttori magnetici (senza contatto)	Apparecchi di comando e segnalazione SIRIUS, ARRESTO DI EMERGENZA, interruttori a fune, pulpiti di comando a due mani, interruttori a pedale, colonne di segnalazione e luci di segnalazione	DP/AS-i F-Link (ASIsafe Solution PROFIsafe)	SIMATIC Mobile Panel 277F IWLAN	Dispositivi di sicurezza SIRIUS 3TK28 1) Dispositivi di sicurezza 2) Dispositivi di controllo arresto 3) Dispositivi di controllo velocità
IEC 62061 (IEC 61508)	Fino a SIL 3	Fino a SIL 3	Fino a SIL 3	Fino a SIL 3	Fino a SIL 3
ISO 13849-1	Fino a PL e	Fino a PL e	Fino a PL e	Fino a PL e	Fino a PL e
EN 954-1 o IEC/EN 61496	Fino a Cat. 4	Fino a Cat. 4	Fino a Cat. 4	Fino a Cat. 4	Fino a Cat. 4
Altro			NFPA 79, NRTL-Listed		NFPA 79, NRTL-Listed
Applicazione/ funzioni di sicurezza	Per la sorveglianza meccanica di dispositivi di protezione, ripari o sportelli di protezione. Per verifiche esatte della posizione.	Applicazioni di arresto di emergenza nell'industria manifatturiera e di processo; segnalazione di stato di macchine e impianti	Gateway sicuro per la trasmissione dei segnali ASIsafe nel telegramma PROFIsafe per le applicazioni di sicurezza nell'automazione di produzione	Servizio e supervisione in prossimità della macchina di impianti di produzione con applicazioni critiche per la sicurezza, esecuzione di compiti rilevanti per la sicurezza, come ad es. eliminazione di errori negli impianti in esercizio Funzioni di sicurezza: • Pulsante di arresto di emergenza • Due tasti di consenso (destra/sinistra) • Identificazione mediante transponder e misurazione della distanza per login e comando sicuri Engineering: – Safety Advanced per STEP 7 V11 nel Portale TIA – Distributed Safety per STEP 7 V 5.5	• Sorveglianza di dispositivi di protezione come ad es. apparecchi di arresto di emergenza, interruttori di posizione e sensori funzionanti senza contatto • Sorveglianza sicura di stato di fermo • Sorveglianza sicura di velocità: – tre valori limite parametrizzabili per stato di fermo, velocità di messa a punto e velocità di funzionamento automatico – collegamento possibile di diversi sensori ed encoder – sorveglianza di ripari di protezione integrata
Possibilità di comunicazione fail-safe	AS-Interface (ASIsafe)	AS-Interface (ASIsafe)	AS-Interface (ASIsafe) e PROFIBUS con profilo PROFIsafe	PROFINET con profilo PROFIsafe, IWLAN con PROFIsafe	

Sistema di gestione motore SIMOCODE pro 3UF7 con moduli di ampliamento fail-safe DM-F	**ASIsafe** **1) Moduli d'ingresso sicuri** **2) Monitor di sicurezza (ASIsafe Solution local)** **3) Uscite AS-i sicure**	**Sistema di sicurezza modulare SIRIUS 3RK3**	**Controllori SIMATIC**	**Periferia SIMATIC**
Fino a SIL 3	Fino a SIL 3	Fino a SIL 3	Fino a SIL 3	Fino a SIL 3
Fino a PL e	Fino a PL e	Fino a PL e	Fino a PL e	Fino a PL e
Fino a Cat. 4	Fino a Cat. 4	Fino a Cat. 4	Fino a Cat. 4	Fino a Cat. 4
NFPA 79, NRTL-Listed	NFPA 79, NRTL-Listed	NFPA 79, NRTL-Listed	NFPA 79, NFPA 85, NNRTL-Listed, IEC 61511	NFPA 79, NFPA 85, NRTL-Listed, IEC 61511
Gestione del motore con funzioni di sicurezza integrate per l'automazione di processo • Disinserzione sicura di motori • **Modulo digitale fail-safe DM-F Local:** per la disinserzione sicura mediante segnale hardware; 2 circuiti di abilitazione a relè, con commutazione comune; 2 uscite a relè, contatti comuni con disinserzione sicura; ingressi per circuito dei sensori, segnale di avvio, collegamento in cascata e circuito di retroazione. • **Modulo digitale fail-safe DM-F PROFIsafe:** per la disinserzione sicura tramite PROFIBUS / PROFIsafe; 2 circuiti di abilitazione a relè, con commutazione comune; 2 uscite a relè, contatti comuni con disinserzione sicura; 1 ingresso per circuito di retroazione; 3 ingressi binari standard • Impostazione delle funzioni di sicurezza direttamente sul DM-F Local o in STEP 7 (DM-F PROFIsafe) Engineering: – tramite il Portale TIA – tramite Simocode ES	1) Collegamento sicuro o interconnessione in rete di interruttori di sicurezza e sensori di sicurezza elettronici 2) Tutte le applicazioni di sicurezza nell'automazione della produzione: • Controllo e analisi di segnali sicuri tramite AS-Interface inclusa la disinserzione su 1–2 circuiti di abilitazione • Possibilità di comando di uscite AS-i sicure per la disinserzione di motori o il comando ad es. di valvole di sicurezza • Accoppiamento sicuro di reti ASIsafe 3)Disinserzione sicura centrale di motori e azionamenti tramite AS-I – Engineering tramite il Portale TIA	Sistema di sicurezza modulare e parametrizzabile per tutte le applicazioni di sicurezza nell'automazione manifatturiera. • Analisi sicura di dispositivi di sicurezza meccanici e funzionanti senza contatto • Funzione di diagnostica integrata • Test dei segnali e monitoraggio del tempo di discrepanza integrati • Semplice realizzazione di funzioni di sicurezza mediante blocchi funzione predefiniti Engineering: – Parametrizzazione tramite MSS ES – Integrazione nel Portale TIA	Controllori fail-safe scalabili • Controllori modulari: CPU315F/317F/319F CPU 414F/416F ET 200F-CPU per ET 200S e ET 200pro • Controllore tecnologico con Motion Control: CPU 317TF-2DP • PC-based Automation: Software-PLC, Embedded Controller, IPC Funzioni di sicurezza: • Diagnostica integrata • Coesistenza di programmi standard e fail-safe in una CPU Engineering: – Safety Advanced per STEP 7 V11 nel Portale TIA – Distributed Safety per STEP 7 V5.5 con F-FUP e F-KOP nonché biblioteca integrata con blocchi di sicurezza certificati dal TÜV – In opzione: Biblioteca con blocchi funzione per presse e bruciatori	Sistemi di periferia scalabili e ridondanti • ET 200eco • ET 200M • ET 200iSP • ET 200S • ET 200pro Funzioni di sicurezza: • Test dei segnali e monitoraggio del tempo di discrepanza integrati • Un sistema di periferia decentrato con unità di ingressi e uscite standard e fail-safe • Configurazione della visualizzazione del test dei segnali e del tempo di discrepanza con STEP 7 Engineering: – Safety Advanced per STEP 7 V11 nel Portale TIA – Distributed Safety per STEP 7 V5.5
PROFIBUS con profilo PROFIsafe	1) AS-Interface (ASIsafe) 2) AS-Interface (ASIsafe Solution local)	Diagnostica tramite PROFIBUS	• PROFINET con PROFIsafe, IWLAN con PROFIsafe	• PROFIBUS con profilo PROFIsafe: tutti i sistemi • PROFINET con profilo PROFIsafe: ET 200S, ET200M, ET 200pro (modulo IWLAN Interface disponibile)

Reazione

Avviatori motore per **• ET 200S (IP20)** **• ET 200pro (IP65)**	**Convertitore di frequenza per** **• ET 200S** **• ET 200pro**	**Convertitori di frequenza** **1) SINAMICS G120C (IP20)** **2) SINAMICS G120 (IP20)** **3) SINAMICS G120D (IP65)**	**Convertitori di frequenza** **SINAMICS G130** **SINAMICS G150**
Fino a SIL 3	Fino a SIL 2	Fino a SIL 2	Fino a SIL 2
Fino a PL e	Fino a PL d	Fino a PL d	Fino a PL d
Fino a Cat. 4	Fino a Cat. 3	Fino a Cat. 3	Fino a Cat. 3
NFPA 79, NRTL-Listed			
Tutte le applicazioni di sicurezza nell'automazione manifatturiera e in compiti di azionamento decentrati come ad es. nella tecnica dei trasporti industriali o negli azionamenti di sollevamento • Avviamento e disinserzione sicura con tecnica di manovra convenzionale ed elettronica • Protezione motore integrata • Disinserzione sicura e selettiva (ET 200S) • Tutti i vantaggi dei sistemi SIMATIC ET 200S e SIMATIC ET 200pro Engineering: – Safety Advanced per STEP 7 V11 nel Portale TIA – Distributed Safety per STEP 7 V5.5	Azionamento centrale integrato nel sistema (convertitore di frequenza) in motori asincroni standard senza encoder Funzioni di sicurezza autarchiche integrate: • Coppia disinserita in sicurezza • Arresto sicuro 1 • Velocità limitata sicura	1) Convertitore di frequenza compatto per applicazioni da 0,37 a 18,5 kW 2) Convertitore di frequenza modulare per applicazioni da 0,37 a 250 kW 3) Convertitore di frequenza decentrato con elevato grado di protezione (IP65) per applicazioni da 0,75 a 7,5 kW Gli apparecchi SINAMICS G120 vengono impiegati nel funzionamento a velocità variabile di motori asincroni nella tecnica dei trasporti industriali, in pompe, ventilatori e compressori nonché in altri aggregati, come ad es. estrusori. Funzioni di sicurezza integrate [1]: • Coppia disinserita in sicurezza (STO) • Arresto sicuro 1 • Velocità limitata sicura • G120: direzione del movimento sicura • G120: comando sicuro del freno • G120: sorveglianza sicura della velocità	Convertitori di frequenza per azionamenti singoli a velocità variabile da 75 a 27.000 kW ad es. pompe, ventole, ventilatori, compressori, nastri trasportatori, estrusori, miscelatori, macine Funzioni di sicurezza integrate: • Coppia disinserita in sicurezza • Arresto sicuro 1
• Solution PROFIsafe: PROFIBUS/PROFINET con profilo PROFIsafe • Solution local: applicazione di sicurezza locale	PROFIBUS/PROFINET con profilo PROFIsafe	PROFIBUS con profilo PROFIsafe, G120 e G120D anche PROFINET [1] le funzioni di sicurezza integrate sono possibili senza encoder. SINAMICS G120C oltre a STO non supporta nessuna ulteriore funzione di sicurezza	PROFIBUS/PROFINET con profilo PROFIsafe

Reazione

			
Azionamento di posizionamento SINAMICS S110	**1) Sistema di azionamento SINAMICS S120** **2) Apparecchi in armadio SINAMICS S150**	**SINUMERIK 840D sl Controllo CNC per macchine utensili**	**Controllo numerico per macchine utensili SINUMERIK 828D**
Fino a SIL 2	Fino a SIL 2	Fino a SIL 2	Fino a SIL 2
Fino a PL d	Fino a PL d	Fino a PL d	Fino a PL d
Fino a Cat. 3	Fino a Cat. 3	Fino a Cat. 3	Fino a Cat. 3
	NFPA 79, NRTL-Listed*	NFPA 79, NRTL-Listed	NFPA 79, NRTL-Listed
Servoazionamento monoasse per semplici compiti di posizionamento con motori sincroni/asincroni con potenze da 0,12 a 90 kW. Le funzioni di sicurezza integrate sono possibili in parte anche senza encoder: • Coppia disinserita in sicurezza • Arresto sicuro 1 e 2 • Arresto operativo sicuro • Velocità limitata sicura • Direzione del movimento sicura • Sorveglianza sicura della velocità • Comando sicuro del freno	1) Sistema di azionamento per compiti di regolazione ad elevata performance da 0,12 a 4.500 kW nella costruzione di macchine e impianti, ad es. per macchine confezionatrici o per la lavorazione delle materie plastiche, sistemi di manipolazione, treni di laminazione o macchine per la carta 2) Azionamenti singoli a velocità variabile a potenza elevata (da 75 a 1.200 kW) come banchi di prova, centrifughe per zucchero, troncatrici trasversali, argani a fune o nastri trasportatori Le funzioni di sicurezza integrate sono possibili in parte anche senza encoder: • Coppia disinserita in sicurezza • Arresto sicuro 1 e 2 • Arresto operativo sicuro • Velocità limitata sicura S120: Booksize/Blocksize: • Direzione del movimento sicura • Sorveglianza sicura della velocità • Comando sicuro del freno**	Controllo numerico con tecnica di sicurezza integrata nel controllore e azionamento per macchine utensili (tornitura, fresatura, rettifica, roditura ...) Funzioni di sicurezza: • Coppia disinserita in sicurezza • Arresto sicuro 1 e 2 • Controllo sicuro dell'accelerazione • Arresto operativo sicuro • Velocità limitata sicura • Posizione limitata sicura • Gestione sicura dei freni • Comando sicuro del freno • Test di frenatura sicura • Camme software sicure • Ingressi/uscite di sicurezza • Logica programmabile sicura • Test di collaudo integrato	Controllo numerico per torni e fresatrici con tecnica di sicurezza integrata nell'azionamento. Il SINUMERIK 828D è un controllo CNC panel-based per applicazioni altamente complesse con torni e fresatrici di normale impiego nell'officina Funzioni di sicurezza integrate: • Coppia disinserita in sicurezza • Arresto sicuro 1 e 2 • Arresto operativo sicuro • Velocità limitata sicura • Senso di rotazione sicuro (in prep.) • Controllo sicuro della velocità • Comando sicuro del freno
PROFIBUS/PROFINET con profilo PROFIsafe	PROFIBUS/PROFINET con profilo PROFIsafe	PROFIBUS con profilo PROFIsafe	PROFIBUS con profilo PROFIsafe

* vale solo per SINAMICS S120 Booksize ** non vale per S150 e per S120 Chassis

Siemens S.p.A.
Industry Sector
Industry Automation
Control Components and Systems Engineering
Viale Piero e Alberto Pirelli 10
20126 MILANO, ITALIA
Tel. 0224363333/Fax.0224362890

www.siemens.it/safety

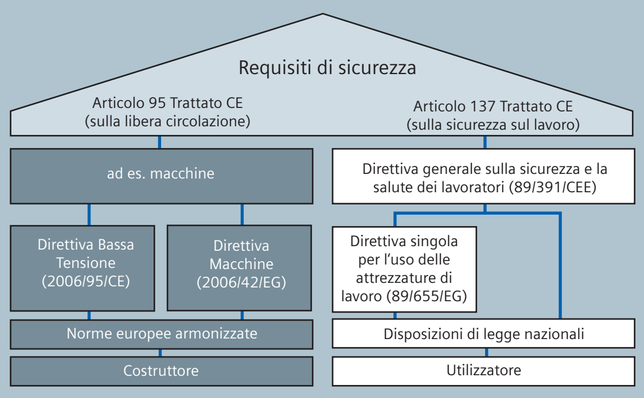
Con riserva di modifiche 05/11
No. di ordinazione: E20001-A230-M103-V5-7200
DISPO 27610
21/33938 XX03.52.1.15. 0511 PDF
Stampato in Germania

E20001-Y290-M103-V5-7200

Sicurezza funzionale di macchine e impianti –

Applicazione della Direttiva Europea sulle Macchine

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
EN ISO 14121-1	Sicurezza del macchinario	Principi per la valutazione del rischio

Requisiti funzionali e di sicurezza per controllori di sicurezza

Disegno e realizzazione di controllori di sicurezza

EN 62061:2005 **Sicurezza del macchinario** Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza	**EN ISO 13849-1:2006** **Sicurezza del macchinario** Parti dei sistemi di comando legate alla sicurezza, Parte 1: Principi generali di progettazione Norma successiva alla EN 954-1:1996, periodo di transizione fino alla fine dell'anno 2011)
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 e ogni situazione pericolosa
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 di sicurezza e informazione dell'utilizzatore)

La norma EN ISO 14121 contiene informazioni dettagliate sui passi da 1 a –4.

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

EN 62061: 2005 **(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 13849-1:2006 **(Norma successiva alla EN 954-1:1996, periodo di transizione fino alla fine dell'anno 2011)**

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	altre misure		SIL 1	SIL 2	SIL 3
Reversibile, cure mediche	2				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)

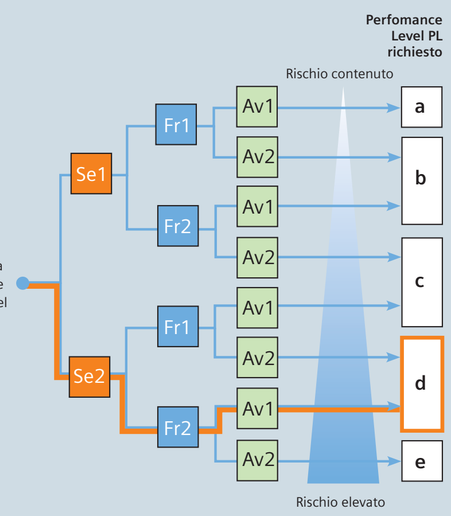
Parametri di rischio

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

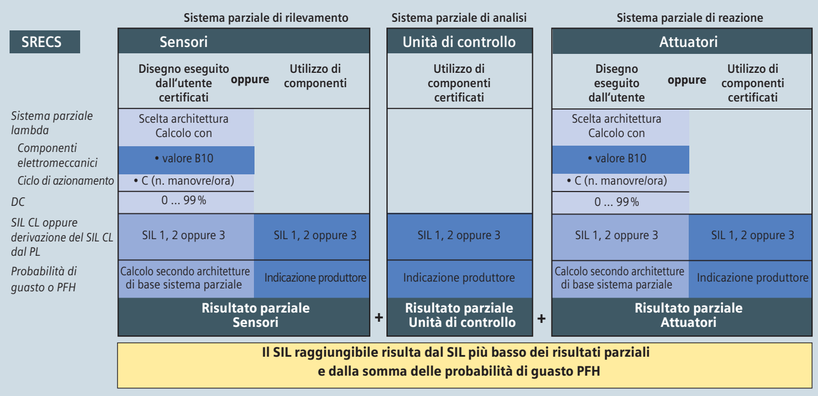
Fr = frequenza e/o durata dell'esposizione al pericolo
- Fr1 = da raro a frequente e/o il periodo di esposizione al rischio è breve
- Fr2 = da frequente a permanente e/o il periodo di esposizione al rischio è lungo

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

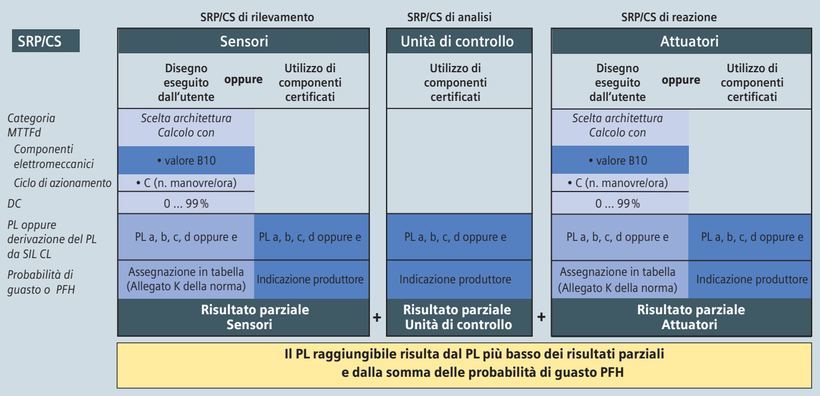


Configurazione della funzione di sicurezza e determinazione dell'integrità della sicurezza ottenuta



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.



Tutti i sensori insieme formano un SRP/CS.

Tutti gli attuatori insieme formano un SRP/CS (calcolo tramite $1/MTTF_d = 1/MTTF_{d1} + 1/MTTF_{d2}$ ...).

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.

SIL e PL sono riproducibili tra loro

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

Safety Integrated

Answers for industry.

SIEMENS