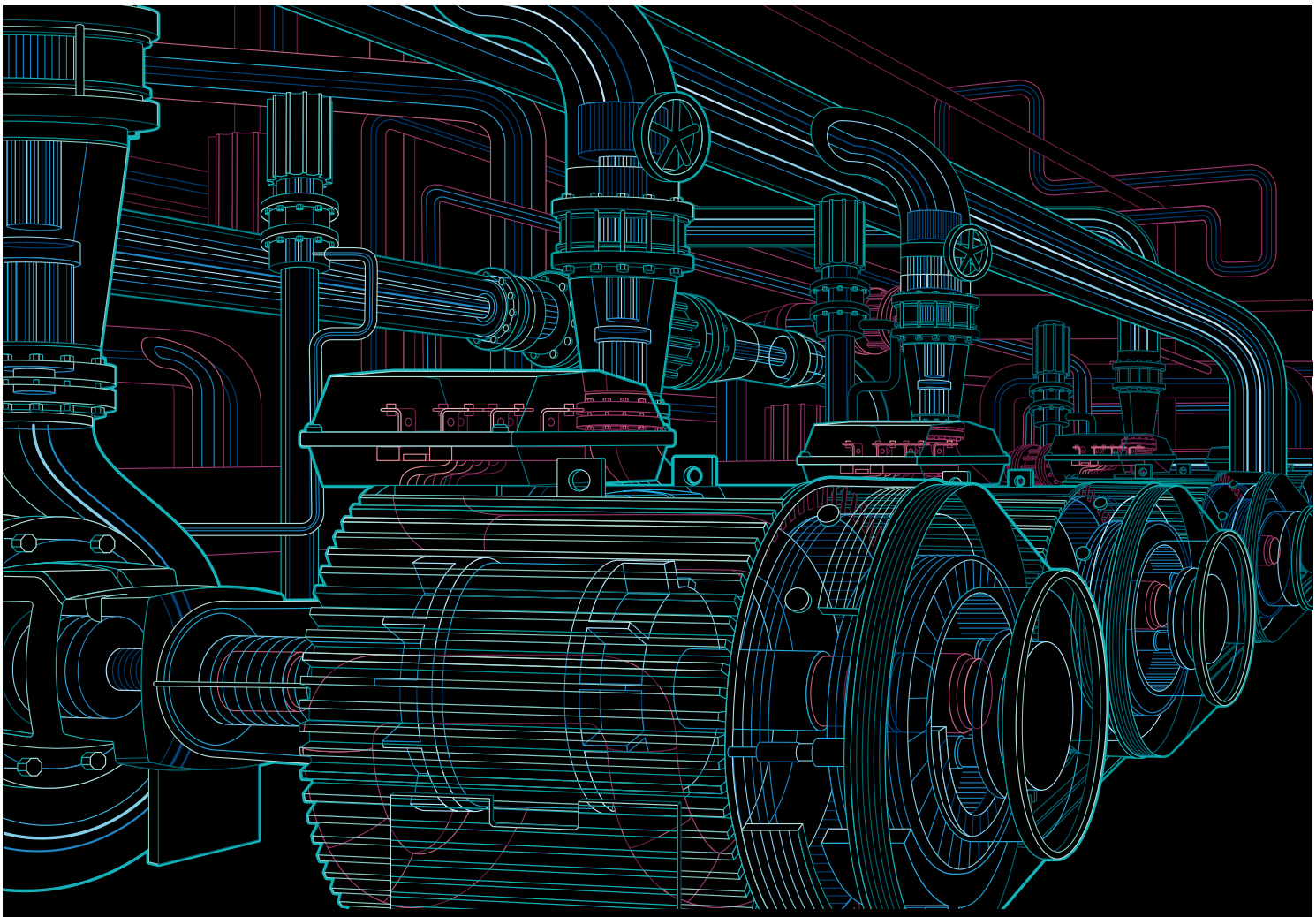


Sicurezza e sicurezza funzionale.
Guida generale

Power and productivity
for a better world™

ABB, da sempre attenta al mondo della sicurezza, offre un portafoglio di prodotti e di soluzioni di automazione innovativo e completo in grado di rispondere a tutti i requisiti imposti dalla normativa sulla sicurezza delle macchine.

Sommario

Considerazioni preliminari

Area di crescente importanza

Questo documento è stato redatto per consentire agli utenti, ai responsabili della definizione delle specifiche, ai costruttori di macchine e agli operatori coinvolti in tali attività, di comprendere meglio i requisiti indicati nella Direttiva Macchine dell'Unione europea 2006/42/CE, nonché le misure necessarie per conformarsi alla direttiva e alle norme armonizzate ivi indicate.

Le leggi nazionali degli Stati membri dell'Unione Europea prevedono che le macchine soddisfino i requisiti essenziali di salute e sicurezza EHSR (Essential Health and Safety Requirements) definiti dalla Direttiva Macchine 2006/42/CE.

Le norme armonizzate specificate nella Direttiva costituiscono una delle vie preferenziali per dimostrare la conformità.
Questo significa che tutte le nuove macchine immesse sul mercato all'interno dell'Unione Europea devono soddisfare gli stessi requisiti legali. Le stesse norme sono riconosciute anche in diverse zone fuori dall'Europa, ad esempio mediante l'adozione di tabelle di equivalenza.
Questo facilita la commercializzazione e la spedizione di macchine tra diversi paesi sia all'interno che all'esterno dell'Unione Europea.
La sicurezza delle macchine è una delle aree di interesse in più rapida crescita nell'ambito dell'automazione industriale. Le nuove strategie di sicurezza consentono ai costruttori di migliorare la propria produttività e la competitività sul mercato. La sicurezza diventa parte integrante della funzionalità della macchina e non è più una modifica aggiunta solo per ottenere la conformità alle leggi vigenti.

Introduzione
Sicurezza e sicurezza funzionale

I sistemi di sicurezza funzionale sviluppati attraverso un processo definito e che utilizzano sotto-sistemi certificati per raggiungere specifici livelli di sicurezza sono ormai una necessità per il mercato.

Questa guida generale descrive le norme che devono essere tenute in considerazione durante la progettazione di una macchina al fine di garantirne la sicurezza funzionale.

Lo scopo di questo documento è spiegare, in termini generali, le procedure da seguire per soddisfare i requisiti della Direttiva Macchine 2006/42/CE e ottenere la marcatura CE.

Nell'ottica di questa guida, l'obiettivo delle soluzioni di sicurezza è la protezione da danni e lesioni. I sistemi di sicurezza funzionale raggiungono questo obiettivo riducendo la probabilità di eventi non desiderati, minimizzando così il numero di incidenti durante l'utilizzo delle macchine.

Le norme specifiche definiscono la sicurezza come assenza di rischi non accettabili. Il modo più efficace per ridurre i rischi consiste nell'eliminarli a livello di progettazione. Tuttavia, se una riduzione del rischio in fase di progettazione non è una soluzione possibile o praticabile, la protezione mediante sistemi di sicurezza passiva e funzionale rappresenta spesso la scelta migliore. Arrestare una macchina velocemente e in sicurezza non solo riduce i rischi, ma aumenta anche il tempo di operatività e la produttività della macchina perché riduce i tempi di fermo ed evita arresti improvvisi. Nello stesso tempo, risultano soddisfatti tutti gli obblighi di legge e viene garantita la sicurezza delle persone e dell'ambiente. La sicurezza funzionale delle macchine viene in genere ottenuta mediante sistemi che monitorano e, quando necessario, assumono il controllo delle funzioni della macchina, in modo da garantirne un funzionamento sicuro. Tali sistemi implementano le funzioni di sicurezza richieste e necessarie. I sistemi di sicurezza funzionale, infatti, sono progettati per rilevare le condizioni di pericolo e riportare la macchina a uno stato di funzionamento sicuro oppure per garantire l'esecuzione delle azioni desiderate, ad esempio un arresto di emergenza.

Il monitoraggio può includere fattori quali la velocità, l'arresto, la direzione di rotazione e l'inattività. Quando il sistema sta eseguendo una funzione di sicurezza attiva, ad esempio il monitoraggio della velocità di avanzamento, e si verifica uno scostamento dal comportamento previsto, ad esempio la macchina funziona a velocità troppo elevata, il sistema di sicurezza rileva tale irregolarità e riporta attivamente la macchina in condizioni di sicurezza. Tale risultato può essere raggiunto, ad esempio, mettendo in atto un arresto di emergenza e riducendo la coppia dell'albero motore. Un eventuale guasto al sistema di sicurezza fa aumentare immediatamente il rischio correlato al funzionamento della macchina.

Direttiva Macchine 2006/42/CE

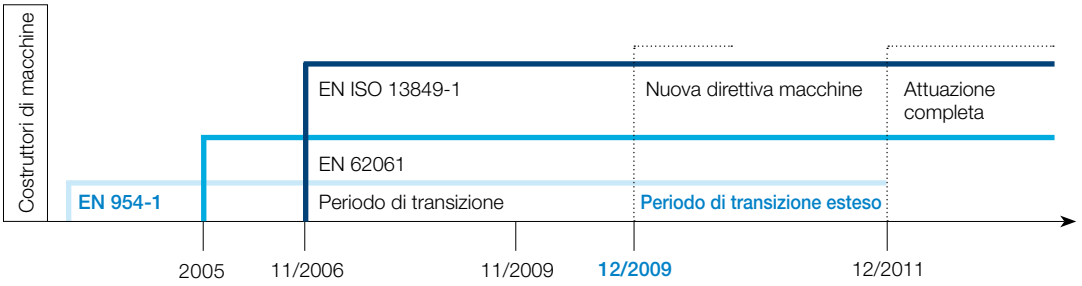
La Direttiva Macchine e le relative norme armonizzate definiscono i requisiti essenziali di salute e sicurezza EHSR (Essential Health and Safety Requirements) per le macchine a livello dell'Unione europea.

L'idea alla base della Direttiva Macchine è garantire che una macchina sia sicura e che venga progettata e costruita in modo tale da poter essere utilizzata, configurata e sottoposta a manutenzione durante tutte le fasi del ciclo di vita con livelli di rischio minimi per le persone e per l'ambiente.

L'EHSR stabilisce che i costruttori di macchine debbano applicare i seguenti principi in quest'ordine:

- eliminare o ridurre nella misura maggiore possibile i fattori di pericolo, tenendo in considerazione gli aspetti relativi alla sicurezza durante le fasi di progettazione e costruzione della macchina;
- applicare tutte le misure di protezione necessarie contro i pericoli che non è possibile eliminare;
- informare gli utenti dei rischi ancora presenti nonostante l'adozione di tutte le misure di protezione realizzabili; specificando tutti i requisiti relativi all'addestramento del personale o all'utilizzo di dispositivi di protezione individuale.

Due sistemi di norme ISO e IEC



Nota.
Secondo la convenzione utilizzata nell'elenco delle norme armonizzate, le norme EN ISO sono indicate includendo anche la dicitura "ISO", mentre le norme EN IEC sono indicate senza la dicitura "IEC", ovvero solo con EN. Anche il presente documento segue questa convenzione.

Nota.
Una tabella che illustra l'adeguatezza di queste due nuove norme per la progettazione di sistemi con tecnologie particolari può essere trovata all'interno delle norme stesse.

Due nuovi standard

I costruttori di macchine che implementano sistemi di sicurezza funzionale in conformità con la Direttiva Macchine hanno la possibilità di scegliere fra due standard europei alternativi, sviluppati rispettivamente dall'ISO (Organizzazione Internazionale per la Standardizzazione) e dalla IEC (Commissione Elettrotecnica Internazionale). I due standard si chiamano EN ISO 13849-1 e EN 62061. Entrambi sostituiscono il vecchio standard EN 954-1, che diventerà obsoleto il 31 dicembre 2011, dopo un periodo di transizione di 3+2 anni. Inoltre, entrambi fanno parte delle norme di base per la sicurezza delle macchine per la minimizzazione del rischio (EN ISO 12100-1: 2003) e per la valutazione e riduzione del rischio (EN ISO 14121-1: 2007). La Figura 1 illustra questa gerarchia.

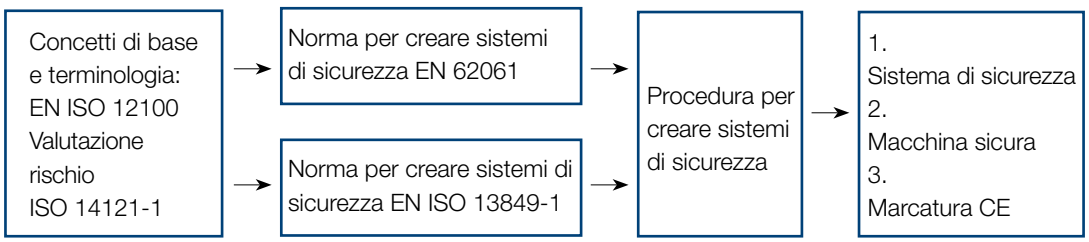
Le norme per la sicurezza elettrica sono formalmente definite così: EN ISO 13849-1: 2008 (Sicurezza delle macchine – Parti del sistema di controllo correlate alla sicurezza – Principi generali di progettazione), EN 62061: 2005 (Sicurezza delle macchine – Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza). Tutti i riferimenti a queste norme presenti nel documento si riferiscono alle versioni sopra indicate. I costruttori possono scegliere se e quale norma di sicurezza utilizzare (tra ISO 13849-1 o EN 62061). Tuttavia, per assicurare coerenza, si raccomanda di utilizzare la stessa norma dall'inizio alla fine.

I due sistemi forniscono risultati molto simili e i livelli SIL (Safety Integrity Levels) e PL (Performance Levels) sono paragonabili. (vedere Tabella 7).
Questo documento riporta esempi di risultati di sicurezza e integrità per entrambe le norme.

ISO 13849-1, per la realizzazione di macchine sicure

La norma EN ISO 13849-1 fornisce ai costruttori istruzioni per la realizzazione di macchine sicure. Queste istruzioni comprendono indicazioni per la progettazione, l'integrazione e la convalida dei sistemi e possono essere utilizzate per le parti correlate alla sicurezza dei sistemi di controllo e di diverse tipologie di macchina, indipendentemente dalla tecnologia e dal tipo di energia utilizzati. Nelle norme sono inoltre inclusi requisiti speciali per le parti correlate alla sicurezza che dispongono di sistemi elettronici programmabili. Questa norma copre tutti i dispositivi inclusi nell'intera funzione di sicurezza (una catena di sicurezza completa può essere ad esempio: sensore – logica – attuatore).

Figura 1.



PL (Performance Level)

La norma EN ISO 13849-1 definisce il modo in cui viene determinato il PL (Performance Level) richiesto per un sistema di sicurezza e il modo in cui il PL ottenuto viene verificato. Il livello PL indica l'efficienza e l'affidabilità con cui un sistema di sicurezza è in grado di eseguire una funzione di sicurezza in condizioni prevedibili. Sono disponibili cinque livelli di prestazioni: a, b, c, d, e.
Il valore PL "e" indica il livello più alto di affidabilità del sistema di sicurezza, mentre il valore PL "a" indica quello più basso. Vedere l'esempio a pag.13.

EN 62061, per la progettazione di sistemi elettrici di sicurezza

La norma EN 62061 riguarda la progettazione dei sistemi elettrici di sicurezza. È una norma specifica del settore macchine e si inserisce nel quadro della norma IEC 61508. La norma EN 62061 comprende indicazioni per la progettazione, l'integrazione e la convalida di sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza. Tale norma copre l'intera catena di sicurezza, ad esempio sensore – logica – attuatore.

SIL (Safety Integrity Level)

La norma EN 62061 specifica il modo in cui viene definito il livello SIL (Safety Integrity Level).
Il livello SIL è una rappresentazione del livello di integrità delle funzioni di sicurezza. Sono disponibili quattro livelli di integrità della sicurezza: 1, 2, 3 e 4. "SIL 4" corrisponde al livello più alto di integrità della sicurezza, mentre "SIL 1" corrisponde al livello più basso. Nelle macchine vengono utilizzati solo i livelli 1-3. Vedere l'esempio a pag. 12.

Nota.
A differenza della norma EN ISO 13849-1, nella norma EN 62061 non vengono trattati i requisiti relativi ai dispositivi di controllo non elettrici correlati alla sicurezza delle macchine.

Conformità ai requisiti della Direttiva Macchine

La Direttiva Macchine 2006/42/CE prevede che le macchine siano sicure. Tuttavia, considerato che non è possibile azzerare totalmente il rischio, l'obiettivo più importante è ridurre il rischio al minimo. La conformità a questo obiettivo può essere raggiunta in due modi:

- conformarsi ai requisiti stabiliti dalle norme armonizzate oppure
- affidare a terzi autorizzati il compito di attestare la conformità di una macchina.

Raggiungere e gestire la sicurezza funzionale

Per raggiungere un livello di sicurezza funzionale conforme all'EHSR della Direttiva Macchine, ovvero la prima alternativa, è necessario seguire alcuni passi. Per ognuno di questi passi, bisognerà considerare l'intero sistema e l'ambiente con cui esso interagisce. Questi passi comprendono valutazione del rischio, individuazione e implementazione delle funzioni di sicurezza necessarie per la riduzione del rischio e verifica del funzionamento delle suddette funzioni di sicurezza.
Tutte le attività di sicurezza funzionale devono essere gestite durante il ciclo di vita della macchina. Un sistema di gestione del progetto e della qualità sotto forma di piano per la sicurezza è il miglior modo per ottenere la conformità.

Piano per la sicurezza

La norma EN 62061 individua in un piano per la sicurezza lo strumento necessario per conformarsi ai requisiti previsti dalla Direttiva Macchine. Il piano per la sicurezza identifica tutte le attività pertinenti, descrive i criteri e le strategie da adottare per soddisfare i requisiti di sicurezza funzionale, identifica le responsabilità, individua o definisce le procedure e le risorse per la creazione della documentazione, descrive la strategia per la gestione della configurazione, include piani di verifica e convalida.
Tale piano deve essere appositamente progettato e documentato, nonché opportunamente aggiornato, per ciascun sistema di sicurezza.

Nota.
A differenza della norma EN 62061, la norma EN ISO 13849-1 non specifica le attività da eseguire nel piano per la sicurezza. Rimane comunque necessario eseguire attività simili per soddisfare completamente i requisiti della Direttiva Macchine.

Dopo aver creato un piano per la sicurezza conforme alla norma EN 62061, è possibile passare agli aspetti più pratici, seguendo la procedura in 7 passi illustrata nella Tabella 1, che inizia con la valutazione e riduzione del rischio.

Tabella 1.
Procedura da seguire per soddisfare i requisiti della Direttiva Macchine per la sicurezza funzionale. Di seguito ognuno di questi passi è illustrato in maggior dettaglio.

Tabella 1

Passo	Azioni richieste
Passo 1 - Valutazione e riduzione del rischio	Analizzare i rischi e valutare come eliminarli o minimizzarli (per la strategia in 3 passi, vedere EN ISO 12100-1)
Passo 2 - Definizione dei requisiti di sicurezza	Definire il tipo di funzionalità e prestazioni di sicurezza necessarie per eliminare il rischio o ridurlo ad un livello accettabile
Passo 3 - Implementazione di un sistema di sicurezza funzionale	Progettare e creare le funzioni del sistema di sicurezza
Passo 4 - Verifica della sicurezza funzionale	Assicurarsi che il sistema di sicurezza soddisfi i requisiti definiti
Passo 5 - Convalida della sicurezza funzionale	Ripetere la valutazione del rischio e assicurarsi che il sistema di sicurezza riesca realmente a ridurre il rischio come previsto
Passo 6 - Creazione della documentazione relativa a un sistema di sicurezza funzionale	Produrre documentazione sulla progettazione e documenti per l'utente
Passo 7 - Verifica della conformità	Verificare la conformità della macchina rispetto alla ai requisiti EHSR della Direttiva Macchine tramite una valutazione della conformità e delle caratteristiche tecniche

Passo 1.
Valutazione e riduzione del rischio

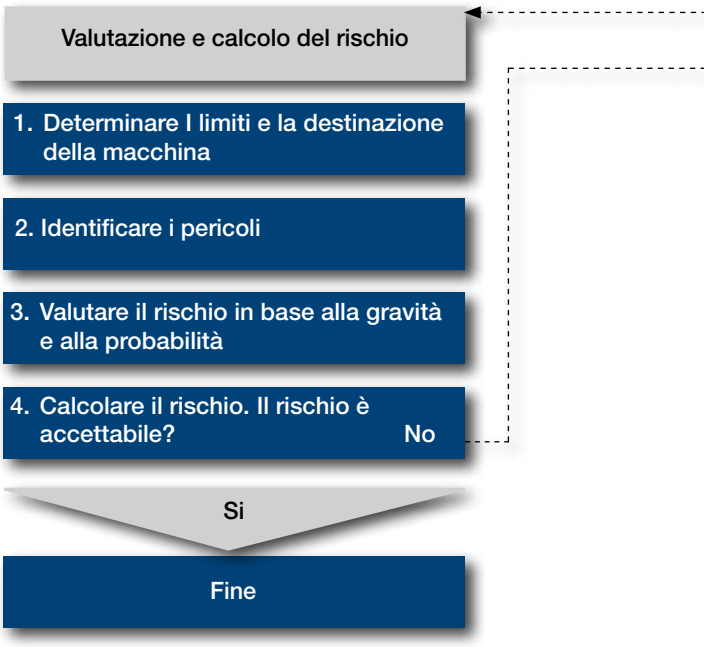
Valutazione del rischio

La valutazione del rischio è il processo in base al quale i rischi vengono analizzati e calcolati. Il termine rischio indica la conseguenza di un danno, combinata con la probabilità che tale danno si verifichi, in caso di esposizione a un pericolo. La Direttiva Macchine 2006/42/CE prescrive che i costruttori eseguano obbligatoriamente le operazioni di valutazione del rischio i cui risultati siano tenuti in considerazione durante tutte le fasi di progettazione di una macchina. Ogni rischio considerato “elevato” deve essere ridotto a un livello accettabile apportando modifiche al progetto o applicando misure di protezione adeguate. Il processo di valutazione del rischio indica al costruttore tutti i requisiti necessari per la realizzazione di macchine intrinsecamente sicure. È estremamente importante valutare i rischi in fase di progettazione. In genere, tale approccio è infatti più efficace che non fornire istruzioni all’utente per il funzionamento sicuro dell’apparecchiatura. In base alla norma EN ISO 12100-1 il processo di valutazione del rischio si articola in due parti: analisi del rischio e calcolo del rischio. Il termine analisi si riferisce all’identificazione e alla stima dei rischi, mentre il termine calcolo implica decidere se il livello di rischio è accettabile o deve essere ridotto. Il calcolo del rischio viene eseguito in base ai risultati dell’analisi e le eventuali decisioni circa la necessità di una riduzione del rischio vengono prese in base alla procedura di calcolo. È necessario eseguire il calcolo del rischio separatamente per ciascuna fonte di pericolo. La Figura 2 illustra i passi del processo di valutazione e calcolo del rischio secondo la norma ISO 14121-1: i limiti della macchina descritti nella Figura 2 comprendono limiti di utilizzo, limiti di spazio, limiti ambientali e limiti di durata. Valutare la gravità del rischio significa considerare le potenziali conseguenze, mentre la probabilità del rischio comprende la frequenza, la probabilità e la possibilità di evitare il danno.
Se il risultato dell’analisi e del calcolo del rischio descritti nella Figura 2 è SI, l’obiettivo di riduzione del rischio si considera raggiunto e la procedura di riduzione del rischio termina. In questo caso significa che la macchina ha raggiunto un adeguato livello di sicurezza secondo la Direttiva Macchine.

Se il risultato è NO, significa che il rischio è ancora inaccettabile ed è necessario applicare misure di riduzione del rischio e poi tornare al passo 2 dell’analisi del rischio.

Figura 2.
Valutazione e calcolo del rischio secondo la norma ISO 14121-1. Creare sempre la documentazione relativa al processo di valutazione del rischio per ogni singola fonte di pericolo.

Figura 2.



Riduzione del rischio

Il metodo più efficace per ridurre al minimo i rischi consiste nell'eliminarli in fase di progettazione, ad esempio apportando modifiche al progetto o al funzionamento della macchina. In ogni caso, se non è possibile eseguire il processo di riduzione del rischio e garantire la conformità ai requisiti applicando le norme armonizzate, in accordo con la Direttiva Macchine, la norma ISO 12100-1 articola il metodo per la riduzione del rischio in tre passi principali:

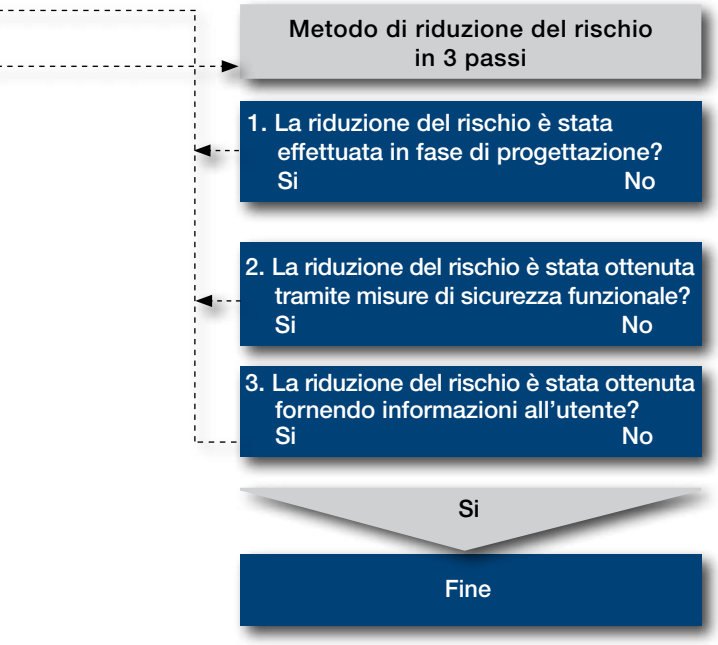
- misure per una progettazione intrinsecamente sicura (creazione di un progetto con maggiori garanzie di sicurezza, modifica del processo);
- misure di sicurezza e di protezione complementari (funzioni di sicurezza, sicurezza passiva);
- informazioni per l'uso (avvertenze, segnali e dispositivi di avviso sulla macchina, istruzioni operative, misure protettive adottate dal cliente, ad esempio corsi di formazione).

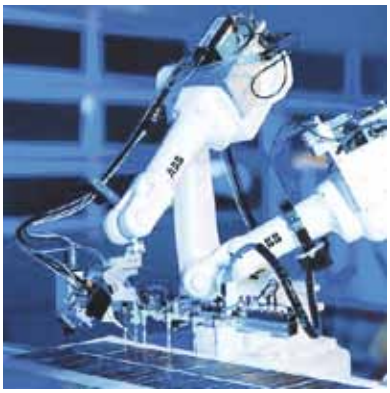
Gli utenti delle macchine e le organizzazioni possono fornire preziosi feedback sulla sicurezza e i progettisti dovrebbero sollecitarne le opinioni durante la fase di definizione delle misure protettive.

La Figura 2 rappresenta lo schema di riduzione del rischio in tre passi.
Figura 2 - Riduzione del rischio in base alla norma ISO 12100-1. Creare sempre documentazione sui rischi residui da fornire all'utente con le istruzioni operative.
L'ultimo punto (informazioni per l'uso) è anche definito gestione del rischio residuo. Il rischio residuo è quello rimanente dopo che tutte le misure di protezione sono state prese in considerazione e implementate. Poiché l'impiego della tecnologia non consente di garantire la totale assenza di rischio, alcuni rischi residui non possono comunque essere eliminati. Tutti i rischi residui devono essere riportati nelle istruzioni operative.
Gli utenti delle macchine e le organizzazioni giocano un ruolo importante nella riduzione del rischio, per questo in genere vengono informati su tutti gli aspetti importanti da chi ha progettato la macchina (costruttore). Le misure di riduzione generalmente adottate da un'organizzazione comprendono:

- introduzione di procedure di utilizzo sicure, supervisione in fase di utilizzo, sistemi di controllo dell'utilizzo;
- introduzione e utilizzo di misure di sicurezza aggiuntive;
- utilizzo di dispositivi di protezione individuale;
- formazione degli utenti;
- lettura (e applicazione conseguente) delle istruzioni operative e di sicurezza.

Dopo aver eseguito il processo di riduzione del rischio, è necessario esaminarne i risultati per verificare che le misure adottate abbiano adeguatamente ridotto il rischio a un livello opportuno.
Tale verifica può essere eseguita ripetendo il processo di valutazione.





Passo 2.
Definizione dei requisiti di sicurezza

Misure di sicurezza aggiuntive vanno specificate, terminata la fase di riduzione del rischio implemetabile durante la progettazione. Queste misure aggiuntive di riduzione del rischio si basano sulla sicurezza funzionale.

Nota.
Una funzione di sicurezza deve essere specificata, verificata (funzionamento e prestazioni di sicurezza) e convalidata separatamente per ogni fonte di pericolo identificata.

Tabella 2.
La tabella di definizione del SIL illustra la procedura da seguire per determinare l'integrità della sicurezza. Il risultato complessivo nell'esempio citato è SIL 2.

Funzioni di sicurezza

Una funzione di sicurezza rappresenta una funzione di una macchina il cui guasto può determinare un immediato aumento del rischio. Più semplicemente, comprende le misure da adottare per ridurre la probabilità che un evento indesiderato possa verificarsi e rappresentare un pericolo. Una funzione di sicurezza non fa parte del funzionamento di una macchina. In caso di errore della funzione di sicurezza, la macchina può quindi funzionare normalmente, ma il rischio di lesioni per l'operatore aumenta.

Definire una funzione di sicurezza è molto importante e include sempre due elementi:
- Azione (l'operazione da eseguire per ridurre il rischio)
- Prestazioni di sicurezza (SIL, Safety Integrity Level, o PL, Performance Level)

Esempio di funzione di sicurezza

Pericolo - un albero rotante esposto può causare lesioni ad un operatore che si avvicina molto.
Azione - per impedire che l'albero provochi lesioni personali, il motore deve arrestarsi entro un (1 s) secondo dall'apertura del dispositivo di sicurezza. Una volta definita la funzione di sicurezza che esegue l'azione, viene determinato il relativo livello di sicurezza richiesto, come descritto di seguito. Questo completa il processo di definizione della funzione di sicurezza.

Prestazioni e integrità della sicurezza

L'integrità della sicurezza misura le prestazioni di una funzione di sicurezza e indica la probabilità che tale funzione, quando richiesto, venga eseguita. L'integrità della sicurezza richiesta per una funzione viene determinata durante la fase di valutazione del rischio e viene espressa dal livello di integrità della sicurezza (Safety Integrity Level, SIL) o dal livello di prestazioni (Performance Level, PL) raggiunto, a seconda della norma utilizzata. Pur basandosi su tecniche di valutazione diverse di una funzione di sicurezza, le due norme restituiscono risultati comparabili e utilizzano termini e definizioni simili.

Come determinare il SIL richiesto (EN 62061)

Di seguito viene riportato il processo da eseguire per determinare il livello SIL richiesto:
1. Determinare la gravità delle conseguenze provocate da un evento pericoloso
2. Determinare il punteggio per la frequenza e la durata dell'esposizione al danno da parte di un operatore
3. Determinare il punteggio per la probabilità che l'evento pericoloso si verifichi durante l'intervallo di esposizione
4. Determinare il punteggio per la possibilità di evitare il danno o di limitarne la portata

Tabella 2.

Probabilità che si verifichi un danno					
Fr		**Pr**		**Av**	
Frequenza, durata		**Probabilità evento pericoloso**		**Possibilità di evitare il danno**	
<= ora	5	Molto elevata	5		
> 1h <= giorno	**5**	Probabile	4		
> giorno <= 2 settimane	4	Possibile	**3**	Impossibile	5
> 2 settimane <= 1 anno	3	Raramente	2	Possibile	**3**
> 1 anno	2	Trascurabile	1	Probabile	1
					Totale: 5 + 3 + 3 = 11

Gravità del danno		Classe SIL				
Gra				**Classe Cl**		
Conseguenze (gravità)		**3-4**	**5-7**	**8-10**	**11-13**	**14-15**
Morte, perdita di un occhio o di un braccio	4	SIL2	SIL2	SIL2	SIL3	SIL3
Permanente, perdita dita	**3**			SIL1	**SIL2**	SIL3
Reversibile, con cure mediche	2				SIL1	SIL2
Reversibile, solo primo soccorso	1	Altre misure				SIL1
						È necessaria una funzione di sicurezza SIL2.

Esempio

La Tabella 2 mostra lo schema per l'assegnazione del SIL e contiene i parametri utilizzati per determinare il punteggio relativo all'esempio di un'analisi del rischio per un albero rotante esposto.

- Un operatore risulta esposto al pericolo più volte al giorno. Frequenza (Fr) = 5
- È possibile che si verifichi l'evento pericoloso. Probabilità (Pr) = 3
- Il pericolo può essere evitato. Possibilità di evitare il pericolo (Av) = 3
- La somma di Fr, Pr e Av (5+3+3) = 11
- La conseguenza dell'evento pericoloso è la lesione irreversibile, con possibile perdita delle dita. Gravità (Se) = 3

In quest'esempio il livello complessivo, secondo la tabella 2, è SIL2. Le tabelle utilizzate per determinare il livello sono riportate nella norma.
Una volta definito il SIL è possibile implementare il sistema di sicurezza (vedere Passo 3: implementazione di un sistema di sicurezza funzionale).

Come determinare il PL richiesto (ISO 13849-1)

Il PL è un parametro alternativo al SIL. Per determinare il livello di prestazione (PL) richiesto, selezionare una delle alternative tra le categorie riportate di seguito e utilizzare il grafico (Figura 3) per creare un "percorso" per il raggiungimento di tale PL.
Nel grafico, i livelli di prestazione sono definiti come a, b, c, d, e.

- Determinare la gravità del danno:
- S1 Lieve, in genere lesione reversibile
- S2 Grave, in genere lesione irreversibile inclusa la morte

Determinare la frequenza e la durata dell'esposizione al pericolo:

- F1 Da raramente a spesso e/o tempo di esposizione breve
- F2 Da frequentemente a costantemente e/o tempo di esposizione lungo

Determinare la possibilità di evitare il pericolo o di limitare il danno causato dall'evento pericoloso:

– P1 Possibile in determinate condizioni
– P2 Poco probabile

Esempio

Analisi del rischio per un albero rotante esposto.

- La conseguenza dell'evento pericoloso è la lesione irreversibile grave. Gravità = S2.
- Un operatore risulta esposto al pericolo più volte al giorno. Frequenza = F2.
- È possibile evitare o limitare il danno causato dall'evento pericoloso. Possibilità = P1

Dall'analisi dello schema si evince che il valore del PL (PLr) è d.

Come per il SIL, le tabelle utilizzate per determinare il punteggio sono incluse nella norma e una volta definito il PLr, è possibile implementare il sistema di sicurezza.

Figura 3.

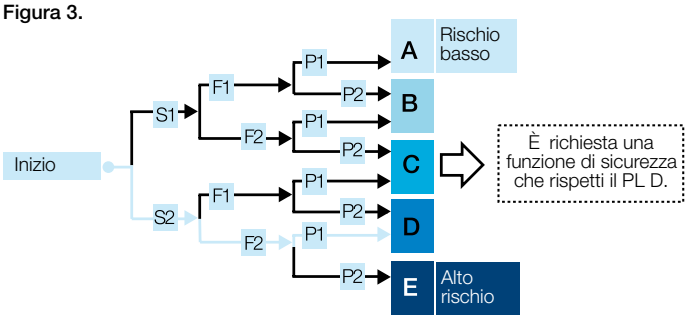


Figura 3.
Il grafico del rischio PL illustra la procedura da seguire per stabilire il livello di prestazioni di sicurezza necessario. Il risultato totale di questo esempio è PL d.

Passo 3.
Implementazione di un sistema di sicurezza funzionale

Per realizzare una funzione di sicurezza, è necessario, in fase di progettazione, rispettare il SIL/PL determinato al Passo 2: definizione dei requisiti di sicurezza. L'implementazione delle funzioni di sicurezza risulta infatti facilitata se alcuni dei calcoli relativi alla sicurezza e all'affidabilità sono già stati eseguiti e i sottosistemi sono certificati. L'implementazione e la verifica dei processi hanno carattere iterativo e vengono eseguite parallelamente.

Durante l'implementazione, lo strumento della verifica viene infatti utilizzato per garantire il raggiungimento del livello di sicurezza definito nel sistema implementato. Per ulteriori informazioni sui processi di verifica, vedere il Passo 4: verifica della sicurezza funzionale. Sono disponibili molti software di calcolo per verificare i sistemi di sicurezza funzionale. Queste applicazioni consentono di semplificare molto il processo di creazione e verifica del sistema.

Nota.
Se si utilizzano sottosistemi non certificati, può essere necessario eseguire calcoli relativi alla sicurezza per ciascuno di essi. Nelle norme EN 62061 e EN ISO 13849-1 sono incluse informazioni sul processo e sui parametri di calcolo necessari.

I passi generali necessari per implementare un sistema di sicurezza funzionale includono:

1. Definizione dei requisiti di sicurezza sotto forma di SIL e/o PL in base alla norma EN 62061 e/o EN ISO 13849-1.

2. Scelta dell'architettura da utilizzare per il sistema di sicurezza. Le norme EN ISO 13849-1 e EN 62061 forniscono architetture di base con le relative formule di calcolo.

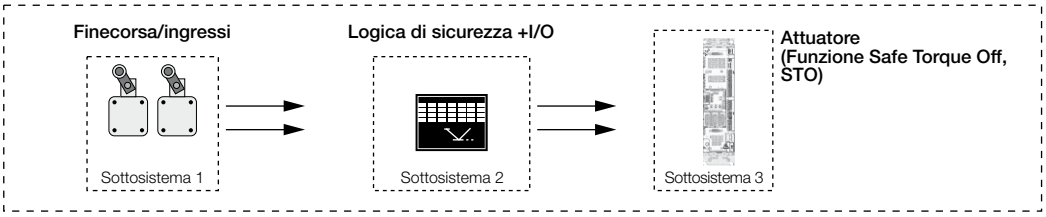
   Determinazione della categoria B, 1, 2, 3 o 4, definita nella norma EN ISO 13849-1 oppure dell'architettura indicata con A, B, C o D, definita nella norma EN 62061 per i sottosistemi e per l'intero sistema. Per ulteriori informazioni sulle architetture designate, fare riferimento alle rispettive norme.

Nota.
Per soddisfare i requisiti dell'EHSR della Direttiva Macchine, tutti i sottosistemi di un sistema di sicurezza funzionale devono avere almeno il livello SIL/PL richiesto dal sistema.

3. Realizzazione del sistema a partire da sottosistemi correlati alla sicurezza – sensore/switch, ingresso, logica, uscita e attuatore. È possibile utilizzare sottosistemi certificati (scelta consigliata) oppure eseguire calcoli relativi alla sicurezza per ciascun sottosistema. Il livello di sicurezza del sistema completo viene determinato sommando i livelli di sicurezza dei sottosistemi.
   Nella Figura 4 è indicata la struttura di una funzione di sicurezza.

4. Installazione del sistema di sicurezza. Per evitare possibilità di errori comuni dovuti a cablaggio errato, fattori ambientali o altre cause simili, è necessario installare il sistema correttamente. Un sistema di sicurezza con problemi di prestazioni dovuti a carenze nell'installazione e assai poco utile e può presentare addirittura rischi intrinseci.

Figura 4



Passo 4.
Verifica della sicurezza funzionale

Passo 4 - verifica della sicurezza funzionale

Verifica del SIL di un sistema di sicurezza (EN 62061)
Per verificare i livelli di integrità della sicurezza, è necessario dimostrare che le prestazioni di sicurezza, ossia l'affidabilità, della funzione di sicurezza creata siano superiori o uguali all'obiettivo, definito durante la fase di valutazione del rischio. Quando disponibili utilizzare sottosistemi certificati perchè il costruttore ne ha già definito i valori per determinare l'integrità della sicurezza a livello di sistema (SILCL) e l'integrità della sicurezza casuale dell'hardware (PFHd).

Per verificare il SIL di un sistema di sicurezza contenente sottosistemi certificati:

1. Determinare l'integrità della sicurezza a livello di sistema utilizzando i valori del SILCL (SIL Claim Limit) definiti per i sottosistemi.
   L'acronimo SILCL indica il valore massimo del SIL per cui il sottosistema è adatto dal punto di vista strutturale. Viene utilizzato come indicatore per determinare il SIL raggiunto.
   Il SILCL dell'intero sistema non può mai essere superiore al SILCL del sottosistema con valore più basso.

2. Calcolare l'integrità della sicurezza dell'hardware del sistema utilizzando i valori di PFHd (Probability of a dangerous Failure per Hour) definiti per i sottosistemi. L'acronimo PFHd indica il valore di guasto casuale dell'hardware utilizzato per determinare il livello SIL. Generalmente, i valori di PFHd vengono forniti dai costruttori dei sottosistemi / componenti.

3. Utilizzare l'elenco di controllo CCF (Common Cause Failure) per verificare che tutti gli aspetti necessari alla creazione dei sistemi di sicurezza siano stati presi in considerazione.
   Le tabelle relative all'elenco di controllo CCF sono reperibili nella norma EN 62061 "Allegato F".

4. Considerati i punti ottenuti in base all'elenco e dal confronto del punteggio complessivo con i valori elencati nella norma EN 62061 Allegato F, Figura 6, Tabella 4 si ottiene il coefficiente CCF (ß). Questo valore viene utilizzato per la stima della probabilità rappresentata dal PFHd.

5. Determinare il SIL raggiunto in base alla Tabella 3.

Figura 5

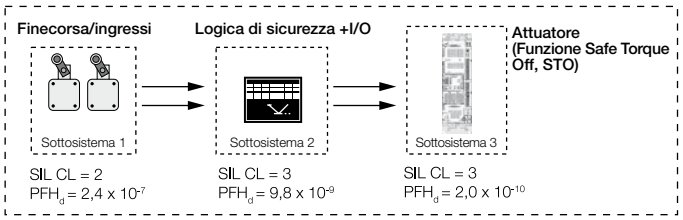
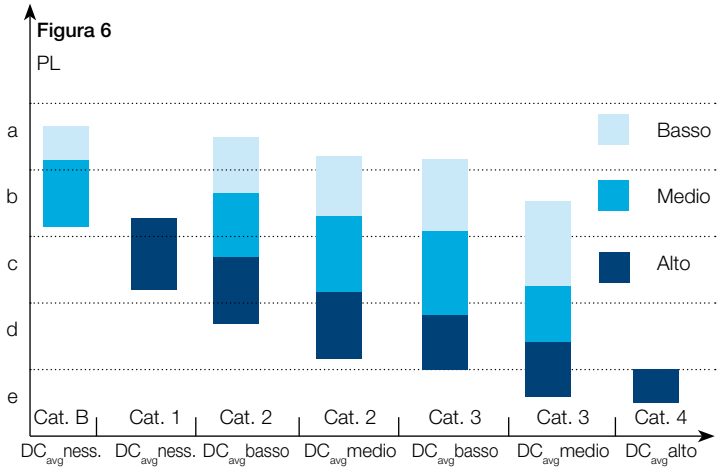


Tabella 3.

I valori rappresentati sono nella modalità alto numero di manovre.

SIL	Probabilità di guasti pericolosi per ora (1/h)
SIL 1	≥ 10^{-6} fino a < 10^{-5}
SIL 2	≥ 10^{-7} fino a < 10^{-6}
SIL 3	≥ 10^{-8} fino a < 10^{-7}

Figura 6



MTTFd.

- Basso 3 anni <MTTFd < 10 anni
- Medio 10 anni < MTTFd < 30 anni
- Alto 30 anni < MTTFd < 100 anni

Nota.

Il canale MTTFd arriva solo fino a 100 anni. Un singolo componente (sottosistema) può andare oltre.

Esempio

Verifica del SIL per il sistema di sicurezza funzionale relativo all'albero rotante. (Figura 5).

Integrità della sicurezza a livello di sistema:
SILCLsys ≤ (SIL CL sottosistema) più basso -> SIL Claim Limit 2

Integrità della sicurezza casuale dell'hardware:
PFHd = PFHd1+PFHd2+PFHd3 = 2,5 x 10-7 < 10-6

Il sistema soddisfa i requisiti del SIL 2 secondo la Tabella 3.

Tabella 3. Determinazione del SIL in base al valore del PFHd ottenuto dall'intero sistema di sicurezza. Nell'esempio precedente il sistema soddisfa i requisiti del SIL 2.

Verifica del PL del sistema di sicurezza (EN ISO 13849-1)

Per verificare il livello di prestazioni (PL), è necessario stabilire la corrispondenza tra il PL della rispettiva funzione di sicurezza e il PLr richiesto. Se più sottosistemi fanno parte di un'unica funzione di sicurezza, i relativi livelli di prestazioni devono essere uguali o superiori al livello di prestazioni richiesto per tale funzione.

Per verificare il PL di un sistema di sicurezza contenente sottosistemi certificati:

1. determinare la predisposizione del sistema a guasti CCF (Common Cause Failure) utilizzando l'elenco di controllo CCF. Il punteggio minimo richiesto è 65. (Le tabelle relative all'elenco di controllo CCF sono reperibili nella norma ISO 13849-1:2008, Allegato I).

2. Determinare il PL raggiunto in base al grafico a barre utilizzando i seguenti parametri definiti:
   - categoria;
   - MTTFd (Tempo medio prima di un guasto pericoloso);
   - DC (Copertura diagnostica).

L'acronimo MTTFd indica l'intervallo di tempo medio prima del verificarsi di un guasto pericoloso, mentre l'acronimo DC rappresenta il numero di guasti pericolosi rilevabili mediante strumenti di diagnostica.

Per ulteriori informazioni sui dettagli di calcolo, fare riferimento alla norma EN ISO 13849-1.
Immettere i valori ottenuti nel diagramma grafico PL (Figura 6) da cui è possibile determinare il PL risultante.

Esempio di verifica del PL

Verifica del sistema di sicurezza funzionale dell'albero rotante. (figura 6)

Figura 6. Verifica del PL relativo all'esempio dell'albero rotante. Nell'esempio precedente, il sistema rientra nella categoria PL d.

Per raggiungere il PLr definito nell'esempio precedente, tenere presente quanto segue:

- L'architettura designata rientra nella Categoria 3;
- Il valore di MTTFd è alto;
- Il valore medio di DC è basso.

Il sistema è conforme al valore d del PL in base alla figura 6. La Tabella 4 mostra come determinare il PL in base al valore del PFHd ottenuto per l'intero sistema di sicurezza.
Il risultato (d) è lo stesso.

Confronto tra i valori del SIL e del PL

Benché i metodi di valutazione adottati dalle due norme siano diversi è possibile confrontarne i risultati con guasto casuale dell'hardware, come mostra la Tabella 5.

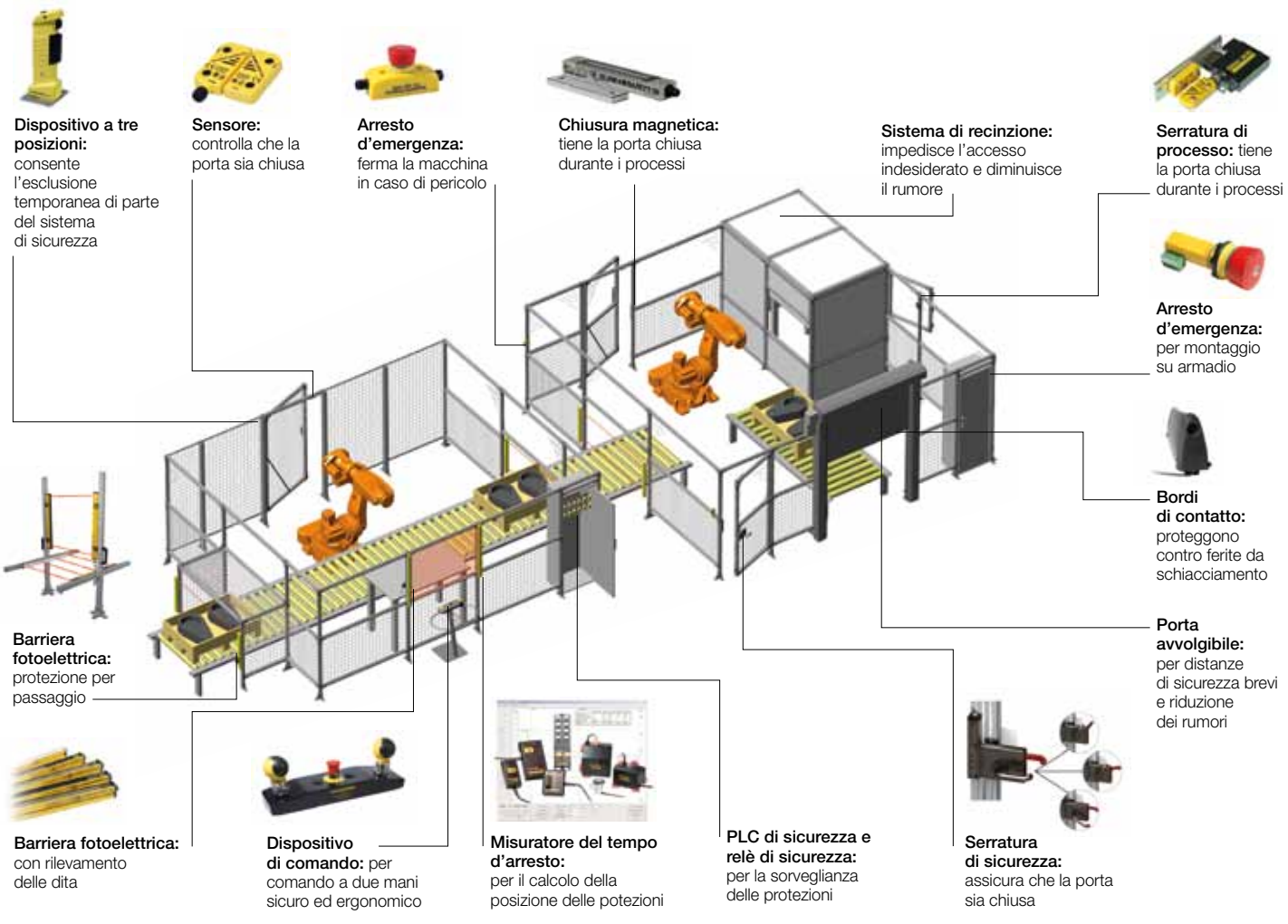
Tabella 4. Determinazione del PL in base al valore del PFH d

PL	Probabilità di guasti pericolosi per ora (1/h)
a	$\geq 10^{-5}$ fino a $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ fino a $< 10^{-5}$
c	$\geq 10^{-6}$ fino a $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ fino a $< 10^{-6}$
e	$\geq 10^{-8}$ fino a $< 10^{-7}$

Tabella 5. Confronto tra i valori di SIL e PIL

Livello integrità di sicurezza SIL	Livello di prestazioni PL
Nessuna corrispondenza	a
SIL 1	b
SIL 1	c
SIL 2	d
SIL 3	e

La gamma completa per rispondere alle esigenze di sicurezza industriale proposta da Jokab Safety, una società del Gruppo ABB.



Passi 5, 6 e 7

Per ulteriori informazioni sulla documentazione richiesta e sulle relative caratteristiche, fare riferimento ai requisiti EHSR nell'allegato I della Direttiva Macchine.

Passo 5 - convalida di un sistema di sicurezza funzionale

É necessario eseguire la convalida di ciascuna funzione di sicurezza per garantire la riduzione del rischio nel modo richiesto dal Passo 1 - valutazione e riduzione del rischio.

Per determinare la validità del sistema di sicurezza funzionale, è necessario verificare il sistema in base al processo di valutazione del rischio eseguito all'inizio della procedura per soddisfare i requisiti EHSR della Direttiva Macchine. Il sistema risulta valido se effettivamente riduce i rischi analizzati e calcolati durante il processo di valutazione.

Passo 6 - creazione della documentazione relativa a un sistema di sicurezza funzionale

La macchina viene considerata conforme ai requisiti definiti nella Direttiva Macchine solo dopo che ne è stata documentata la progettazione ed è stata creata l'apposita documentazione per l'utente.

Per essere effettivamente utile, la documentazione deve essere redatta con la massima attenzione. Il contenuto essere accurato e conciso, ma nel contempo esaustivo e facilmente comprensibile da parte dell'utente. Nella documentazione per l'utente devono essere riportati tutti i rischi residui, accompagnati dalle corrette istruzioni per l'utilizzo sicuro della macchina. Deve essere possibile accedere alla documentazione e modificarne il contenuto. La documentazione per l'utente viene fornita con la macchina.

Passo 7 - verifica della conformità

Una macchina può essere immessa sul mercato solo se il costruttore ne garantisce la conformità ai requisiti EHSR e alle norme armonizzate. È inoltre necessario verificare che la combinazione relativa a ciascuna funzione delle parti correlate alla sicurezza sia conforme ai requisiti definiti.

Per verificare la conformità con la Direttiva Macchine, è necessario dimostrare quanto segue:

- la macchina è conforme ai requisiti EHSR (Essential Health and Safety Requirements) pertinenti definiti nella Direttiva Macchine
- la macchina è conforme ai requisiti previsti da altre possibili Direttive correlate a quella sopra indicata. (La conformità a questi requisiti può essere garantita dal rispetto delle norme armonizzate pertinenti)
- il fascicolo tecnico è aggiornato e disponibile
- nel fascicolo sono incluse informazioni relative alla conformità della macchina alle disposizioni contenute nella Direttiva Macchine
- sono state applicate procedure di valutazione della conformità. (Risultano eventualmente soddisfatti i requisiti speciali relativi alle macchine elencati nell'Allegato IV della Direttiva Macchine)
- la dichiarazione di conformità CE è stata rilasciata e fornita con la macchina

Il fascicolo tecnico deve includere tutte le informazioni di progettazione, fabbricazione e funzionamento atte a dimostrare la conformità della macchina. Per ulteriori informazioni sul contenuto del fascicolo tecnico, fare riferimento all'Allegato VI della Direttiva Macchine 98/37/CE o all'Allegato VII della nuova Direttiva Macchine 2006/42/CE quando quest'ultima entrerà in vigore.
Dopo la constatazione di conformità viene apposta la marcatura CE. Le macchine che recano la marcatura CE e sono provviste della dichiarazione di conformità CE sono considerate conformi ai requisiti della Direttiva Macchine.

Glossario

CCF (Common Cause Failure, guasto di modo comune)
Condizione di guasto di più sottosistemi provocata da un unico evento. Tutti i guasti sono causati da tale evento, senza che l'uno sia tuttavia conseguenza dell'altro.

Danno
Lesione fisica o danno alla salute.

DC (Diagnostic Coverage, copertura diagnostica)
Efficacia del monitoraggio dei guasti rilevati da un sistema o un sottosistema. Equivale al rapporto tra il numero di guasti pericolosi rilevati e il numero totale di guasti pericolosi.

EHSR (Essential Health and Safety Requirements, requisiti essenziali di sicurezza e di salute)
Requisiti che la macchina deve soddisfare per conformarsi alla Direttiva Macchine dell'Unione europea e ottenere la marcatura CE. Tali requisiti sono elencati nell'Allegato I della Direttiva Macchine.

EN
Acronimo di "EuroNorm". Questo prefisso viene utilizzato in riferimento alle norme armonizzate.

Funzione di sicurezza
Funzione appositamente progettata per aggiungere sicurezza a una macchina e il cui guasto può determinare un immediato aumento dei rischi.

IEC (International Electrotechnical Commission)
Commissione elettrotecnica internazionale
Organizzazione mondiale per la definizione di standard composta da tutti i comitati elettrotecnici nazionali.
www.iec.ch

ISO (International Organization for Standardization)
Organizzazione internazionale per la normazione
Federazione mondiale di tutti gli organismi nazionali responsabili della definizione di standard. www.iso.org

Marcatura CE
Marchio di conformità obbligatorio per macchine e molti altri tipi di prodotti commercializzati nell'ambito dello Spazio Economico Europeo (SEE). Con l'apposizione della marcatura CE, il costruttore garantisce la conformità del prodotto a tutti i requisiti essenziali previsti dalle Direttive europee pertinenti.

MTTFd (Mean Time To dangerous Failure, intervallo di tempo medio prima di un guasto pericoloso)
Intervallo di tempo medio previsto prima del verificarsi di un guasto pericoloso

Altri riferimenti:

Technical guide No.10	Doc.No: 3AVA000048753 rev.B
Safety Handbook	Doc.No: 1SAC103201H0201
Prodotti di automazione ABB - Approccio alla sicurezza funzionale e all'affidabilità dei componenti elettromeccanici ed elettrici	Doc.No: 2CMT002568
Functional Safety and reliability data	Doc.No: 2CSC422007B0901
Jokab Safety. Il manuale della sicurezza	Doc.No: 1SDC110008D0901

Norma armonizzata
"Norma armonizzata" significa norma adottata da almeno uno degli Istituti di standardizzazione europei ed elencata nell'Allegato I della Direttiva 98/34/EC sulla base di una richiesta della commissione in conformità con l'art.6 della Direttiva.

Pericolo
Potenziale fonte di pericolo.

PFHd (Probability of dangerous Failure per Hour)
(probabilità di guasti pericolosi all'ora)
Valore medio indicante la probabilità che si verifichi un guasto pericoloso nel corso di un'ora. PFHd viene utilizzato per determinare il valore del SIL o del PL di una funzione di sicurezza.

PL (Performance Level)
(livello di prestazioni)
Livello (a, b, c, d, e) assegnato per specificare la capacità di un sistema di sicurezza di eseguire una determinata funzione in condizioni prevedibili.

PLr (Required Performance Level)
Livello di prestazioni richiesto, basato sulla valutazione del rischio.

Rischio
Valore corrispondente alla possibilità che il danno si verifichi combinato con il livello di gravità del danno stesso.

Sicurezza
Assenza di rischi non accettabili di lesioni o danni alla salute delle persone, sia diretti che indiretti come conseguenza di danni alle cose o all'ambiente.

Sicurezza funzionale
La sicurezza funzionale è un tipo di sicurezza che si basa su sistemi o dispositivi che operano correttamente in risposta agli input esterni.

SIL (Safety Integrity Level)
(livello di integrità della sicurezza)
Livello (1, 2, 3, 4) assegnato per specificare la capacità di un sistema di sicurezza elettrico di eseguire una determinata funzione in condizioni prevedibili. Nelle macchine vengono utilizzati solo i livelli 1, 2 e 3.

SILCL (SIL Claim Limit)
(limite SIL richiesto)
Livello di integrità della sicurezza (SIL) massimo che è possibile richiedere per un sistema elettrico, tenendo conto sia dei vincoli di architettura sia dell'integrità della sicurezza a livello di sistema.

Sottosistema
Componente di una funzione di sicurezza caratterizzato da un livello SIL o PL specifico che influisce sul livello di sicurezza dell'intera funzione. Il malfunzionamento di uno qualsiasi dei sottosistemi può determinare il guasto dell'intera funzione di sicurezza.

Contatti

www.abb.com/drives
www.abb.com/lowvoltage
www.abb.com/motors&generators
www.abb.com/plc
functional.safety@it.abb.com
www.jokabsafety.com

www.abb.com

1SDC007600B0901 - 02/2011

Power and productivity
for a better world™