

## Principi di sicurezza

### Sistemi di controllo correlati alla sicurezza

Company - MAYKIT WRIGHT LTD  
Facility - Tool room - East Factory.  
Date - 8/29/95  
Operator profile - Apprentice/Fully skilled.

Equipment Identity & Date	Directive Conformity	Risk Assessment Report Number	Accident History	Notes	Hazard Identity	Hazard Type	Action Required	Implemented and Inspected - Reference
Bloggs center lath. Serial no. 8390726 Installed 1978	None claimed	RA302	None	Electrical equipment complies with BS EN 60204 E-Stops fitted (replaced 1989)	Chuck rotation with guard open	Mechanical Entanglement Cutting	Fit guard interlock switch	11/25/94 J Kershaw Report no 9567
					Cutting fluid	Toxic	Change to non toxic type	11/30/94 J Kershaw Report no 9714
					Swarf cleaning	Cutting	Supply gloves	11/30/94 J Kershaw Report no 9715
Bloggs turret head milling m/c Serial no 17304294 Manuf 1995 Installed May 95	M/c Dir. EMC Dir	RA416	None		Movement of bed (towards wall)	Crushing	Move machine to give enough clearance	4/13/95 J Kershaw Report no 10064

Figura 31

### Sistemi di controllo correlati alla sicurezza

Cos'è un sistema di controllo correlato alla sicurezza (spesso abbreviato con la sigla SRCS – Safety Related Control Systems)? Si tratta della parte di un sistema di controllo di una macchina atta a impedire che si verifichi una condizione pericolosa. Può essere un sistema dedicato separato o essere integrato all'interno del normale sistema di controllo della macchina.

La sua complessità va da un sistema semplice, come l'interruttore di interblocco di una porta e l'interruttore per un arresto di emergenza collegati in serie fino alla bobina di controllo di un contattore di potenza o a un sistema composto che comprende sia dispositivi semplici che complessi, comunicanti attraverso software e hardware.

Per garantire la funzione di sicurezza, il sistema deve continuare a funzionare correttamente in tutte le condizioni prevedibili.

Come progettare un sistema che soddisfi questi requisiti e, una volta fatto ciò, come rappresentarlo?

Lo standard ISO 13849-1 "Parti dei sistemi di controllo correlate alla sicurezza" si occupa di tali punti. Definisce cinque categorie di riferimento utili per descrivere le prestazioni dei sistemi di controllo correlati alla sicurezza (vedere la figura 32 per un riepilogo di tali categorie).

**Nota:** Nota 1: la categoria B non prevede misure speciali per la sicurezza ma costituisce la base per le altre categorie.

**Nota:** Nota 2: più errori provocati da una causa comune o inevitabili conseguenze del primo guasto devono essere considerati quale un solo guasto.

**Nota:** Nota 3: la revisione dei guasti può essere limitata a una combinazione di due errori se questo può essere giustificato, ma nel caso di circuiti complessi (ad esempio circuiti a microprocessori) è possibile che sia necessario prendere in considerazione più errori contemporaneamente.

Come decidere di quale categoria si ha bisogno? Per tradurre questi requisiti nella specifica di un progetto di sistema occorre interpretare i requisiti di base.

Spesso si pensa erroneamente che la categoria 1 fornisca la minore protezione e che la categoria 4 garantisca quella migliore. *Questo non è il principio che regola le categorie.* Si tratta di punti di riferimento che descrivono le prestazioni funzionali di diversi metodi per garantire la sicurezza dei sistemi di controllo correlati alla sicurezza e dei relativi componenti.

#### La categoria 1 è volta alla PREVENZIONE degli errori

Si ottiene utilizzando principi progettuali, componenti e materiali adeguati. La semplicità del principio di funzionamento e del progetto, e le caratteristiche stabili e prevedibili del materiale, sono i punti essenziali di questa categoria.

Le categorie 2, 3 e 4 richiedono che se il guasto non può essere prevenuto, deve essere RILEVATO (e quindi devono essere presi i provvedimenti necessari). Il monitoraggio e il controllo sono essenziali per queste categorie. Il solito (ma non l'unico) metodo di monitoraggio consiste nel replicare le funzioni essenziali per la sicurezza (ad esempio la ridondanza) e confrontare il funzionamento.



## Principi di sicurezza

### Sistemi di controllo correlati alla sicurezza

Riepilogo dei requisiti	Comportamento del sistema	Principio
<p><b>CATEGORIA B</b> (vedere la nota 1)</p> <ul style="list-style-type: none"> <li>- Le parti correlate alla sicurezza del sistema di controllo della macchina e/o l'attrezzatura protettiva, oltre ai relativi componenti, devono essere progettati, costruiti, selezionati, assemblati e combinati in conformità con gli standard pertinenti affinché resistano alle influenze previste.</li> </ul>	Quando si verifica un guasto, questo può comportare una perdita della funzione di sicurezza.	Per selezione dei componenti (verso la PREVENZIONE Per errori)
<p><b>CATEGORIA 1</b></p> <ul style="list-style-type: none"> <li>- Si applicano i requisiti della categoria B, inoltre occorre usare componenti di sicurezza e principi di sicurezza di comprovata efficienza.</li> </ul>	Vedi categoria B, ma con maggior affidabilità della funzione correlata alla sicurezza (maggiore è l'affidabilità, minore è la possibilità di guasto)	
<p><b>CATEGORIA 2</b></p> <ul style="list-style-type: none"> <li>- Si applicano i requisiti della categoria B inoltre occorre usare principi di sicurezza di comprovata efficienza.</li> <li>- Le funzioni di sicurezza devono essere controllate all'avviamento della macchina e periodicamente dal sistema di controllo della macchina. Qualora sia rilevato un guasto deve essere creato uno stato sicuro e, se ciò non fosse possibile, deve essere lanciato un allarme.</li> </ul>	<p>La perdita della funzione di sicurezza è rilevata dal controllo.</p> <p>Il verificarsi di un guasto può comportare la perdita della funzione di sicurezza tra gli intervalli di controllo.</p>	Per struttura (verso il RILEVAMENTO degli errori)
<p><b>CATEGORIA 3</b> (vedere le note 2 e 3)</p> <ul style="list-style-type: none"> <li>- Si applicano i requisiti della categoria B e principi di sicurezza di comprovata efficienza.</li> <li>- Il sistema deve essere progettato in modo che un singolo guasto in una sua parte qualsiasi non comporti la perdita della funzione di sicurezza.</li> </ul>	<p>Quando si verifica un singolo guasto, la funzione di sicurezza viene sempre eseguita.</p> <p>Alcuni ma non tutti gli errori vengono rilevati.</p> <p>Un accumulo di errori non rilevati può comportare la perdita della funzione di sicurezza.</p>	
<p><b>CATEGORIA 4</b> (vedere le note 2 e 3)</p> <ul style="list-style-type: none"> <li>- Si applicano i requisiti della categoria B inoltre occorre usare principi di sicurezza di comprovata efficienza.</li> <li>- Il sistema deve essere progettato in modo che un singolo guasto in una sua parte qualsiasi non comporti la perdita della funzione di sicurezza.</li> <li>- Il singolo guasto viene rilevato in concomitanza o prima della richiesta successiva alla funzione di sicurezza. Se tale rilevamento non è possibile, l'accumulo di errori non deve comportare la perdita della funzione di sicurezza.</li> </ul>	<p>Quando si verificano gli errori, la funzione di sicurezza viene sempre eseguita.</p> <p>Gli errori vengono rilevati in tempo utile per prevenire la perdita della funzione di sicurezza.</p>	

Figura 32

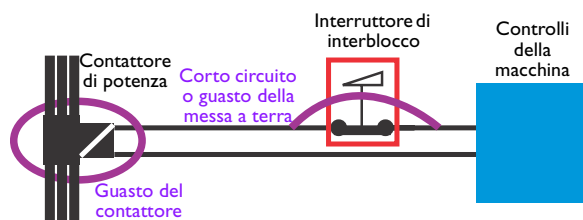


Figura 33

L'esempio della figura 33 rappresenta un sistema semplice, composto dall'interruttore di interblocco di una porta di protezione collegato in serie con la bobina di controllo di un contattore di potenza.

Se si tiene conto che l'obiettivo è ottenere l'affidabilità totale senza la possibilità che si verifichi un guasto che conduca a una condizione pericolosa, quali categorie non sono appropriate?

Se si fa riferimento alla figura 32, quale tipo di categoria è la più adatta? la prevenzione degli errori o il loro rilevamento?

Il primo passaggio sta nel suddividere il sistema nei suoi componenti principali e analizzarne le modalità di potenziale avaria.



## Principi di sicurezza

### Sistemi di controllo correlati alla sicurezza

In questo caso i componenti sono i seguenti:

1. Interruttore di interblocco.
2. Contattore.
3. Cablaggio.

L'**interruttore di interblocco** è un dispositivo meccanico. Il compito che svolge è semplice: aprire i contatti quando viene aperta una porta di protezione. Soddisfa i requisiti della categoria 1 e, usando i corretti principi di progettazione e materiali, si può dimostrare che, se usato entro i parametri operativi definiti, non provocherà errori che conducano a una condizione pericolosa. Ciò è possibile perché il dispositivo è relativamente semplice e ha caratteristiche prevedibili e attestabili.

Il **contattore** è un dispositivo leggermente più complesso e può comportare alcune possibilità teoriche di guasto. I contattori realizzati da produttori affidabili sono dispositivi estremamente affidabili. Le statistiche mostrano che i guasti sono rari e generalmente possono essere attribuiti alla cattiva installazione o manutenzione.

I contatti dei contattori devono sempre essere protetti da un dispositivo di apertura in caso di sovracorrente che ne prevenga la saldatura.

I contattori devono essere ispezionati regolarmente per controllare l'eventuale formazione di crateri eccessivi o la presenza di connessioni allentate che possono provocare surriscaldamento e deformazione.

È necessario verificare che il contattore sia conforme agli standard del caso che riguardano le caratteristiche e le condizioni d'uso richieste.

Se si tiene conto di tutti questi fattori, è possibile mantenere al minimo le possibilità di guasto. Ma in alcune situazioni anche questa piccola possibilità non è accettabile e per aumentare il livello di sicurezza occorre usare la replicazione e il monitoraggio.

Anche il **cablaggio** che collega i componenti deve essere preso in considerazione. I guasti di corto circuito o di messa a terra non rilevati possono provocare una condizione pericolosa, ma se è correttamente progettato e installato in conformità con standard quali IEC/EN 60204, le possibilità di guasto vengono notevolmente ridotte.

Questo sistema può fornire un elevato livello di sicurezza adatto a molte situazioni. Sia il contattore che il cablaggio sono passibili di guasti improbabili, sebbene teoricamente possibili. In alcuni casi è possibile, prendendo le dovute precauzioni (ad esempio relative alla protezione dei cavi e all'instradamento) eliminare tutte le possibilità di guasto. Se questo non è possibile, generalmente le tecniche relative alle categorie 2, 3 e 4, quali la replicazione e il monitoraggio, sono più pratiche e convenienti.

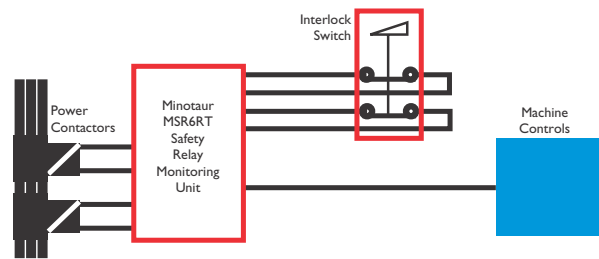


Figura 34

La figura 34 mostra un sistema che soddisfa i requisiti della categoria 3. Un'unità di monitoraggio a relè Guardmaster MINOTAUR MSR6RT è usata per monitorare un circuito di controllo a due canali. Un qualsiasi guasto che si verifica sul cablaggio o i contattori sarà rilevato da Minotaur alla richiesta successiva alla funzione di sicurezza. **NOTA:** sebbene l'interruttore di interblocco ora abbia contatti a polo doppio, è ancora un **dispositivo** che soddisfa i requisiti della categoria 1, facente parte di un **sistema** che soddisfa i requisiti della categoria 3.

La domanda successiva è quando e in che grado occorre attuare tali misure?

La risposta più semplice è dire che dipende dal risultato della valutazione del rischio. Questo approccio è certamente corretto, ma occorre anche comprendere che bisogna tenere conto di tutti i fattori e non solo del livello di rischio presso il punto pericoloso. Ad esempio, si può pensare che se la stima del rischio mostra un elevato livello di rischio, l'interruttore di interblocco deve essere raddoppiato e monitorato. Tuttavia, in molte circostanze, il dispositivo, vista la sua applicazione, la struttura del progetto e la semplicità, non presenterà guasti pericolosi e non vi saranno guasti non rilevati da monitorare.

Di conseguenza, **il tipo di categoria usata dipende sia dalla valutazione del rischio sia dalla natura e dalla complessità del dispositivo o del sistema**. È inoltre chiaro che nel caso in cui un sistema completo soddisfi i requisiti della categoria 3, ad esempio, può comprendere dispositivi della categoria 1.

Se vi è la possibilità che si verifichino guasti, maggiore è il livello di rischio, calcolato durante la stima del rischio, più è giustificato l'uso di misure che li prevengano o li rilevino. Il tipo di categoria deve essere selezionato in modo da rappresentare il metodo più adatto ed efficace per ottenere tale risultato. È importante ricordare che la stima del rischio è un fattore, ma anche la natura del dispositivo o del sistema protettivo e le caratteristiche operative della macchina devono essere prese in considerazione.

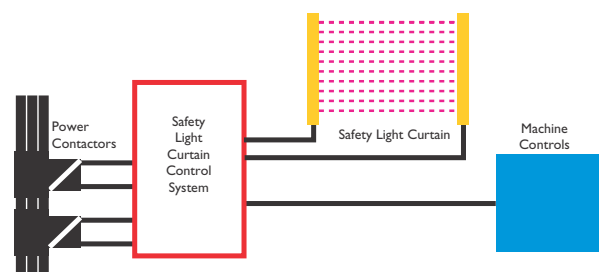


Figura 35

