Prevenzione e innovazione

Stato dell'arte

Emilio Moroni

Le domande generate dalle innovazioni richiedono nuove risposte, che possono discostarsi dalle richieste delle attuali norme di sicurezza. Peraltro, i soli test sul prodotto finale non sono sufficienti. L'esame Ce effettuato dagli Organismi Notificati richiede il supporto di tecniche di sicurezza durante il processo di sviluppo, o meglio, durante l'intero ciclo di vita di un prodotto. Sono quattro le pietre miliari per concordare, eseguire e documentare i passi di collaudo durante la verifica di sistemi di sicurezza computerizzati: definizione delle specifiche, sviluppo del progetto, produzione di un prototipo, completamento del campione di prodotto sperimentale.

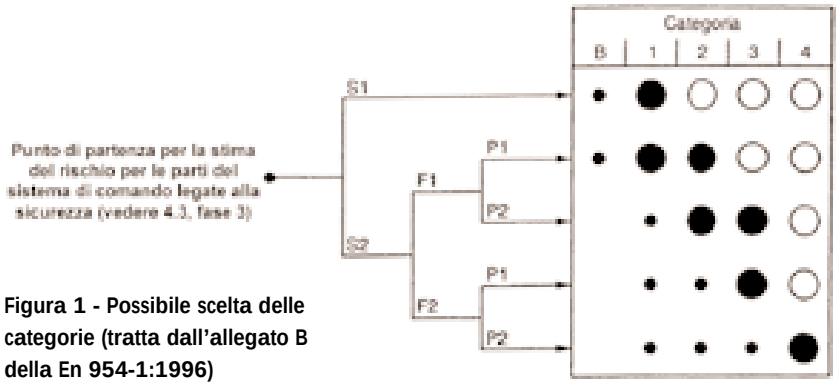

Figura 1 - Possibile scelta delle categorie (tratta dall'allegato B della En 954-1:1996)

Keyword

Innovazione tecnologica nella sicurezza delle macchine, limiti della normativa

Le condizioni di lavoro nel settore del servizio industriale sono caratterizzate in modo crescente da tre elementi. I prodotti sono fabbricati sempre più secondo la richiesta del cliente. Allo stesso tempo, comunque, la produzione richiede l'uso di impianti di complessità sempre maggiore e che includono misure di sicurezza integrate e flessibili. In secondo luogo la società è modellata dall'aumento del collegamento in rete di luoghi di lavoro individuali. Anche le bozze di progetto preliminari sono presentate su computer e sono poi scambiate fra tutti i gruppi del processo produttivo, tramite complessi sistemi di comunicazione, per completare i dettagli. Una terza caratteristica è la concentrazione del capitale. Gli sviluppi del prodotto sono molto costosi ma i prezzi dei prodotti di massa continuano a diminuire. Le tre caratteristiche di innovazione nel settore del servizio industriale hanno un impatto sulle nuove tecniche di prevenzione.

L'innovazione nel settore industriale

La moderna produzione industriale è sintetizzata dall'espressione "just in time". I prodotti sono fabbricati all'istante su richiesta del cliente; i componenti necessari non sono tenuti a magazzino, ma realizzati come e quando servono. Ciò richiede un processo produttivo flessibile, direttamente congiunto alla richiesta dei clienti. A causa dell'assenza di parti stoccate, e a causa degli obblighi della produzione individuale, il rifornimento deve essere fatto per la modifica singola dei dispositivi di sicurezza del macchinario. Una seconda conseguenza degna di nota, della produzione "just in time" è che, a causa della mancanza di scorte, tutti i processi di lavoro sono portati a termine con ritmi temporali incredibili. L'uso di tecniche a sicurezza integrata permette di gestire gli interventi senza intralciare la produzione. In un progetto complesso diffuso su rete, le conseguenze dell'eliminazione di un errore non sono immediatamente evidenti per i reparti responsabili della manutenzione. Barriere fisse e ripari protettivi sono di ostacolo alla manutenzione sicura della macchina.

Come già indicato, le moderne attrezzature di produzione non sono più costituite da un insieme di macchine singole, ma da impianti collegati. Il materiale grezzo entra nella fabbrica da un lato e il prodotto finito esce dall'altro. Oltre all'influenza sulla produzione, l'aumento della diffusione su rete incide su ogni aspetto delle condizioni di lavoro. La diffusione su rete dei singoli posti di lavoro ha reso l'intero processo produttivo più com-

plesso. L'aumento della complessità dà luogo a nuovi rischi. Un'ulteriore caratteristica della produzione diffusa su rete è la concentrazione di funzionalità nel software, il che aumenta a sua volta la complessità.
I prodotti industriali sono diventati più facili da usare, più piccoli e nello stesso tempo più a buon mercato nel corso degli ultimi quindici anni. Questo sviluppo è legato all'introduzione della tecnologia dei microprocessori. Funzioni che nel passato erano compiute da hardware complesso e spesso costoso sono ora incluse in moduli software. Lo stesso software porta a un forte aumento nei costi di sviluppo, accoppiato a una riduzione di prezzo dell'articolo prodotto in massa. La stessa situazione riguarda la tecnologia di sicurezza. Negli ultimi quindici anni i prezzi dei componenti di sicurezza sono rapidamente caduti, mentre i costi di sviluppo continuano ad aumentare. Il risultato è una prevenzione orientata allo sviluppo, a partire dal concetto iniziale di un progetto di produzione, procedendo per i successivi gradi di sviluppo, fino all'attività di routine e manutenzione.

Prevenzione orientata allo sviluppo

In futuro saranno essenziali i seguenti passi verso una prevenzione orientata allo sviluppo: i provvedimenti dettagliati saranno sostituiti da obiettivi definiti; ciò aumenterà a sua volta il bisogno di consulenza, il supporto al processo di sviluppo sostituirà il collaudo di un prodotto e la ricettività verso nuovi sviluppi sostituirà la pura e semplice conformità alle norme. A causa della veloce evoluzione e della natura complessa dello sviluppo del processo di produzione, i particolari della tecnica di sicurezza non possono più a lungo essere standardizzati, se una norma deve restare comprensibile in ogni parte, e le sue disposizioni devono essere valide almeno da cinque a dieci anni. È molto più importante che siano definiti obiettivi che influenzano il modo di pensare di un progettista di tecnologia di sicurezza, o anche di un tecnico della manutenzione che lavora con tale tecnologia. Obiettivi di questo tipo devono essere formulati in modo tale da restare validi indipendentemente dalla specifica soluzione tecnica [1].
Un esempio mostrerà come un obiettivo definito dalla Direttiva Macchine è stato trasformato in una norma favorevole all'innovazione. Per quanto riguarda l'argomento dei circuiti di comando, il Requisito Essenziale di Sicurezza e Salute (Res) 1.2.7 della Direttiva Macchine "*avaria del circuito di comando*" stabilisce: "*un'anomalia della logica del circuito di comando, o un'avaria o un deterioramento del circuito di comando non devono creare situazioni pericolose*".
La norma En 954-1: 1996 [2] traduce questa richiesta fondamentale in cinque *categorie* di controllo (denominate B, 1, 2, 3 e 4). La Figura 1 mostra come la *categoria* sia determinata da una semplice stima del rischio basata sulla gravità della lesione (S1 lieve, S2 grave), la frequenza e/o tempo di esposizione al pericolo (F1 rara, F2 elevata), la possibilità di evitare il pericolo (P1 possibile, P2 scarsamente possibile). Questo concetto molto forte ha permesso, per circa dieci anni, indipendentemente dalla tecnologia impiegata, controlli relativi alla sicurezza, che vanno da un circuito con un piccolo numero di componenti a complessi controlli computerizzati.
I moderni sistemi di comando e controllo introducono problematiche che non sono sufficientemente trattate dai Res. Questo si evidenzia in modo particolare esaminando mac-

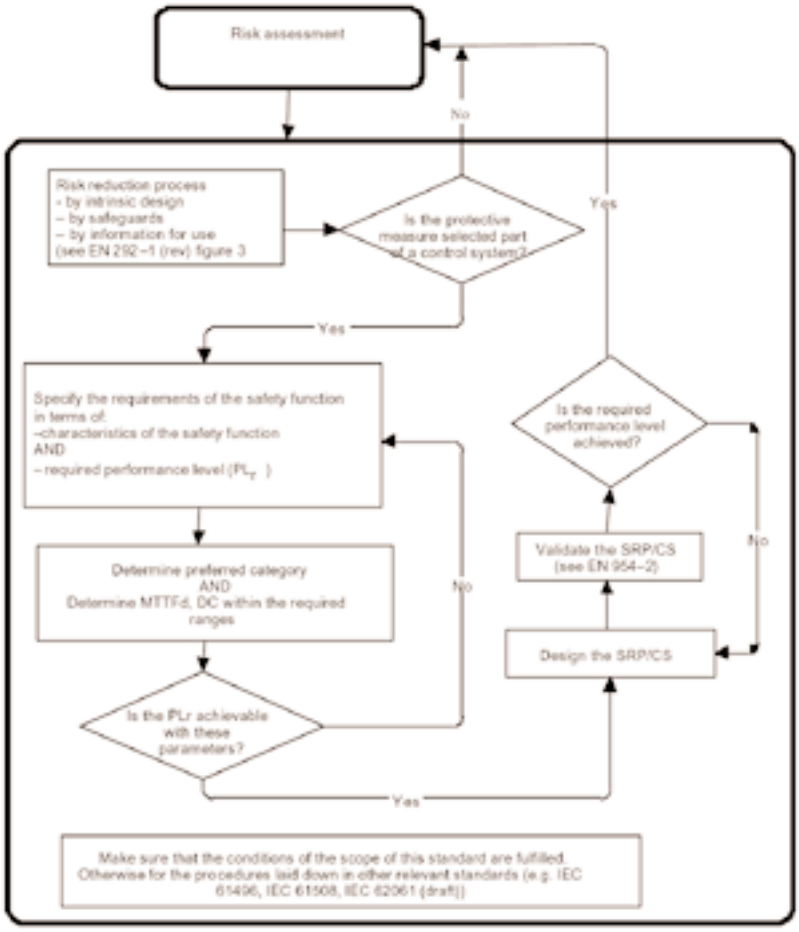

Figura 2 - Processo iterativo per il progetto di funzioni di sicurezza

chine che incorporano dispositivi e Sistemi Elettronici Programmabili (Pes) che svolgono funzioni di sicurezza. L'approccio della Direttiva Macchine per quelle parti che vengono considerate "stato dell'arte" è di raccomandare, nel limite del possibile, che siano progettate e realizzate per tendere verso gli obiettivi prefissi dai Res [3]. Se da un alto questa è sicuramente una posizione ragionevole dal punto di vista legislativo in previsione dei futuri sviluppi tecnologici, dall'altro porta inevitabilmente a una necessità di tecniche per la valutazione[1] e stima[2] del rischio che assicurino i progettisti, gli utilizzatori e gli organi di controllo che le misure applicate garantiscono una sufficiente riduzione del rischio. I principi enunciati nelle norme En 1050 [4] ed En 292 [5] sono stati ben definiti ed elaborati, ma manca una guida alla loro applicazione. In pratica possono essere utilizzate tecniche diverse, ma spesso rimangono alcune ambiguità circa i loro criteri e quindi i risultati ottenuti sono inconsistenti. Il requisito chiave di qualsiasi progetto è quello di avere specifiche chiare e correttamente definite, in modo tale che il progettista possa rispettare gli obiettivi stabiliti.

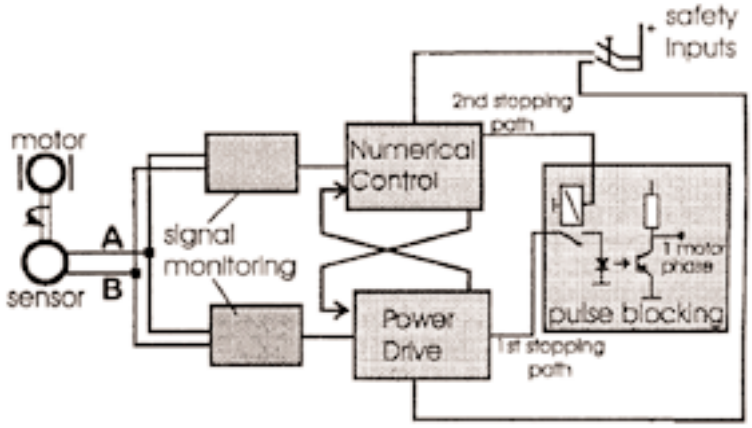

Figura 3 - Architettura di comando di una macchina utensile

L'abilità di un sistema di comando nello svolgere funzioni di sicurezza può essere espressa in termini di prestazioni come misura della sicurezza funzionale, considerata parte della sicurezza generale della macchina. La Direttiva Macchine è basata in generale sulle pratiche stabilite nel progetto dei sistemi di comando delle macchine, come ad esempio il circuito di interblocco delle protezioni. Queste misure di protezione vengono comunemente studiate e realizzate solo dopo che il progetto per la parte funzionale del sistema di comando è stata realizzata. Tuttavia questo approccio sta lasciando il passo a soluzioni integrate con il sistema di comando, grazie all'uso dell'elettronica. La parte di circuito che realizza queste soluzioni spesso comprende complessi sistemi elettronici nei quali: il modo di guasto di almeno un componente non è ben definito, o il funzionamento in condizioni di guasto non può essere completamente determinato, o non esistono dati sufficienti (provenienti dal campo) per determinare il tasso di guasto.
Complessi dispositivi elettronici, programmabili e non, come circuiti a larga (Lsi) o larghissima (Vlsi) scala di integrazione, circuiti integrati per specifiche applicazioni (Asic), controllori logici programmabili (Plc), microcontrollori ecc., sono sempre più utilizzati. In pratica risulta estremamente difficile stabilire la "sicurezza" delle loro prestazioni.
A questo scopo due norme possono essere utilizzate come riferimento per l'analisi dei sistemi elettronici con funzioni di sicurezza: la Iec 62061 [6] e la E 954-1: 1996.
La IEC 62061, sviluppata dal gruppo di lavoro Iec/Tc44/Wg7, dovrebbe rappresentare l'implementazione nel settore delle macchine della pubblicazione base Iec 61508 [7]. Entrambe le norme indicano un approccio strutturato attraverso il progetto, ma mentre la En 954 è rivolta a tutte le tecnologie utilizzate nei sistemi di comando la Iec 62061 è principalmente (ma non esclusivamente) indirizzata verso le applicazioni elettriche, elettroniche ed elettroniche programmabili (E\E\PE). Entrambe richiedono che le funzioni di sicurezza vengano classificate: la Iec 62061 prevede che le funzioni di sicurezza rispettino un determinato livello di sicurezza (Safety Integrity Level: Sil), mentre la En 954-1 classifica le parti del sistema di comando in categorie. C'è una significativa differenza nel modo in cui i Sil e le categorie sono stati concepiti e definiti che porta ad una difficile comparazione in prospettiva di sviluppare una strategia capace di unirne i contenuti.

Problematiche della norma En 954-1: 1996

Di seguito viene riportato un elenco di osservazioni nate dal processo di sviluppo e convalida di parti dei sistemi di comando con funzione di sicurezza.
• Per raggiungere un adeguato livello di sicurezza è necessario fornire maggiori avvertenze circa la convalida.
• I requisiti fondamentali delle diverse categorie sono semplici da seguire e legati alla tolleranza dei guasti. Tuttavia, i requisiti ad

[1] En 292-1, punto 3.8 valutazione del rischio: valutazione globale della probabilità e della gravità di possibili lesioni o danni alla salute in una situazione pericolosa per scegliere le adeguate misure di sicurezza.
[2] Linee guide lee: la stima del rischio può essere considerata quella parte del processo di valutazione dei rischi che stabilisce il livello di rischio in termine di conseguenze e probabilità di accadimento.

esempio della categoria 3 non prevedono il rilevamento di tutti i guasti pericolosi, ma solo di alcuni. È quindi necessaria una decisione soggettiva circa i guasti che debbono o meno essere individuati.

• La norma è stata concepita per individuare mezzi pratici di valutazione e attuazione. Sfortunatamente, quello che sembra a prima vista un metodo facilmente praticabile diventa estremamente soggettivo quando applicato. L'allegato B è l'unico modo per determinare la categoria richiesta. A causa della natura soggettiva dell'allegato B, persone differenti possono giungere a conclusioni differenti nel determinare la categoria poiché non esistono mezzi oggettivi. Deve quindi essere fornito un maggior numero di dettagli all'utilizzatore di tale allegato. Ad esempio possono essere effettuate ricerche per stabilire la probabilità di evitare il danno in diverse applicazioni industriali e in differenti condizioni, disponendo quindi i dati in tabelle.

• I principi della norma si basano sui guasti singoli e multipli dei componenti. Questo sembra essere un modo semplici per definire la prestazione della funzione di sicurezza. Tuttavia, ci sono molti guasti, i quali in combinazione, possono portare ad un pericolo. Molti di questi guasti vengono considerati improbabili, altamente improbabili o addirittura impossibili e possono essere molto differenti quando si utilizzano tecnologie diverse. Poiché la decisione di escludere questi guasti dall'analisi può essere soggettivo, è necessario considerare il tasso di guasto tramite database o l'esperienza legata al campo.

• La norma non fornisce mezzi per valutare e assicurarsi dell'integrità del software.

• La norma accenna solamente alla manutenzione. In un sistema di protezione (il quale può intervenire anche raramente), è importante svolgere regolarmente test manuali di prova (in assenza di una diagnostica automatica) per verificarne l'integrità.

• La En 954-1 è una norma di progetto e non fornisce indicazioni circa la realizzazione del sistema progettato. Un sistema ottimamente progettato può avere una ridotta integrità se realizzato in maniera non accurata. Ad esempio, un sistema multi-canale, il cui cablaggio è stato separato usando cavi unifilari allo scopo di evitare guasti di causa comune (esempio cortocircuito), potrebbe avere erroneamente i cavi raggruppati insieme tramite fascette. Lo stadio di convalida non tiene conto delle variazioni che possono avere origine da specifiche costruttive non sufficientemente dettagliate. Il sistema di qualità del costruttore deve quindi assicurare che non vi siano deviazioni dal campione esaminato.

• Considerando i sotto-sistemi come componenti singoli e applicando a essi il principio dell'esclusione del guasto, è possibile determinare una categoria senza il bisogno di calcoli complessi. Tuttavia, il tasso di guasto di un complesso sotto-sistema può essere notevolmente maggiore di quello di un singolo componente. Quindi la categoria di un sotto-sistema a doppio canale non può essere considerata equivalente a quella di un componente di un sistema a doppio canale.

Ad esempio un interblocco realizzato tramite due relè non può essere confrontato con uno basato su due complessi Plc, anche se entrambi raggiungono la categoria 3. Quindi due sistemi con la medesima categoria possono essere considerati equivalenti solamente se usano la stessa tecnologia e un numero paragonabile di componenti.

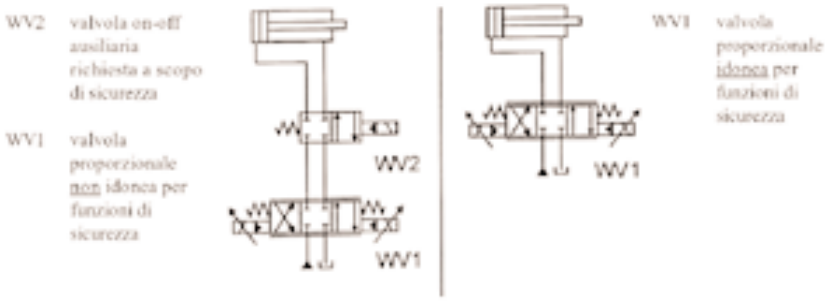

Figura 4 - Tecnologia di sicurezza esterna (a sinistra) e integrata (a destra) alle valvole proporzionali

• Fattori diversi distorcono il significato delle categorie introducendo un'erronea gerarchia. Ad esempio:

- la norma è basata sul funzionamento del sistema in presenza di guasti. Le moderne tecnologie permettono sofisticate diagnostiche automatiche in grado di rilevare quasi il 100% dei guasti. Un sofisticato sistema a canale singolo può avere un integrità maggiore di un semplice sistema multi-canale;
- un sistema altamente affidabile, basato su una tecnologia semplice, al quale deve essere assegnata una categoria 1 a causa del suo stato di canale singolo, può in pratica avere un integrità confrontabile, o addirittura maggiore, di un sistema multi-canale che utilizza una tecnologia complessa, e quindi difficoltosa da convalidare. La possibilità di una erronea valutazione può essere minimizzata considerando gli aspetti probabilistici allo scopo di stimare il reale valore di riduzione del rischio.

In conclusione è possibile affermare che la En 954-1: 1996 tenta di evitare la necessità di

un calcolo quantitativo utilizzando una metodologia semplice: un grafico per la stima del rischio[3]. L'applicazione è legata quindi a sistemi di comando estremamente semplici e richiede un uso soggettivo delle conoscenze tecniche. La norma enfatizza il fatto che il grafico di rischio non è la valutazione dei rischi, ma un approccio basato sui rischi per determinare la categoria appropriata per le parti dei sistemi di comando con funzioni di sicurezza. La guida dell'allegato B "*dovrebbe essere considerata come parte della valutazione dei rischi fornita dalla En 1050 e non come sostituzione di essa*". Non vi è alcun tentativo di classificare i rischi.
La norma non considera la probabilità con cui avviene un evento pericoloso e quindi non è possibile utilizzare alcun fattore per la riduzione del rischio. Tuttavia questo può essere usato per giustificare l'uso di una categoria diversa a quella data dall'uso del grafico di rischio. La gravità della lesione è selezionata in termini di conseguenze "consuete" piuttosto che delle peggiori conseguenze. Solamente due livelli di gravità comportano una scarsa differenziazione.

La revisione della norma En 954-1

Dalle considerazioni espresse al paragrafo precedente emerge la necessità di un approccio quantitativo della norma En 954-1 basato su dati realistici. Ciò è ancor più vero quando le parti dei sistemi di comando che svolgono funzioni di sicurezza (Safety Related Part of Control Systems: Srp/Cs) possono essere realizzate tramite hardware e software, essere separate od integrate al sistema e possono svolgere solamente funzioni di sicurezza oppure essere una parte di una funzione operativa (esempio un comando a due mani utilizzato come mezzo per l'avvio del ciclo). La loro progettazione e convalida deve essere parte integrante del processo di valutazione e riduzione dei rischi.
La revisione della norma [8] considera l'abilità di una parte del sistema di comando nello svolgere funzioni di sicurezza in condizioni prevedibili, classificandola in cinque Livelli di Prestazione di sicurezza (PL) definiti in termini di probabilità di guasti pericolosi del sistema. Quest'ultima dipende da diversi fattori: la struttura del sistema (categoria), il meccanismo di rilevamento dei guasti (Copertura Diagnostica - DC), l'affidabilità dei componenti (tempo medio al guasto pericoloso - MTTFd; guasto di causa comune - CCF), il processo di sviluppo, le condizioni ambientali e le procedure operative.
Di seguito viene fornita una minima descrizione dei fattori che concorrono all'individuazione del Livello di Prestazione richiesto (PL_r), come riportato in Figura 2.

Livello di prestazione (Performance Level - PL)
Abilità nello svolgere una funzione di sicurezza in condizioni prevedibili allo scopo di ottenere la riduzione del rischio prevista. I livelli sono divisi in cinque gruppi (Tabella 1).

Tabella 1 - Livelli di prestazione (PL)

Livello di prestazione	Probabilità media di un guasto pericoloso per ora [1/h]
a	$10^{-5} \le PDF < 10^{-4}$
b	$3.10^{-6} \le PDF < 10^{-5}$
c	$10^{-6} \le PDF < 3.10^{-6}$
D	$10^{-7} \le PDF < 10^{-6}$
E	$10^{-8} \le PDF < 10^{-7}$

Livello di prestazione richiesto (Required Performance Level - PL_r)
Livello di prestazione per raggiungere la riduzione richiesta del rischio (Figura 2) per ogni funzione di sicurezza.

Tempo medio al guasto pericoloso (Mean Time To Dangerous Failure - MTTFd)
Valor medio del tempo operativo durante il quale si presume che un singolo canale di un sistema non presenti guasti pericolosi. Il valore del MMTFd per ogni canale (singolo o di un sistema ridondante) è definito in base alla Tabella 2.

Tabella 2 - Tempo medio al guasto pericoloso

Indicaz. del MMTFd	Valori di MTTFd
Basso	3 anni ≤ PDF < 10 anni
Medio	10 anni ≤ PDF < 30 anni
Alto	30 anni ≤ PDF < 100 anni

Esistono diversi data-base che forniscono i valori di MTTFd per componenti elettrici/ elettronici (Tabella 3). Prendendo ad esempio la raccolta tedesca Sn 29500 si evincono i seguenti valori per i transistori (usati come interruttori).

[3] Il grafico di rischio riportato nell'allegato B della En 954-1:1996 è un adattamento dell'approccio indicato nella Din V19250 Tecnologia di comando - Aspetti fondamentali di sicurezza da considerare per gli equipaggiamenti di misura e comando.

Tabella 3 - Valori di MTTFd per transistori

Componenti	Esempi	MTTF[anni]	MTTFd [anni]		Osservazioni
			Tipico	Peggiore	
Bipolari	TO18, TO92, SOT23	34247	68493	6849	50% guasti pericolosi
Bipolari a bassa potenza	TO5, TO39	5708	11416	1142	50% guasti pericolosi
Bipolari di potenza	TO3, TO220, D-Pack	1941	3881	388	50% guasti pericolosi
Fet	Giunzioni Mos	22831	45662	4566	50% guasti pericolosi
Mos di potenza	TO3, TO220, D-Pack	1142	2283	228	50% guasti pericolosi

Per stimare il MTTFd per ogni canale è necessario usare la seguente formula:

$1/MTTFd = \sum_i 1/MTTFd,i = \sum_j n_j/MTTFd,j$

Prendendo ad esempio un circuito stampato è possibile individuare il MTTFd (Tabella 4).

Copertura diagnostica
(Diagnostic Coverage - DC)
Frazione della probabilità dei guasti pericolosi individuati λ_{DD} e della probabilità di tutti i guasti pericolosi λ_{total}:

$DC = \sum\lambda_{DD}/\sum\lambda_{total}$

La copertura diagnostica può essere definita per l'intero sistema o per parti di esso. I valori sono definiti nella Tabella 5.

Tabella 5 - Copertura diagnostica

Definizione di DC	Valori di DC
Nessuna	DC < 60%
Bassa	60% ≤ DC < 90%
Media	90% ≤ DC < 99%
Alta	99% ≤ DC

Guasto di causa comune
(Common Cause Failure - CCF)
Guasti di differenti oggetti, risultanti da un singolo evento, dove questi guasti non sono conseguenza uno dell'altro.

Esempi di prodotti innovativi

Optoelettronica

L'attuale stato dell'arte permette l'uso senza limitazioni in una grande varietà di applicazioni di barriere immateriali. Funzioni di inibizione e blanking (anche flottante) rappresentano uno specifico contributo alla tecnica intelligente. La tecnologia laser sta invadendo il campo delle presse piegatrici in assenza di una normativa specifica. Già negli anni Ottanta si indagò sull'uso di scanner laser a protezione dei movimenti di veicoli guidati automaticamente. Durante la ricerca, vennero determinate le prescrizioni fondamentali per l'applicazione di questi sistemi in qualità di dispositivi protettivi: coefficienti di riflessione minima, possibilità di controllo on-line della capacità di rilevamento, programmazione sicura di diverse zone di protezione e la sicurezza dell'hardware programmabile. Oggi questi sistemi sono usati come dispositivi di protezione anche per macchine fisse. Nuove caratteristiche tecniche, come l'elevata flessibilità di zone di protezione individualmente regolabili e attivabili, portano a una notevole accoglienza di questi dispositivi nell'automazione industriale. Negli ultimi sei anni più di 50 mila dispositivi sono stati usati in tutto il mondo con esperienze positive.

Tabella 4 - Calcolo di MTTFd per un circuito stampato

j	Componenti	Unità (n_j)	MTTFd,j	1 / MTTFd,j	n_j / MTTFd,j
1	Bipolari	2	1142	0.000876	0.001752
2	Resistenze	5	11416	0.000088	0.000438
3	Capacità	4	5708	0.000175	0.000701
4	Relè	4	1256	0.000796	0.003185
5	Contattori	1	32	0.031250	0.031250
$\sum_j n_j$ / MTTFd,j					0.037325
MTTFd [anni]*					26.79

**Si noti come l'influenza maggiore in questo esempio provenga dai contattori*

Convertitori di frequenza

In passato, i movimenti complessi e molto veloci dei robot non potevano essere controllati in sicurezza. Di conseguenza l'unico sistema di protezione era rappresentato da recinzioni. Le esigenze dell'industria necessitano però dell'interazione sempre più frequente

fra robot e lavoratore. Sono stati allora realizzati nuovi dispositivi per monitorare la posizione e la velocità, con il risultato che in particolari applicazioni questi robot possono lavorare senza alcuna recinzione.
Un concetto similare è stato usato durante la verifica di un sistema di comando di una macchina utensile da parte dell'istituto tedesco Bia [9]. Di seguito viene fornita una breve descrizione del sistema e delle considerazioni che hanno portato al suo sviluppo.
Il centro di lavoro è protetto da barriere materiali che individuano due zone: un magazzino utensili ed un'area di lavoro. La frequenza di accesso dell'operatore è sicuramente elevata per l'area di lavoro mentre l'ingresso al

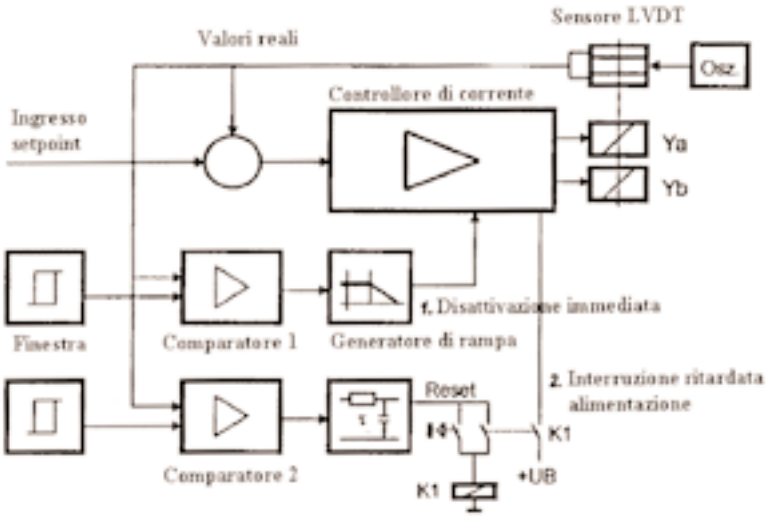

Figura 5 - Possibile schema a blocchi delle valvole proporzionali di seconda generazione

magazzino è legato ad operazioni di configurazione a inizio ciclo o manutenzione. Può accadere che il caricatore, comandato da un azionamento, contenga alcune decine di utensili, il cui cambio debba essere effettuato manualmente. È quindi necessario aprire le protezioni mobili di accesso, installare un nuovo utensile, chiudere le protezioni e ruotare il caricatore nella successiva posizione. L'operatore è quindi portato a manomettere il dispositivo di interblocco delle protezioni allo scopo di migliorare l'ergonomia del suo lavoro. Ovviamente questo introduce il rischio di rimanere gravemente ferito nell'eventualità di guasto del sistema di comando.
Allo stesso modo in caso di lavorazioni molto costose l'operatore vuole osservare i movimenti della macchina da vicino. Nelle macchine a comando manuale l'operazione è sicuramente possibile poiché tutti i movimenti devono essere comandati direttamente dall'operatore. Lo stesso può essere fatto su macchine automatiche comandate in modo sicuro. Si rende quindi necessario un controllo sicuro dello spazio e della velocità nelle aree pericolose. Generalmente le misure di sicurezza richiedono dispositivi esterni, come contattori, rilevatori di posizione, camme. Nel caso di intervento della funzione di sicurezza i dispositivi comandano l'interruzione del circuito di potenza della macchina. Questo può generare guasti ai transistori di potenza e ai contattori dovuti all'interruzione di carichi induttivi, perdita del riferimento di posizione, ecc. Inoltre è necessario sottolineare le influenze dei dispositivi esterni sulle prestazioni delle funzioni di sicurezza.
Un fattore molto importante è infatti il tempo di reazione dell'operatore. Questi agisce generalmente tramite un dispositivo di consenso il cui rilascio comporta l'arresto della macchina. Per cui l'azione decisiva è riconoscere velocemente un pericolo e rilasciare l'attuatore di consenso. Quando l'operatore è concentrato sui potenziali pericoli, si può avere un tempo di reazione fino a 400 ms, con un conseguente spazio di arresto degli assi di alcune decine di centimetri. Nel caso più realistico in cui l'operatore è concentrato sul processo piuttosto che sui potenziali pericoli, il tempo di reazione è superiore ad un secondo e di conseguenza lo spazio di arresto più di un metro. L'integrazione della funzione di sicurezza porta ad una drastico abbattimento dei tempi di risposta quando i limiti di posizione e velocità vengono violati.
In Figura 3 è mostrata una tipica architettura di una macchina utensile. In questo sistema vengono utilizzati due controllori per ragioni funzionali: un controllo numerico ed un azionamento. Il Cn è responsabile dell'interpolazione nello spazio, mentre l'azionamento controlla il movimento degli assi. Tutte le funzioni di sicurezza possono essere realizzate tramite questi due canali software (Tabella 6). La ridondanza e la diversità implicano che un singolo guasto non comporta la perdita della funzione di sicurezza. Due sono infatti i percorsi di arresto:

- spegnimento degli impulsi di comando generati dall'azionamento (1st stopping path);
- sezionamento dell'alimentazione degli opto-accoppiatori che trasmettono gli impulsi allo stadio finale dell'azionamento (2nd stopping path).

Entrambi i canali sono in grado di arrestare i movimenti degli assi in maniera indipendente. L'architettura è dotata di un monitoraggio incrociato e di una dinamicità forzata, ma non è in grado di rilevare tutti i guasti.

L'azionamento e il Cn calcolano indipendentemente i valori legati a funzioni di sicurezza e verificano i percorsi di ingresso e uscita. Tutti i parametri vengono monitorati da entrambi i canali e confrontati con i valori dell'altro percorso. Allo scopo di ottenere un elevato valore di copertura diagnostica (indice dell'affidabilità del circuito di monitoraggio nell'individuare un guasto) non viene effettuata la comparazione dei soli segnali di uscita ma anche dei risultati dei calcoli intermedi (esempio valori di posizione, velocità, ingressi e uscite). Per rilevare un guasto nell'elaborazione di segnali statici in ingresso è necessario commutare i segnali entro il tempo di riconoscimento del guasto (tipicamente un ciclo operativo).
Ad esempio i segnali di ingresso di un arresto di emergenza cambiano raramente, ossia solo alla pressione del relativo pulsante. Se si forza il cambiamento di questi segnali di ingresso ridondanti per un brevissimo tempo, ad esempio durante un arresto della macchina, si permette all'azionamento e al Cn di verificare la corretta esecuzione e bloccare il sistema in caso di incongruenza.

Oleodinamica

I circuiti idraulici usano sempre più valvole proporzionali, le quali commutano il loro stato in maniera proporzionale a un segnale elettrico in ingresso [10]. In passato queste valvole non potevano essere usate per funzioni di sicurezza senza la ridondanza di valvole on-off, poiché non rispettavano i requisiti relativi alle caratteristiche di attuazione e il ricoprimento positivo sufficiente ad assicurare il blocco del fluido nella posizione di riposo (Figura 4, a sinistra). Questa configurazione è complessa, costosa, e tecnicamente "inferiore". Una soluzione sicuramente più conveniente implica lo svolgimento di funzioni di sicurezza da parte della sola valvola proporzionale (Figura 4, a destra).
Poiché le caratteristiche di sicurezza non erano definite dalle norme e nemmeno erano riportate nelle schede tecniche dei costruttori, esisteva una certa incertezza. Vennero stilati i principi di collaudo sulla base dei requisiti delle norme Iso, En e Din. Furono anche presi in considerazione l'esperienza e i criteri di valutazione raggiunti durate i test preliminari. Lo schema dei principi di collaudo venne discusso anche con i maggiori produttori di valvole e con commissioni competenti interessate e presentato al gruppo di lavoro Din responsabile delle valvole idrauliche [11]. Di seguito viene riportata una breve panoramica delle caratteristiche di sicurezza legate alle valvole proporzionali. Ad oggi esistono tre differenti generazioni di valvole proporzionali per il controllo di direzione che possono svolgere una funzione di sicurezza. La differenza consiste sostanzialmente nell'elettronica di controllo, poiché i componenti idraulici e meccanici sono principalmente gli stessi in tutte le versioni. Una tipica valvola proporzionale per il controllo di direzione è dotata di due stadi e due solenoidi proporzionali. Entrambi gli stadi (principale e pilota) sono muniti di controllo di posizione. La valvola lavora ad anello chiuso, con un confronto continuo tra il comando impartito e la posizione reale assunta. Nello stato non alimentato, sia lo stadio pilota che quello principale sono centrati tramite molle. Lo stadio principale è costruito in modo tale da avere un ricoprimento positivo. La prima generazione è caratterizzata dal fatto che in caso di intervento della funzione di sicurezza i solenoidi vengono diseccitati tramite contatti elettromeccanici. Inoltre non è presente alcun controllo del raggiungimento della corretta posizione di sicurezza e della portata per poter ad esempio assicurare una velocità dell'attuatore comandato.
Il taglio dell'alimentazione dei solenoidi della valvola proporzionale tramite contatti non è una soluzione appropriata, poiché, come detto precedentemente, la maggior parte di queste valvole lavora in anello chiuso. Una soluzione tecnicamente migliore è rappresentata dalle valvole di seconda generazione, le quali portano la valvola in posizione di sicurezza applicando un appropriato segnale e mantenendo la valvola in questa posizione tramite un controllo ad anello chiuso. Solamente quando la valvola esce dal range per-

Tabella 6 - Funzioni di sicurezza del sistema di comando

Funzione di sicurezza	Descrizione
Arresto sicuro	Il processo viene arrestato nel più breve tempo possibile
Blocco della ripartenza	Non sono possibili movimenti inaspettati dopo aver arrestato il processo
Arresto funzionale	Il motore è sempre controllato dall'azionamento. Il Cn e l'azionamento controllano eventuali movimenti inattesi comandando immediatamente l'arresto
Velocità ridotta	L'azionamento e il Cn assicurano che la velocità non superi il limite impostato
Movimento passo-passo	L'azionamento e il Cn assicurano lo spostamento relativo
Posizione assoluta	L'azionamento e il Cn assicurano che gli assi non escano dai limiti di posizione impostati

messo attorno alla posizione di sicurezza, i solenoidi vengono diseccitati tramite l'apertura di contatti elettromeccanici, come nelle valvole di prima generazione. Per ottenere lo stesso livello di sicurezza il tempo di risposta del sistema deve ovviamente essere adeguato. In Figura 5 viene illustrato questo principio tramite uno schema a blocchi. La posizione sicura della valvola viene monitorata tramite un sistema lineare di rilevamento della posizione (sensore Lvdt), il quale, in combinazione con altri componenti, esegue il confronto tra la posizione comandata e quella reale. È preferibile che il sistema di rilevamento della posizione per il normale funzionamento della valvola non sia usato per svolgere questa funzione, ma sia indipendente. Tuttavia, l'uso è possibile nel caso in cui vengano rispettati particolari requisiti relativi al progetto dei componenti, alla struttura del sistema di controllo ed ai potenziali guasti.
Tramite un comparatore a finestra è possibile individuare la massima deviazione permessa dello spool dalla posizione di sicurezza. Nel caso in cui il valore permesso venisse superato una unità di comparazione (comparatore 1 in Figura 5) interrompe la corrente ai solenoidi tramite elementi allo stato solido. L'interruzione deve essere realizzata nel più breve tempo possibile, ma allo stesso tempo deve essere rampata per abbattere lo spazio percorso dal cassetto. Dopo un breve ritardo la seconda unità di comparazione (comparatore 2 in Figura 5) taglia l'alimentazione alla scheda di controllo tramite i contatti di un relè (K1). La sconnessione resta fino alla pressione dell'interruttore di ripristino, attuato dopo l'eliminazione del guasto.
In conclusione la valvole di seconda generazione raggiungono in maniera elettronica la posizione di sicurezza, la quale è monitorata. I solenoidi vengono diseccitati tramite l'apertura di contatti elettromeccanici solo in caso di deviazione dalla posizione permessa.
Quello che ancora manca è un controllo sicuro della posizione al di fuori di quella di sicurezza, in maniera tale che possa essere controllata la portata del fluido (valvole di terza generazione). In alcune applicazioni infatti una velocità ridotta è l'unica misura di sicurezza attuabile. Tipico è il caso delle presse piegatrici, dove lavorazioni particolari richiedono l'inibizione dei dispositivi di sicurezza, i quali automaticamente permettono il movimento di chiusura degli utensili solo ad una velocità ridotta (minore o uguale a 10 mm/s) abbinata a un comando ad azione mantenuta.

Bus

I sistemi standard "field bus" servono da sistemi intelligenti per la trasmissione di dati nelle macchine. Tali sistemi richiedono la trasmissione di dati per linee su cui tutti i partecipanti comunicano l'un l'altro. I controlli di sicurezza convenzionali impiegano linee separate per la trasmissione di segnali riguardanti la sicurezza. L'obiettivo è quello di studiare sotto quali condizioni i sistemi standard "field bus" possono essere impiegati per la trasmissione di segnali riguardanti la sicurezza. Nel corso degli anni sono stati sviluppati e valutati provvedimenti contro i vari meccanismi di alterazione del segnale. Contemporaneamente i vari livelli della tecnologia di sicurezza dovevano essere rapportati alla qualità della trasmissione di dati, per permettere la valutazione dei provvedimenti e il loro corretto impiego. Oggi questi provvedimenti sono realizzati per i field bus: As-Interface, CanOpen, DeviceNet, Esalan, Interbus, Profibus-Dp e Safety Bus p.

Bibliografia

[1] D. Reinert, *Prevention and Innovation,* 2001 Safety of industrial automated system.
[2] En 954-1 Sicurezza del Macchinario – Parti dei sistemi di comando legate alla sicurezza – Parte 1: principi generali per la progettazione.
[3] Direttiva Macchine 98/37/Ce - Allegato I - Osservazioni preliminari.
[4] En 1050: 1996 Sicurezza del macchinario - Principi per la valutazione del rischio.
[5] En 292-1/2: 1991 Sicurezza del macchinario - Concetti fondamentali, principi generali di progettazione - Terminologia, metodologia di base - Specifiche e principi tecnici.
[6] Iec 62061 Sicurezza del macchinario - Sicurezza funzionale - Sistemi di comando elettrici, elettronici ed elettronici programmabili.
[7] Iec 61508 parti 1-7 Sicurezza funzionale dei sistemi elettrici/elettronici/elettronici programmabili con funzione di sicurezza.
[8] prEn 954-1 Revisione n.10 dell'aprile 2002.
[9] R. Apfeld, M. Umbreit, *Integrated safety in flexible manufacturing systems,* Industrial track paper.
[10] Werner Kleinbreuer, *Safety-related hydraulic proportional technology,* 2001 Safety of industrial automated system.
[11] Pe-Bia-M01; issue 12/2000: Empfehlung fur die Prufung von kontakt-behaftet abgeschalteten elektro-hydraulischen Stetig-Wegeventilen fur sicherheitsbezogene Teile von Steuerungen.

Ing. E. Moroni, Responsabile divisione macchine, Icepi Srl - Organismo Notificato, Pontenure (PC).