PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 16 - numero 3430 di venerdì 14 novembre 2014

Sicurezza delle macchine: sicurezza funzionale e norme tecniche

Informazioni sulla sicurezza funzionale correlata alle funzioni di sicurezza delle macchine. Le norme tecniche EN 954-1, EN/IEC 62061 e EN/ISO 13849-1. Le norme utilizzabili e le procedure di progettazione di un sistema di controllo.

Stezzano (BG), 14 Nov ? Sempre più spesso nei documenti dedicati alle funzioni di sicurezza delle macchine realizzate con tecnologie elettriche, elettroniche ed elettroniche si parla di "**sicurezza funzionale**", un concetto nuovo che si è venuto affermando negli ultimi anni in relazione alla pubblicazione di numerose norme che lo utilizzano: ad esempio le norme IEC 61508, IEC 62061, IEC 61511, ISO 13849-1 e la IEC 61800-5-2; norme entrate in vigore in Europa e pubblicate come norme EN.

Per parlare di sicurezza funzionale, su cui ci eravamo già brevemente soffermati presentando un documento sulla sicurezza delle macchine prodotto dall'azienda Rockwell Automation, facciamo riferimento alla " Guida Applicativa Sicurezza Macchine" realizzata dall'azienda Schneider Electric, una guida che offre utili informazioni in grado di aiutare i costruttori di macchine e gli utenti finali a garantire la sicurezza dei lavoratori con macchine sicure, a norma ed efficienti.

La guida, che ha offerto spunti al nostro giornale per parlare di identificazione/riduzione dei rischi e di progettazione delle funzioni di sicurezza, dedica alla **sicurezza funzionale** un intero capitolo con diversi esempi pratici di applicazioni.

Per presentare la sicurezza funzionale, concetto relativamente recente che viene a sostituire alcune categorie definite dalla norma EN 954-1, nella guida applicativa si ricordano innanzitutto i **principi della norma EN 954-1** e il vecchio "**diagramma di rischio**" da molti "utilizzato in passato per progettare le parti dei sistemi di comando legate alla sicurezza in base alle categorie B da 1 a 4". In particolare "all'utilizzatore veniva richiesto di valutare in modo soggettivo la gravità del danno, la frequenza e/o il tempo di esposizione al pericolo e la possibilità di evitarlo. La gravità della lesione veniva valutata con i parametri da lieve a seria, e l'esposizione al rischio da rara a frequente, da possibile in determinate condizioni a virtualmente impossibile. L'obiettivo era di arrivare alla categoria richiesta per ogni parte del sistema legata alla sicurezza". La teoria alla base di tutto questo è che "più la riduzione dei rischi dipende dal funzionamento corretto del sistema di controllo elettrico di sicurezza e più questo dovrà essere in grado di resistere ai guasti (quali cortocircuiti, saldatura dei contatti, ecc.)".

Veniamo invece alla "**sicurezza funzionale**" che viene definita come "*parte della sicurezza della macchina e del suo sistema di controllo che dipende dal funzionamento corretto dello SRECS, di altri sistemi con tecnologia relativa alla sicurezza e ad impianti esterni per la riduzione del rischio*". Dove lo SRECS (Sistema Elettrico di Controllo Relativo alla Sicurezza) è "il sistema elettrico di controllo di una macchina il cui guasto può produrre un immediato aumento del rischio". E con "funzionamento corretto" si intende che "il sistema deve eseguire correttamente una funzione di sicurezza: questo significa che le funzioni devono essere scelte correttamente".

Se in passato si tendeva a "scegliere sempre componenti con una categoria superiore specificata dalla norma EN 954-1 al posto di componenti di categoria inferiore" (secondo "l'erroneo concetto gerarchico delle categorie"), le norme relative alla sicurezza funzionale "mirano ad incoraggiare i progettisti a **focalizzarsi maggiormente sulle funzioni effettivamente necessarie a ridurre ogni singolo rischio**, oltre che sui livelli prestazionali richiesti a ciascuna funzione, piuttosto che fare semplicemente affidamento su componenti specifici".

Quali norme sono applicabili alla funzione di sicurezza?
Secondo la guida "attualmente la norma EN 954-1 può dirsi quasi superata, mentre le valide alternative disponibili cui fare riferimento sono la norma EN/IEC 62061 e EN/ISO 13849-1. Entrambe le norme permettono una valutazione precisa delle prestazioni di ogni singola funzione e degli elementi di rischio, anche se in modo diverso. In base alla norma EN/IEC 62061 si determina il livello di integrità della sicurezza richiesto (SIL) mentre sulla base della EN/ISO 13849-1 si calcola il Performance Level (PL). In entrambi i casi l'architettura del circuito di controllo che realizza la funzione di sicurezza è un fattore, ma diversamente dalla EN 954-1 le nuove norme prendono in considerazione l'affidabilità dei componenti scelti".

In particolare si indica che con la **norma EN/IEC 62061** "è importante considerare nel dettaglio ogni singola funzione; la norma EN/IEC 62061 richiede la stesura di una specifica dei requisiti di sicurezza (Safety Requirements Specification o SRS). Questa comprende una specifica funzionale (cosa fa in dettaglio) ed una specifica dell'integrità della sicurezza che definisce la probabilità richiesta che una funzione venga eseguita nelle condizioni specificate".
Per comprendere come funziona la norma suddetta la guida presenta l'esempio relativa all'arresto della macchina all'apertura del riparo.

Invece la **norma EN ISO 13849-1** "utilizza una combinazione tra Tempo Medio dei Guasti Pericolosi (MTTFd), Copertura Diagnostica (DC) e architettura (categoria) per determinare il Performance Level PL". Una tabella nella guida mostra un metodo semplificato di valutazione del PL.

Quale norma utilizzare?
La guida ricorda che a meno che una norma di tipo C (le norme tecniche di tipo C trattano i requisiti di sicurezza specifici per una macchina o per un particolare gruppo di macchine) specifichi un livello SIL o PL richiesto, "il progettista è libero di utilizzare indifferentemente le specifiche della norma EN/IEC 62061 o della norma EN/ISO 13849-1, o anche di altre normative. Sia la norma EN/IEC 62061 che la EN/ISO 13849- 1 sono norme armonizzate che assicurano un'automatica presunzione di conformità ai requisiti Essenziali della Direttiva Macchine. Tuttavia occorre ricordare che qualsiasi norma venga scelta questa dovrà essere utilizzata integralmente e che non è possibile mischiare i requisiti di più norme in un unico sistema".
Si ricorda inoltre che:
- è in corso uno studio che "punta ad un' integrazione degli standard IEC e ISO per la redazione di un Allegato comune ad entrambi gli standard, con l'obiettivo finale di produrre eventualmente un'unica norma di riferimento";
- la norma EN/IEC 62061 "è forse più completa in materia di responsabilità relative alla specifica e alla gestione della sicurezza, mentre la EN/ISO 13849-1 è concepita in modo specifico per permettere una più facile transizione dalla EN 954-1".

Rimandando ad una lettura integrale della guida, anche in relazione alla complessità della materia, riprendiamo per concludere un **esempio pratico di applicazione** relativo all'applicazione della norma EN/IEC 62061 ("Sicurezza del macchinario ? Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza") in relazione all'esempio di "un'apertura della protezione con conseguente arresto delle parti mobili di una macchina, ove il mancato arresto potrebbe comportare la rottura di un braccio o l'amputazione di un dito dell'operatore".

Riguardo alla norma si indica che "i **sistemi di controllo elettrici di sicurezza delle macchine** (SRECS) svolgono un ruolo chiave nell'assicurare la sicurezza totale delle macchine ed utilizzano sempre più spesso apparecchi elettronici complessi". La norma è "rivolta in modo specifico al settore delle macchine e deriva della norma EN/IEC 61508".
Per l' approccio funzionale alla sicurezza il procedimento "parte dall'**analisi dei rischi** (EN/ISO 12100) per stabilire i requisiti di sicurezza. Una caratteristica specifica della norma EN/IEC 62061 è quella di spingere in prima istanza l'utilizzatore ad effettuare un'analisi dell'architettura necessaria a realizzare le funzioni di sicurezza, quindi a prendere in considerazione le sottofunzioni e ad analizzare le interazioni prima di procedere alla scelta di una soluzione hardware per il sistema di controllo elettrico di sicurezza della macchina (SRECS)". Per ogni progetto la norma richiede un "**Piano di sicurezza funzionale documentato**" e nella guida sono riportati i contenuti di tale piano.

Si sottolinea inoltre che i vantaggi di questo approccio "sono rappresentati dalla possibilità di offrire un metodo di calcolo comprendente tutti i parametri che possono influire sull'**affidabilità dei sistemi di controllo**. Il metodo consiste nell'assegnare un livello SIL (Safety Integrity Level) ad ogni funzione, tenendo conto di vari parametri" (probabilità di guasto pericoloso dei componenti, tipo di architettura, cause comuni di guasto, probabilità di trasmissione di errori pericolosi in caso di utilizzo di comunicazione digitale, interferenze elettromagnetiche, ...).

Concludiamo l'articolo ricordando che, sempre in relazione all'utilizzo della EN 62061, la **procedura di progettazione di un**

sistema prevede cinque fasi successive alla realizzazione del piano di sicurezza funzionale:
- in base alla valutazione del rischio assegnare un livello di integrità della sicurezza (SIL) e identificare la struttura base del sistema di controllo elettrico (SRECS), descrivendo inoltre ogni funzione di controllo relativa alla sicurezza (SRCF) ad esso correlata;
- scomporre ogni funzione di controllo relativa alla sicurezza (SRCF) in blocchi funzionali (FB); - dettagliare le prescrizioni di sicurezza per ogni blocco funzionale, assegnando i blocchi funzionali ai sottosistemi dello SRECS;
- selezionare il dispositivo per ciascun sottosistema;
- progettare le funzioni diagnostiche come prescritto e verificare il raggiungimento del livello di integrità (SIL) specificato".
Nella guida sono descritte nel dettaglio le varie attività e definiti i parametri correlati ai vari aspetti della progettazione di un sistema.

Ricordiamo che, per ulteriori approfondimenti, sul tema della sicurezza dei sistemi di controllo delle macchine l'Inail ha pubblicato nel 2014 un documento dal titolo: " Sicurezza funzionale dei sistemi di controllo delle macchine: requisiti ed evoluzione della normativa".

Schneider Electric, " Guida Applicativa Sicurezza Macchine" (formato PDF, 2.85 MB).

---

www.puntosicuro.it