a cura di Massimo Granchi

Parti del sistema di comando legate alla sicurezza

Principi generali per la progettazione

La norma tecnica UNI EN ISO 13849-1 definisce i principi generali di progettazione delle parti del sistema di comando legate alla sicurezza. Questa norma è armonizzata ai sensi della Direttiva Macchine 2006/42/CE, pertanto la sua applicazione garantisce la presunzione di conformità nei confronti dei Requisiti Essenziali di Sicurezza e di Tutela della Salute della stessa Direttiva, in particolar modo verso il Requisito 1.2.1 – "Sicurezza ed affidabilità dei sistemi di comando". La norma presenta un'impostazione decisamente innovativa rispetto alla precedente UNI EN 954-1 che resta tuttavia applicabile fino al 31/12/2011. Nel presente articolo analizzeremo le principali differenze tra le due norme evidenziando le novità introdotte dalla norma UNI EN ISO 13849-1.

Dall'approccio deterministico all'approccio probabilistico

Le norme tecniche, nell'ambito della Direttiva Macchine, sono dei documenti che si prefiggono il compito di definire le caratteristiche (tipicamente relative alla sicurezza) di un prodotto secondo lo stato dell'arte in essere e possono essere adottate per conformarsi a determinati Requisiti Essenziali di Sicurezza (RES) della Direttiva senza la necessità che il Fabbricante della macchina debba necessariamente inventarsi soluzioni personali e, a volte, originali; le soluzioni tecniche suggerite dalle norme sono prese, inoltre, dal legislatore come punto di riferimento e un fabbricante che volesse scegliere soluzioni differenti dovrebbe dimostrare, nel Fascicolo Tecnico della Costruzione della macchina (cioè il documento che attesta la conformità della macchina a tutte le direttive applicabili alla stessa), di aver raggiunto un livello di sicurezza almeno pari a quello raggiungibile con l'applicazione della norma armonizzata apposita. Dunque, se negli anni c'è stata, nella pratica, un'evoluzione dello stato dell'arte e un'evoluzione conseguente delle norme, non è invece cambiato lo scopo, cioè il garantire all'utilizzatore delle macchine il maggior livello di sicurezza possibile.

Il Nuovo Approccio, delegando alle norme armonizzate il compito di stabilire lo stato dell'arte in essere, ha, infatti permesso di non modificare di molto il panorama legislativo incentrato sulla Direttiva Macchine, ormai giunta alla Direttiva 2006/42/CE - Direttiva 2006/42/CE del Parlamento Europeo e del Consiglio del 17 maggio 2006 relativa alle macchine e che modifica la direttiva 95/16/CE (rifusione) entrata in vigore, in tutti gli Stati membri delle Comunità, il 29 giugno 2006 con applicazione a partire dal 29 dicembre 2009. Questo significa che tutte le macchine (o meglio, le apparecchiature che rientrano nella definizione di "macchina" come prevista dalla Direttiva stessa) messe in servizio o immesse sul mercato dopo il 29 dicembre 2009 devono essere marcate CE ai sensi della Direttiva Macchine 2006/42/CE.

Dal punto di vista normativo i cambiamenti sono stati molto più evidenti e, pur rispettando i tempi necessari alla loro stesura, le principali norme tecniche hanno visto, parallelamente all'evoluzione della tecnica associata, una evoluzione dalla loro prima stesura. In alcuni casi, l'evoluzione rappresenta un semplice aumento delle informazioni disponibili in merito a un determinato fattore (si pensi a tutto il campo dell'ergonomia e allo studio delle interazioni fra uomo e macchina), in altri casi, invece, l'evoluzione risponde a un necessario mutamento dovuto a tecnologie che precedentemente non esistevano; si pensi a tutti i sistemi di comando elettrici, elettronici ed elettronici programmabili correlati alla sicurezza. Ed è proprio rispetto a questi ultimi che si è avuto il cambiamento più evidente in quanto il precedente approccio deterministico (funziona/è guasto) è stato sostituito da un approccio di tipo probabilistico (stima del livello di prestazione, generalmente espresso come probabilità media di un guasto pericoloso per unità di tempo, per esempio un anno).

L'evoluzione, quindi, dall'approccio deterministico (caratteristico, si potrebbe affermare, della logica cablata) all'approccio probabilistico (caratteristico della logica programmabile) può essere evidenziato confrontando le seguenti norme armonizzate:

- UNI EN 954 - 1: 1998 - Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Principi generali per la progettazione, e
- UNI EN ISO 13849-1: 2009 - Sicurezza del macchinario – Parti dei sistemi di comando legate

alla sicurezza – Parte 1: principi generali per la progettazione.

Nella norma armonizzata UNI EN 954 - 1, i possibili circuiti di comando e di controllo delle macchine vengono classificati in cinque categorie differenti (B, 1, 2, 3 e 4) in funzione di un'affidabilità e una sicurezza crescente; la scelta deve essere compiuta in funzione di una specifica valutazione dei rischi (effettuata secondo lo schema previsto dalla norma) e a rischio maggiore deve corrispondere una categoria più elevata. Tuttavia, tutta l'analisi e dunque la scelta della categoria (e quindi la corrispondente architettura del circuito) da utilizzarsi si incentra sul verificarsi o meno di un guasto che possa portare alla perdita delle funzioni di sicurezza e non sulla probabilità che questo possa avvenire; paradossalmente, un sistema di comando legato alla sicurezza di categoria 1 potrebbe rivelarsi più affidabile nell'arco di vita utile di una macchina di un altro differente (progettato e assemblato con componenti differenti dal precedente), ma di categoria 3 o 4. Questo perché, agli effetti pratici, risulta più utile impostare lo studio del problema dal punto di vista probabilistico che non deterministico. Di fatto la norma UNI EN 954-1 manca di una valutazione probabilistica delle prestazioni dei sistemi di comando e controllo per la sicurezza delle macchine.

La norma UNI EN ISO 13849-1 risponde a questa esigenza introducendo misure concrete e parametri di riferimento per valutare le prestazioni dei dispositivi in termini di affidabilità, copertura diagnostica e immunità in relazione ad una particolare architettura del sistema di controllo. Pertanto, se prima era importante verificare che la progettazione del sistema di comando e controllo correlato con la sicurezza fosse corretto (approccio deterministico), ora è importante valutare la probabilità statistica di occorrenza di un evento non voluto o di un guasto (approccio probabilistico). Tuttavia, proprio la necessità di dover utilizzare parametri specifici per valutare la affidabilità dell'architettura progettata per il sistema di comando e controllo ha reso difficoltosa fin dall'inizio l'applicazione della norma UNI EN ISO 13849-1. Infatti, il fabbricante del sistema di comando e controllo deve ricercare questi parametri presso i fornitori dei componenti dello stesso sistema e non sempre queste informazioni sono facilmente reperibili. Inoltre, i calcoli e le valutazioni che stanno dietro alla scelta della architettura da utilizzarsi per il sistema hanno ulteriormente rallentato l'applicazione della presente norma. Pertanto, sulla Gazzetta Ufficiale della Unione Europea è stata pubblicata, in data 29 dicembre 2009, la post datazione della scadenza di applicabilità della norma UNI EN 954-1 al 31 dicembre 2011. Dunque, sebbene questa norma non sia di fatto espressamente armonizzata alla Direttiva 2006/42/CE è libertà del fabbricante applicarla in alternativa alla UNI EN ISO 13849-1 per la progettazione delle parti del sistema di comando e controllo legate con la sicurezza.

Gli aspetti da considerare

Come detto, la UNI EN ISO 13849-1 fornisce i requisiti di sicurezza e i principi per la progettazione e l'integrazione delle parti del sistema di comando e controllo correlate con la sicurezza (Safety Related Parts od Control System, SRP/CS in inglese). In particolare la norma specifica le caratteristiche, che includono il livello di prestazione PL – Performance Level (suddiviso dalla norma in 5 classi e definito in termini di probabilità di guasto pericoloso orario), necessarie per l'espletamento delle funzioni di sicurezza (le principali sono arresto di sicurezza, riarmo manuale, avvio/riavvio, controllo locale, inibizione dei dispositivi di sicurezza, tempo di risposta, fluttuazione, mancanza e ripristino delle alimentazioni, ecc.).

Scopo della norma è quello di fornire le indicazioni necessarie alla progettazione di un sistema di comando e controllo correlato con la sicurezza che risponda ad un livello di prestazione corrispondente ai requisiti richiesti dalla valutazione dei rischi per ciascuna funzione di sicurezza. Questo livello di prestazione è identificato come PL_r. I parametri necessari al calcolo del valore di PL in modo che corrisponda al valore richiesto dalla valutazione dei rischi (PL_r) sono i seguenti:

- ✔ Tempo medio al guasto pericoloso ($MTTF_d$ - Mean Time To dangerous Failure): tempo atteso di operatività di un sistema prima del manifestarsi del primo guasto.
- ✔ Copertura diagnostica (DC – Diagnostic Coverage): parametro che identifica il rapporto tra la probabilità di rilevare un guasto pericoloso e la probabilità di rilevare il totale dei guasti pericolosi;
- ✔ Guasto dovuto a causa comune (CCF – Common Cause Failure): guasto di diverse entità, risultato di un singolo evento, dove un guasto non è conseguenza di altri guasti.

L'attenzione è dunque rivolta non ad avere un sistema che non si guasti mai, ma a progettare e costruire (o assemblare) un sistema che sia affidabile, in grado cioè di eseguire una specifica funzione di sicurezza, sotto specifiche condizioni operative e ambientali a un dato istante e/o per un prefissato intervallo di tempo; per far questo, è necessario scegliere correttamente i componenti e costruire una adeguata architettura del

a cura di Massimo Granchi

☛ sistema in modo tale da conseguire un PL che risulti adeguato in funzione dei rischi presenti. Compito del fabbricante è dunque quello di sviluppare, in corrispondenza di ogni funzione di sicurezza, una adeguata valutazione del rischio che permetta di progettare un corrispondente e affidabile sistema di comando e controllo.

La valutazione dei rischi secondo la UNI EN ISO 13849-1

La norma UNI EN ISO 13849-1 descrive un esempio di approccio qualitativo per la stima dei rischi e l'assegnazione dei PL applicabili alle funzioni di controllo relative alla sicurezza. In pratica, si determina un indice di rischio (funzione di gravità, frequenza e durata dell'esposizione e possibilità di evitare il pericolo) e, in base a esso, mediante un grafico di rischio, si determina il PL necessario per la corrispondente funzione di controllo relativa alla sicurezza.

Il metodo fornito dalla norma permette di valutare il PL_r come risultato della valutazione dei rischi. Il grafico di rischio identifica il PL_r come appartenente ad una delle cinque classi individuate (a, b, c, d, e). A questo punto il fabbricante deve progettare e realizzare il sistema di comando e controllo in modo da ottenere un PL corrispondente al PL valutato$_r$. A tal proposito deve scegliere l'architettura del sistema (e dunque la categoria, secondo lo stessa logica adottata nella precedente UNI EN 954-1) e i componenti stessi secondo un grafico sempre riportato dalla norma, che mette in relazione le categorie, i valori di DC e di $MTTF_d$ per ciascun canale e il valore di PL del sistema. I valori di DC e di $MTTF_d$ per ciascun canale del sistema e dunque dell'intero sistema, possono essere valutati basandosi sulle tabelle e sulle formule di calcolo presenti nella norma; i valori di $MTTF_d$ di ogni singolo componente del sistema possono essere ottenuti anche dai corrispondenti fabbricanti.

In definitiva compito del fabbricante, dopo aver eseguito la valutazione dei rischi, è quello di implementare le misure protettive necessarie al sistema al fine di ridurre il rischio valutato. Queste misure protettive (applicabili singolarmente o in combinazione) sono distinguibili in:

- ✔ riduzione della probabilità di guasti a livello dei componenti; lo scopo è quello di ridurre la probabilità di guasti che possano far venir meno le funzioni di sicurezza; ciò può essere ottenuto aumentando l'affidabilità dei componenti (ad es, passando da una categoria B alla categoria 1), selezionando componenti testati in modo da ridurre o escludere guasti critici;
- ✔ miglioramento della architettura del sistema di comando e controllo correlato con la sicurezza con lo scopo di evitare gli effetti pericolosi di un guasto; a tal scopo può risultare utile l'utilizzo di una struttura ridondante (doppio canale) e/o monitorata (mediante l'ausilio, in una logica elettromeccanica, di moduli di sicurezza).

Conclusioni

Per la progettazione dei sistemi di comando correlati con la sicurezza, sebbene sia ancora applicabile fino al 31/12/2011 la norma UNI EN 954-1, è consigliabile prendere dimestichezza con la norma UNI EN ISO 13849-1 descritta nel presente articolo. Infatti, oltre a rappresentare comunque quella che sarà la scelta obbligata per il futuro, permette una progettazione del sistema di comando più realistica analizzando lo stesso dal punto di vista della affidabilità dell'intero sistema piuttosto che dal punto di vista delle rottura a guasto del singolo componente. Inoltre la nuova norma presenta alcuni punti a favore, tra cui: l'applicabilità anche ai circuiti elettronici programmabili (che stanno ormai diffondendosi su una grande varietà di applicazioni), l'utilizzazione di architetture predefinite che garantiscono una facile conversione dalla precedente UNI EN 954-1 e la corrispondenza con quanto riportato nelle norme tecniche di tipo C dove è solitamente riportato il PL minimo che deve garantire il circuito di sicurezza di quella specifica macchina.

Massimo Granchi