Sicurezza

Fonte: www.haschemediendesign.com

di **Micaela Caserza Magro, Paolo Pinceti (*)**

LA SICUREZZA FUNZIONALE CORRE SUL FIELDBUS

SI PARLA OGGI DI SICUREZZA 'FUNZIONALE' IN RIFERIMENTO ALLA NORMA CEI/IEC 61508 CHE IMPONE ALLE SOLUZIONI DI AUTOMAZIONE DI PRESENTARE REQUISITI STRINGENTI IN TERMINI DI AFFIDABILITÀ E DISPONIBILITÀ

A ogni processo industriale si può associare in diversa misura il rischio: di ferire o uccidere persone, di provocare danni ambientali, di danneggiare l'impianto e quindi gli investimenti. Nella maggior parte dei processi è semplice eliminare questi rischi e ridurli a livelli accettabili senza la necessità di rispettare requisiti particolari per quanto concerne il sistema di automazione. Al contrario, esistono applicazioni per le quali questo non si verifica, in tali casi è necessario adottare misure particolari e speciali per ridurre il rischio a livello accettabile. Questo comporta l'adozione di soluzioni che abbiano prestazioni in termini di affidabilità e di disponibilità tali da soddisfare i requisiti imposti a livello normativo e/o legislativo. In questo contesto si parla di sicurezza 'funzionale', facendo esplicito riferimento a quanto specificato dalla Norma CEI/IEC 61508 'Sicurezza funzionale dei sistemi elettrici ed elettronici programmabili per applicazioni di sicurezza'.

La sicurezza nell'automazione

L'approccio convenzionale alla sicurezza funzionale prevede un sistema 'hard-wired' basato su tecnologia a relè. Questo perché la tecnologia basata su controllori, PC e reti di comunicazione industriali basate su fieldbus non permettevano di stabilire e calcolare in modo semplice e preciso le probabilità e le modalità di guasto. Si è così assistito a una dicotomia: da una parte l'automazione per il sistema si è sempre più orientata verso applicazioni fieldbus-based, dall'altro l'automazione della parte relativa alla sicurezza è sempre rimasta ancorata alla logica a relè. Questo ha portato ad avere nelle installazioni due apparati completamente indipendenti, con costi aggiuntivi legati al cablaggio e alla differente ingegnerizzazione. La situazione oggi sta cambiando drasticamente, principalmente perché controllori e software sono stati utilizzati e provati in milioni di installazioni, quindi i meccanismi di guasto e le prestazioni di affidabilità e disponibilità sono ormai noti; inoltre, l'introduzione della normativa IEC 61508 ha aperto la possibilità di utilizzare controllori, soluzioni PC-based e software anche nelle applicazioni di sicurezza.

Oltretutto, i meccanismi di error detection di molti tipi di comunicazione digitale sono stati investigati e ben capiti e l'introduzione della normativa IEC 61784-3 ha introdotto diversi profili di comunicazione di tipo 'safe', che possono essere applicati alle reti di comunicazione fieldbus.

Tutti questi fattori hanno portato alla diffusione di sistemi di automazione basati su fieldbus e controllori digitali anche nel mondo della sicurezza funzionale. Vediamo ora una panoramica di quelle che sono le caratteristiche dei fieldbus di sicurezza che si possono impiegare.

Il panorama normativo internazionale: sicurezza e fieldbus

Da un punto di vista normativo, la sicurezza funzionale prende le mosse dalla famiglia delle norme IEC 61508, che definisce i principi base della sicurezza funzionale delle apparecchiature elettriche e le procedure di calcolo necessarie alla comunicazione fieldbus, nel mondo dell'automazione delle macchine. In modo del tutto analogo si può illustrare la relazione esistente tra le diverse normative dei fieldbus e della sicurezza funzionale applicate al mondo dell'automazione di processo (figura 2). Quando si parla di profili di comunicazione dei fieldbus per applicazioni di sicurezza, non è di per sé sufficiente a classificarlo come dispositivo di sicurezza. È invece possibile implementare un sistema di comunicazione di sicurezza utilizzando la stessa infrastruttura di rete usata per l'automazione non di sicurezza, oltre agli stessi strumenti di sviluppo, configurazione e ingegnerizzazione. Questo porta con sé una notevole semplificazione e

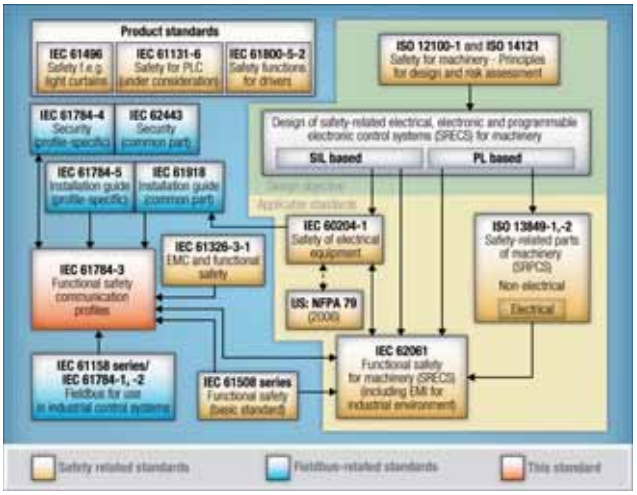


Figura 1 - Normativa 'internazionale' per i fieldbus e la sicurezza funzionale applicabili nell'automazione di fabbrica

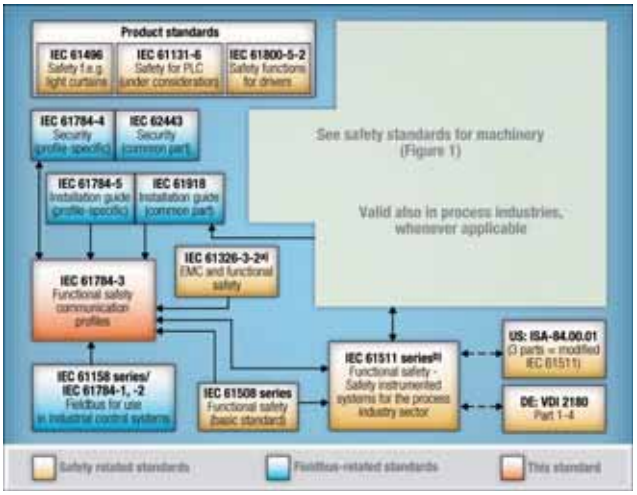


Figura 2 - Normativa 'internazionale' per i fieldbus e la sicurezza funzionale applicabili nell'automazione di processo

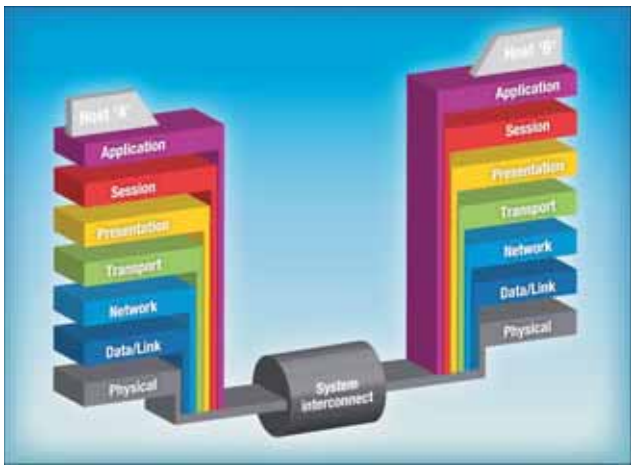


Figura 3 - Il modello ISO/OSI

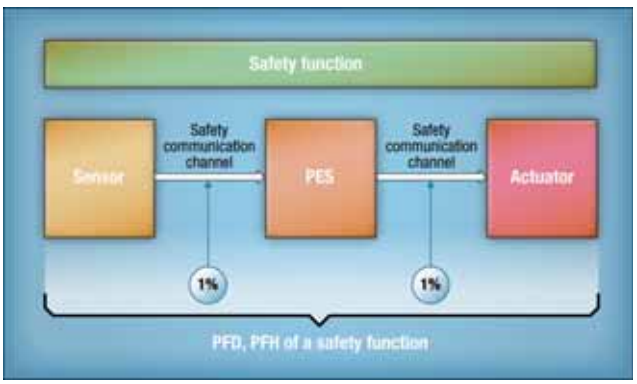


Figura 4 - Comunicazione di sicurezza come parte di una funzione di sicurezza

a una sua valutazione quantitativa. La norma IEC 61508 introduce le procedure per calcolare la probabilità residua di guasto delle cosiddette funzioni di sicurezza, definita Safety Integrity Level, in breve SIL. A partire da questa normativa si sono poi sviluppate diverse serie di normative, che declinano la sicurezza funzionale per diversi ambiti di applicazione. Focalizziamoci ora sulla parte relativa alla comunicazione, in particolare sui profili di comunicazione basati su fieldbus trattati nell'ambito della norma IEC 61784-3. La figura 1 riporta le relazioni tra i principali standard legati alla sicurezza e i principali standard legati poi, ci si riferisce ad alcuni livelli del modello ISO/OSI (figura 3), in particolare al livello Applicazione o Layer 7. Proprio per questo la norma IEC 61784-3 specifica le caratteristiche che devono essere rispettate e implementate per fare in modo che la comunicazione digitale rispetti i livelli di SIL richiesti in IEC 61508. Viene qui specificato solo il meccanismo di sicurezza della comunicazione, mentre la parte di architettura hardware degli oggetti facenti parte del sistema di automazione di sicurezza sono esclusi da questa trattazione. Infatti, l'utilizzo di un profilo di comunicazione di sicurezza da parte di un dispositivo convenzionale riduzione dei tempi e costi di gestione anche della parte di sicurezza.

Sistemi fieldbus legati alla sicurezza

Il punto di partenza dei sistemi di sicurezza funzionale sta proprio in quella che viene chiamata la funzione di sicurezza. È una funzione necessaria a evitare l'insorgere di guasti pericolosi ed è composta, in generale, da una catena costituita da (con la terminologia IEC 61508): sensore per misurare un determinato parametro di processo; Programmable Electronic System (PES), cioè il PLC o controllore che rileva un'a-

nomalia nel processo; attuatore, ossia il dispositivo che agisce sul processo per controllare l'anomalia. Se applichiamo questo concetto a un sistema basato su fieldbus, la catena è costituita da: sensore, canale di comunicazione, esecutore della logica (PES), canale di comunicazione e attuatore (si faccia riferimento alla figura 4).
In questo caso, la comunicazione ha il ruolo di trasportare i dati di sicurezza. Quello che viene raccomandato è che il canale di sicurezza non 'consumi' più dell'1% del massimo PFD (Probability of Failure on Demand, cioè il tasso di guasto) definito dal livello di SIL che si vuole raggiungere per quella specifica funzione.

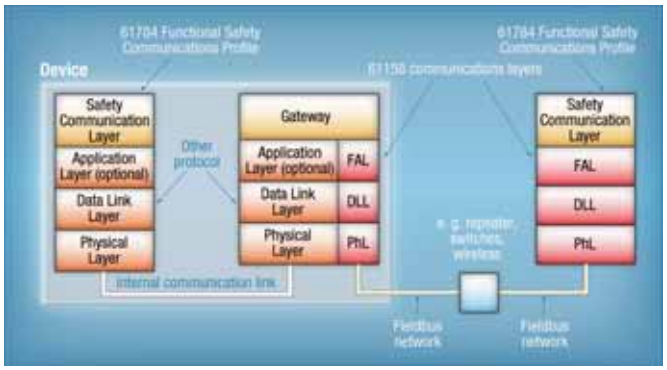


Figura 5 - Esempio di un modello di comunicazione di sicurezza basato sull'approccio 'black channel'

Sistema di comunicazione fieldbus

La norma IEC 61508 permette e prevede due approcci distinti per la parte di comunicazione digitale di sicurezza: il 'white channel', approccio che prevede lo sviluppo ad hoc di un nuovo protocollo di comunicazione per le applicazioni di sicurezza; il 'black channel', approccio in cui è consentito utilizzare un qualunque protocollo di comunicazione esistente e aggiungere un layer per le funzioni di sicurezza. Questo layer aggiuntivo non va a intaccare il protocollo esistente ed è l'unico responsabile di soddisfare i requisiti per la trasmissione dei dati di sicurezza (figura 5). Questo è l'approccio utilizzato da tutti i protocolli di comunicazione standard che si sono avvicinati al mondo della sicurezza.

Le caratteristiche di base

Un sistema di comunicazione fieldbus di sicurezza deve garantire tre funzioni principali: trasmettere dati corretti, far pervenire i dati al giusto destinatario, aggiornare i dati just-in-time. Partendo da questi aspetti base, trattiamo ora dei metodi che sono stati definiti per soddisfare i requisiti richiesti. Possono verificarsi diversi errori quando i messaggi vengono trasferiti in topologie di rete complesse, per guasti hardware, interferenze elettromagnetiche o altre influenze. Un messaggio può essere perso, presentarsi troppo rapidamente, essere inserito da qualche altra parte, essere in ritardo o non nella sequenza corretta, oppure presentare dati corrotti. Vi può anche essere un problema d'indirizzamento, che nelle applicazioni di sicurezza riveste un ruolo essenziale. Nell'ambito di IEC 61874-3 sono stati definiti tutti gli errori di comunicazione che si possono presentare e per ciascuno di essi sono stati definiti e identificati dei metodi che correggono questi errori. La trasmissione dei dati di sicurezza prevede l'implementazione di una serie di meccanismi e metodi che permettano di riconoscere il verificarsi di un errore nella trasmissione e porvi rimedio, portando il sistema in una posizione di sicurezza (figura 6).
I metodi che devono essere implementati comportano una modifica al telegramma dei dati trasmessi e l'inserimento di un certo numero di frame di check e controllo (CRC, sequence number, timestamp ecc.). Proprio perché la struttura del frame di sicurezza è diverso dalla struttura del frame del protocollo 'convenzionale', i messaggi di sicurezza devono essere trasmessi e ricevuti unicamente da componenti hardware di rete che siano di tipo 'safe', vale a dire con architettura hardware tale da garantire prestazioni certe in termini di SIL e con possibilità di comunicazione tali da elaborare il frame di sicurezza che ricevono o inviano.
Tutte queste misure di sicurezza consentono di trasmettere i dati in modo corretto. Inoltre, per garantire che i dati pervengano al giusto destinatario, la parte d'indirizzamento, in fase di configurazione del sistema, prevede anche l'identificazione del percorso di sicurezza e di quali siano gli oggetti coinvolti. In ultimo, per garantire le funzionalità just-in-time si devono calcolare i tempi di risposta delle funzioni di sicurezza (figura 7).

Communication errors	Safety measures: Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption (see 5.3.2)							Only for serial bus	
Unintended repetition (see 5.3.3)								
Incorrect sequence (see 5.3.4)								
Loss (see 5.3.5)								
Unacceptable delay (see 5.3.6)			c					
Insertion (see 5.3.7)				a, b	a			
Masquerade (see 5.3.8)				a	a			
Addressing (see 5.3.9)								

Note: Table adapted from IEC 62280-2 and [19]

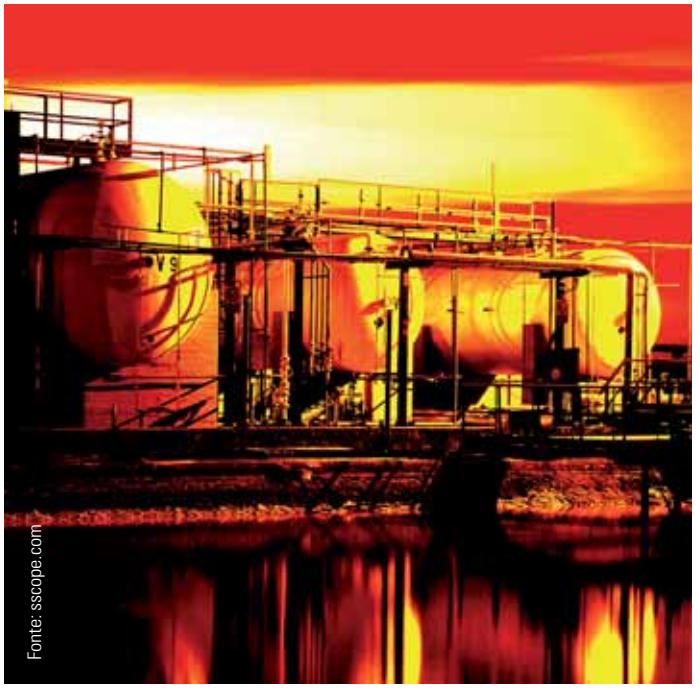
[a] Depends on application
[b] Only for sender identification. Detects only insertion of an invalid source
[c] Required in all cases
[d] This measure is only comparable with a high quality data assurance mechanism if a calculation can show that the residual error rate. A reaches the values required in 5.4.9 when two messages are sent through independent transceivers

Figura 6 - Errori di comunicazione e metodi di soluzione

Figura 7 - Tempo di risposta della funzione di sicurezza

Configurazione di un sistema di sicurezza

Chiarito come sia possibile utilizzare un sistema di sicurezza basato su fieldbus, è necessario illustrare ora come questo debba essere configurato per la messa in esercizio.
Il sistema di sicurezza utilizza hardware dedicato, in termini sia di PES sia di dispositivi (sensori e attuatori), mentre utilizza come infrastruttura di comunicazione la stessa che viene impiegata per la parte di automazione convenzionale. Uno dei grandi vantaggi dell'approccio alla sicurezza basata su fieldbus è che anche la parte di sicurezza può essere configurata direttamente con la stessa engineering workstation utilizzata per il sistema di automazione convenzionale. Pertanto, la configurazione della parte di sicurezza, in termini sia d'indirizzamento, sia di logica, possono essere fatti nello stesso modo e con i medesimi strumenti che vengono utilizzati per il sistema di automazione.



Fonte: sscope.com

Conclusioni

Il nuovo approccio alla sicurezza funzionale prevede di poter utilizzare soluzioni fieldbus-based e con l'impiego di controllori logici programmabili (PES). Questa apertura è stata resa possibile grazie alla norma IEC 61508 e permette di integrare il sistema di sicurezza direttamente all'interno del sistema di automazione utilizzando la stessa infrastruttura e gli stessi strumenti di configurazione e programmazione. Il sistema di sicurezza prevede che le apparecchiature hardware impiegate (sensori, attuatori, PES) siano dedicate e realizzate in modo adeguato per rispondere ai requisiti di affidabilità definiti dal livello SIL che si vuole aggiungere. Oltre alle apparecchiature hardware è necessario prevedere un profilo del protocollo di comunicazione che sia riconosciuto come un profilo di sicurezza. Questo significa che il profilo aggiuntivo è un layer sovraimposto a quelli del modello ISO/OSI del protocollo utilizzato e che è responsabile unicamente della trasmissione dei dati di sicurezza.
Le caratteristiche peculiari del layer di sicurezza sono quelle di avere dei meccanismi di error detection e indirizzamento speciali, ma quello che realmente è importante è che il sistema di sicurezza possa essere integrato direttamente in quello di automazione.

(*) Dipartimento Diten, Università di Genova, comitato tecnico Fieldbus & Networks