La protezione dei fieldbus

Mariano Severi

La norma IEC 61508 tratta di sicurezza funzionale e sistemi 'safety-related', mentre gli aspetti di 'safety' e 'security' dei fieldbus sono oggetto di IEC 61784

Fonte: www.jkcustomnetworks.com

I continui cambiamenti nei processi produttivi e la crescente complessità delle installazioni nella maggior parte dei settori industriali pongono oggi nuove sfide per quanto concerne gli aspetti di affidabilità e sicurezza. L'obiettivo è la definizione di nuove soluzioni che consentano di identificare, limitare o prevenire malfunzionamenti che possano indurre danni nel sistema o agli operatori, ivi inclusi gli eventuali errori causati dagli addetti stessi.

Le cause di malfunzionamento possono essere diverse, ad esempio la definizione di specifiche non corrette, l'omissione di adeguate procedure di sicurezza, l'insorgere di guasti a componenti hardware, l'occorrenza di errori umani, l'impatto di fattori ambientali come temperatura d'esercizio, stress meccanici, compatibilità elettromagnetica. La salvaguardia da tali eventi o circostanze accidentali viene genericamente indicata come 'safety' del sistema. La protezione invece da attacchi o aggressioni non casuali, eventualmente finalizzati al furto di informazioni, che pure comporta in alcuni casi ingenti danni all'azienda 'vittima', viene indicata come 'security'. Per soddisfare requisiti e funzionalità in ambito sicurezza, si è assistito negli ultimi anni a un crescente impiego di dispositivi e apparecchiature elettriche, elettroniche e programmabili. Lo standard IEC 61508 regolamenta tale impiego.

Alcuni punti fermi

Negli anni passati la tecnologia dei bus di campo ha trovato rapida diffusione nella maggior parte dei settori industriali per la trasmissione delle informazioni e rappresenta ormai una realtà piuttosto consolidata. Rispetto alle tradizionali soluzioni assicura, infatti, maggiore flessibilità e modularità, espansione e manutenzione più semplici, minori costi d'installazione e gestione. Non deve quindi stupire il recente interesse via via in aumento verso l'impiego di tale tecnologia anche nell'ambito delle funzionalità di sistema orientate alla sicurezza.

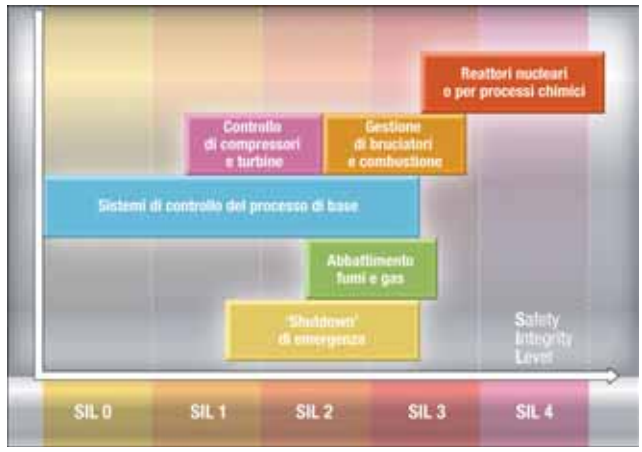
La diffusione dei bus di campo è stata certamente favorita da una serie di iniziative di standardizzazione, che hanno portato alla definizione delle specifiche IEC 61158 e IEC 61784 parti 1 e 2. Nell'ottica dell'impiego dei bus di campo in applicazioni legate alla sicurezza lo standard IEC 61784 è stato quindi esteso, con le parti 3 e 4, per includere raccomandazioni e informative per quanto concerne gli aspetti di safety e

security, in accordo alle normative di carattere generale incluse nella specifica IEC 61508.

Sicurezza funzionale e sistemi 'safety-related'

Lo standard IEC 61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PES)* copre gli aspetti di sicurezza funzionale nei sistemi che utilizzano apparecchiature o dispositivi elettrici, elettronici o programmabili; le specifiche si applicano indistintamente a ogni tipo d'industria. La norma copre tali aspetti lungo l'intero ciclo di vita del prodotto, individuando fino a 16 distinte fasi che riguardano le attività di analisi, realizzazione e operatività del sistema. Contiene parti normative e sezioni puramente informative, con linee guide che possono servire come riferimento per l'implementazione delle specifiche.

Con il termine 'functional safety' si intende quella parte degli aspetti di sicurezza del sistema che riguarda la sua capacità di operare correttamente in risposta agli stimoli. Un esempio è l'impiego di un sistema di limitazione della velocità in funzione della temperatura di un motore elettrico. Deriva dai requisiti sulle funzionalità di sicurezza evidenziati dalle analisi di rischio e dalle richieste d'integrità di sicurezza, che individuano il livello di certezza rispetto al quale tali funzionalità sono espletate. Ogni funzione di sicurezza è così caratterizzata da un parametro SIL (Safety Integrity Level) compreso tra uno e quattro, che definisce appunto il livello d'integrità di un dispositivo; tale parametro caratterizza in particolare la probabilità di occorrenza di danni pericolosi da un valore minimo di un evento ogni milione di ore per i sistemi di classe 1, a un evento su 1 bilione per quelli di classe 4. Il livello 3, che considera accettabile un malfunzionamento ogni 100 milioni di ore, è tipicamente quello più alto supportato dalla maggior parte delle applicazioni industriali. Due sono, poi, i modi operativi considerati all'interno dello standard per ogni funzione di sicurezza: 'low demand mode' e 'high demand mode' (o 'continuous mode'). La distinzione si basa sulla frequenza di occorrenza della funzione, prendendo come riferimento il limite di un intervento per anno. Le applicazioni low demand intervengono solo su richiesta, in presenza di un malfunzionamento del sistema; le funzioni continue operano invece costantemente, per mantenere il sistema nel suo normale stato di sicurezza. Con il termine 'safety-related system' si intende invece l'insieme delle risorse hardware, software e umane che concorrono alla realizzazione di una specifica funzionalità di sicurezza in un EUC (Equipment Under Control). L'EUC è definito formalmente come l'apparato, macchinario, apparecchiatura o installazione usati per una qualsiasi attività in ambito industriale, medicale o altro. Tipici esempi di EUC sono quindi i sistemi di spegnimento di emergenza degli impianti, i sistemi di controllo e monitoraggio remoto di un'installazione industriale, i sistemi di controllo 'fly-by-wire' di un aeromobile, i dispositivi medicali impiegati per funzionalità vitali. Un sistema 'E/E/PE safety-related' è considerato a bassa complessità se le modalità di fallimento di ogni singolo componente sono ben definite e, quindi, si è in grado di determinarne esattamente lo stato in presenza di malfunzionamenti noti.



Livelli SIL tipici richiesti per le funzioni di sicurezza in varie applicazioni

Safety e security nei fieldbus

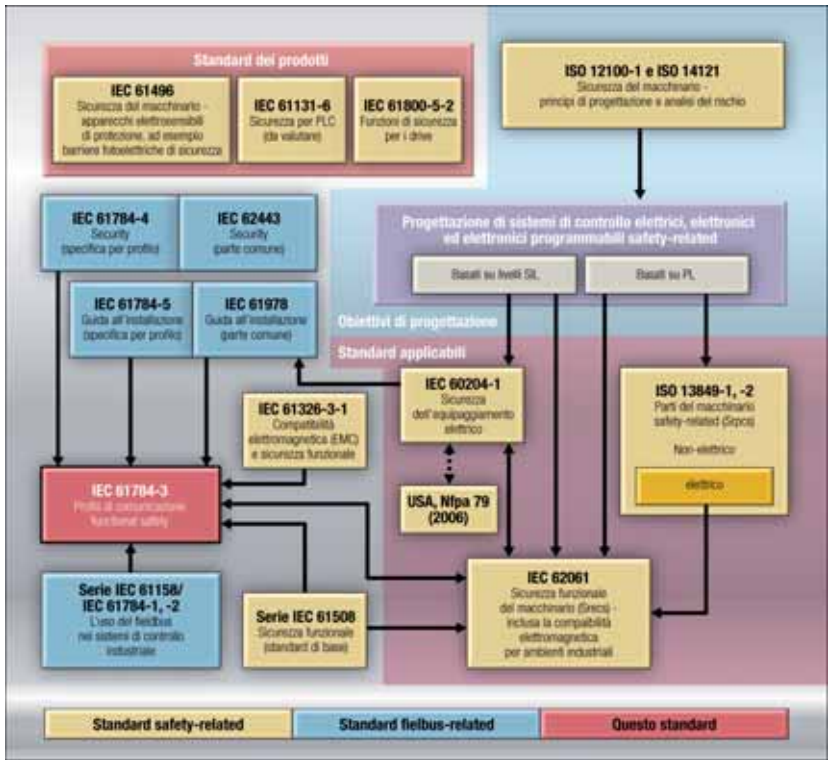
I fieldbus tradizionali non sono adeguati a espletare funzioni di sicurezza, in quanto, pur avendo in molti casi una capacità intrinseca di rilevamento degli errori nella trasmissione delle informazioni, non sono in grado di individuare indipendentemente e rapidamente eventuali malfunzionamenti all'interno della rete. Lo standard IEC 61784, che standardizza le tecnologie dei bus di campo, è stato pertanto esteso negli ultimi anni includendovi le parti 3 e 4 che affrontano, appunto, i problemi di safety e security mediante la definizione di livelli accessori nel protocollo di comunicazione. Le architetture definite sono in accordo alle raccomandazioni di carattere generico espresse nello standard IEC 61508.

Diversi sono i livelli che possono essere individuati nel protocollo di comunicazione. In particolare, il livello di safety implementa gli algoritmi di autenticazione dei dati che servono alla sicurezza della rete. Fornisce quindi i servizi necessari ad assicurare un adeguato livello di confidenza nella correttezza e validità del trasporto delle informazioni tra due o più nodi connessi al bus, o della messa in sicurezza nel caso di errori o malfunzionamenti del bus stesso. Tali malfunzionamenti possono verificarsi a tutti i livelli del protocollo di comunicazione, dagli errori nella comunicazione dovuti a disturbi sul mezzo fisico, fino a errori logici nei nodi, ad esempio la ripetizione non prevista dei messaggi, l'introduzione di un ritardo inaccettabile nella generazione di un messaggio di controllo o di risposta

ecc. Diverse sono le soluzioni messe in opera. In certi casi, vengono adottate delle architetture ridondate, che prevedono una replica delle connessioni. A livello di protocollo sono quindi introdotti campi del messaggio che permettono di verificare la corretta sequenza della trasmissione e di associare ai dati le informazioni temporali. Sono definiti 'time slot' di comunicazione e 'time out' per la risposta secondo uno schema di complessità crescente a seconda del SIL della funzione di sicurezza che si intende implementare. Sono inoltre previsti dei messaggi di sicurezza che consentono di verificare il corretto funzionamento della rete e procedure d'intervento ed eventualmente di ripristino, che consentono di terminare la comunicazione in corso in caso di malfunzionamento, per portare quindi il sistema in uno stato di sicurezza. Il canale di comunicazione di sicurezza non deve interferire con il normale flusso di dati e deve occupare al minimo la banda di trasmissione.

Lo standard IEC 61784-3 definisce i principi comuni per la trasmissione di messaggi di sicurezza all'interno di una rete bus basati sul concetto di 'black channel' definito dalla specifica IEC 61508; impone inoltre che i protocolli di sicurezza funzionale non si basino su particolari implementazione del mezzo fisico di connessione. Si compone di una parte generale, che introduce una panoramica di requisiti e raccomandazioni comuni per i profili Fscp (Functional safety communication profiles) e di una sezione che descrive particolari implementazioni. Nella revisione dello standard, pubblicata nel 2007, sono stati inclusi protocolli quali FF SIS, CIP Safety, Profisafe e Interbus Safety. Nella prossima edizione dovrebbero essere inserite anche le implementazioni Ethercat Safety e Safetynet p (Germania), Rapisafe (Korea), EPA Safety (Cina), CC-link Safety (Giappone) e P-Net Safety (Danimarca).

Per fare un esempio concreto, Profisafe (Profibus safety o Profinet safety) è stato il primo esempio di protocollo di sicurezza funzionale per automazione distribuita; adotta una numerazione progressiva dei messaggi, il monitoraggio dei time out nelle spedizioni delle informazioni, l'autenticazione di sorgente e destinazione della trasmissione, il controllo mediante CRC (Cyclic Redundancy Checking) dei dati.



Lo standard IEC 61784-3 in relazione alle altre specifiche e raccomandazioni

Il caso del wireless

Se le funzioni di safety interessano in qualche modo il funzionamento della rete dal suo interno, i profili di security trovano invece principalmente applicazione nei sistemi di comunicazione aperti. In questo caso, danni al sistema possono derivare dal rischio di accessi non autorizzati alla rete e alle informazioni in essa contenute. L'esempio probabilmente più evidente da questo punto di vista è rappresentato dall'utilizzo di reti wireless, nel qual caso il mezzo di comunicazione è ovviamente accessibile a chiunque purché all'interno della zona di copertura, e le frequenze sono in genere di pubblico dominio. Le tecnologie di questo tipo più diffuse in ambito automazione sono Bluetooth (fino a 10 m), Wlan (fino a 100 m) e Zigbee (fino a 300 m). In merito a questi aspetti, lo standard IEC 61784-4 definisce i seguenti profili di sicurezza: CP-EPI per la connessione di reti esterne alla rete di controllo; CP-IRA per l'accesso interattivo da remoto alla rete di controllo; CP-ICC per l'accesso del centro di controllo alla rete di controllo condivisa.

I metodi di security suggeriti si basano su algoritmi d'identificazione e riconoscimenti dei nodi connessi; nelle applicazioni più critiche possono essere adottati algoritmi crittografici per la cifratura delle informazioni. Un termine spesso usato in questo settore è quello di 'computational safety', ossia sicurezza computazionale. Un algoritmo di crittografia viene definito 'computational safe' se la sua violazione richiede un numero non disponibile di operazioni. Allo stato attuale sono ritenuti tali gli algoritmi che hanno complessità computazionale esponenziale. ■