

INTRODUZIONE AI PROTOCOLLI DI COMUNICAZIONE SAFETY

Bus di comunicazione per applicazioni di sicurezza

Con impianti produttivi sempre più avanzati e complessi, i maggiori produttori di sistemi di sicurezza propongono soluzioni di comunicazione in grado di offrire maggiore flessibilità, riduzione dei cablaggi, diagnostica integrata, dimensioni di ingombro ridotte, alte prestazioni, risposte in tempo reale. Una recente giornata di studio Anipla sui bus di comunicazione per applicazioni di sicurezza è stata l'occasione per fare il punto della situazione.

Armando Martin

La sicurezza occupa un ruolo fondamentale in tutti i sistemi di automazione industriale ed è comunemente accettato che debba avere priorità assoluta nella progettazione e nell'ingegnerizzazione delle macchine di produzione e dei sistemi di automazione industriale.

Per sicurezza (nell'accezione resa in inglese con il termine "safety") si intende l'insieme di tutte le soluzioni meccaniche, elettriche, elettroniche, informatiche e progettuali che garantiscono a persone e macchine di non riportare danni, ovvero di prevenire situazioni di pericolo

attivo e passivo. Quando si verificano situazioni di guasto o malfunzionamento, è indispensabile che vi siano dei dispositivi che intervengano in modo che il sistema raggiunga uno stato sicuro a prova di errore (fail-safe). Un

dispositivo o un sistema **fail-safe** presenta particolari caratteristiche di robustezza, facilità di controllo e manutenzione.

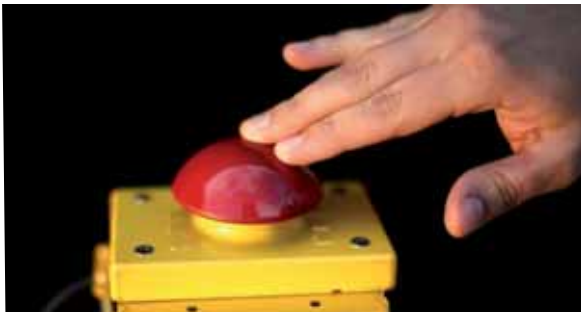
Un altro obiettivo principe a livello ingegneristico, per le applicazioni "critiche" in cui è necessario che gli impianti continuino a operare anche in caso di guasti, si parla invece di logica "**fault-tolerant**". In questo caso l'obiettivo è raggiunto aumentando la disponibilità e l'affidabilità del sistema attraverso la ridondanza. Nasce quindi l'esigenza di integrare, rispetto al sistema di automazione tradizionale, una piattaforma indipendente il cui scopo è di rilevare e gestire i guasti sui singoli componenti e sulle loro connessioni.

Prima però va ricordato che in ambito indu-

striale si distinguono per lo meno 4 tipi di sicurezza:

- 1) sicurezza funzionale legata al funzionamento globale di strumentazione e sistemi in condizioni di sicurezza (PLC compresi);
- 2) sicurezza elettrica derivante da contatti o sovraccarichi di circuiti e conduttori;
- 3) sicurezza intrinseca collegata al rischio di esplosione;
- 4) security che consiste in un approccio sistematico per la protezione delle reti e delle tecnologie informatiche.

Il concetto di **sicurezza funzionale** dipende dal funzionamento corretto di un sistema o di un'apparecchiatura, in risposta ai suoi parametri iniziali dal punto di vista elettrico, elettronico ed elettronico programmabile. In tema di sicurezza funzionale il parametro più usato per valutare macchine e impianti è il SIL (livello di integrità della sicurezza), ovvero un numero discreto indicante il valore della probabilità che un SIS (sistema strumentale di sicurezza) esegua correttamente una funzione di sicurezza strumentale, entro un periodo di tempo prestabilito. Fondamentale è anche la valutazione della **sicurezza elettrica** che si ottiene progettando e costruendo macchine elettriche equipaggiate in modo tale da evitare qualsiasi contatto diretto con cavi di corrente o parti conduttrici. Per quanto riguarda la sicurezza intrinseca e la direttiva Atex 94/9/CE, la corretta scelta dei dispositivi da utilizzare richiede di conoscere a quale gruppo di sostanze esplosive appartengono le miscele infiammabili eventualmente presenti nell'ambiente e a quali classi di temperatura appartengono i dispositivi elettrici da installare. Nei fieldbus e nei cablaggi il concetto di sicurezza intrinseca è basato sui modelli FISCO (Fieldbus Intrinsically Safe COnccept) e



FNICO (Fieldbus NonIncendive COnccept), normati dalla IEC 60079-27, o da altri approcci come Entity e High Power Trunk. Tali modelli richiedono l'adesione a poche ma precise regole di cablaggio e installazione.

Reti di sicurezza e flessibilità

Per rete di comunicazione orientata alla sicurezza si intende anzitutto una rete orientata alla salvaguardia di se stessa e dei componenti che vengono interconnessi. Si intende inoltre una rete specializzata nella gestione di funzioni dedicate alle applicazioni safety. Rispetto a una rete standard, una rete safety è generalmente caratterizzata da minori cablaggi, diagnostica integrata, dimensioni di ingombro ridotte, alte prestazioni, risposte in tempo reale. È inoltre importante che un bus safety possa poggiarsi su

una piattaforma indipendente per rilevare e gestire i guasti sui singoli componenti e sulle loro connessioni.

Le scelte tecnologiche adottabili spaziano dall'impiego di PLC di sicurezza alla differenziazione dell'hardware su piattaforme PC based (configurazioni multi-processore). Un sistema di comunicazione safety può anche prevedere l'utilizzo di software per applicazioni critiche (aeronautica, oil&gas, energia, industria di processo ecc.) e la capacità di gestire influenze esterne (vibrazioni, EMC ecc.) sui vari componenti del sistema.

Allo stato attuale la diffusione di vere e proprie reti di sicurezza è ancora limitata da costi significativi investimenti dilazionati, da normative complesse, dal basso livello di conoscenza delle tecnologie e dalla diffusione di

I principali protocolli di comunicazione per la sicurezza

Standard	Norma	Consorzio o Principali sostenitori	Applicazioni	Web
AS-i	EN 50295, IEC 62026-2	AS-International Association	Sensori e attuatori, movimentazione materiali	as-interface.net
CANopen Safety	EN 50325-5, EN 50325-4	CAN in Automation	Macchine mobili, applicazioni outdoor, sensoristica	www.can-cia.org
CC-Link Safety	IEC61508, SIL3, EN954-1	CLPA (Mitsubishi, Keyence, Yokogawa, M-System, NEC)	Macchine operatrici, impianti distribuiti, alta velocità (fino a 10 Mbps)	www.clpa-europe.com
CIP Safety	IEC 61784	ODVA (Rockwell Automation, ABB, B&R, Cisco ecc.)	Macchine automatiche	www.odva.org
DART	IEC 60079-11	Pepperl+Fuchs	Sicurezza intrinseca, strumentazione	www.technology-dart.com
DeviceNet Safety	EN 954-1 (Cat.4), ISO13849-1 (PLe), IEC 61508 / SIL3	ODVA (Rockwell Automation, ABB, B&R, Cisco ecc.)	Macchine automatiche, linee di produzione, applicazioni con rapido tempo di risposta	www.odva.org
Ethernet/IP Safety	IEC 61508/SIL3	ODVA (Rockwell Automation, ABB, B&R, Cisco ecc.)	Applicazioni con distanze elevate e grandi pacchetti dati	www.odva.org
Fieldbus Foundation	ISA SP50, IEC 61804, IEC 61508, IEC 61158	Fieldbus Foundation (Pepperl+Fuchs, MTL, PR Electronics, Yokogawa, ABB, Emerson, Stahl, Wika ecc.)	Oil&Gas, controllo attuatori, food&beverage, pulp&paper	www.fieldbus.org
Fieldbus Foundation H1	IEC 1158-2	Fieldbus Foundation	Sicurezza intrinseca	www.fieldbus.org
Hart	IEC 61804	Hart Communication Foundation (ABB, Endress+Hauser, Emerson, Pepperl+Fuchs, Siemens ecc.)	Controllo strumentazione, monitoraggio processi	www.hartcomm.org
Interbus Safety	EN ISO 13849-1; (SIL) CL 3; EN IEC 62061	Interbus Club (Phoenix Contact, Baumer, Festo, Rexroth, Rockwell Automation, Wago ecc.)	Integrazione componenti, macchine automatiche, sistemi di produzione	www.interbusclub.com
Open Safety	IEC 61784-3 Fscp 13; SIL 3	EPSP (B&R, ZHW, ABB, Wago, Lenze, Pepperl+Fuchs ecc.)	Macchine modulari, sistemi aperti	www.open-safety.com
Powerlink Safety	IEC 61508 / SIL 3	EPSP (B&R, ZHW, ABB, Wago, Lenze, Pepperl+Fuchs ecc.)	Macchine automatiche alte prestazioni	www.ethernet-powerlink.org
Profibus PA	DIN E 19245 -4, EN 50170, IEC 61158-2	PNO (Siemens, Endress+Hauser, Phoenix Contact, Pepperl+Fuchs, Bosch Rexroth, Mitsubishi ecc.)	Automazione di processo, Sicurezza intrinseca	www.profibus.com
ProfiSafe	IEC 61508	PNO (Siemens, Endress+Hauser, Phoenix Contact, Pepperl+Fuchs, Bosch Rexroth, Mitsubishi ecc.)	Comunicazione standard e safety su un unico bus	www.profibus.com
SafetyBus p	IEC 61508 / SIL 3	Safety Network International (ABB, Harting, Pilz, Festo, Honeywell, Yokogawa ecc.)	Sistemi distribuiti	www.safetybus.de
Safety Over EtherCat	IEC 61508 / SIL 3	EtherCat Technology Group (Beckhoff, Lenze, Hirschmann ecc.)	Comunicazione standard e safety su un unico bus	www.ethercat.org
Safeethernet	IEEE 802.3 / SIL3	Hima	Sistemi distribuiti (processo, building, macchine)	www.safeethernet.de
Sercos Safety	IEC 61784-3; SIL 3, IEC 61508	Sercos International (ABB, Schneider, Sew Eurodrive, Danaher, Bosch ecc.)	Motion control, integrazione di sistemi	www.sercos.com
Wireless Hart	IEC 62591; IEEE 802.15.4	Hart Communication Foundation (ABB, Endress+Hauser, Emerson, Pepperl+Fuchs, Siemens ecc.)	Reti mesh, monitoraggio di processo, PAM, Remote IO	www.hartcomm.org

sistemi proprietari non certificati. L'evoluzione delle tecniche elettroniche e del quadro normativo stanno però ponendo le basi per un reale salto di qualità nella diffusione di reti e sistemi di sicurezza integrati. L'implementazione di sistemi di comunicazione specifici per la sicurezza è un fatto di cui dovranno tenere conto costruttori di macchine, progettisti e sistemisti di rete nei prossimi anni. Il principale vantaggio delle reti safety è quello di garantire, in forma diretta, rigido sincronismo temporale, ripetibilità, autodiagnosi, profili dedicati per dispositivi fail-safe con tempi di latenza ridotti, funzioni specifiche (arresto controllato, velocità controllata ecc.). Questi vantaggi sono accompagnati da requisiti di integrità della comunicazione: gestione avanzata degli errori, ridondanza nei cablaggi, unificazione della rete fieldbus.

Una rete di sicurezza può essere implementata secondo **architetture diversificate e flessibili**. Adottando un approccio distribuito o integrato è possibile la messa in rete di componenti di ingresso e uscita distribuiti (per esempio pulsanti di arresto di emergenza o accessi di sicurezza collegati localmente mediante moduli I/O), riducendo il cablaggio e sfruttando un'impostazione flessibile dei parametri di comunicazione per mezzo dello stesso bus. Viceversa la separazione tra rete di sicurezza e rete di controllo standard può essere vantaggiosa quando è necessario standardizzare parti di una macchina o di un impianto che agiscono attraverso bus di campo differenti. In questo caso o se le logiche di sicurezza sono molto semplici (es. non sono richieste la trasmissione e la condizione di segnali sicuri nelle diverse zone di un impianto) è opportuno realizzare sistemi di sicurezza locali, indipendenti da quelli di automazione standard.

Standard sul mercato

In un mercato in costante crescita e che prevede l'installazione di circa 4 milioni di nodi di reti di sicurezza entro il 2013 (Arc Advisory 2010), la diffusione di hardware safety è accompagnata dall'affermazione di sistemi di comunicazione specifici come AS-i Safety, DeviceNet Safety, SafetyBUS p, Fieldbus Foundation, Profinet / Profisafe, Sercos III, CIP Safety. I protocolli di comunicazione con profili dedicati per l'esecuzione di azioni su dispositivi fail-safe sono implementati intervenendo sul modello ISO/OSI a livello di device profile e application layer. La crescente adesione di produttori e l'aumento dei prodotti conformi a tali protocolli sembrano favorire l'approccio specialistico alle reti di comunicazione safety. Gli standard assicurano ottimizzazione del traffico, elevata larghezza di banda, ridotti tempi di risposta, alta velocità di connessione, funzioni di networking (bridging, routing ecc.), drastica riduzione della manutenzione e della messa in servizio. La recente **standardizzazione** di bus indipendenti e tendenzialmente aperti, ovvero utilizzabili con i principali bus di campo e i sistemi Ethernet industriali, è un'ottima premessa perché i problemi di interoperabilità tra costruttori siano superati e non gravino su progettisti e utenti delle reti. ■