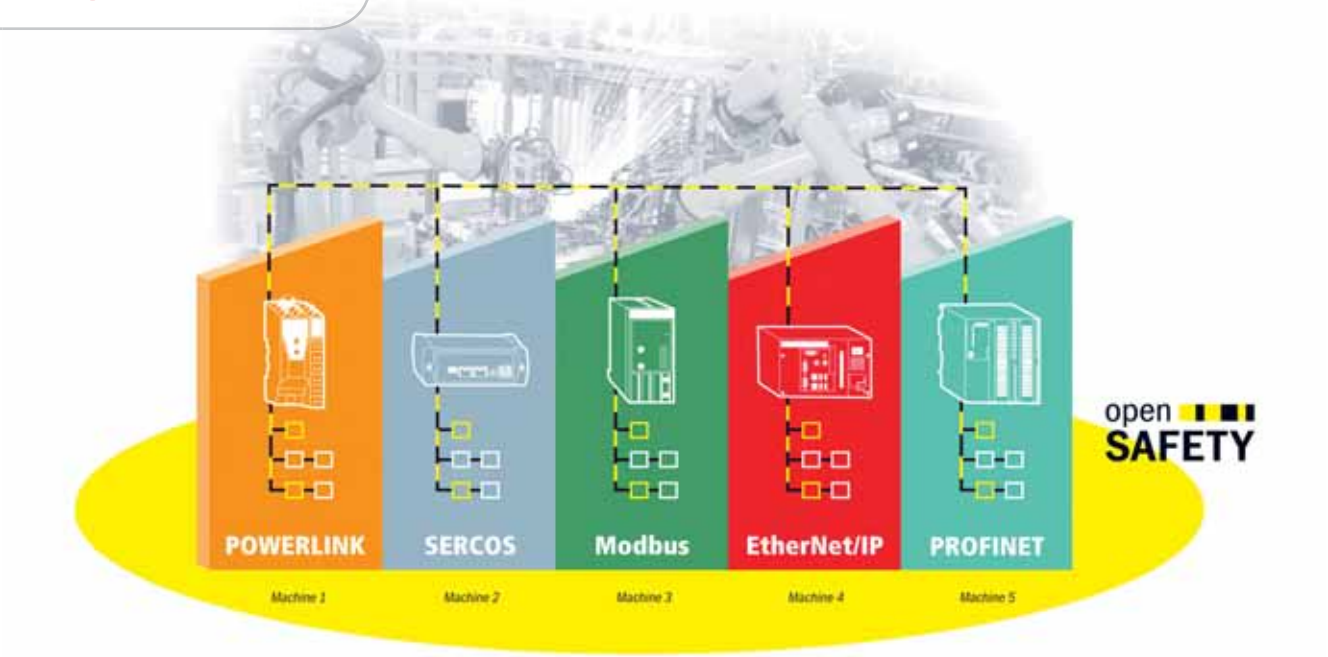
di **Massimo Giussani**



Fonte: Epsg

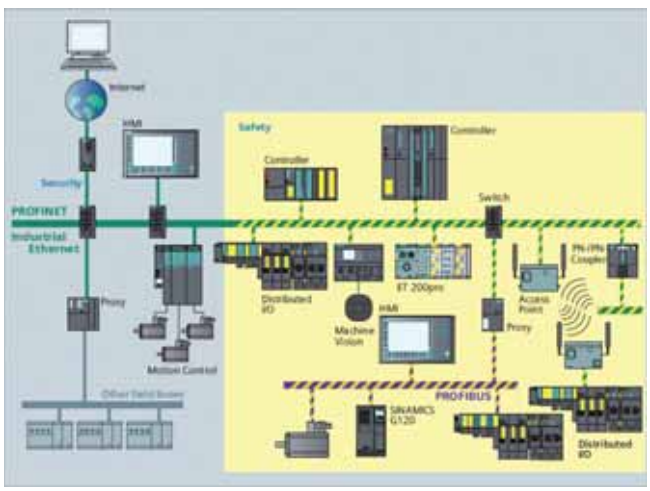
Comunicazioni... al servizio della sicurezza

I sistemi di comunicazione sono la trama che connette i dispositivi per la prevenzione delle situazioni di pericolo in ambito industriale

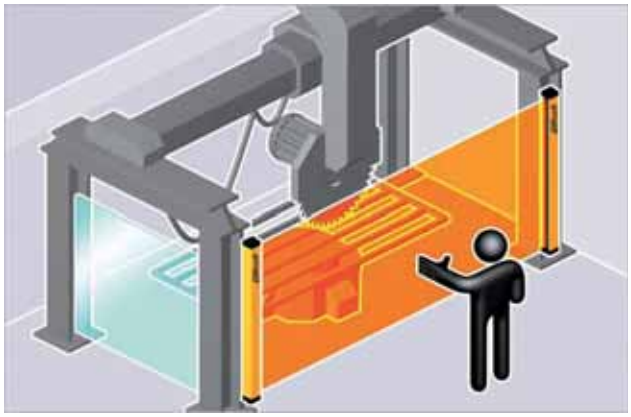
La sicurezza degli impianti industriali, intesa come tutela dell'incolumità dei lavoratori e salvaguardia dell'ambiente, prima ancora che di minimizzazione dei guasti e dei danni alle cose, deve molto all'evoluzione dei sistemi di comunicazione. Il passaggio dalla logica cablata alle architetture digitali ha infatti aperto nuovi e più elaborati scenari di prevenzione degli incidenti e di gestione delle emergenze. Oggi è possibile operare scelte complesse che tengano conto di tutta una serie di condizioni al contorno, in modo da salvaguardare la produttività senza per questo sacrificare l'incolumità dei lavoratori, o compromettere la sicurezza dell'ambiente di lavoro. Così, al verificarsi di un evento critico, invece di interrompere indiscriminatamente l'alimentazione, disattivando tutte le uscite del PLC che controlla il macchinario (causando così un improduttivo fermo macchina), un controllore logico dedicato alla sicurezza può mettere fuori linea solo la parte dell'impianto le cui operazioni potrebbero sfociare in situazioni di pericolo. La complessità delle decisioni che possono essere formulate è tanto più elevata, quante più informazioni possono essere inviate agli I/O intelligenti.

Un ulteriore vantaggio dell'impiego di dispositivi dotati di modalità avanzate di comunicazione è rappresentato dal trasferimento di informazioni diagnostiche, che, indicando quali sono i componenti con un elevato grado di usura o con alta probabilità di guasto, contribuiscono a prevenire futuri fermi macchina o potenziali condizioni di rischio per gli operatori.

Il ruolo determinante nell'implementazione di questa intelligenza decisionale spetta al software, sia a livello applicativo, sia a livello di driver nei singoli nodi, ma il lavoro più importante di prevenzione e messa in sicurezza viene svolto a un livello più vicino all'hardware.



La rete informatica gestionale e quella di controllo processo sono completate da una rete di sicurezza, che ha lo scopo di salvaguardare l'incolumità delle persone, dell'ambiente e delle cose



Barriere ottiche e dispositivi a scansione laser permettono di estendere il controllo a intere aree o volumi attorno all'area attiva della macchina

Prevenire gli incidenti, limitare i danni

Il mercato offre un'ampia scelta di dispositivi atti a suggerire i comportamenti corretti, guidare gli operatori e avvertirli in caso di trasgressione delle norme di sicurezza, costringerli a effettuare le manovre corrette e impedire quelle potenzialmente pericolose. Si va dai semplici pulsanti per l'azionamento in sicurezza e l'arresto delle macchine utensili, alle barriere ottiche e agli scanner laser che individuano situazioni di pericolo, passando per i sistemi di comunicazione e videosorveglianza per il monitoraggio delle operazioni critiche, per arrivare ai PLC e agli elaboratori dedicati alla sola gestione della sicurezza.

I dispositivi più semplici sono a volte quelli più importanti: le pulsantiere di sicurezza costringono gli operatori a tenere le mani lontano dalle aree pericolose durante il funzionamento delle macchine utensili, mentre pedane dotate di interruttori assolvono alla stessa funzione rilevando la presenza, o l'assenza, dell'operatore in aree in cui dovrebbe o non dovrebbe stare.

Barriere ottiche e dispositivi a scansione laser permettono di estendere il controllo a intere aree o volumi attorno all'area attiva della macchina. Altri interruttori si occupano di verificare che tutte le protezioni siano in posizione, prima di dare il consenso all'avvio delle operazioni, mentre i pulsanti per l'arresto di emergenza offrono un mezzo immediato, a chi rileva situazioni di pericolo, di fermare le operazioni e mettere in sicurezza la macchina. In questo quadro, entrano in gioco anche i sistemi di videosorveglianza e di comunicazione tradizionali, che permettono la supervisione delle operazioni più delicate da parte di personale in una postazione dedicata. Con l'aumento della potenza di calcolo dei moderni microprocessori si sono resi disponibili anche sistemi di visione artificiale in grado di riconoscere autonomamente il presentarsi di situazioni di pericolo. Sul fronte della prevenzione, infine, si possono impiegare grandi display alfanumerici a LED per evidenziare situazioni di pericolo e, se sono controllati da un sistema intelligente, connesso a sensori sul campo, suggerire la corretta condotta di sicurezza in base al particolare contesto operativo.

Mettere in sicurezza in caso di guasto

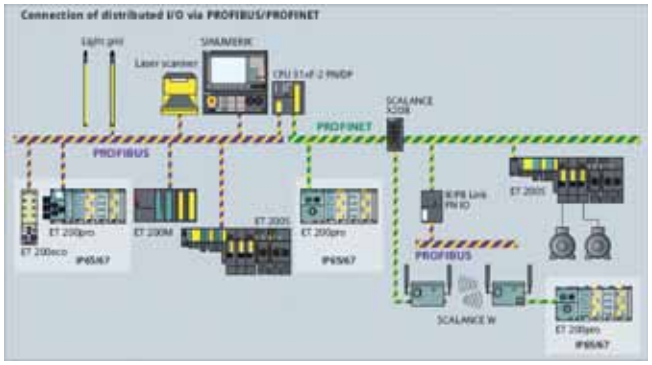
Pur nella loro eterogeneità, i vari dispositivi di sicurezza hanno tutti un elemento in comune: devono essere collegati alla macchina o al relativo sistema di controllo, in maniera tale da rendere virtualmente impossibile il venire meno della propria funzione di protezione. Si tratta di una prerogativa dei componenti di sicurezza che riguarda tanto il dispositivo in sé, quanto la rete della quale fa parte. Al dispositivo viene richiesto di comunicare tutte le possibili condizioni di malfunzionamento (mancanza di alimentazione, guasto al processore, deriva delle caratteristiche al di fuori dei limiti accettabili ecc.), inviando un segnale di errore al sistema di sicurezza. In nessun caso il verificarsi di un malfunzionamento del dispositivo deve potersi ripercuotere sul resto del sistema. Simili requisiti si applicano anche alla rete di comunicazione, che deve essere in grado di rilevare eventuali malfunzionamenti dei nodi che ne fanno parte, delle rispettive interfacce di comunicazione e del mezzo di trasmissione.

A differenza delle reti tradizionali, che possono tollerare ritardi nel trasferimento dei dati, perché, per esempio, è stato necessario ritrasmettere un messaggio a causa di errori non recuperabili, una rete 'di sicurezza' deve essere in grado di agire attivamente sui dispositivi per evitare danni alle cose o alle persone. Questo tipo di rete è generalmente costituita da un bus di campo dotato di un riconoscimento degli errori particolarmente robusto e di un meccanismo di reazione che, qualora si verifichino determinati eventi, o non via sia certezza dell'affidabilità delle informazioni ricevute, provveda alla messa in sicurezza dei dispositivi critici. Si tratta di una modalità operativa che prevede la disattivazione dei sottosistemi che possono causare danni a cose o persone (come un utensile, un braccio robotico, una pressa) e nell'attivazione dei dispositivi di segnalazione ed

emergenza (come lampeggianti e sirene, ma anche ventole e valvole per la rimozione di fluidi nocivi ecc.).

Caratteristiche dei bus di sicurezza

Nel corso degli anni il tradizionale anello di corrente 4-20 mA è stato lentamente soppiantato da metodologie di cablaggio strutturato, che hanno portato sostanziali vantaggi in termini di riduzione dei costi di cablaggio, di facilità di ampliamento e manutenzione, nonché di flessibilità d'impiego. Il ricorso ai bus per la gestione dei dispositivi di sicurezza è motivato dall'esigenza di cablare un numero sempre più elevato di interruttori, fotocellule, barriere ottiche e apparati di sicurezza, nonché dalla richiesta di una maggiore flessibilità dal punto di vista del trasferimento delle informazioni e della semplicità di configurazione. I moderni sistemi bus gestiscono moli di informazioni una volta impensabili e possono permettersi di raccogliere dati diagnostici, che contribuiscono a incrementare la sicurezza

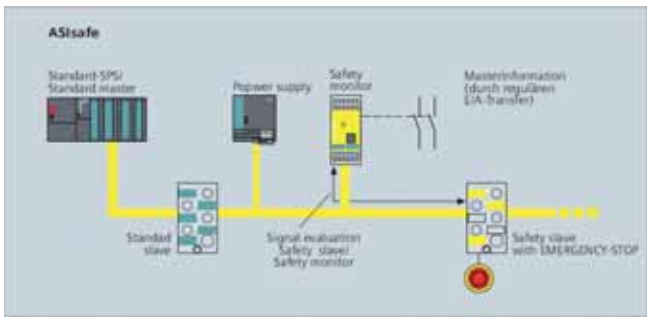


Profisafe estende il protocollo standard del bus Profibus secondo un approccio a canale nero

degli impianti, prevenendo i malfunzionamenti. Oggi non solo è normale vedere sistemi di sicurezza a bus in tecnologia digitale, ma si è anche sviluppato un orientamento verso sistemi ibridi, che utilizzano lo stesso bus per trasmettere i dati di processo, le informazioni diagnostiche e i messaggi pertinenti alla sicurezza. Alcune delle caratteristiche comuni ai principali bus di sicurezza sono il determinismo, l'esistenza di stati di messa in sicurezza e la ridondanza. Il determinismo implica che tutti i messaggi inerenti la sicurezza del sistema vengano trasmessi entro finestre temporali ben definite, così che sia possibile identificare l'insorgere di problemi in base alla mancata o errata durata della trasmissione dei dati. Se i messaggi di un dispositivo giungono al controllore senza rispettare il vincolo temporale, il sistema può essere messo in stato di sicurezza. La ridondanza può essere implementata in hardware o in software. Alcuni sistemi fanno uso di due canali e due CPU per verificare la coerenza dei dati di sicurezza ricevuti, mentre altri implementano protocolli che richiedono di trasmettere due volte, in un differente ordine, gli stessi dati sul medesimo canale. Sebbene dei meccanismi di verifica dell'integrità dei dati siano sempre presenti, la ridondanza hardware non è strettamente necessaria e diverse architetture di sicurezza riescono a soddisfare le certificazioni senza ricorrere a una costosa duplicazione del cablaggio. È tuttavia essenziale disporre di un metodo che assicuri la correttezza delle informazioni ricevute, o quantomeno limiti la probabilità di errore al di sotto di un limite accettabile, compatibilmente con i rischi di guasti, fermi macchina e danni a cose o persone. Esistono diversi meccanismi per assicurare l'integrità dei dati, così come esistono diverse cause di errore: guasti hardware, bachi nel software, rumore, diafonia, interferenze ad alta frequenza, congestione della rete, ritardi di propagazione ecc.. Tra le tecniche più collaudate, si possono citare il tradizionale controllo ciclico di ridondanza, la numerazione dei pacchetti dati, la marcatura temporale dei messaggi e i meccanismi di ritrasmissione delle informazioni andate perdute.

Standard di sicurezza

L'installazione dei dispositivi e sistemi di sicurezza è tipicamente regolamentata da normative e leggi volte a tutelare l'incolumità e la salute dei lavoratori, oltre che a prevenire danni alle proprietà e all'ambiente. Nella Comunità europea le normative di riferimento sono la Direttiva Quadro sulla Salute e Sicurezza sul Lavoro (89-391 EC), la Direttiva Macchine (2006-42 EC), la Direttiva Bassa Tensione (2006-95 EC) e la Direttiva Compatibilità Elettromagnetica (2004-108 EC). Con l'armonizzazione degli standard internazionali che si occupano di sistemi di sicurezza, i produttori di macchine e sistemi di controllo hanno potuto proporre, certificare e installare le proprie soluzioni di sicurezza in tutto il mondo. Questo ha contribuito a colmare il divario tecnologico che separava i bus di sicurezza dai più aggiornati bus per il controllo di processo e l'automazione di fabbrica. A oggi, le soluzioni di safety offerte vanno dalle più spartane connessioni in logica cablata dei vari dispositivi di sicurezza,



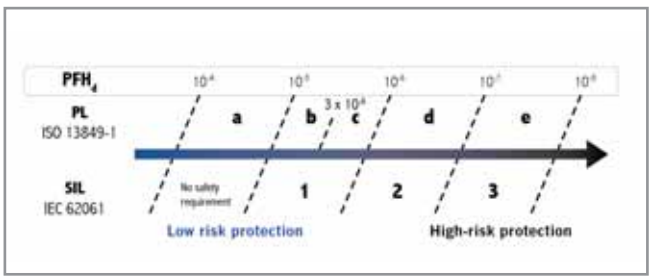
Il bus di sicurezza AS-i Safe permette di integrare direttamente su una rete AS-i tutta una serie di dispositivi di sicurezza

ai bus dedicati, i cui nodi sono dotati di interfacce certificate espressamente pensate per le funzioni di sicurezza. I principali standard di sicurezza sono, non sorprendentemente, il risultato dell'evoluzione dei più diffusi bus di campo 'tradizionali'. Le due tecnologie che hanno conosciuto il maggiore successo in termini di quote di mercato, con un installato di diversi milioni di dispositivi, sono Fieldbus Foundation SIS (Safety Instrumented System) e Profisafe, mentre AS-i Safe è una soluzione particolarmente semplice e flessibile, che permette di integrare direttamente su una rete AS-i dispositivi di sicurezza come pulsanti di arresto d'emergenza, barriere ottiche e sensori per porte di sicurezza ed esclusione dalle aree a rischio.

Questione di probabilità

Tutte le possibili cause di errore che possono determinare situazioni di pericolo devono essere identificate prima che l'impianto venga messo in linea. La Normativa IEC 61508 si occupa della sicurezza funzionale dei sistemi elettronici programmabili, in particolare delle reti di sicurezza, e copre l'intero ciclo di vita del sistema, dalla progettazione al decomissionamento e allo smaltimento.

Questo standard ha posto l'accento sulle modalità di determinazione del livello di integrità di sicurezza (SIL - Safety Integrity Level), espresso in termini di probabilità media oraria di un guasto o un errore critico. Tipicamente, le applicazioni di sicurezza in ambito industriale sono caratterizzate da un livello SIL3. La certificazione in base alla Norma IEC 61508 richiede che i produttori effettuino insieme agli utilizzatori delle valutazioni di rischio per le potenziali cause di guasto, fornendo una valutazione delle conseguenze e delle relative probabilità che si



I livelli di sicurezza SIL (descritti nella normativa IEC 62061) e PL (norma ISO 13849-1) sono classificati in base alla probabilità media che in un'ora si verifichi un guasto o un errore critico (PFH)

verifichino. La norma EN 954-1, relativa alla sicurezza delle macchine, è stata anch'essa ampliata in quest'ottica probabilistica e tradotta nella normativa EN ISO 13849-1. Il documento, che va sotto il nome di "Sicurezza delle macchine, Parti relative alla sicurezza dei sistemi di controllo - Parte 1: Principi generali di progetto", fornisce gli strumenti probabilistici per la stima delle evenienze di errore dei sistemi di controllo.

Canali in bianco e nero

Le soluzioni di sicurezza basate su bus possono essere di due tipi: a 'canale nero' e a 'canale bianco'. In primo tipo di approccio si utilizzano infrastrutture esistenti, non espressamente pensate per la trasmissione di dati di sicurezza, e si relega l'implementazione delle funzioni specifiche di controllo degli errori, integrità e ridondanza a uno strato di livello superiore, posizionato tra lo stack di comunicazione e lo strato applicazione.

Questo strato di sicurezza viene tipicamente garantito come conforme al livello SIL3 e risulta essere in grado di tollerare tra i suoi nodi la presenza di dispositivi non di sicurezza. Due esempi di questo approccio sono Profisafe, il cui sistema di trasmissione standard può essere usato tanto per i messaggi di sicurezza, quanto per le tradizionali comunicazioni di controllo di processo, e CIP Safety, che permette di implementare le funzioni di sicurezza in maniera indipendente dal mezzo (si applica, per esempio, a bus come Controlnet, Devicenet e Sercos). Il progresso tecnologico e la diffusione ormai sempre più capillare di bus di campo a standard aperto e adattabili alle esigenze di gestione della sicurezza sono tra i motivi della diffusione dell'approccio a canale nero negli impianti più moderni. Oltre a diminuire i costi dell'hardware per via dell'impiego di componenti off-the-shelf, presenta il vantaggio di minori costi di gestione per via della facilità di configurazione e del riutilizzo delle conoscenze maturate con i bus di campo tradizionali. L'approccio a canale bianco prevede, invece, l'esistenza di un'infrastruttura di comunicazione dedicata in termini di bus e di protocollo di comunicazione, che vanno ad affiancarsi a quelli che gestiscono i dati di produzione. È il caso di Safetybus p, messo a punto da Pilz. I componenti che realizzano l'infrastruttura di rete, il bus di comunicazione e i nodi di sicurezza richiedono una certificazione specifica per la particolare architettura usata.

Capita allora che in un impianto di produzione si trovino PLC a doppia tecnologia, per gestire la produzione da un lato, barriere di sicurezza, rivelatori di presenza, pulsanti di emergenza e interruttori di consenso dall'altro. I vantaggi di questo approccio risiedono nella separazione fisica delle reti, che possono evolvere in maniera indipendente in base alle esigenze, anche di budget, dell'utilizzatore.

Uno standard aperto e comune

Un interessante approccio a canale nero è rappresentato dal protocollo OpenSafety, promosso da Epsg (Ethernet Powerlink Standardization Group) con l'intento di riunire sotto un unico standard aperto di sicurezza tutte le reti utilizzate in ambito industriale. Lo scopo è quello di ridurre i costi di sviluppo delle soluzioni di sicurezza, appoggiandosi ad architetture di rete esistenti senza aggiungere ulteriori royalty.

OpenSafety è un protocollo che risiede nello strato di applicazione della pila OSI e rende possibile lo scambio di messaggi di sicurezza, fino al livello SIL3, attraverso reti Industrial Ethernet e a bus di campo (in particolare Sercos III, Modbus TCP, Ethernet/IP e Powerlink) e soluzioni dedicate sviluppate per uso interno. Il protocollo provvede a incapsulare i messaggi di sicurezza in trame, che contengono codici di controllo di ridondanza ciclica e meccanismi di salvaguardia dell'integrità. I datagrammi vengono inviati tramite tunneling sulle reti esistenti e si mescolano con il traffico dati 'tradizionale'. I dispositivi di sicurezza conformi allo standard OpenSafety riconoscono automaticamente il contenuto e provvedono a estrarre le informazioni d'interesse. Le funzioni di sicurezza possono così essere implementate in maniera indipendente dal particolare protocollo di trasporto usato.

È bene tenere presente, tuttavia, che le prestazioni del sistema sono limitate in prima istanza da quelle della rete su cui si appoggia lo strato applicativo OpenSafety. Se i tempi di risposta sono eccessivi, la rete è congestionata o disturbata da interferenze o, comunque, le condizioni operative rendono impossibile rispettare i vincoli di determinismo e integrità dei dati previsti dal protocollo applicativo, i nodi interessati vengono posti in sicurezza, con le prevedibili conseguenze sul funzionamento dell'impianto controllato. Il protocollo è liberamente scaricabile all'indirizzo *www.ixxat.com/zugangsdaten_powerlink_safety_en.html*.