Sicuri prendendo… il bus

Massimo Giussani

Il ricorso a una tecnologia digitale e programmabile per implementare le funzioni di sicurezza in ambito industriale ha cominciato ad affermarsi solo alcuni anni or sono, con considerevole ritardo rispetto all'evoluzione dei sistemi di controllo e di automazione. Tale ritardo è dovuto a una molteplicità di ragioni, non ultima la naturale resilienza degli utenti industriali ad abbracciare una tecnologia che non abbia ancora provato la sua ragion d'essere in termini d'incremento della produttività o di diminuzione dei costi.

Con la diffusione delle architetture a bus, la flessibilità e le prestazioni delle reti di controllo tradizionali vengono estese alla gestione della sicurezza

Tecnicamente il ricorso ai bus per la gestione dei dispositivi di sicurezza è motivato dall'esigenza di cablare un numero elevato di interruttori, fotocellule, barriere ottiche e dispositivi di sicurezza e dalla richiesta di una maggiore flessibilità dal punto di vista del trasferimento delle informazioni e della semplicità di configurazione.

L'evoluzione della tecnologia ha portato all'offerta di sistemi, anche aperti, che abbattono i costi di cablaggio iniziale, permettono di aggiungere nuovi componenti senza richiedere un rifacimento sostanziale e consentono la raccolta di dati diagnostici in un'ottica di manutenzione preventiva.

Dai relè ai bus digitali

Una rete di sicurezza è generalmente costituita da un bus di campo dotato di un riconoscimento degli errori particolarmente robusto e di un meccanismo di reazione che consenta la messa in sicurezza dei dispositivi critici, qualora si verifichino determinati eventi o se le informazioni ricevute non sono ritenute sufficientemente affidabili. A diffe-

Fonte: Vimar

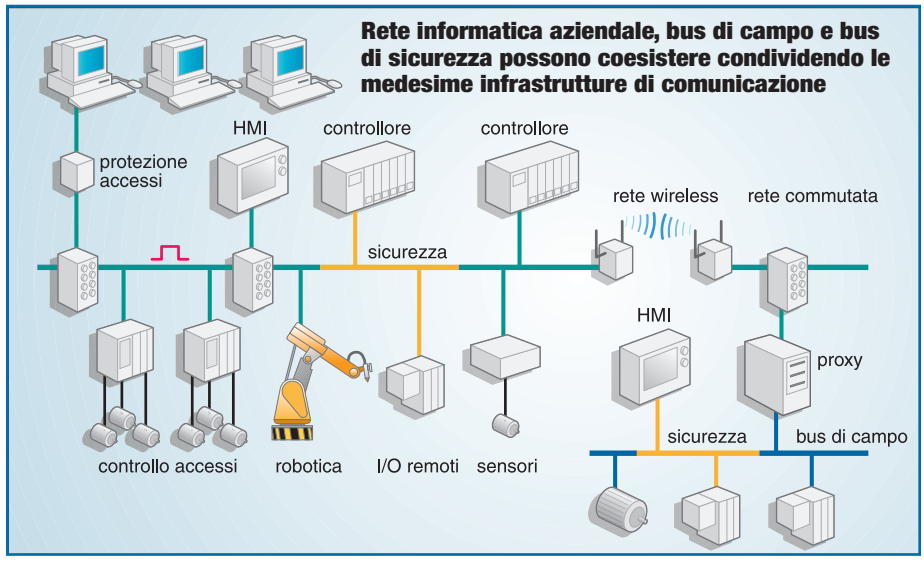
renza delle reti tradizionali, che possono tollerare ritardi nel trasferimento dei dati, perché è stato necessario, ad esempio, chiedere una ri-trasmissione a causa di errori non recuperabili, una rete di sicurezza deve essere in grado di agire attivamente sui dispositivi, per evitare danni a cose o persone.

I sistemi di sicurezza hanno subito, seppure con un considerevole ritardo dovuto al mancato aggiornamento delle normative e all'assenza di uno standard aperto, la stessa evoluzione dei sistemi di controllo degli impianti di produzione. All'inizio le varie attività di un impianto di produzione venivano regolate per mezzo di relè, che richiedevano però cablaggi elaborati e complessi quadri di controllo realizzati 'ad hoc'. Il passaggio alle logiche programmabili ha reso i sistemi più flessibili dal punto di vita della configurazione e dell'adattamento a nuove esigenze produttive, mentre l'adozione dei bus di campo ha permesso di ridurre la complessità e i costi del cablaggio grazie a un approccio più strutturato. L'avvento del digitale e la disponibilità di standard aperti, che hanno consentito l'interoperabilità sulla medesima rete di centinaia di dispositivi di vario tipo e di differenti produttori, hanno finalmente portato all'affrancamento dei sistemi di controllo ad automazione da costosi e ingessati apparati proprietari. I sistemi di sicurezza sono a lungo rimasti relegati ai primi stadi di questo sviluppo, in parte per problemi di certificazione e, conseguentemente, di esportazione; in parte per la titubanza degli utilizzatori nel passare a soluzioni non sufficientemente rodate.

I progressi della tecnologia digitale, l'affermazione di standard aperti adatti a gestire le operazioni di sicurezza e la recente armonizzazione delle normative in merito hanno portato una 'ventata' di modernizzazione anche in questo settore. Oggi non solo è normale vedere sistemi di sicurezza a bus in tecnologia digitale, ma si è sviluppato anche un orientamento verso sistemi ibridi, che impiegano lo stesso bus per trasmettere i dati di processo, le informazioni diagnostiche e i messaggi pertinenti alla sicurezza.

I vantaggi dell'approccio basato su bus

Il mercato mette a disposizione un'offerta variegata di soluzioni di sicurezza. Si spazia dal semplice controllo affidato a pulsanti, barriere e commutatori da connettere tra loro in logica cablata, ai PLC dedicati per il controllo locale dei dispositivi di sicurezza, fino a sistemi dotati d'intelligenza più o meno avanzata, in grado di dialogare su un bus digitale con aree selezionate dell'impianto.



Il principale vantaggio dato dall'impiego di controllori avanzati di sicurezza rispetto all'antiquata logica cablata risiede nella possibilità di operare scelte ragionate a seguito del verificarsi di un evento critico.

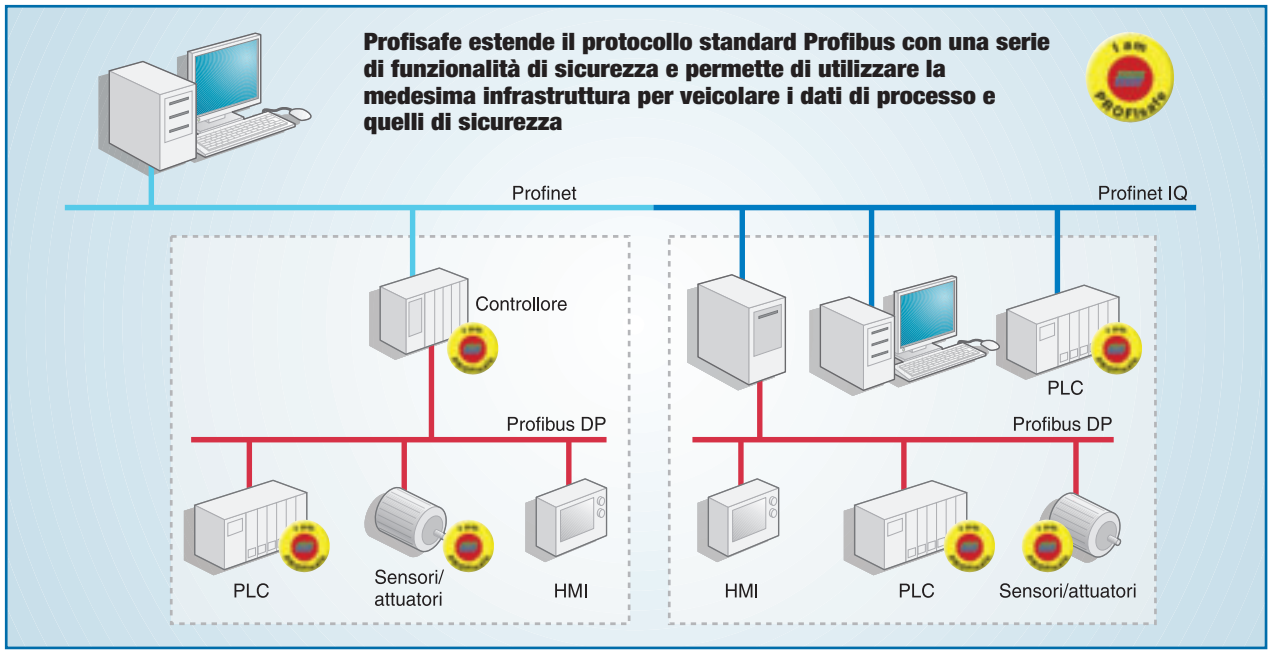
Anziché sospendere l'alimentazione a tutte le uscite del PLC, ponendo le condizioni per un improduttivo fermo-macchina, il controllore separato può disattivare solo la parte dell'impianto le cui operazioni potrebbero risultare pericolose, lasciando inalterato il funzionamento di tutto il resto o della singola macchina. L'impatto sulla produttività può essere dunque sufficiente a giustificare i maggiori investimenti richiesti, ferme restando la semplificazione delle operazioni di cablaggio e di configurazione. Chiaramente, la complessità delle decisioni è legata alla quantità di informazioni che possono essere gestite dai controllori e inviate attraverso il bus agli I/O intelligenti. Un 'bonus' che deriva dall'utilizzo di dispositivi dotati di modalità avanzate di comunicazione è rappresentato dal trasferimento di dati diagnostici che contribuiscono a prevenire futuri fermo-macchina, indicando quali sono i componenti con un elevato grado di usura o con alta probabilità di guasto. In tutto questo, a fare la 'parte del leone' è il software, sia a livello applicativo, sia di driver nei singoli nodi.

Caratteristiche dei bus di sicurezza

Alcune delle caratteristiche comuni ai principali bus di sicurezza sono: il determinismo, l'esistenza di stati di messa in sicurezza, la ridondanza.

Per quanto concerne il primo punto, tutti i messaggi inerenti la sicurezza del sistema devono essere trasmessi in un delimitato intervallo temporale, in modo che sia possibile identificare l'insorgere di problemi in base alla mancata o errata trasmissione dei dati. Se i messaggi di un dispositivo giungono al controllore senza rispettare tale vincolo, l'unità stessa può essere messa in stato di sicurezza.

La 'messa in sicurezza' è una modali-



tà operativa che consiste tipicamente nella disattivazione degli elementi 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, ad esempio lampeggianti e sirene, oppure ventole e valvole per la rimozione di fluidi pericolosi.

La ridondanza può essere implementata in hardware o in software. Ad esempio, alcuni sistemi fanno uso di due canali e due CPU per verificare la coerenza dei dati di sicurezza ricevuti; 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.

Integrità certificata

Disporre di un metodo che assicuri la correttezza delle informazioni ricevute o che consenta di tenere le probabilità di errore al di sotto di un limite accettabile, compatibilmente con i rischi di guasti, fermo-macchina e danni a cose o persone, è chiaramente fondamentale.

I meccanismi per assicurare l'integrità dei dati possono essere di vario tipo, anche perché altrettanto diverse possono essere le cause di errore: guasti hardware, bachi nel software, rumore, diafonia, interferenze ad alta frequenza, intasamento della rete, ritardi di propagazione. Tra le tecniche collaudate si possono citare il tradizionale controllo ciclico di ridondanza, la numerazione dei pacchetti di dati, la marcatura temporale dei messaggi e le ritrasmissioni.

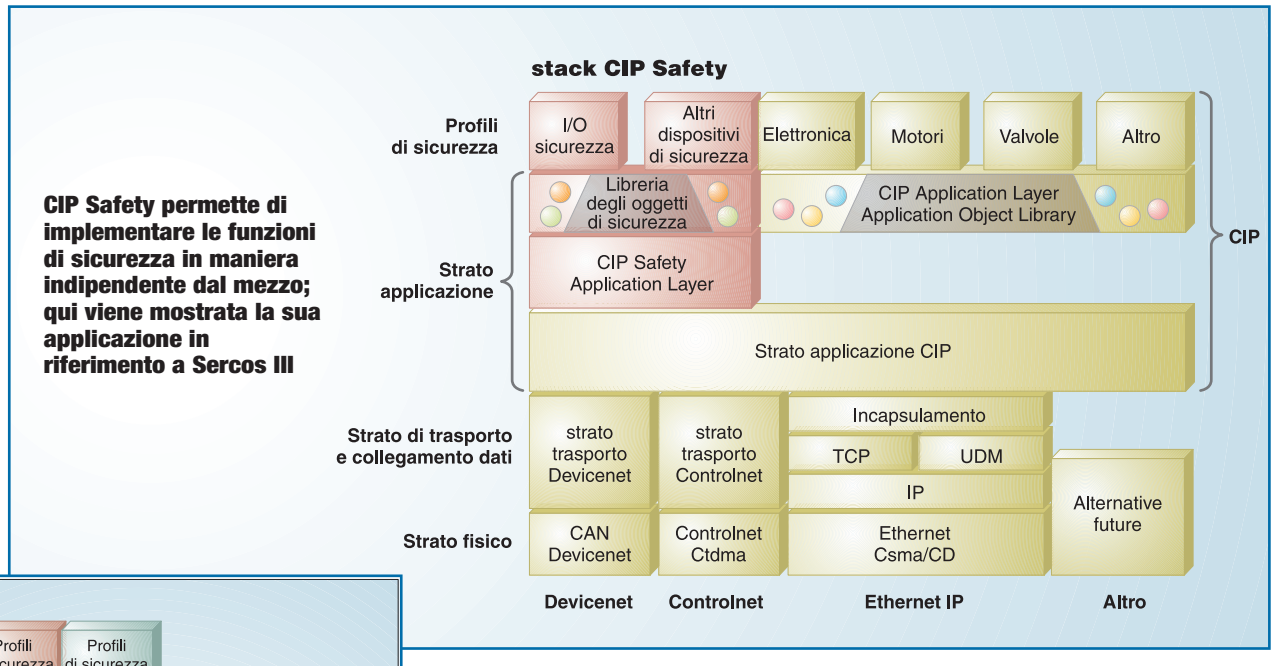
Diverse normative internazionali si occupano della descrizione dei metodi di controllo degli errori di comunicazione. In particolare, la recente norma IEC 61508 si occupa della sicurezza funzionale dei sistemi elettronici programmabili e soprattutto delle reti di sicurezza. Essa pone l'accento sulle modalità di determinazione del livello d'integrità di sicurezza SIL (Safety Integrity Level).

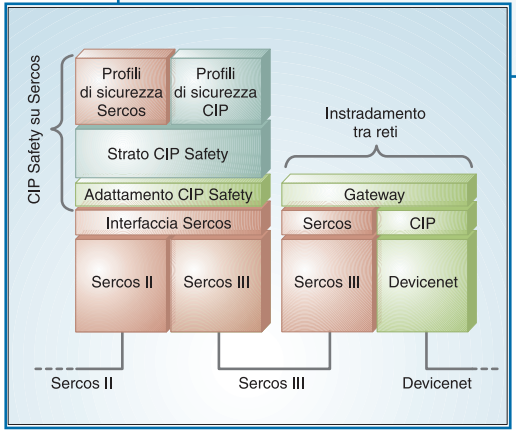
Le applicazioni di sicurezza in ambito industriale devono avere tipicamente un livello SIL3. La certificazione in base alla norma IEC 61508 richiede che i produttori effettuino insieme agli utilizzatori delle valutazioni di rischio per le potenziali cause di guasto, fornendo una valutazione delle conseguenze e delle relative probabilità che tali guasti si verifichino.

La norma EN 954-1, relativa alla sicurezza delle macchine, è stata ampliata in quest'ottica probabilistica e tradotta nel-

PRINCIPALI STANDARD DI SICUREZZA ATTUALMENTE DISPONIBILI

Bus di sicurezza	Organizzazione - Azienda proponente	Web
AS-i Safety at Work	AS-International Association	www.as-interface.net
Canopen Safety	CiA-CAN in Automation	www.can-cia.org
CIP Safety	Odva-Rockwell Automation	www.odva.org
Interbus Safety	Interbus Club-Phoenix Contact	www.interbusclub.com
Profisafe	PNO-Siemens	www.profibus.org
Safetybus p	Safetybus P Club International-Pilz	www.safetybus.com
Sercos Safety	IGS	www.sercos.com





la normativa EN ISO 13849-1, che la sostituirà a partire dal 30 novembre 2009. Il nuovo 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.

Un'offerta variegata

L'armonizzazione degli standard internazionali riferiti ai sistemi di sicurezza ha messo i produttori nella posizione di realizzare, certificare e commercializzare soluzioni di sicurezza di vario genere e ha di fatto gettato un ponte sopra il divario tecnologico che separava questi sistemi dai più aggiornati bus per il controllo di processo e l'automazione di fabbrica.

Ad oggi, le soluzioni disponibili spaziano dai semplici dispositivi di sicurezza interconnessi in logica cablata, ai bus dedicati, che richiedono componenti certificati, dotati di interfacce specificamente pensate per le funzioni di sicurezza, fino ai sistemi in grado di appoggiarsi a infrastrutture pre-esistenti per mezzo di opportuni protocolli degli strati superiori.

La denominazione attribuita alle soluzioni di sicurezza basate su bus sono: a 'canale nero' e a 'canale bianco'.

Quest'ultimo approccio prevede 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 da un lato la produzione, dall'altro barriere di sicurezza, i rivelatori di presenza, i pulsanti d'emergenza e gli interruttori di consenso. 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'utente.

L'approccio a canale nero, invece, fa uso di infrastrutture esistenti non espressamente pensate per la trasmissione di dati di sicurezza e delega 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 conforme al livello SIL3 ed è in grado di tollerare la presenza sul bus di dispositivi non di sicurezza. Esempi di questo approccio sono Profisafe, estensione di sicurezza per il bus di campo Profibus, e CIP Safety, che permette di implementare le funzioni di sicurezza in maniera indipendente dal mezzo e si applica a bus come Controlnet, Devicenet e Sercos.

Il progresso tecnologico e la presenza sempre più capillare di bus di campo a standard aperto, adattabili alle esigenze di gestione della sicurezza, sono tra i motivi della diffusione di questo approccio negli impianti più moderni. Oltre a diminuire i costi dell'hardware per via dell'impiego di componenti generici, questa soluzione presenta il vantaggio di minori costi di gestione, data la facilità di configurazione e la possibilità di riutilizzo delle conoscenze maturate sui bus di campo tradizionali. ■