Integrati ma separati

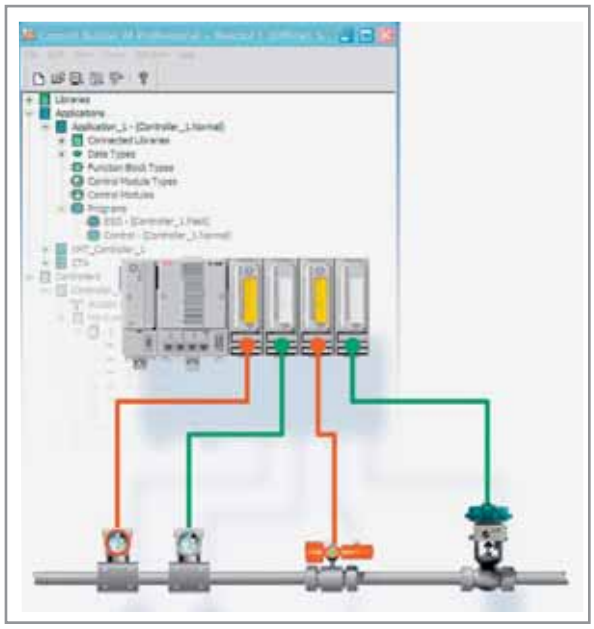
La possibilità per gli utenti di automazione di far coesistere funzioni di controllo e funzioni di sicurezza apre la via a nuovi orizzonti

Roger W. Prew*

In passato nelle soluzioni di automazione era necessario investire in due sistemi separati, ovvero un sistema base per il controllo di processo (Bpcs) e un sistema strumentale di sicurezza SIS (Safety Instrumented System). Oggi i produttori hanno varie possibilità di far coesistere funzioni di controllo e di sicurezza in un unico sistema condividendo il processore, benché secondo alcuni non ci possa essere compatibilità se non a discapito dell'integrità globale, quindi della sicurezza funzionale. Si tratta di un dibattito aperto, nel quale ABB interviene proponendo l'architettura combinata di sicurezza e controllo 800xA High Integrity, inclusa nel sistema per l'automazione 800xA. Con tale architettura, ABB ha dimostrato che l'integrazione è possibile, pur mantenendo separate le funzioni di sicurezza e controllo grazie a moderne tecniche di elaborazione ad alta integrità, ai firewall e alla diagnostica attiva. Il sistema avviamento risulta inoltre pienamente conforme agli standard di sicurezza internazionali.

I vantaggi del sistema unico

A livello macroscopico, l'integrazione di un sistema SIS e di un sistema Bpcs diminuisce i costi di esercizio e i costi di progettazione, ingegnerizzazione e implementazione delle modifiche. Nella fase di definizione del sistema, la flessibilità di poter trasferire gli I/O e le funzioni tra il SIS e il Bpcs, senza alterare l'architettura di sistema, semplifica il processo di design e consente di ottenere una soluzione più efficiente ed economica. In fase di integrazione, la stessa flessibilità assicura che la separa-

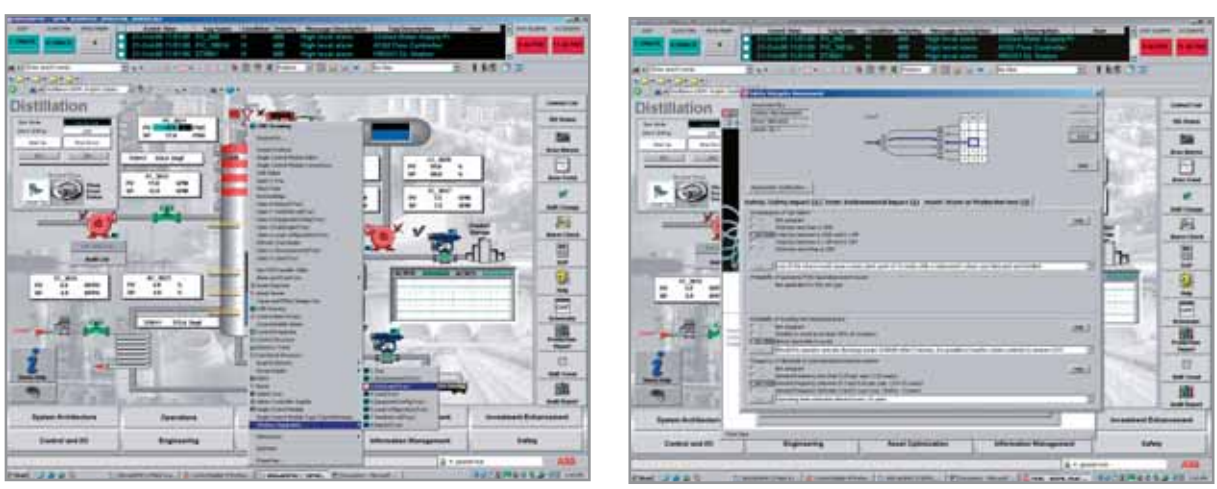


Con il sistema 800xA HI di ABB aumenta l'accesso ai dati da parte del sistema di sicurezza e dei tool di gestione di applicazioni e processi del DCS

zione tra Bpcs e SIS rispecchi i requisiti effettivi e non sia forzatamente imposta a un'architettura pensata molto tempo prima. A ciò si aggiungono i risparmi sui costi, derivanti dall'utilizzo condiviso di strumenti di configurazione, reti di comunicazione, ricambi, manutenzione, addestramento, assistenza e aggiornamenti e la possibilità di accedere a un patrimonio di dati più ricco, in comune tra il sistema di sicurezza e i tool di gestione di applicazioni e processi del sistema di controllo distribuito. Abilitare il collegamento in tempo reale tra i parametri delle due componenti è possibile solo eseguendo le due applicazioni nello stesso controller e significa ripartire i costi dei dispositivi di campo e dei cablaggi tra i due sistemi, ottimizzando l'architettura fisica. La totale integrazione consente peraltro di mettere a disposizione del sistema di gestione delle risorse Bpcs tutti i dati relativi alle cosiddette 'funzioni strumentali di sicurezza' (SIF); inoltre, il vasto patrimonio di dati e gli strumenti di analisi del Bpcs possono essere sfruttati in modo coerente e uniforme anche dal SIS.

Normative e standard

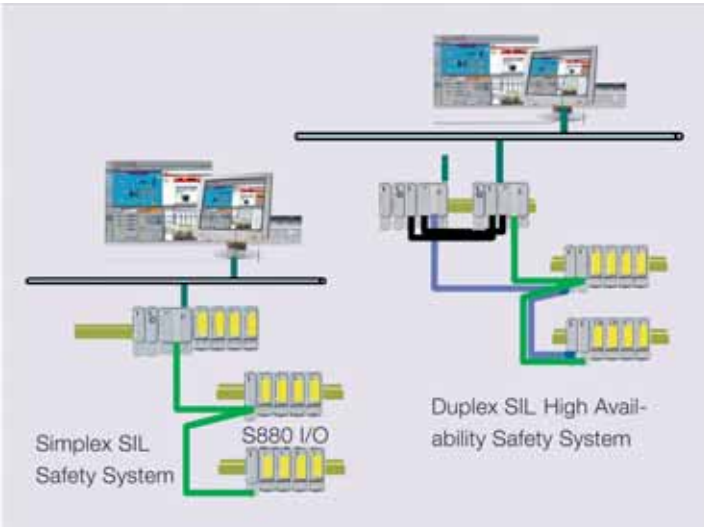
La sicurezza dei processi ha assunto via via un'importanza maggiore in ambito industriale: oggi essa è una competenza che rientra nel curriculum di ingegneri e tecnici e sono state sviluppate apposite linee guida per regolamentare questa area critica. L'attuale standard generico per i sistemi elettronici e programmabili IEC 61508 è il risultato degli sforzi congiunti compiuti dalle industrie e dagli enti normatori negli ultimi trent'anni: l'obiettivo dello standard è promuovere l'adozione di adeguate strategie di mitigazione del rischio in tutti i settori ove sono presenti processi pericolosi.
Questa norma generica e la norma specifica per le industrie di processo IEC 61511, nate come raccomandazioni, sono ormai considerate 'buone prassi' dai normatori, oltre che un valido riferimento per verificare il livello di sicurezza dei sistemi elettrici, elettronici ed elettronici programmabili. I due standard sono utilizzati come benchmark per i sistemi industriali installati con vincolo di prescrizione. La norma IEC 61511, in particolare, definisce i metodi di valutazione dei rischi associati a particolari processi pericolosi e determina il livello di riduzione del rischio che il sistema o i sistemi di sicurezza devono raggiungere. Ha valore prescrittivo quando stabilisce che il rischio deve essere soppesato e ridotto "al minimo livello ragionevolmente praticabile". Non specifica, tuttavia, quali tecnologie e architetture debbano essere implementate per ottenere questo risultato. Il sistema 800xA HI raggiunge questo obiettivo poiché condivide l'unità di elaborazione e altri componenti con il DCS e ottimizza molti aspetti del Bpcs.



Rappresentazione grafica dei rischi per una funzione di protezione contro un evento pericoloso

Tecnologie attuali

Molti sistemi di sicurezza stand alone reperibili oggi sul mercato sono anteriori alla pubblicazione delle norme IEC e impiegano tecnologie di varia natura per ottenere il livello di alta integrità richiesto dalle applicazioni di sicurezza ai fini del controllo. Il concetto di 'alta integrità' presuppone una doppia logica di funzionamento, 'fail safe' (il sistema reagisce ai guasti in modo predeterminato e sicuro) e 'fault tolerant' (il sistema non si blocca in caso di guasto ad alcuni componenti, ma continua a funzionare eventualmente con funzionalità ridotte). Un sistema fault tolerant non è necessariamente anche fail safe: una configurazione ridondante o con ridondanza modulare tripla non lo rende automaticamente idoneo alle applicazioni di sicurezza. Un sistema 'fail safe', da parte sua, non deve necessariamente essere ridondante per conformarsi al suo SIL: la ridondanza è integrata solo per ottimizzare le caratteristiche di affidabilità e disponibilità del sistema. Oggi è del resto possibile escludere già in fase di progettazione molte avarie pericolose e la copertura diagnostica al 100 per cento protegge l'integrità senza ricorrere alla duplicazione: i requisiti di fail safe per l'integrità della sicurezza e di fault tolerance per la disponibilità possono essere considerati in maniera indipendente e utilizzati quando e dove opportuno. C'è un acceso dibattito in merito all'affidabilità dell'hardware dei sistemi elettronici e programmabili, ma la moderna elettronica ad alta integrazione con tecnologia a montaggio superficiale è comunque considerata altamente affidabile, tanto che, in un SIS, l'hardware del 'logic solver' è l'elemento più affidabile dell'intero loop di sicurezza come dimostra il fatto che alcuni attuali sistemi semplici hanno indici Mtbf (Mean Time Between Failures) migliori rispetto alla passata generazione di sistemi a ridondanza doppia o tripla, dove l'affidabilità non triplica né quadruplica, perché il tasso di guasto è proporzionale al numero di componenti e alla complessità.



Architettura del sistema di sicurezza 800xA HI

Una nuova generazione di sistemi

Grazie alla sua flessibilità, il sistema 800xA di ABB centra idealmente due importanti obiettivi: coniugare le funzioni di sicurezza e controllo in un unico controller e tenere le funzioni separate all'interno della medesima rete integrata. Il sistema 800xA HI (High Integrity) non è un DCS modificato né un DCS cui sono state aggiunte delle funzionalità di sicurezza, bensì è un sistema interamente progettato per rispondere ai requisiti del mercato della sicurezza e delle attuali norme in materia. I programmi di sicurezza, infatti, sono compilati utilizzando un compilatore di istruzioni certificato per 800xA HI. Perché un sistema di sicurezza sia conforme alle norme vigenti in questo campo deve soddisfare quattro condizioni: l'affidabilità (PFD), nel cui concetto rientra il fatto che i dati relativi ai sottosistemi che partecipano a una funzione di sicurezza devono comporre il set di dati certificati in modo da poter valutare il SIL dell'intero loop; l'indice SFF (Safe Failure Fraction), che misura la capacità del sistema di rilevare e scongiurare avarie pericolose; la valutazione di ogni vincolo o vantaggio per l'integrità derivanti dall'architettura di sistema, documentando le relative implicazioni sul SIL; l'integrità sistematica, che deve ottemperare alle clausole dello standard.

Lo sviluppo del sistema di sicurezza 800xA HI ha tenuto conto di queste quattro condizioni: il team di ingegneri ha lavorato secondo processi di gestione della sicurezza funzionale sottoposti a rigorose verifiche di controllo e il progetto è stato approvato in ogni sua fase dal TÜV. Uno specialista in materia di certificazione, supportato da consulenti esterni, ha sovrinteso alla progettazione per garantire la piena conformità di tutti i componenti del sistema ai requisiti richiesti.

Il sistema di sicurezza di ABB condivide l'unità di elaborazione e altri componenti con il DCS, ottimizzando molti aspetti del pacchetto B, poiché aumenta la copertura diagnostica, comporta un modello di esecuzione deterministico, è sinonimo di maggiore affidabilità e precisione dei valori misurati, nonché delle azioni di controllo. Inoltre, permette una comunicazione più rapida tra il Bpcs e le funzioni del SIS, consentendo di ottimizzare il controllo di processo nel rispetto dei confini di sicurezza stabiliti.

A ciascuno il suo spazio

Al di là della vitalità del dibattito, gli standard IEC 61508 e IEC 61511 riconoscono di fatto che la funzione di sicurezza e altre funzioni possono risiedere nello stesso sistema se "si può provare che l'implementazione delle funzioni di sicurezza e delle altre funzioni è sufficientemente indipendente (ovvero se il guasto di una funzione non correlata alla sicurezza non determina una pericolosa avaria delle funzioni di sicurezza)" (IEC 61508-2 punto

7.4.2.3). Le norme esigono anche che la possibilità di guasti dipendenti dal modo comune sia ridotta a un livello accettabile (IEC 61511 Parte 1 punto 9.5.1/2). Il sistema 800xA tiene conto di queste norme: la sua natura modulare è infatti conforme alle prescrizioni degli standard per quanto riguarda la separazione funzionale e i guasti di modo comune. Il partizionamento della memoria, i contesti di esecuzione separati, i firewall e le tecniche di gestione degli stack, collegati ai due ambiti di protezione ed elaborazione dei dati, garantiscono che i programmi di sicurezza e quelli di altra natura, eseguiti nel medesimo ambiente di elaborazione, siano effettivamente separati e non interferiscano l'uno con l'altro. L'integrità della funzione di sicurezza è assicurata limitando le comunicazioni generali con l'interfaccia uomo-macchina (MMI) alla capacità di sola lettura e istituendo una funzione 'safe write' per la sovrascrittura che si può abilitare solo con un intervento manuale sul controller. La comunicazione 'peer to peer' tra le funzioni di sicurezza e le altre funzioni è strettamente controllata per proteggere l'integrità della funzione di sicurezza. Il controllo a ridondanza ciclica CRC (Cyclic Redundancy Check) e i controlli di rilevanza permettono di considerare la rete peer to peer alla stregua di supporto fisico ininfluente. Per la riduzione del rischio è stata inoltre eseguita un'attenta analisi secondo il metodo Lopa (Layers of Protection Analysis), un metodo semplificato per la valutazione del rischio alla luce di criteri di tolleranza che permettono di stabilire se le protezioni esistenti sono adeguate o richiedono un ulteriore potenziamento. L'analisi ha confermato che gli indici Lopa per le funzioni di protezione implementate nell'applicazione DCS e operanti in un nodo combinato controllo-sicurezza o in un nodo 800xA separato sono equivalenti a quelli delle funzioni implementate in architetture con sistemi di sicurezza e controllo totalmente differenti. I vantaggi per l'integrità dati dall'esecuzione delle applicazioni Bpcs nel controller di 800xA HI eclissano i rischi aggiuntivi determinati dai possibili guasti di modo comune. Inoltre, i programmi di sicurezza vengono compilati utilizzando un compilatore di set di istruzioni limitato, certificato per 800xA HI: durante il processo di compilazione, ulteriori verifiche e controlli CRC garantiscono l'integrità del programma di sicurezza compilato. L'esecuzione a blocchi dell'applicazione durante il runtime viene testata secondo criteri di ordine, esecuzione e check di discrepanza; le comunicazioni interne tra gli elementi di elaborazione e gli I/O sono duplicate e sottoposte a doppia verifica; l'uso di hardware diverso e dissimile per gli I/O e i processori e la presenza di un sistema operativo in tempo reale (Rtos) certificato TÜV nel modulo di sicurezza assicurano infine la piena conformità del sistema 800xA HI ai requisiti di integrità della norma IEC 61511.

Affidabilità e disponibilità

Il sistema 800xA HI è dunque intrinsecamente fail safe, con copertura diagnostica pressoché totale anche come applicazione semplice: ABB dichiara un indice SFF del 99,9 per cento, il che esclude che ci siano modalità di guasto pericoloso non rilevate all'interno del sistema; si tratta di un risultato ottenuto in virtù di un hardware progettato per essere pienamente conforme a SIL 3. La differenziazione dell'hardware negli I/O, il CRC locale e il controllo dei blocchi, coadiuvati dall'architettura di processore/modulo di sicurezza, eliminano i guasti di modo comune. I risultati convalidati dell'analisi Fmea (Failure Mode and Effects Analysis) e i tassi di guasto collocano il prodotto nella fascia di eccellenza del 6 per cento della categoria SIL 3. I valori PFD sono pubblicati e si basano su un 'proof test interval' di otto anni. Nei settori di gas e petrolio, in particolare, i sistemi di sicurezza con logic solver promettono un funzionamento ininterrotto per almeno quindici anni e la piena compatibilità con aggiornamenti, modifiche e ottimizzazioni nello stesso arco di tempo. Il sistema 800xA HI offre un'architettura ridondante che può essere implementata in modo indipendente a livello di I/O e al livello dell'operatore per abilitare capacità di fault tolerance e quindi aumentare la disponibilità in un sistema che già vanta ottime caratteristiche di integrità. Il sistema ridondante è anche in grado di aggiornare l'applicazione di sistema in tutta sicurezza e on line. ■

Il sistema 800xA HI di ABB è certificato a norma IEC 61508 e IEC 61511 ed è approvato dal TÜV

ABB readerservice.it n. 84

*Traduzione e adattamento a cura di Mario Brianza