Reti safety per l'industria

Cristina Paveri (*)

Fonte: blog.princeton.edu

La sicurezza nelle reti di automazione: un confronto fra Profisafe, Safety over Ethercat, Powerlink Safety, Ethernet/IP Safety e Devicenet Safety

Ogni processo industriale è più o meno associato al rischio di danni o lesioni; alcune applicazioni speciali quali macchine utensili, robot e processi chimici presentano un rischio molto elevato. Il tasso di guasto garantito dalle tecnologie di automazione standard è insufficiente per queste applicazioni, quindi occorre adottare soluzioni apposite per la sicurezza.
Se un tempo, poi, l'automazione di sicurezza era cablata e basata su relè, oggi è possibile ottenere soluzioni flessibili ed efficienti grazie all'integrazione di microcontrollori, moduli logici compatti e software collaudati per milioni di operazioni in applicazioni di sicurezza. Essenziale per il successo dell'integrazione è lo scambio sicuro dei dati tra i componenti.

Il livello di sicurezza

La norma IEC 61508, di riferimento per le apparecchiature elettriche, introduce un approccio statistico al calcolo della probabilità di guasto e la determinazione del livello di sicurezza funzionale SIL (Safety Integrity Level). Il livello SIL3, ad esempio, richiede per l'intero sistema di sicurezza una probabilità di un guasto pericoloso per ora (PFH) pari a 10^{-7}, riservandone una percentuale dell'1 per cento al protocollo (PFH<10^{-9}).

Profisafe

Il protocollo Profisafe è nato con l'obiettivo di ridurre la probabilità di errore nella trasmissione dei dati fino al livello SIL3 certificato. Facilmente realizzabile, è compatibile con applicazioni che già utilizzano Profibus e Profinet; consente infatti la coesistenza su un unico canale di messaggi standard e di sicurezza sui bus preesistenti, senza precludere la possibilità di separazione fisica tra comunicazioni standard e di sicurezza. Omologato per le comunicazioni wireless (Wlan e Bluetooth), Profisafe è utilizzabile su dorsali Ethernet industriali aperte e offre elevata disponibilità, bassa dissipazione di potenza e tempi di risposta brevi (ms); è indipendente dai canali di trasmissione (cavi di rame, fibre ottiche, wireless) visti come 'black channel', dalle velocità di trasmissione e dai meccanismi di rilevamento degli errori. I parametri sono definiti e ottimizzati, come per Profibus e Profinet, nel file GSD (General Station Description). Profisafe, basandosi sulla comunicazione ciclica tra controllore di bus e dispositivi di campo, permette il rilevamento immediato di ogni dispositivo guasto mediante 'polling'. La relazione di comunicazione tra il controllore di bus e i dispositivi di campo è 1:1.
Il byte di controllo del messaggio dall' host e il byte di stato da un determinato dispositivo servono a sincronizzare il trasmettitore e il ricevitore. Il numero sequenziale non viene trasmesso nel messaggio di Profisafe: il trasmettitore e il ricevitore utilizzano i propri contatori sincronizzati con il byte di controllo o di stato. Il controllo della sincronizzazione avviene tramite l'inclusione dei valori del contatore nel calcolo del CRC.

Safety over Ethercat

Per realizzare la comunicazione sicura dei dati su Ethercat, il gruppo ETC ha sviluppato il protocollo Safety over Ethercat, certificato TÜV al livello SIL3/IEC61508. Questo protocollo 'sicuro' permette la coesistenza di informazioni di sicurezza e standard nello stesso sistema di comunicazione a canale singolo; la soluzione è indipendente dal protocollo e dai supporti di comunicazione visti come 'black channel' e dal meccanismo di rilevamento degli errori, oltre a non presentare limitazioni quanto alla lunghezza dei dati di sicurezza, alla velocità di trasmissione e al tempo ciclo. Ogni frame di sicurezza contiene i dati di sicurezza del processo e il back up dei dati e viene elaborato nei dispositivi a livello dell'applicazione.
Safety over Ethercat è in grado di gestire errori nei dati, quali corruzione, ripetizione, scambio, perdita, ritardo, inserimento, mascheratura e indirizza-

Ogni processo industriale implica dei rischi, per cui è fondamentale valutarne il grado di sicurezza, in conformità alla normativa vigente

mento non valido. In particolare, per evitare l'accumulo di ritardi tra diversi cicli e assicurare la corretta ricezione del messaggio, Safety over Ethercat si basa su un tempo globale e sulla registrazione cronologica. Tra le varie misure di sicurezza spiccano l'assegnazione di un numero di sessione e di un identificativo univoco per connessione e slave, l'utilizzo del 'checksum' CRC e di un numero sequenziale. La relazione univoca fra master e slave permette di monitorare l'intero percorso master-slave e di assicurare carichi moderati di accesso al sistema di comunicazione, per evitare limitazioni alla larghezza di banda.

Powerlink Safety

Il protocollo di sicurezza Powerlink Safety è realtime e aperto, SIL3 certificato TÜV con cicli di comunicazione dell'ordine dei microsecondi; indipendente dal protocollo di trasporto, è utilizzabile anche per reti diverse (CAN). Per le caratteristiche di temporizzazione e il ridotto jitter, Powerlink è la base ideale per Powerlink Safety, pur non rappresentando un prerequisito essenziale. Powerlink Safety supera le limitazioni alla larghezza di banda riservando a ciascun nodo la banda necessaria; assicura l'integrità del trasferimento dei dati impedendo duplicazioni, perdite o manipolazioni e inserimenti, riconoscendo le sequenze errate o i ritardi eccessivi, verificando periodicamente il funzionamento di tutti i segmenti della rete di sicurezza e, per interruzioni o trasferimenti incompleti, attivando le funzioni di sicurezza o avviando l'arresto di emergenza. Il formato del telegramma è flessibile, la lunghezza del frame variabile in base alla quantità dei dati. I nodi di sicurezza della rete riconoscono automaticamente il contenuto, senza che sia necessario configurare il tipo e la lunghezza del frame.
Questo protocollo raggruppa tutte le funzioni di sicurezza nello strato di sicurezza di Powerlink e, poiché utilizza solo gli strati relativi all'applicazione del modello OSI, è indipendente dal bus impiegato. Suddivide il formato dei dati in due sotto-frame di contenuto identico e ne garantisce l'integrità mediante checksum: durante la lettura, il protocollo utilizza i checksum per verificare che i frame siano completi e, successivamente, confronta il contenuto dei dati dei sotto-frame. Grazie ai tempi ciclo molto brevi (100 μs), rileva i guasti praticamente senza ritardo.
Una rete Powerlink Safety può contenere fino a 1.023 domini di sicurezza e fino a 1.023 nodi per ciascun dominio. I domini di sicurezza possono estendersi su reti diverse e disomogenee; in ogni dominio un controllore della configurazione di sicurezza (SCM) monitora continuamente tutti i nodi di sicurezza ed è responsabile del salvataggio dei parametri, dell'assegnazione e della convalida degli indirizzi e della trasmissione di un segnale, che verifica la configurazione di ogni nodo.
Infine, Powerlink Safety può gestire la comunicazione produttore/consumatore e server/client e consente agli utenti di definire zone d'intervento separate, mentre la produzione continua nelle altre.

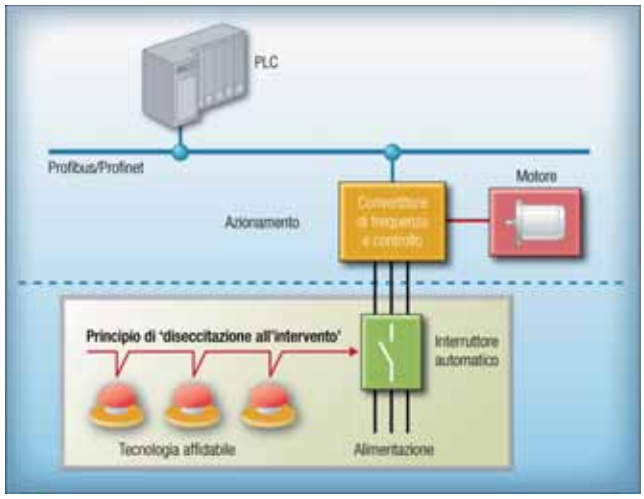
Ethernet/IP Safety

Passando a Ethernet/IP Safety, si tratta qui dell'implementazione della tecnologia CIP Safety nella rete Ethernet. CIP Safety amplia la copertura applicativa delle reti CIP per includere applicazioni di sicurezza funzionale, quali barriere fotoelettriche e arresti d'emergenza, e comprende gli oggetti, i servizi e i profili necessari ai dispositivi e alle applicazioni di sicurezza. La funzione di sicurezza è incorporata in ciascun dispositivo, anziché nell'infrastruttura di rete, perciò CIP Safety con-

CARATTERISTICHE DI SICUREZZA DI PROFISAFE

Errore dati/Soluzione	Numero sequenziale	Timeout	Codice identificativo	CRC
Ripetizione	•			
Perdita	•	•		
Inserimento	•		•	•
Sequenza	•			
Corruzione				•
Ritardo		•		
Indirizzamento			•	
Mascheratura		•	•	•
Guasti memoria		•		

sente a dispositivi standard e di sicurezza di funzionare sulla stessa rete aperta. Gli utilizzatori possono scegliere tra diverse architetture, con o senza



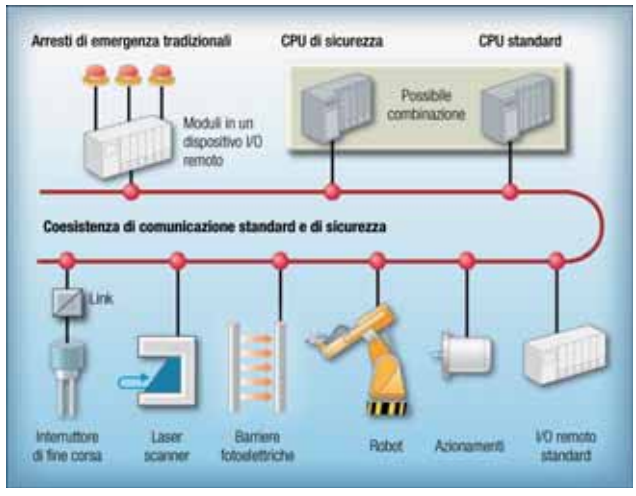
Il concetto di sicurezza classico

un PLC di sicurezza, per le proprie reti funzionali. CIP safety permette la comunicazione tra dispositivi di sicurezza di diversi fornitori sulle reti CIP standard, è certificato TÜV in conformità a IEC 61508/SIL3 e garantisce l'integrità della trasmissione mediante il rilevamento degli errori. Su Ethernet/IP è ideale per applicazioni con distanze elevate, pacchetti di sicurezza grandi e resa superiore.

Ethernet/IP Safety è in grado di offrire una comunicazione peer-to-peer ad alte prestazioni e di supportare un'ampia varietà di dispositivi di sicurezza.

Devicenet Safety

Estensione di sicurezza di Devicenet, Devicenet Safety consente a dispositivi standard e di sicurezza di coesistere sulla stessa rete con o senza PLC di sicurezza. L'integrità del loop di controllo non è influenzata dai dispositivi di controllo standard, indipendentemente dalla combinazione di prodotto utilizzata. Il protocollo consente la comunicazione locale o 'peer-to-peer' con un tempo di risposta rapido e, poiché si basa anch'esso sulla tecnologia CIP, supporta funzioni di 'bridging' e 'routing'. Il controllore di sicurezza di un segmento può connettersi, ad esempio, ai sensori di un altro segmento tra-



L'approccio a singolo canale

mite una dorsale Ethernet/IP ad alta velocità; tutti i nodi comunicano come se si trovassero sullo stesso segmento. La chiusura del loop è realizzata mediante switch e ponti standard.

Un'unica rete Devicenet Safety è in grado di contenere al massimo 64 dispositivi; dal momento, poi, che CIP Safety supporta l'architettura 'multi-link', il numero massimo di dispositivi è illimitato. La segmentazione della rete Devicenet Safety consente l'ottimizzazione dei loop di sicurezza 'time-critical': l'integrazione scalabile di più segmenti di rete permette, infatti, tempi di chiusura del loop più brevi. Inoltre, supporta l'utilizzo di più controllori sulla stessa rete e ciascun controllore supervisiona più dispositivi o I/O per semplificare la sincronizzazione. La verifica della robustezza avviene a livello dell'intero sistema, anziché dei singoli nodi, e la diagnostica avanzata permette di controllare anche carichi esterni. Devicenet offre: supporti robusti collaudati in ambienti sfavorevoli ad alto rumore, controllo automatico della duplicazione degli indirizzi di nodo, possibilità di rimuovere e sostituire i dispositivi alimentati, un contatore errori per ciascuna connessione alla rete, definizione della priorità in base alla configurazione ed elaborazione di messaggi basati sulla connessione per identificare i dati corrotti.

Chi già utilizza Devicenet può continuare a usare il cablaggio preesistente: è sufficiente aggiungere i dispositivi Devicenet Safety alla rete in essere per ottenere un'applicazione di sicurezza di livello SIL3. Gli OEM possono progettare macchine indipendenti, ciascuna dotata della propria sottorete, e l'utente finale può interbloccare più macchine impiegando una dorsale Ethernet/IP, senza compromettere le prestazioni di altre macchine. ■

FORMATO DEL MESSAGGIO PROFISAFE

Dati ingresso/uscita	*Byte di controllo/stato*	*CRC*
		Dati I/O
		Parametri
		Numero sequenziale
Max 12 o 123 byte	*1 byte*	*3 o 4 byte*

(*) Fonte Internet: www.profisafe.net, www.odva.org, www.ethercat.org, www.ethernet-powerlink.org; http://literature.rockwellautomation.com/idc/groups/literature/documents