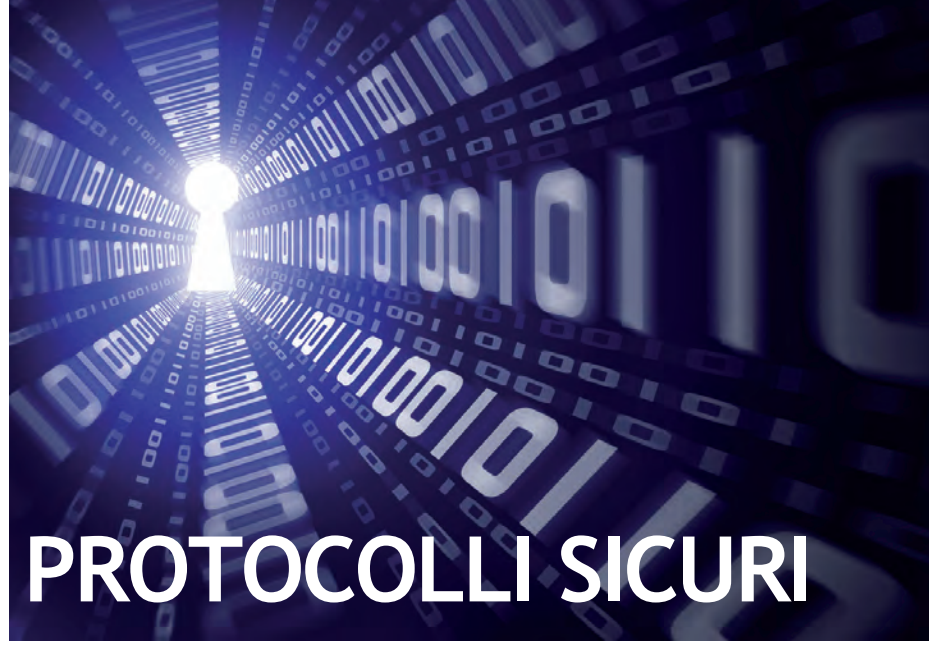
Sicurezza



PROTOCOLLI SICURI

LE RETI E I PROTOCOLLI DESTINATI ALLE APPLICAZIONI DI SICUREZZA MOSTRANO UN TREND VERSO L'APERTURA DELLE SPECIFICHE E UNA PREDILEZIONE PER LE ARCHITETTURE BASATE SU ETHERNET

di **Massimo Giussani**

La capacità delle reti di comunicazione di assicurare l'integrità dei dati che regolano il funzionamento di macchine e linee di produzione è un requisito essenziale per garantire la sicurezza degli impianti e l'incolumità del personale. A partire dal 1 gennaio 2012 i costruttori di macchine e i system integrator devono sottostare alla norma ISO EN 13849-1 per asserire la presunzione di conformità delle proprie applicazioni alla Direttiva Macchine dell'Unione Europea. Questa norma, gestita da Cenelec, governa i principi fondamentali e le prestazioni dei sistemi di sicurezza per il controllo di macchine e dispositivi e di fatto armonizza le specifiche deterministiche della normativa EN954-1 con quelle probabilistiche e sistemistiche contenute in IEC 62061. Le soluzioni di sicurezza spaziano da semplici interruttori e barriere di sicurezza interconnesse in logica cablata, a estensioni di infrastrutture di reti preesistenti per mezzo di opportune modifiche ai protocolli, fino a bus dedicati che richiedono interfacce specificamente pensate per le funzioni di sicurezza. L'offerta è variegata e commensurata a quella dei bus di campo industriali che controllano gli impianti ai quali afferiscono i dispositivi di sicurezza.

Di seguito verranno brevemente illustrate le caratteristiche di una significativa, ma necessariamente incompleta, selezione di bus di sicurezza. Tutte le soluzioni sono caratterizzate dalla presenza di un rilevamento degli errori particolarmente robusto e da un meccanismo di reazione che provvede a mettere in sicurezza l'impianto (o parte di esso) qualora si verifichi una situazione anomala. Seguendo il trend che ha caratterizzato l'evoluzione dei bus di campo industriali negli ultimi anni, i bus di sicurezza mostrano un orientamento verso le soluzioni basate su Ethernet e l'apertura delle specifiche per evitare, o quantomeno contenere, il vendor lock-in.

AS-i Safety at Work

AS-i (Actuator Sensor Interface) è una soluzione di rete industriale che si contraddistingue per semplicità e bassi costi. Si tratta di una tecnologia supportata da numerosi produttori di dispositivi industriali e che, tramite opportuni gateway, viene spesso impiegata a complemento di bus di più alto livello, come DeviceNet, Interbus, Profibus e numerose varianti di Ethernet industriale. Frutto della collaborazione di un consorzio di costruttori,

Bus di Sicurezza	Ente di Riferimento e/o primo proponente	Indirizzo web
AS-I Safety at Work	AS-International Association	www.as-interface.net
Canopen-Safety	CiA - Bosch	www.can-cia.org
CIP Safety	Odva - Rockwell Automation	www.odva.org
Fieldbus Foundation-FIS (FF-FIS)	Fieldbus Foundation - ISA	www.fieldbus.org
Functional Safety over Ethercat (FSoE)	Ethercat Technology Group (ETG) – Beckhoff Automation	www.ethercat.org
Interbus-Safety	Interbus Club - Phoenix Contact	www.interbusclub.com
OpenSafety	Ethernet Powerlink Standardization Group (Epsg) - B&R	www.opensafety.org
Profisafe	Profibus International (PI), PNO - Siemens	www.profibus.org
Safetybus-p	Safetybus-p Club International - Pilz	www.safetybus.com
Sercos Safety	Sercos International	www.sercos.org

Tabella 1 - Una selezione dei principali bus di sicurezza

le specifiche AS-i dettagliano lo strato fisico, quello di accesso ai dati e il protocollo di comunicazione di un bus master-slave su un doppino in rame. I dispositivi di I/O degli impianti industriali (attuatori, sensori, dispositivi di emergenza) integrano o sono collegati a un'interfaccia AS-i (slave) che si connette, tramite economiche prese vampiro, a una caratteristica piattina gialla dalla guaina autoripristinante. Con Safety at Work, l'interfaccia AS-i permette di integrare sulla stessa rete anche i dispositivi di sicurezza (funghi per l'arresto d'emergenza, interruttori accoppiati, barriere ottiche...), con prestazioni conformi agli standard SIL3 (En 62061), PLe (ISO 13849-1) e CAT4 (EN 954-1).

I dati di sicurezza vengono veicolati sul bus per mezzo di un codice dinamico, una tabella 8 x 4 bit univocamente associata a ciascun dispositivo di emergenza e memorizzata in fase di configurazione in un controllore dedicato (Safety Monitor).

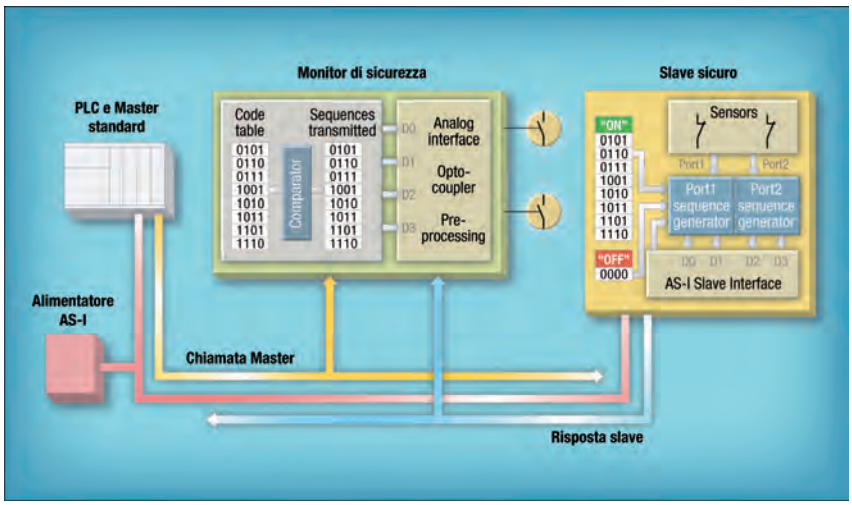


Fig. 1 - AS-i Safety at Work offre una soluzione semplice e a basso costo per mettere in rete i dispositivi di sicurezza

Durante il funzionamento dell'impianto, il Safety Monitor confronta la tabella ciclicamente inviata dai dispositivi con i codici in memoria e in caso di difformità provvede a prendere le misure necessaria alla messa in sicurezza dell'impianto.

Canopen Safety e Safetybus p

Canopen è un protocollo che si appoggia allo strato fisico di CAN (Controller Area Network), un bus di comunicazione industriale particolarmente apprezzato nel settore automotive e diffuso anche nell'ambito dell'automazione industriale. L'estensione CiA 304 dell'infrastruttura Canopen permette di arricchire il protocollo con le funzionalità necessarie alla gestione di una rete di sicurezza conforme alle specifiche SIL3. Le modifiche al meccanismo di trasporto dati permettono di introdurre fino a 64 nodi 'produttori' di dati pertinenti alla sicurezza dell'impianto, in coesistenza con i tradizionali nodi 'non sicuri'. Un'altra soluzione di rete che si basa sullo strato fisico di CAN, modificandone lo strato di collegamento dati e aggiungendovi meccanismi per la gestione dei dati di sicurezza nello strato applicativo, è Safetybus P. Si tratta di un bus multimaster con topologia lineare che integra solo dispositivi di sicurezza conformi Sil3 e Cat4. I sensori e gli attuatori sono connessi a Safetybus p per mezzo di moduli I/O decentralizzati che inviano messaggi quando viene rilevato un cambiamento nello stato dei nodi. I vari componenti possono essere configurati in base all'appartenenza a gruppi logici che possono essere disattivati in maniera intelligente nel caso venga rilevato un'errore in una delle loro parti.

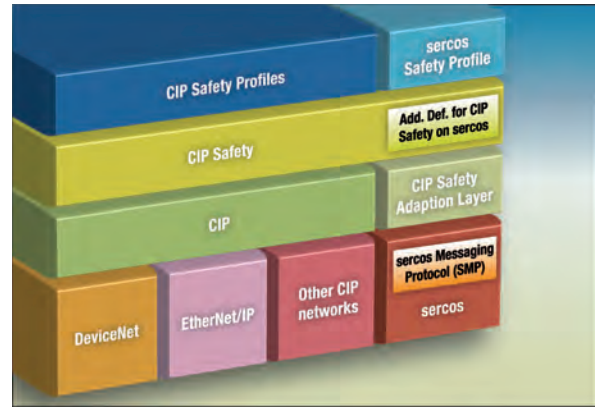


Fig. 2 - CIP Safety è una soluzione aperta multiprotocollo che si adatta a diverse varianti di Ethernet industriale e ai protocolli conformi CIP

CIP Safety: anche per Sercos

Con la diffusione di Ethernet in ambito industriale hanno fatto la loro comparsa numerose varianti di bus di campo basate sulle specifiche Ieee 802.3, il cui indubbio vantaggio è quello di offrire le vantaggiose economie di scala di una tecnologia di massa a larga diffusione mondiale. Ancora più aperto si è rivelato l'approccio adottato dall'architettura Common Industrial Protocol (CIP) messa a punto da Odva, l'associazione di produttori Devicenet, un'altra delle soluzioni di rete industriale basate su CAN. Con CIP, Odva ha realizzato una piattaforma aperta in grado di integrare reti industriali eterogenee che comprendono Devicenet, Ethernet/IP (ora anche Modbus TCP), Controlnet e Componet. L'indipendenza dal particolare mezzo usato è comune anche al protocollo di sicurezza CIP Safety che permette di integrare sulla stessa rete dispositivi tradizionali e di sicurezza realizzati da una molteplicità di produttori ed ha recentemente aggiunto Sercos alla lista di tecnologie supportate.

CIP Safety è un protocollo di sicurezza conforme alle specifiche Sil3 (Iec 61508) che utilizza un meccanismo di tipo 'produttore-consumatore' (qui denominati, rispettivamente, target e originator) per lo scambio dei dati tra i nodi. La flessibilità del protocollo fa sì che le comunicazioni tra sensori e attuatori possano essere sia di tipo peer-to-peer, sia gestite da specifici controllori di sicurezza. Le funzionalità aggiuntive sono implementate nello strato più alto della pila Iso-Osi, circostanza che conferisce ai nodi la responsabilità del controllo dell'integrità dei dati e rende possibile l'instradamento delle informazioni di sicurezza attraverso router standard. Il ricorso a una infrastruttura CIP comune a più sottoreti rende possibile la comunicazione tra celle Cip Safety appartenenti a reti in tecnologia differente.

Il protocollo si occupa di trasferire da una cella all'altra solo le informazioni di sicurezza pertinenti alla celle di destinazione, risparmiando banda a favore di più rapidi tempi di reazione. Una marcatura temporale fornisce il mezzo per verificare

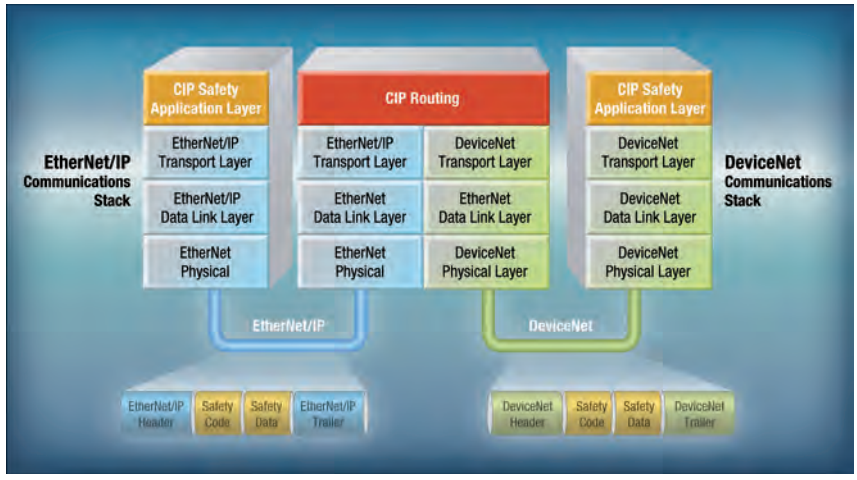


Fig. 3 - Uno dei vantaggi di CIP Safety è di permette il dialogo tra dispositivi di sicurezza appartenenti a reti differenti

l'attualità dei messaggi di errore e la sincronizzazione dei nodi di sicurezza mentre la correzione degli errori di trasmissione è affidata a codici CRC di lunghezza variabile in base al tipo di messaggio. Ciascun nodo viene associato a un identificatore univoco, denominato Unid (Unique Node Identifier), che deve essere impostato (tramite microinterruttori o più efficientemente, via software) in fase di configurazione della rete. L'Unid assomma in sé un codice analogo all'indirizzo Mac per il nodo e un identificatore della rete di cui fa parte. Il fatto che la stessa rete di sicurezza possa estendersi su più reti di comunicazione differenti, come Ethernet/IP, DeviceNet e Sercos III, rappresenta uno degli aspetti più interessanti di CIP Safety. Sercos III rappresenta l'evoluzione verso Ethernet del bus seriale in tempo reale ampiamente utilizzato nel contesto del motion control. Sercos International mette a disposizione con licenza Lgpl il software necessario alla realizzazione dei dispositivi master e commercializza i circuiti Asic e le Fpga da integrare all'interno dei dispositivi slave. Prima dell'accordo tra SI e Odva, gli utilizzatori di Sercos potevano comunque appoggiarsi a un'estensione nativa del protocollo denominata Sercos Safety. Compatibile con le interfacce Sercos II e III, Sercos Safety supporta applicazioni di sicurezza centralizzate e decentralizzate conformi a Sil3 anche ai tempi di ciclo più brevi. Una particolarità di questo protocollo di tipo 'produttore-consumatore' è la possibilità di instaurare comunicazioni dirette tra i nodi slave senza dover necessariamente passare attraverso un controllore master, circostanza che permette di ridurre i tempi di risposta alle situazioni di emergenza.

Sempre più aperti: Opensafety

Interoperabilità tra reti differenti e comunicazione diretta tra i nodi slave sono proprietà condivise da un'altra soluzione di sicurezza sempre più popolare per la sua completa apertura: Opensafety. Inizialmente messo a punto da B&R Automation come estensione di sicurezza per il bus Powerlink, Opensafety si è presto affermato come soluzione in grado di adattarsi a qualsiasi rete o bus di campo industriale, anche dedicata, anche non basata su Ethernet.

Lo standard è gestito da Epsg (Ethernet Powerlink Standardization Group) e il codice sorgente per la realizzazione dei dispositivi master e slave è liberamente disponibile con licenza BSD.

Anche in questo caso il modello di trasmissione dei dati è del tipo 'produttore-consumatore'; ogni nodo ha un identificatore univoco denominato Udid (Unique Device Id) che viene ottenuto combinando l'indirizzo Mac del dispositivo e un codice ad esso associato dal produttore. La rete viene configurata dinamicamente in fase di boot con la lettura degli identificativi da parte del Safety Network Management, una sorta di dispositivo master che gestisce la rete. Terminata la configurazione ha inizio il trasferimento ciclico dei dati dai nodi produttori a quelli consumatori. 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 dati sono inviati tramite tunneling sulle reti esistenti e si mescolano al traffico dati tradizionale. I dispositivi di sicurezza conformi allo standard Opensafety riconoscono automaticamente il contenuto e provvedono ad estrarre le informazioni di interesse. Il frame Opensafety è costituito da due sottoframe gemelli ciascuno dei quali dotato del proprio controllo di ridondanza ciclica.Opensafety si adatta a reti di grandi dimensioni, essendo pos-

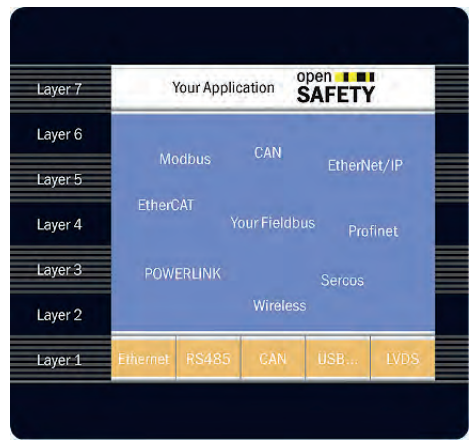


Fig. 4 - Opensafety è un approccio a canale nero che si adatta a qualsiasi bus industriale

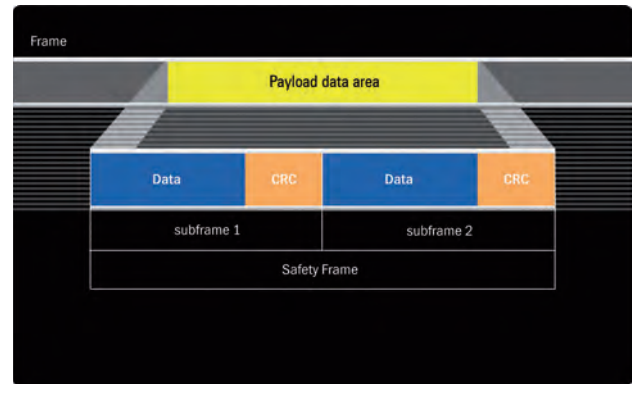


Fig. 5 - Ogni frame Opensafety è costitutito da due sottoframe gemelli con controllo ciclico di ridondanza indipendente

sibile mettere in comunicazione tra loro per mezzo di opportuni gateway fino a 1.023 domini di rete, ciascuno dei quali con un massimo di 1.023 nodi.

Profisafe e FSoE

Gli utilizzatori delle reti promosse da Profibus International (Profibus DP, Profibus PA e Profinet e Profinet over Wireless) possono appoggiarsi a Profisafe,

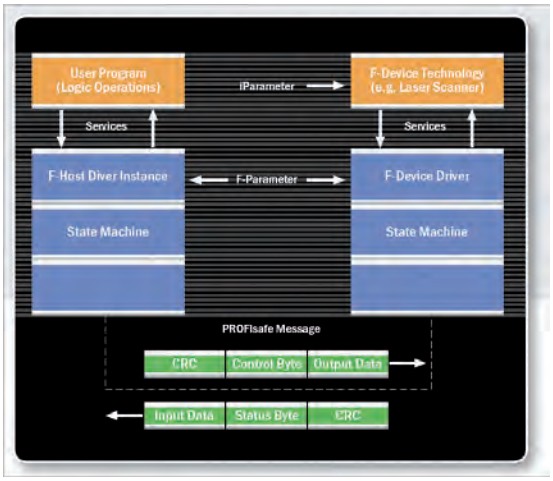


Fig. 6 - Profisafe è la soluzione di sicurezza espressamente pensata per le reti di casa Profibus International

un protocollo di sicurezza Sil3 nativo per queste architetture che consente di condividere le informazioni di sicurezza con quelle di automazione e controllo di processo. Il software Profisafe può essere utilizzato anche su alcune varianti aperte di Ethernet industriale. Profisafe utilizza un approccio di tipo master e slave (qui ribattezzati F-Host e F-Device) che non prevede comunicazione diretta tra nodi slave. I nodi sono identificati univocamente per mezzo del loro F-parameter e trasmettono informazioni di sicurezza dotto forma di messaggi denominati PDU (Protocol Data Unit) di sicurezza. Per mantenere gli errori di trasmissione al di sotto dei limiti della certificazione Sil3 vengono utilizzati controlli CRC e una numerazione sequenziale dei telegrammi di sicurezza.
Ogni volta che un telegramma di sicurezza viene ricevuto, un temporizzatore di tolleranza viene resettato per assicurare che vengano ricevute solo trasmissioni valide e aggiornate. Come Profisafe, anche Failsafe over Ethercat (FSoE) è un'estensione di sicurezza che utilizza un approccio a canale nero con un meccanismo di trasmissione del tipo 'master-slave'. L'obbiettivo di FSoE è Ethercat, un bus ad alte prestazioni basato su Ethernet le cui specifiche sono gestite da Beckhoff, azienda dalla quale gli sviluppatori possono ottenere il codice Vhdl per realizzare le Fpga da integrare nei nodi slave. Il protocollo di sicurezza FsoE è comunque aperto come parte dello standard internazionale Iec 61784-3 ed è certificato per prestazioni conformi al livello Sil3. Le comunicazioni cicliche tra master e slave avvengono attraverso Safety PDU e includono verifica temporale a entrambi gli estremi, controllo ciclico di ridondanza e identificazione univoca del nodo slave e della connessione. In fase di configurazione l'utilizzatore provvede a dotare ciascun nodo di un proprio identificativo univoco impostando manualmente dei microinterruttori sul dispositivo. Il trasferimento dei parametri di sicurezza può avvenire automaticamente dal master verso gli slave durante la fase di inizializzazione.

Il protocollo FF-SIS (SIF)

Come logico attendersi, anche Fieldbus Foundation offre agli utilizzatori dei propri bus di campo, ampiamente diffusi nell'ambito del controllo di processo, estensioni in grado di offrire livelli di sicurezza conformi alle specifiche Iec 61508 o Iec 61511. Le soluzioni di sicurezza espressamente pensate per i bus FF sono state messe a punto nell'ambito del progetto Foundation SIF (Safety Instrumented Functions) che ha visto il coinvolgimento diretto degli utenti finali e l'appoggio di Fielbus Foundation. Il protocollo FF-SIS (Fieldbus Foundation Safety Instrumented Systems) è stato recentemente esteso con il supporto di dispositivi a doppia modalità per il bus di campo FF H1. Questo significa che lo stesso dispositivo può essere configurato per funzionare come nodo nel controllo di processo o come dispositivo di sicurezza.