Fonte: www.opendoorrei.com

di **Massimo Giussani**

LA SICUREZZA È OPEN SOURCE

CON OPENSAFETY E POWERLINK, EPSG OFFRE UNA SOLUZIONE DI SICUREZZA APERTA, OPEN SOURCE ED ESENTE DA ROYALTY CHE SI INTEGRA CON DIVERSE TIPOLOGIE DI DISPOSITIVI E RETI INDUSTRIALI

Nel contesto dell'automazione industriale, 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. I dispositivi di segnalazione e di emergenza atti a prevenire o limitare i danni derivanti da guasti o da un uso improprio sono connessi alle macchine e al sistema di controllo per mezzo delle cosiddette reti di sicurezza. Si tratta di reti, talvolta dedicate, dotate di un riconoscimento degli errori particolarmente robusto e di un meccanismo di reazione che provvede a mettere in sicurezza l'impianto nel caso in cui si sospetti una compromissione dei dati o si verifichino determinati eventi critici.

Fonte: www.open-safety

Il protocollo di sicurezza OpenSafety si colloca nello strato applicazione della pila ISO-OSI e si adatta ai molteplici bus di campo impiegati in automazione industriale

Soluzioni open source

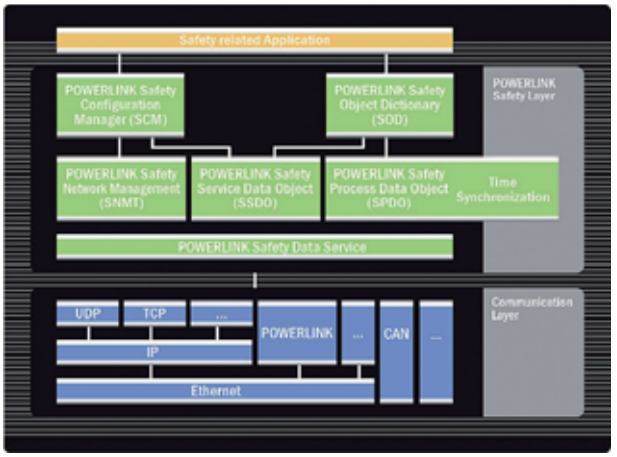
Errori nel trasferimento dei dati possono essere causati da una molteplicità di cause: malfunzionamenti a livello di hardware o software, interferenze elettromagnetiche di vario tipo, riflessioni per incorretto adattamento d'impedenza, ritardi di propagazione, errori d'instradamento, perdita o incorretta ricostruzione dei pacchetti e problemi di congestione della rete. Si possono utilizzare diversi meccanismi per verificare la correttezza delle informazioni trasferite e confinare le probabilità di errore al di sotto di una soglia ritenuta accettabile dalle normative e dalla legislazione. Tra le tecniche più collaudate figurano la ridondanza (dell'hardware o dei dati), la marcatura temporale dei messaggi e la numerazione dei pacchetti dati. Se uno o più meccanismi di verifica dell'integrità dei dati sono sempre presenti, lo stesso non si può dire della ridondanza hardware, sono infatti diverse le architetture di sicurezza certificate che non richiedono un'onerosa duplicazione del cablaggio. In particolare, negli ultimi anni hanno trovato applicazione sistemi ibridi che utilizzano il medesimo bus di campo per trasmettere i dati di processo, quelli diagnostici e i messaggi pertinenti la sicurezza. Con la diffusione di Ethernet sul piano di fabbrica è cresciuto anche l'interesse per soluzioni aperte basate su questa tecnologia: l'accoppiata Powerlink - OpenSafety rappresenta un caso emblematico anche per l'assenza di costi di licenza e la disponibilità di codice sorgente.

Rispettivamente introdotte da B&R Automation nel 2001 e da Ethernet Powerlink Standardization Group (Epsg) nel 2009, queste soluzioni industriali sono ora entrambe gestite dall'organismo indipendente Epsg, che ne cura l'evoluzione e ne mette a disposizione specifiche e sorgenti (con licenza BSD). La peculiarità di OpenSafety, protocollo applicativo conforme alle specifiche IEC 61784-3 Fscp 13, risiede nella libertà che offre agli utilizzatori di appoggiarsi a diversi tipi di bus di campo, rendendo possibile l'implementazione di un'unica soluzione di sicurezza estesa a tutto l'impianto senza gli oneri di un costoso vendor lock-in.

A proposito di Powerlink

Nello specifico, Powerlink è un bus di campo in tempo reale che unisce i meccanismi di Canopen alla conformità allo standard Ieee 802.3. Gratuitamente disponibile come soluzione software open source a partire dal 2008, è caratterizzato da tempi di ciclo dell'ordine dei microsecondi, che lo rendono adatto a supportare protocolli di sicurezza basati sull'approccio a canale nero. La sua indipendenza da hardware di tipo proprietario ne fa una soluzione svincolata da qualsiasi produttore e dai relativi costi di licenza.

In quanto incarnazione industriale dell'ubiqua tecnologia Ethernet, Powerlink mette a disposizione degli utilizzatori caratteristiche cruciali, come la comunicazione slave-to-slave, che velocizza lo scambio di dati tra i nodi senza richiedere il passaggio attraverso un dispositivo master (modalità talk-through), e il supporto delle tecniche di multiplazione, che permettono di ottimizzare la banda e di allocare intervalli temporali separati in base al dispositivo e alla criticità delle informazioni da veicolare. Altre caratteristiche di Powerlink sono la possibilità di inserire o disconnettere un dispositivo dalla rete senza comprometterne l'operatività (hot-plug), l'arbitraggio e il supporto della ridondanza. Powerlink gestisce in maniera pressoché indipendente i messaggi provenienti dalle applicazioni real-time, in particolare quelle che gestiscono le informazioni di sicurezza, e non realtime. Uno dei PC industriali o dei PLC della rete viene designato ad agire come master (managing node) per la sincronizzazione di tutti gli altri dispositivi, che si comportano da slave (controlled node). Durante un ciclo Powerlink si susseguono tre fasi distinte: durante la prima fase (start period) il nodo master invia un frame d'inizio ciclo che permette a tutti i nodi controllati di sincronizzarsi; il jitter in questi casi può essere abbassato a soli 100 ns. La seconda fase (cyclic period) è quella della trasmissione sincrona dei dati.

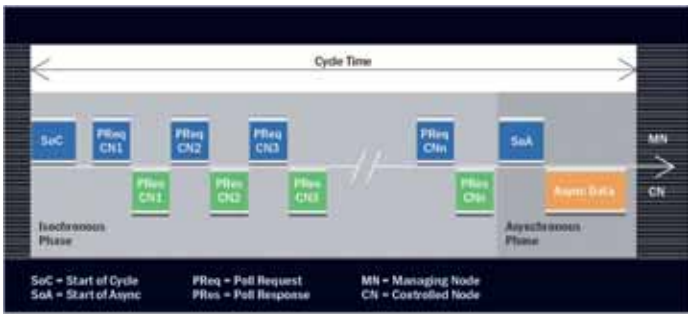


Fonte: www.ethernet-powerlink.org

Evoluzione di Powerlink Safety, OpenSafety si colloca sopra lo strato di comunicazione fornito da Powerlink per offrire varie funzioni localizzate nello strato applicazione

Powerlink ricorre a un misto di procedure d'interrogazione dei nodi (polling) e di multiplazione per ascoltare tutti i nodi controllati e ottimizzare la banda.

Ogni nodo controllato dal dispositivo master risponde immediatamente con un messaggio che viene ricevuto da tutti gli altri nodi. La terza e ultima fase (data exchange) è quella della trasmissione asincrona, che riguarda le informazioni non critiche dal punto di vista temporale come quelle di configurazione e inizializzazione del sistema o i dati utente; grossi quantitativi di dati possono essere spezzati in pacchetti multipli che vengono inviati nel corso di diversi cicli. Durante la fase asincrona vengono utilizzati frame IP standard normalmente gestibili da un qualsiasi router Ethernet senza toccare i dati critici presenti nella fase sincrona. La possibilità che Powerlink offre ai diversi nodi controllati di dialogare direttamente tra loro (cross-traffic) viene utilizzata dal protocollo di sicurezza OpenSafety per garantire tempi di reazione particolarmente brevi.



Fonte: www.ethernet-powerlink.org

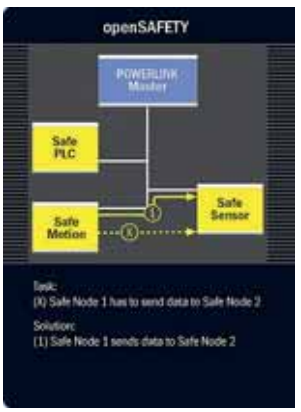
Ogni ciclo Powerlink si compone di tre fasi: inizializzazione, ossia di sincronizzazione; fase sincrona, di trasferimento dei dati di sicurezza; fase asincrona, di trasmissione delle informazioni non critiche per la sicurezza

Focus su OpenSafety

OpenSafety nasce nel 2009 come evoluzione di Powerlink Safety, l'estensione per la sicurezza di Ethernet Powerlink introdotta da Epsg due anni prima. Si tratta di un protocollo a canale nero che risiede nello strato applicazione della pila ISO-OSI.

In linea generale, le soluzioni di sicurezza basate su bus possono essere di due tipi: a 'canale nero' e a 'canale bianco'. Nell'approccio a canale nero 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. Il protocollo provvede a incapsulare i messaggi di sicurezza in frame che contengono codici di controllo di ridondanza ciclica e altri meccanismi di salvaguardia dell'integrità dei dati. Grazie a questo tipo di approccio OpenSafety non richiede un cablaggio dedicato per veicolare le informazioni di sicurezza, a differenza di quanto accade con sistemi più tradizionali. I dispositivi di sicurezza conformi allo standard OpenSafety riconoscono automaticamente il contenuto dei messaggi e provvedono a estrarre le informazioni di loro pertinenza. Le funzioni di sicurezza possono così essere implementate in maniera indipendente dal particolare protocollo di trasporto in uso: OpenSafety può essere utilizzato da una molteplicità di reti Industrial Ethernet e bus di campo: vi possono essere soluzioni OpenSafety basate, oltre che logicamente su Powerlink, su Ethernet/IP, Modbus TCP, Profinet e Sercos III. Grazie alla disponibilità del codice sorgente, inoltre, OpenSafety può essere utilizzato anche con soluzioni dedicate sviluppate dall'utente.

Le prestazioni del sistema di sicurezza nel suo complesso sono limitate da quelle della rete su cui si appoggia lo strato applicativo di OpenSafety. Se i tempi di risposta si fanno eccessivamente lunghi, 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 di sicurezza, i nodi interessati finiscono con l'essere messi in sicurezza, con tutte le prevedibili conseguenze sul funzionamento dell'impianto controllato.

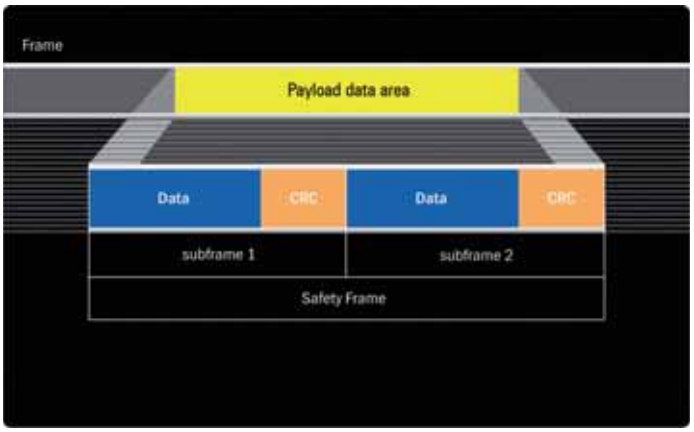


Fonte: www.open-safety

La modalità di comunicazione diretta slave-to-slave messa a disposizione da Powerlink viene sfruttata da OpenSafety per ridurre i tempi di reazione a situazioni di emergenza

Stando gli esperti di Epsg le prestazioni di OpenSafety sono in grado di soddisfare i requisiti richiesti dalla maggior parte delle applicazioni industriali. Il protocollo, che può contare su tempi di ciclo dell'ordine dei microsecondi, offre un'elevata reattività anche grazie al meccanismo del talk-through, che abilita la comunicazione diretta tra nodi, per esempio tra una barriera ottica e il

controllore locale che gestisce il movimento di una pressa, evitando di perdere tempo passando più volte attraverso un dispositivo master. Questa superiore velocità di reazione si traduce in una sensibile riduzione delle distanze di arresto degli elementi in movimento e contribuisce al raggiungimento dei livelli di sicurezza degli impianti conformi



Fonte: www.open-safety

Per minimizzare la probabilità che un errore di trasmissione non venga rilevato, i dati di sicurezza sono trasmessi sotto forma di due sottoframe identici, ciascuno dotato del proprio codice CRC

alle norme SIL (Safety Integrity Level). Attualmente OpenSafety è certificato SIL3 secondo IEC 61508 ed è pertanto adatto all'impiego in ambito industriale; i promotori di Epsg intendono conseguire anche la conformità SIL4 per consentirne l'impiego anche nei settori automotive, avionico e aerospaziale, dei trasporti, della difesa e dell'energia.

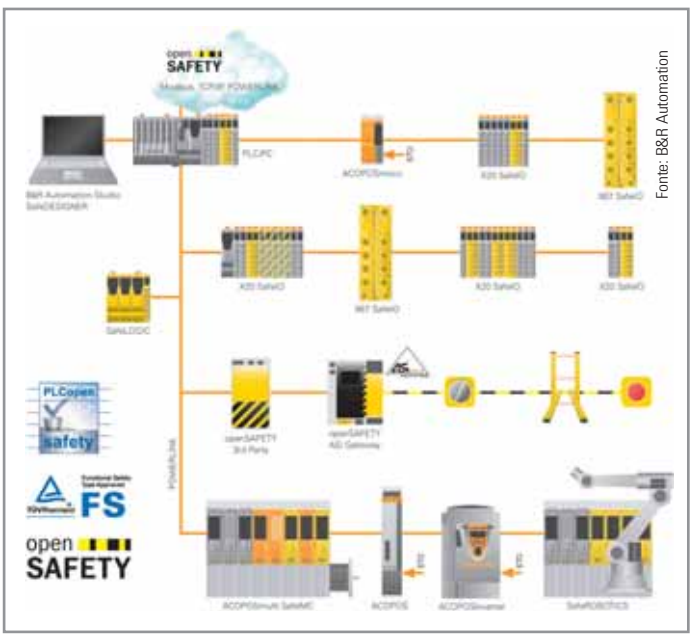
OpenSafety è in grado di accomodare numerose sottoreti di diverso tipo seguendo una topologia flessibile

L'integrità è tutto

Il protocollo OpenSafety incapsula i dati di sicurezza in un frame Ethernet standard a prescindere dal tipo di informazioni trasmesse (trasferimento dati, informazioni di configurazione, sincronizzazione): sono i nodi della rete che riconoscono automaticamente il contenuto rendendo così superfluo specificare il tipo di frame e la sua lunghezza. OpenSafety si occupa di verificare l'integrità di tutti i dati trasmessi, controllando che siano trasferiti nella giusta sequenza, senza interruzioni od omissioni e tenendo traccia di tutti gli eventuali errori riscontrati. I dati di sicurezza sono disposti in due frame identici dotati di codice di correzione degli errori a ridondanza ciclica (CRC) e accomodati entro un unico frame standard Ethernet. La ridondanza dei dati e la presenza di codici CRC duplicati rende altamente improbabile il mancato rilevamento di un errore di trasmissione: per non essere colto, l'errore dovrebbe presentarsi identico in entrambi i sottoframe ed eludere nel medesimo modo il controllo ciclico di ridondanza. Il protocollo effettua il controllo di ridondanza ciclica di tutti i dati trasferiti e, grazie ai ridotti tempi di ciclo, gli eventuali errori sono rilevati tempestivamente, anche quando ci si appoggia a reti non hard realtime. Per evitare scambi accidentali, inoltre, i frame sono dotati di un identificativo a 8 o 16 bit che contiene, codificati, parte del campo indirizzo, il tipo di telegramma contenuto e il tipo di frame.

Un altro meccanismo di prevenzione e identificazione degli errori è la marcatura temporale di tutti i pacchetti dati, che permette di stabilire le corrette sequenze d'invio e ricezione per il giusto assemblaggio delle informazioni inviate nel corso di più cicli. Il time-stamping previene anche le doppie ricezioni e permette di rivelare ritardi di trasmissione potenzialmente forieri di malfunzionamento dei nodi. Non solo: grazie alla sincronizzazione e al relativo basso jitter OpenSafety è in grado di tenere conto dei ritardi di propagazione ed elaborazione nelle varie porzioni eterogenee di rete, armonizzando così la coesistenza di sottoreti di sicurezza dedicate, estremamente veloci, e di reti basate su bus di campo che possono risentire di una lentezza congenita, che sarebbe altrimenti scambiata per malfunzionamento.

È possibile suddividere una rete OpenSafety in 1.023 domini di sicurezza, connessi tra loro per mezzo di gateway e dotati ciascuno di 1.023 nodi. Le reti possono essere organizzate per gerarchia o per zone, in maniera tale da permetterne il funzionamento indipendente e garantire l'operatività del resto dell'impianto quando una sua parte viene messa off-line per manutenzione o aggiornamento. Ogni dominio è gestito da un Safety Configuration Manager (SCM) che passa ciclicamente in rassegna tutti i nodi assegnatigli alla ricerca di variazioni.



Fonte:www.opensafety.org

Fonte: B&R Automation

I gestori di configurazione assegnano indirizzi univoci ai dispositivi di sicurezza del proprio dominio, ne verificano il corretto funzionamento e conservano in memoria i parametri di configurazione che non possono essere memorizzati direttamente nei nodi. Quando uno dei dispositivi del proprio dominio viene sostituito, provvedono a trasferire in maniera automatica i dati di configurazione, sollevando l'utilizzatore da tale incombenza.