# Sicurezza e bus di campo

foto: www.miky.ch

Valerio Alessandroni

## Minacce alla sicurezza

*Quali sono le principali minacce alla sicurezza, intesa come safety, che si possono verificare in un'architettura d'automazione basata su fieldbus? Come si possono affrontare tali minacce?*

Risponde **Andrea Graglia** (Siemens): "Dal punto di vista della safety l'innovazione tecnologica permette oggi di scegliere soluzioni sicure e affidabili, basate su tecnologia elettronica e su bus di campo industriali". Non ci sono minacce derivanti dall'impiego di questi sistemi, ma solo accorgimenti da tenere in considerazione quando si scelgono prodotti e soluzioni, nonché in fase di progettazione. Il costruttore deve per prima cosa adottare prodotti costruiti per applicazioni di sicurezza, non adattare sistemi elettronici standard ad applicazioni di sicurezza. "Siemens, ad esempio, dispone di PLC standard per applicazioni non sicure e di PLC F, che possono svolgere funzioni standard d'automazione come compiti di failsafe", prosegue **Graglia**. "Solo questi ultimi possono essere impiegati per applicazioni di sicurezza". Una volta scelto un controllore sicuro, bisogna sincerarsi che il bus di campo che si vuole impiegare sia idoneo a trasmettere i dati in sicurezza. I prodotti sono garantiti dalle certificazioni rilasciate dagli organismi notificati, che il fornitore di componenti di sicurezza è tenuto a rilasciare.

**Andrea Graglia**

**La sicurezza, intesa sia come safety che come security, è la caratteristica più importante di molti fieldbus**

Per quanto riguarda, invece, la fase di progettazione, secondo **Graglia** bisogna prestare attenzione al software della macchina, che determina le funzioni di sicurezza, così come si fa di solito con i circuiti elettromeccanici. "Per fare un'analogia con il mondo elettromeccanico, non è sufficiente utilizzare una centralina di sicurezza certificata, ma occorre anche inserirla in modo corretto all'interno degli schemi della macchina, altrimenti può non servire a nulla". Si può ritenere che l'impiego dell'elettronica e dei bus di campo garantisca un grado di sicurezza maggiore non tanto a livello hardware, quanto a livello progettuale e gestionale d'impianto. Per esempio, nel caso di un impianto molto esteso, il progettista si può trovare a dover collegare in serie tutti i comandi d'emergenza delle varie macchine, il che significa posare decine di metri di cavi elettrici. "Purtroppo quello che talvolta accade è che di fronte a questa spesa non vengano collegate tutte le emergenze delle macchine; quindi l'impianto risulta non in sicurezza", riferisce **Graglia**.

Un altro esempio è legato alla diagnostica: nel caso in cui si verifichi un malfunzionamento nei circuiti di sicurezza, che richieda nel caso elettromeccanico tempi molto elevati di riconoscimento, comunemente sugli impianti viene realizzato un by-pass delle sicurezze, per poter lavorare nonostante il guasto. Utilizzando invece la logica elettronica, si possono identificare e risolvere molto più velocemente i guasti e non si è costretti a lavorare senza sicurezze.

Secondo **Maurizio Franzoso** (Pilz Italia) nelle applicazioni più moderne e nei sistemi d'automazione industriale più all'avanguardia sono sempre più ricercate caratteristiche quali flessibilità, facilità d'installazione, elevate prestazioni e affidabilità dei componenti, che vanno a integrarsi per realizzare sistemi efficienti e completi. "I bus di campo sono connessioni intelligenti, che permettono di ridurre drasticamente il

numero di cavi utilizzati, incrementando le funzionalità complessive", egli afferma. "Essi forniscono una disponibilità di collegamenti virtuali molto elevata, che consente di espandere a piacere il sistema, aggiungendo nuovi dispositivi senza comportare ulteriori cablaggi. Tutto ciò vale allo stesso modo per la sicurezza, che sta assumendo un ruolo fondamentale nell'ambito dei sistemi industriali".

**Franzoso** prosegue spiegando che la sicurezza è l'insieme di tutte quelle soluzioni meccaniche, elettriche, elettroniche e informatiche, sia hardware che software, nonché progettuali, che garantiscono a persone e macchine di non riportare danni, prevengono e scongiurano situazioni di pericolo sia attivo che passivo per entrambi. "Le minacce alla sicurezza sono fondamentalmente di tre tipi: macchine e processi intrinsecamente pericolosi, guasti di tipo elettrico o meccanico ai componenti e, terzo ma non ultimo, una progettazione errata o non conforme dei sistemi pericolosi", precisa **Franzoso**. "Quando non si possono evitare situazioni di guasto meccanico o elettrico, per qualsiasi motivo, è indispensabile che vi siano dei dispositivi che intervengano in modo puntuale e sicuro, in modo che il sistema o l'impianto agisca in condizioni di sicurezza senza possibilità d'errore, raggiungendo cioè uno stato sicuro e definito (logica fail-safe), o definendo delle procedure di funzionamento tali da assicurare la continuità in sicurezza (logica fault-tolerant)".

"Nessun bus è attualmente pensato con criteri che garantiscano safety e/o security", afferma **Enzo Maria Tieghi** (Vision Automation). "Per identificare le minacce e le vulnerabilità di un sistema è necessaria un'attenta verifica preliminare del disegno, delle scelte sia di architettura, sia di materiali, dell'installazione, dell'implementazione, della manutenzione e della gestione durante il normale utilizzo, senza dimenticare che il fattore umano è spesso causa di falle nella sicurezza". Secondo **Tieghi** è necessario procedere a un'analisi dei rischi per verificare quali siano le aree su cui puntare maggiormente l'attenzione per migliorare i parametri di safety e security. Inoltre, è da tenere in considerazione che le condizioni a cui è sottoposto il sistema sono dinamiche. Non basta dunque eseguire uno studio preliminare, a tavolino, ma occorre mantenere alto il livello di attenzione e 'aggiustare il tiro' quando necessario inserendo nuove procedure e nuovi strumenti.

## Protezione dei dati

*Parlando di sicurezza intesa come security, in che modo un'architettura basata su fieldbus può assicurare la protezione dei dati trasmessi?*

Afferma **Giorgio Santandrea** (Siemens): "Per quanto riguarda la sicurezza intesa come security, è necessario fare alcune precisazioni sul significato del termine. Con esso si intende la protezione della rete e dei dati che la percorrono da possibili accessi non autorizzati che possono avere cause diverse e perseguire scopi differenti". I motivi variano dallo spionaggio industriale alla manipolazione, da errori d'indiriz-

zamento ad attacchi provenienti sia dall'interno, sia dall'esterno (hacker) dell'azienda. Considerando tali ragioni secondo **Santandrea** è indubbio che le reti realizzate con i bus di campo tradizionali del mondo automazione (ad esempio, AS-Interface e Profibus) siano intrinsecamente sicure. Esse infatti sono dedicate alla pura comunicazione in sistemi d'automazione e le possibilità di accesso dall'esterno sono pressoché nulle. Però, se si considerano soluzioni di comunicazione più moderne, basate ad esempio su Ethernet, la security assume un ruolo fondamentale. La possibilità che una rete di questo tipo sia accessibile dall'esterno diventa molto elevata; è quindi necessario pensare a come proteggere da accessi non autorizzati i dati che viaggiano al suo interno. Fortunatamente, per questo sono disponibili le soluzioni già impiegate per il mondo office e IT, visto che le problematiche di protezione delle reti Ethernet sono già state ampiamente affrontate.

**Giorgio Santandrea**

"Alcune contromisure consistono, ad esempio, nell'utilizzo di firewall che impediscono l'accesso indesiderato di utenti all'interno delle reti o di connessioni VPN (Virtual Private Network), tramite le quali, grazie a protocolli quali IPSec, è possibile mettere in comunicazione più sotto-reti Ethernet in modo sicuro mediante reti Ethernet potenzialmente non sicure (come Internet)", sottolinea **Santandrea**.

Secondo **Franzoso** la protezione dei dati trasmessi si può assicurare in vari modi, per prima cosa tramite il protocollo di trasmissione. Esso deve fornire protezione contro gli errori, controllare la ripetizione o la perdita di informazioni, oppure le sequenze di dati non corrette, i messaggi contenenti dati corrotti, i ritardi e le interferenze tra i dati che riguardano la sicurezza e quelli standard. Si deve implementare almeno una misurazione di tutte queste possibili cause d'errore, affinché si giunga a un buon livello di monitoraggio e controllo della trasmissione delle informazioni.

Un secondo metodo di protezione potrebbe utilizzare sistemi a codifica crittografata.

"Studiare l'architettura per migliorare la protezione dei dati è già un buon punto di partenza; significa che vi è consapevolezza anche per l'aspetto della security", afferma **Tieghi**.

"L'architettura in quanto tale non porta in automatico maggiore security. Si pensi a una struttura con molte ridondanze, con documentazione lacunosa, messa in campo con componentistica scadente, con personale non specializzato e con criteri d'installazione che lasciano a desiderare".

Per non parlare della manutenzione e della gestione: anche una rete o sistema realizzati secondo le migliori regole, se non vengono gestiti e mantenuti con adeguata documentazione e preservando l'integrità con componenti a specifica, divengono in poco tempo ingestibili e non rispettano i requisiti di prestazione dichiarati. "Non per niente, tra le pratiche di buona gestione vi sono gli audit periodici e la rivalutazione dei sistemi", conclude **Tieghi**.

## La normativa

*Come sta evolvendo la normativa per tenere conto di queste nuove esigenze?*

"Innanzitutto, per quanto riguarda la safety, bisogna precisare che la Direttiva Macchine, che rappresenta la legge in materia, non fa menzione all'impiego di dispositivi elettronici e bus di campo per applicazioni di sicurezza, anche perché il testo non entra nel dettaglio progettuale delle macchine", osserva **Graglia**. "Per quanto riguarda le norme, vi sono alcune interessanti novità a cui fare riferimento, come la IEC 62061 che regola la sicurezza funzionale dei sistemi di controllo elettrici, elettronici e programmabili legati alla sicurezza, o come la ISO 13849-1 che regola gli aspetti di sicurezza delle macchine". Alcune norme armonizzate, invece, come spesso accade nei settori in cui la tecnologia progredisce velocemente, faticano a stare al passo. In particolare, la vecchia EN 60204-1 ("Equipaggiamento elettrico delle macchine") non prevedeva l'impiego dei bus di campo per l'arresto d'emergenza. Questo perché la stesura della norma risale a quasi un decennio fa, quando si incominciava appena a parlare di PLC di sicurezza e quando i sistemi di sicurezza erano ancora puramente elettromeccanici. "Fortunatamente sta per uscire la revisione di questa norma, in cui verrà eliminato questo capitolo ormai anacronistico e non conforme allo stato dell'arte", conclude **Graglia**.

Secondo **Franzoso** attualmente vi è grande fermento nel campo della normativa di sicurezza per le macchine, i sistemi e gli impianti.

Chiari esempi sono la revisione delle norma EN 954-1 (ISO 13849-1) riguardante le parti dei sistemi di comando relative alla sicurezza e la nuova IEC 62061 "Functional safety of Srecs" (Safety-related electrical, electronic and programmable electronic control systems) nell'ambito del processo. Nel primo caso (EN 954-1) permarranno le categorie di sicurezza, ma verrà introdotto il concetto di 'performance level': la nuova ISO 13849-1 si baserà su considerazioni non solo qualitative riguardo ai concetti di sicurezza, ma anche su parametri quantitativi. Verrà introdotto il termine di probabilità di guasti pericolosi del sistema, dipendenti dalla struttura del sistema stesso, dai meccanismi di fault detection (DC - Diagnostic Coverage), dall'affidabilità dei componenti (Mttf - Mean time to failure, CCF - Common Cause Failure) e dalla progettazione dei processi, stress operativi, condizioni ambientali, procedure operative. Nel secondo caso (IEC 62061) saranno definiti i cosiddetti SIL (Safety Integrity Level) che derivano dalla norma IEC 61508.

È permesso l'utilizzo di Pecs (Sistemi elettrici ed elettronici a

logica programmabile) per la realizzazione di funzioni di sicurezza nell'ambito macchine (senza esclusioni), a patto che sussistano le caratteristiche desiderate sia per l'hardware, sia per il software.

Afferma **Tieghi**: "Più che le norme, sembra stiano facendo significativi passi avanti gli standard internazionali. A parte i bus sponsorizzati dai diversi vendor, sui quali si riversano numerose novità di prodotto (che spesso sono risultato di segnalazioni all'interno dei comitati di standardizzazione dettati dal mercato), si stanno affacciando alcuni standard per l'aspetto di security. Si pensi al comitato SP99 di ISA sulla security dei sistemi di controllo, oltre ai criteri dettati da Cidx per la chimica, AGA per le reti di telecontrollo gas, Nerc per il mercato energia/elettrico ecc.".

Secondo **Tieghi** non si può prevedere se vi sarà, e soprattutto quando vi sarà, una standardizzazione su queste problematiche; quel che è certo è che si sta acuendo l'interesse degli organismi europei e nazionali.

## Caratteristiche speciali

*Che cosa distingue un fieldbus orientato alla sicurezza da uno per applicazioni generiche?*

"Nel caso di Siemens i bus utilizzati supportano dei protocolli di sicurezza", afferma **Graglia**. "Ciò significa che il bus inteso come mezzo fisico non cambia per applicazioni di sicurezza, quello che cambia è il controllore a monte, che realizza, rispetto alla gestione standard della comunicazione, dei controlli aggiuntivi sui telegrammi e che verifica la correttezza e la rapidità della trasmissione".

"La sicurezza, per sua natura, non può 'aspettare in coda'; quindi deve avere un trattamento diverso da tutte le altre funzioni in ambito d'automazione e di processo. Merita il più alto grado di attenzione e trattamento", afferma **Franzoso**. "Ciò che deve distinguere un fieldbus orientato alla sicurezza da uno per applicazioni generiche è la massima priorità e un sistema dedicato alla sicurezza indipendente dall'automazione standard, ma aperto ad essa. Nasce cioè l'esigenza di integrare, rispetto alla parte d'automazione tradizionale, una piattaforma indipendente il cui scopo è rilevare i guasti sui singoli componenti e sulle connessioni e i collegamenti tra i dispositivi e i componenti stessi, se questi sono presenti". Essendo l'evoluzione (le applicazioni) sempre più orientate ad architetture maggiormente articolate e complesse, i sistemi tendono ad avere molti componenti decentralizzati e remoti, in grado di scambiare, trattare e attuare l'informazione ricevuta. "Per questa ragione l'esigenza di sviluppare un bus di campo il cui scopo fondamentale è quello di trattare la sicurezza è cresciuta in modo esponenziale", aggiunge **Franzoso**. "Primo obiettivo reale da raggiungere è realizzare dispositivi e componenti da dislocare in campo con determinate caratteristiche, ossia moduli di sicurezza rispondenti in tutto e per tutto alle normative vigenti e in grado di gestire i compiti di sicurezza in modo autonomo".

**Maurizio Franzoso**

Ogni dispositivo deve essere progettato e realizzato come un componente con le caratteristiche prima descritte. Per esempio, un doppio microprocessore sui nodi del bus e un doppio chip certificato sulle interfacce bus, con microprocessori di marche differenti, che apportano al sistema caratteristiche di ridondanza e diversità, per evitare i guasti di modo comune, insieme con l'autocontrollo degli stessi (con autotest incrociato allo start-up e in ciclo) realizzano e garantiscono questo primo livello di sicurezza. Il secondo obiettivo è fare in modo che la 'safe data transmission', cioè la gestione vera e propria dello scambio delle informazioni di sicurezza, garantisca i più alti livelli di sicurezza con tempi di reazione immediati.

"La rete di sicurezza non deve nascere 'da zero', ma partendo da sistemi che presentano una filosofia di fondo particolarmente adatta a queste considerazioni (bus a evento). Si devono utilizzare soluzioni e piattaforme ideali per ottenere massime funzionalità di sicurezza, cioè i migliori meccanismi di error detection ed error recovery", sottolinea **Franzoso**. "Agendo sul livello 7 del modello ISO/OSI, modificando ad hoc il protocollo, andando a ridondare tutti i meccanismi di rilevazione dell'errore e garantendo che un possibile disturbo di comunicazione venga sempre diagnosticato, si riesce a garantire tutti quelli che sono i meccanismi necessari allo scopo: trasferire i dati in modo sicuro e veloce (ne sono un chiaro esempio le caratteristiche di doppio CRC, echo mode, error counting, send/receive ID e i test ciclici di collegamento)".

**Enzo Maria Tieghi**

L'utilizzo di componenti sicuri, insieme a una gestione priva di errori dei dati e delle informazioni devono essere, di fatto, alla base dei moderni sistemi di sicurezza su fieldbus.

"Come già detto, anche il sistema più sicuro può essere usato in modo scriteriato e non sicuro", afferma **Tieghi**. "Ad ogni modo, il disegno, i componenti e le persone che utilizzano il sistema sono gli elementi che fanno la differenza. Come non esiste un apparato sicuro al 100%, non esiste 'il bus più sicuro'". La scelta del bus dipende dall'applicazione e la sicurezza deve essere parte della decisione presa. Una buona analisi dei rischi può servire a identificare i criteri per tale scelta. ■

**Pilz Readerservice.it n. 59**
**Siemens Readerservice.it n. 60**
**Vision Automation Readerservice.it n. 61**