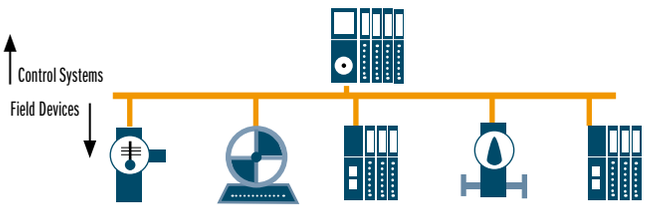
a cura di Roberto Carminati*

RETI INDUSTRIALI: IL PERICOLO NELL'OMBRA

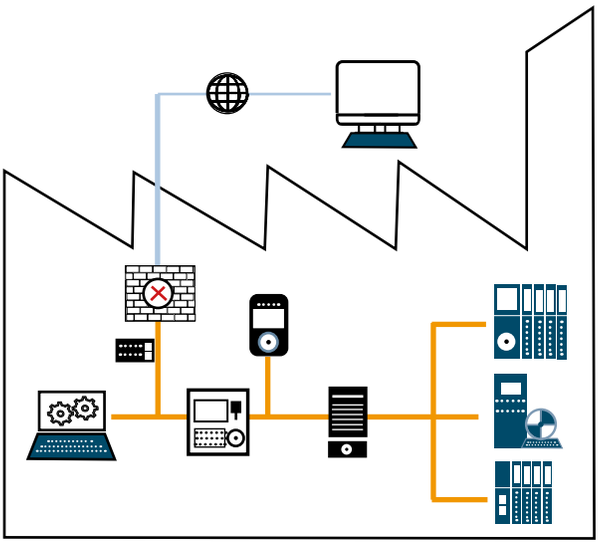
LA NASCITA E LA DIFFUSIONE DELLE RETI AZIENDALI BASATE SU INDUSTRIAL ETHERNET E PROTOCOLLO PROFINET HA IN LARGA PARTE FACILITATO LE COMUNICAZIONI IT E IOT MA AL TEMPO STESSO HA ESTESO LE SUPERFICI ESPOSTE A POTENZIALI ATTACCHI ESTERNI. DIFENDERSENE È POSSIBILE, MA A PATTO CHE SI RISPETTINO ALCUNI ACCORGIMENTI

Bus di campo è il termine per indicare in un processo automatizzato lo standard di comunicazione tra diversi dispositivi (nodi) quali sensori o attuatori, presenti in ogni macchina e impianto di automazione: linee di assemblaggio automatizzato, magazzini automatici, impianti di processo generici, dal farmaceutico alle centrali termoelettriche. Ogni macchina o impianto usa bus specifici sia per la comunicazione all'interno di macchine molto complesse dotate di una qualsiasi automazione sia per permettere la comunicazione tra singoli attuatori che devono coordinarsi, come un semplice automatismo e un nastro trasportatore. (fig. 1)

In principio gli impianti di automazione erano cablati punto a punto tramite un filo, creando una contorta ragnatela. La nascita di sistemi basati su bus di campo permette di collegare i nodi di un impianto con un solo cavo creando una rete in cui tutti sono connessi con tutti e visibili tra loro. Con l'affermazione del concetto di bus di campo, l'integrazione col mondo IT è cresciuta d'importanza. Ci si è chiesti se le tecnologie di rete usate negli uffici, per esempio Ethernet, già strutturate e capaci di trasportare grosse quantità di dati, potessero adattarsi agli impianti produttivi. Lo scenario ideale prevedeva di basare i sistemi di automazione su Ethernet. Questo comporta difficoltà pratiche di utilizzo. Ethernet non è in grado di fornire le prestazioni in tempo reale necessarie per



(fig. 1) Esempio di schema filare di una rete di automazione realizzata con bus di campo



(fig. 2) Rete di automazione basata su sistema di comunicazione PROFINET con accesso al web passando da un FIrewall

l'I/O industriale, superflue per i requisiti delle attività di ufficio. Non soddisfa il determinismo d'alta precisione necessario per il controllo del movimento avanzato, non garantendo la consegna di ogni singolo bit informativo; non è in grado di resistere alle condizioni fisiche presenti in ambienti di produzione: forti campi elettromagnetici e temperature elevate. Tali criticità sono state superate approdando a quello Industrial Ethernet su cui poggia anche Profinet.

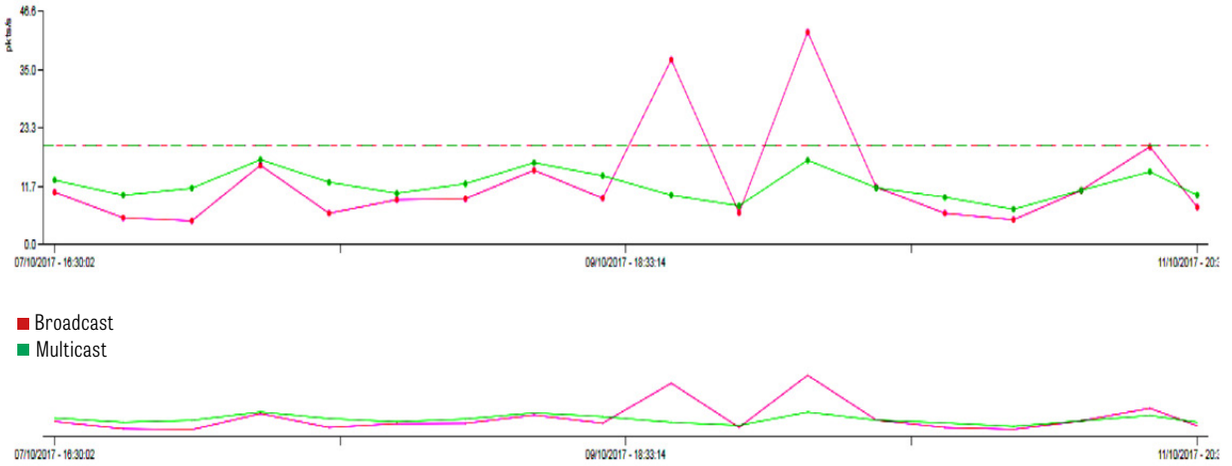
Profinet: chi era costui?

Profinet è un protocollo di comunicazione per lo scambio dati; e la soluzione Industrial Ethernet più avanzata al mondo. È un concetto moderno per gli standard di automazione e del tutto compatibile con Office Ethernet. Può operare nei difficili ambienti industriali e fornire la velocità e la precisione richieste dagli impianti produttivi. Può fornire funzioni aggiuntive: sicurezza, gestione dell'energia, integrazione IT. Fra gli altri vantaggi, le architetture altamente scalabili; l'accesso ai dispositivi di campo sulla rete; manutenzione e assistenza da qualsiasi luogo; miglior diagnostica della categoria; costi minori per il monitoraggio dei dati di produzione/qualità. Profinet è diffusissimo fra le aziende ma gran parte di esse non ne ha coscienza e attribuisce la comunicazione a una generica rete. Ma le potenzialità del protocollo sono vaste e di rado sfruttate lasciando ampi margini di miglioramento alle prestazioni della rete e dell'intera azienda, che vi fonda la sua parte produttiva e più delicata. (Fig.2)

Ogni sensore può comunicare direttamente col cloud, col vantaggio di poter estrapolare il dato da ogni singolo sensore in impianto, ma ponendo problemi di security che l'IT affronta ogni giorno con soluzioni che permettono di verificare la coerenza tra le policy di sicurezza implementate e lo scambio dati tra i nodi della rete. Purtroppo tali strategie di verifica e controllo non possono applicarsi direttamente alle reti di produzione perché sicurezza e disponibilità del dato sono esigenze contrapposte. Nell'IT l'accesso al dato dev'essere in primis sicuro; nelle reti industriali l'esigenza è opposta. I protocolli di comunicazione industriale prevedono lo scambio di messaggi con controllo deterministico, rivolto ad apparati di fabbrica ad alte prestazioni. Occorre quindi dare priorità alla disponibilità immediata del dato, in contrasto coi requisiti di verifica nell'ambito della sicurezza.

I nemici delle reti di automazione industriale

Progettazione Topologica. Minaccia autoindotta e fattore spesso trascurato è la presenza di dispositivi non legati alla rete di produzione. È essenziale conoscere la topologia della rete ed estenderla con nuove feature e sistemi in modo coerente per evitare problemi legati al traffico di device che compromettano la sicurezza della rete.
Access point wireless non gestiti e spesso dimenticati dopo la fase di commissioning nei cabinet delle macchine in impianto. Magari posati in fase di installazione delle macchine dai programmatori e poi dimenticati accesi, attivi a tutti gli effetti.
Accesso fisico - Porte ethernet poste sulle ante degli armadi. È a tutti gli effetti un accesso diretto e non controllato alla rete di produzione. Anche qui la comodità di accesso porta con sé la facilità d'accesso per i malintenzionati.
Switch managed non configurati. Hanno tutti valori di default, proprio come sul manuale del fornitore. Rischio d'attacco Man-In-The-Middle: una volta che un criminale arriva al dispositivo può impossessarsene e riconfigurarlo a piacere, bloccando l'impianto o deviando il traffico. Interfacce di configurazione. Cambiare sempre le password di default. Sorvegliare il comportamento del sistema. Aggiornare i firmware dei dispositivi in campo con le ultime versioni disponibili, che di solito integrano standard di sicurezza più alti. I produttori di dispositivi sono sempre più attenti alla security e hanno dotato le ultime versioni dei firmware di sistemi a protezione degli accessi alle pagine di configurazione. Attacchi DoS. È un attacco alla rete di produzione che mira alla saturazione delle risorse di rete. La generazione o propagazione incontrollata di pacchetti broadcast o multicast (volontaria o involontaria) può mettere in ginocchio la rete di produzione, inondata di messaggi non utili. Richiesta di connessioni TCP anomale. Bisogna sorvegliare il comportamento del sistema. Fare manutenzione, aggiornare i firmware dei dispositivi in campo. L'IT manager deve creare reti fruibili dai manutentori evitando metodi personali capaci di bypassare le sicurezze di rete.



(fig.3) Grafico dello storico dell'analisi del traffico presenta sulla rete di automazione generato dal sistema di monitoraggio permanente PNT-Online di CSMT per l'analisi delle reti Profinet

Non solo cybersecurity

Perciò, la sicurezza a livello di rete industriale è trascurata: l'imperativo è limitare un eventuale accesso fisico diretto alla rete di produzione. Ma oltre alla cybersecurity le reti moderne introducono altri aspetti. Quelle di automazione industriale, al tempo di Industry 4.0, necessitano caratteristiche specifiche: non solo la garanzia di uno scambio sicuro di informazioni in tempo reale, ma di poter trasportare moli di dati per le quali spesso non erano state progettate. Nella fabbrica digitale, comunicazione dei dati e networking sono centrali. Ci si deve prender cura delle reti partendo da un'adeguata progettazione, passando per l'analisi diagnostica e proseguendo con la manutenzione, per evitare imprevisti, downtime, fermi-impianto in apparenza immotivati. In ambito diagnostico CSMT Polo tecnologico di Brescia ha sviluppato un tool per l'analisi di ogni nodo della rete e per ricavare dati quali indirizzo IP, nome dispositivo, mac address vendor, versione firmware, malfunzionamenti, livello di traffico, topologia di rete, errori di trasmissione e tipologia di pacchetti in transito sulla rete, riuscendo a rilevare comportamenti anomali di tutto il sistema di comunicazione. La rilevazione parte dalla raccolta dei dati utili, processati da software basati su tool di intelligenza artificiale che, in tempo reale, rilevano eventuali malfunzionamenti, intrusioni, errori, segnalandoli ai responsabili perché agiscano tempestivamente. I sistemi di comunicazione industriale sono però un tema di nicchia. Ricavare informazioni preziose dalla rete di produzione è possibile, usando gli strumenti giusti, in mano a persone formate. CSMT, centro di competenza italiano per Profibus e Profinet offre corsi riconosciuti a livello internazionale per chi voglia specializzarsi e comprender meglio il funzionamento e le potenzialità di tali tecnologie: progettisti di reti di automazione o, con temi più specifici, manutentori e installatori.

Un caso di successo reale

Un'azienda molto strutturata con impianti complessi e reti molto estese aveva da mesi iniziato a lamentare fermi impianto apparentemente immotivati, di solito risolti col classico reset o uno spegni e riaccendi. Alla lunga, pur se brevi, i fermi iniziavano a esser fastidiosi: l'impianto doveva esser riavviato più volte per turno, con immaginabili disagi e costi. Dopo un'attenta analisi da parte di CSMT si decise d'installare uno strumento di monitoraggio permanente della rete Profinet, per registrare ciò che accadeva, specie in coincidenza con fermi impianto che sembravano sempre più casuali. I risultati delle scansioni del tool PNT-Online, creato da CSMT stesso, hanno evidenziato un comportamento anomalo della rete. Nell'immagine si osservano due picchi che svelano l'improvviso triplicarsi del traffico rispetto al funzionamento normale. Un nodo in rete stava perciò generando un traffico tale da saturare le capacità di gestione di alcuni dispositivi mandandoli in blocco e causando il fermo impianto generale. I dati hanno mostrato che il picco era dovuto a una serie di PC connessi alla rete di produzione. Collaborando con gli esperti IT dell'azienda si è visto che i nodi incriminati erano PC colpiti da ransomware che cercava un punto di uscita sulla rete per criptare gli HDD saturando il canale e bloccando gli strumenti. Fortunatamente l'azienda aveva ben segmentato le reti di produzione separandole dal resto della rete con firewall e router, impedendo che dalla rete di produzione si potesse raggiungere l'esterno. Un tecnico chiamato a verificare la sua macchina di riferimento, chiamato ad aggiornare il firmware di un dispositivo, data la segmentazione della rete che impediva l'accesso a Internet avrebbe potuto malauguratamente decidere di usare il tethering del cellulare per scaricare quel file, pochi byte. Lasciando il PC connesso alla rete di produzione e collegandosi allo smartphone avrebbe potuto creare un bridge e permesso al ransomware di inviare i codici per criptare gli hard drive dei PC, bloccando così definitivamente la produzione. Per questo è essenziale controllare periodicamente la rete di automazione per vedere chi è connesso e quali dati transitino e trarre informazioni sul suo funzionamento, con strumenti specifici e di monitoraggio, rivolgendosi a personale specializzato. (Fig.3) ■

* dal contributo di:
Daniele Rovetta, Profibus Profinet Project Manager di CSMT e **Gabriele Zanetti**, Head of Technology Transfer Engineering di CSMT