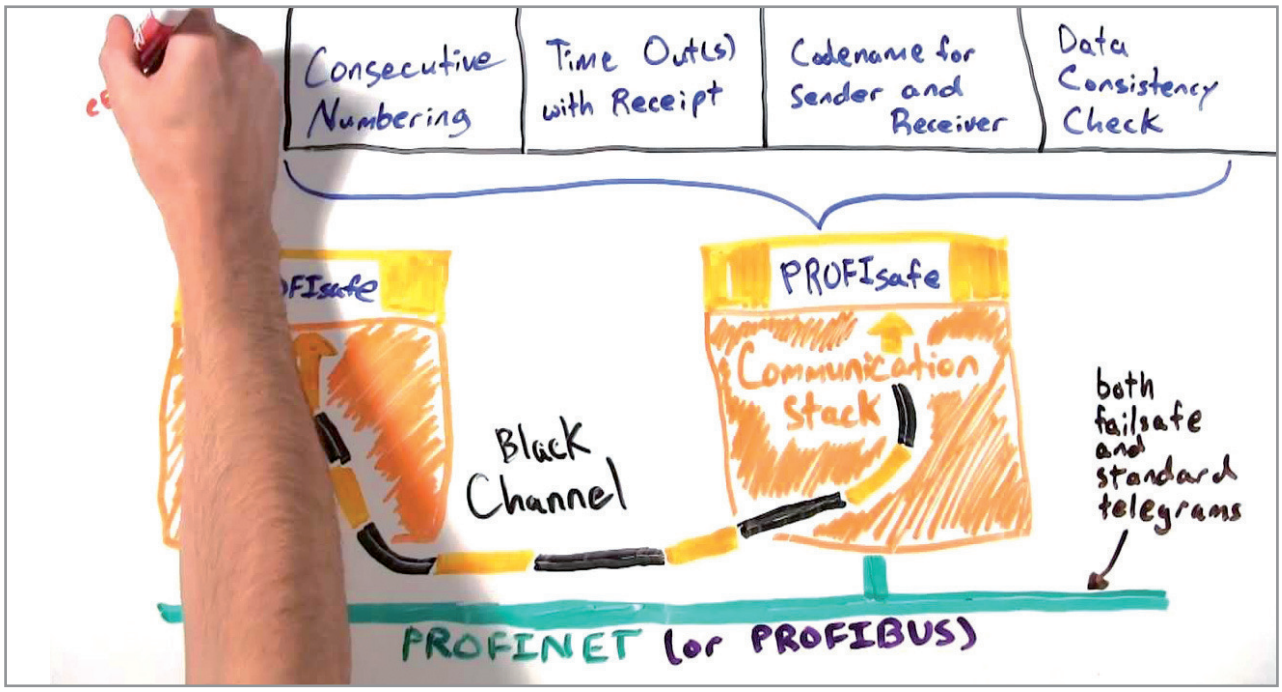
Sicurezza

SICURI CON PROFINET

di **Carlo Marcantoni Taddei**

VEDIAMO GLI STRUMENTI CHE LO STANDARD DI COMUNICAZIONE REALTIME PROFINET OFFRE PER AFFRONTARE LE PROBLEMATICHE DI SAFETY, OLTRE A QUELLE DI SECURITY



Fonte: i.ytimg.com

Profinet è uno dei più diffusi standard di comunicazione industriale basati su Ethernet ed è supportato dal consorzio PI (Profibus & Profinet International), che vanta una presenza mondiale con centri di competenza, centri di training e laboratori di test distribuiti in una trentina di nazioni. Rispetto alla 'safety' Profinet permette di integrare la catena che realizza le funzioni di sicurezza nella comunicazione Ethernet che gestisce, con significativi vantaggi. Un altro discorso riguarda poi gli aspetti legati alla 'security' in ambito Ethernet, gli attacchi possibili e le misure difensive che Profinet permette di adottare.

Una comunicazione Ethernet realtime

La comunicazione Profinet è basata sullo standard Ethernet secondo Ieee 802.1Q, il che fa sì che la comunicazione di processo possa utilizzare lo stesso mezzo trasmissivo impiegato da altri protocolli di trasmissione dati, per esempio TCP/IP, realizzando così delle economie di costi e contemporaneamente assicurando, grazie ai meccanismi di schedulazione delle trasmissioni implementati da Profinet, la trasmissione dei dati realtime nel rispetto dei tempi di ciclo richiesti dal processo industriale controllato, fino ad arrivare, se richiesto, a prestazioni realtime isocrone, come necessario nel controllo assi (si veda *figura 1*).

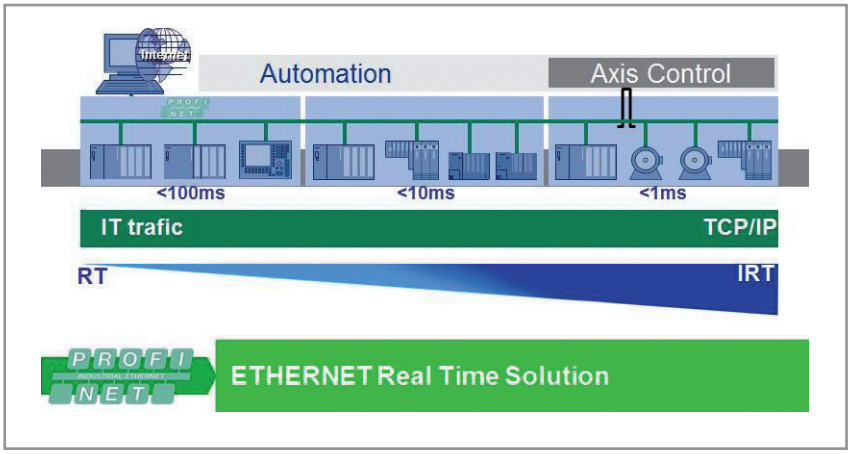


Figura 1 - Profinet è una soluzione adatta a tutte le esigenze di realtime

La flessibilità di Profinet permette di integrare anche, ove necessario, diversi standard di comunicazione wireless. Inoltre, si può realizzare l'integrazione di rami della rete industriale che utilizzano fieldbus seriali, grazie al concetto di 'proxy': un device che può essere collegato da un lato alla dorsale Profinet e dall'altro al fieldbus seriale (Profibus, FF H1 ecc.), permettendo così che il controllore della rete Profinet dialoghi con i device slave del fieldbus (il proxy funge da master della rete fieldbus). Un'altra importante caratteristica di Profinet è la ridondanza scalabile, ovvero la possibilità di utilizzare il grado di ridondanza desiderato, tale da permettere la comunicazione anche in presenza di guasti e/o interruzioni del mezzo trasmissivo. La ridondanza scalabile permette di impiegare: protocolli che gestiscono topologie ridondanti di cablaggio, con crescente capacità di eliminazione del disturbo del guasto alla comunicazione realtime (MRP - Media Redundancy Protocol, Mrrt - Media redundancy for realtime telegrams, Mrpd - Media redundancy with preplanned delay); controller ridondante in stand by; ridondanza di controller e I/O device; ridondanza dell'interfaccia di connessione alla rete di ogni device. Infine, il profilo CiR (Configuration in Run) di Profinet permette un'agevole sostituzione dei device o dei loro moduli senza disturbare il regolare funzionamento di altri device sulla stessa rete.

La sicurezza declinata in Profinet

Veniamo ora alle caratteristiche di Profinet attinenti l'ambito della sicurezza, intesa prima di tutto come prevenzione di incidenti e malfunzionamenti pericolosi (safety). Un altro aspetto della sicurezza è legato, come sappiamo, alla prevenzione da attacchi informatici che possono pregiudicare l'integrità e la disponibilità del processo e dei macchinari produttivi (security).

Per cominciare, la safety si basa sul concetto di 'analisi del rischio': si individuano i potenziali rischi e si valuta sia la probabilità del verificarsi dell'evento dannoso, sia l'entità probabile del danno che l'evento comporta. Come risultato si ottiene una tabella in base alla quale si prendono le decisioni relative all'accettabilità o meno del rischio in cui si incorrerebbe (si veda *figura 2*).

Se il rischio supera il limite di accettabilità, si prendono in considerazione le misure che possono mitigare la 'rischiosità', sia riducendo l'entità del danno subito quando il rischio dovesse concretizzarsi, sia riducendo la probabilità di accadimento dell'evento. Se le misure

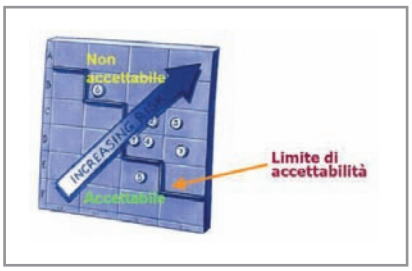


Figura 2 - Analisi del rischio

sono economicamente sostenibili, ovvero se il loro costo è inferiore al prodotto della probabilità di accadimento dell'evento avverso moltiplicata per il costo previsto del danno subito, allora è possibile rientrare nella zona della tabella in cui il rischio è accettabile. Vengono implementate in questi casi delle funzioni di safety, realizzando altrettante catene di safety (sensore, logic solver, attuatore), che devono rispondere a precisi requisiti di affidabilità del loro funzionamento. Generalmente, questa viene espressa riferendosi ai livelli di safety 'SIL' (Safety Integrity Level) che sono riportati in *figura 3*.

Probability of failure on demand (low demand operation)	
SIL	PFD
1	10^{-1} - 10^{-2}
2	10^{-2} - 10^{-3}
3	10^{-3} - 10^{-4}
4	10^{-4} - 10^{-5}

Probability of failure per hour (continuous operation)	
SIL	PFH
1	10^{-5} - 10^{-6}
2	10^{-6} - 10^{-7}
3	10^{-7} - 10^{-8}
4	10^{-8} - 10^{-9}

Figura 3 - Probability of failure - SIL (Safety Integrity Level)

In una catena di safety la comunicazione deve avere una probabilità di guasto non superiore all'1% di quella di tutta la catena: il protocollo Ethernet, da solo, non è in grado di garantire questo alto livello di affidabilità. Il profilo Profisafe permette di utilizzare lo stesso canale (dorsale Ethernet) impiegato per la trasmissione dei dati realtime, anche per la trasmissione dei comandi relativi ai dispositivi che implementano la safety dell'impianto (sensori, attuatori, processori logici), come previsto dalle norme IEC 61508. Questo è reso possibile grazie a meccanismi addizionali di controllo, che riducono la probabilità di guasto del canale di comunicazione al di sotto dell'1% richiesto. Si evita così la necessità di avere sensori, attuatori, processori logici e cablaggio che implementano la catena di safety completamente separati dalla rete di comunicazione standard, con evidenti risparmi in termini di costi per il cablaggio e per apparecchiature extra. Altro vantaggio: l'ambiente di sviluppo software è lo stesso sia per le logiche di funzionamento dell'impianto, sia per le logiche specifiche della safety. Inoltre, l'integrazione nella rete di controllo dell'impianto permette di registrare quando i dispositivi e le logiche di safety intervengono nel corso delle operazioni quotidiane, il che può permettere un ulteriore risparmio nei test periodici della safety, che potrebbero, in tutto o in parte, diventare non necessari, qualora risultasse dai log che i dispositivi sono già entrati in azione. Infine, l'utilizzo dei controllori di processo anche per le logiche safety permette un intervento più graduale, in alcuni casi, permettendo per esempio di adottare una riduzione di velocità in luogo di un arresto, in determinate situazioni.

In definitiva, Profisafe è una tecnologia supplementare di Profinet che permette di ridurre la probabilità residua di errore nella trasmissione dei dati tra controllore fail-safe e dispositivi (sensori ed attuatori) fail-safe. La trasmissione utilizza il mezzo trasmissivo, per il quale non sono imposti requisiti addizionali da Profisafe (si dice che viene utilizzato come un 'black channel'): la riduzione della probabilità residua di errore nella trasmissione è realizzata grazie a uno strato software addizionale (indicato come 'Safety layer' (si veda *figura 4*).

In particolare, per ridurre gli errori di trasmissione si utilizzano:

• la numerazione consecutiva dei messaggi, che permette di evitare o rilevare

perdite, errori di sequenza, inserimenti, ripetizioni di messaggi;
• un watchdog che rileva perdite o eccessivi ritardi, nonché l'arrivo di messaggi inaspettati e, quindi, erronei;
• un nome in codice univoco assegnato a ciascun dispositivo Profisafe, oltre al nome già usato nella rete Profinet, che diminuisce la probabilità di errori di indirizzamento al destinatario e di identificazione del mittente;

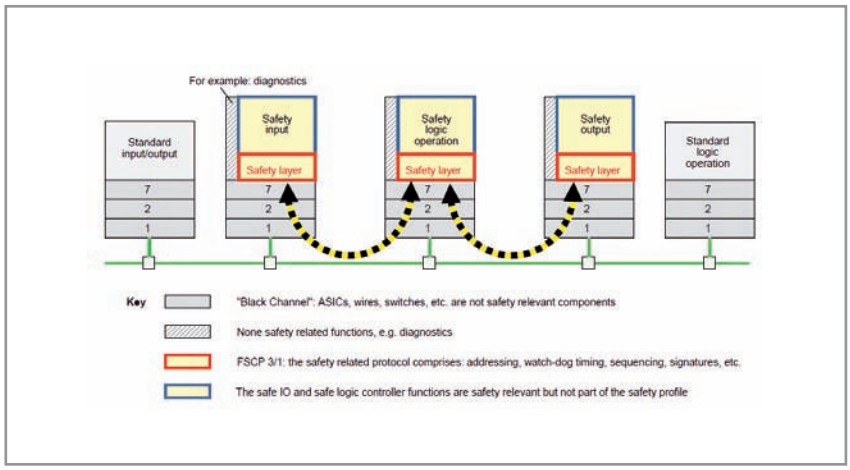


Figura 4 - Architettura dei layer di safety

• il controllo di ridondanza ciclico (CRC), che calcola una 'checksum' per verificare che il messaggio non sia corrotto e che include nel calcolo della stringa di controllo anche il numero del messaggio e il nome in codice Profisafe.
In aggiunta ai messaggi Profisafe, che possono imporre a un device di mettersi in condizione 'safe', per esempio arrestando un motore o aprendo o chiudendo una valvola, anche errori di trasmissione non rimediabili, rilevati dai meccanismi sopra descritti, per esempio un 'time-out' segnalato da un watchdog, possono causare la transizione alla condizione 'safe' dei dispositivi che li rilevano.
Il numero di nodi Profisafe installati ha superato i due milioni e questo profilo è disponibile in molte famiglie di dispositivi che coprono tutte le necessità dell'industria manifatturiera e di processo.

Non esiste safety senza security...

Lo standard Profinet fornisce tutte le caratteristiche necessarie al funzionamento performante e senza errori di una rete di controllo industriale, grazie all'alta velocità di trasmissione (100 Mbps) e riservando alle comunicazioni realtime la quantità di banda necessaria al rispetto dei tempi di ciclo richiesti dal tipo di processo realizzato dall'impianto. Inoltre, Profinet offre il contesto necessario per raggiungere un elevato livello sia di safety che di security. Nel primo caso grazie al profilo Profisafe, che, grazie a uno strato software addizionale, permette di raggiungere il livello di affidabilità richiesto nella comunicazione interna alle catene di safety implementate nell'impianto.
Quanto alla security, Profinet permette di utilizzare i dispositivi e le misure di sicurezza esistenti, o che verranno ideati in futuro, per le reti Ethernet, che, grazie alla loro enorme diffusione, sono sempre al centro dell'attenzione dei produttori di logiche e dispositivi di protezione.
Per raggiungere gli obiettivi di safety e security prefissati sono necessarie altresì accurate fasi di analisi, progettazione e monitoraggio della rete, in quanto il mantenimento di un livello elevato di sicurezza è il frutto di un processo continuo che inizia in fase di progettazione dell'impianto e prosegue poi per tutto il ciclo di vita, con opere di manutenzione e aggiornamento continue.

Due parole sulla security

Va innanzitutto detto che 'security' e 'safety' si possono considerare, per certi aspetti, due facce della stessa medaglia: si utilizzano per entrambe analoghe metodologie di analisi del rischio; inoltre, un incidente di security può avere pesanti conseguenze anche in termini di safety. Basti pensare alle possibili conseguenze della deliberata intrusione e manomissione del sistema di controllo di un impianto petrolchimico.
Profinet ha stabilito una metodologia di test nell'ambito della certificazione dei dispositivi, per valutarne la capacità di continuare a fornire il servizio in presenza di sovraccarichi di traffico sulla rete. Una rete Profinet ben progettata riserva al traffico realtime una parte del tempo di ciclo tale da assicurare il regolare funzionamento della rete industriale con il rigoroso rispetto dei tempi di risposta necessari.
Tuttavia, in un'ottica di security, va valutata e certificata la resistenza dei dispositivi nei confronti di attacchi di tipo DoS (Denial of Service), in cui si possono provocare deliberatamente sovraccarichi nel flusso di dati, con l'intento di pregiudicare il rispetto delle tempistiche realtime.
A seconda della capacità di resistenza emersa nel corso del test, i dispositivi vengono classificati in 'Netload Class I' ('Basic robustness against Netload') o in 'Netload Class III' ('Advanced robustness against Netload').
Naturalmente, la certificazione della robustezza dei dispositivi Profinet non esaurisce la problematica di security, che richiedono un processo continuo di verifica dell'adeguatezza delle misure adottate. Va però sottolineato che Profinet, adottando il protocollo Ethernet standard, permette l'utilizzo di tutte le misure che lo stato dell'arte della security delle reti Ethernet mette a disposizione.
L'ambito dell'automazione industriale presenta alcune caratteristiche che rendono l'approccio alla cyber security in parte diverso da quello adottato in 'ufficio'. Le principali sono:
• una grande eterogeneità di hardware, software e sistemi operativi, che aumenta la difficoltà di raggiungere un livello omogeneo di security;
• un funzionamento continuo e ininterrotto degli impianti, che rende necessario subordinare aggiornamenti importanti per la security alla disponi-

bilità degli intervalli di manutenzione;
• la rapidità dei tempi di risposta richiesti, che può essere compromessa da sovraccarichi intenzionali o accidentali del flusso dati;
• la dispersione, con certe architetture, dei dati in un gran numero di apparecchiature, che aumenta la difficoltà di proteggerli adeguatamente;
• l'impatto in termini di salute delle persone e di inquinamento dell'ambiente che problemi di security possono implicare quando impattano su un impianto industriale.

La concomitanza temporale del focus sulle problematiche di cyber security e della diffusione dei protocolli Ethernet based, come Profinet, non deve indurre a pensare che la connessione alla dorsale Ethernet anche di attuatori e sensori, resa possibile dai protocolli a base Ethernet, sia all'origine delle problematiche di cyber security.

Infatti, i sistemi ERP, MES, DCS e Scada sono raggiungibili tramite rete Ethernet anche usando fieldbus seriali. Inoltre, i fieldbus seriali generalmente sono predisposti per rilevare messaggi corrotti (grazie al controllo del CRC), ma non gestiscono adeguatamente i messaggi con un CRC corretto e un contenuto non corretto.

Un attaccante che riesca ad avere accesso fisico all'impianto industriale, dunque, potrebbe sfruttare questa caratteristica per attaccare livelli più elevati della rete, inviando contenuti opportunamente manipolati da device di campo manomessi.

Le misure da adottare

Vediamo ora quali misure di protezione si possono mettere in campo per salvaguardare la security delle reti industriali.

Innanzitutto, bisogna prevedere una linea di difesa mediante firewall, in grado di fermare attacchi provenienti dall'esterno (Internet o rete aziendale d'ufficio, alla quale la rete industriale sia connessa). Ovviamente, anche tutti gli altri accessi remoti alla rete industriale presenti, per esempio per la manutenzione remota, devono essere catalogati e protetti da connessioni sicure (per esempio con VPN - Virtual Private Network).

Si tratta poi di configurare e monitorare la rete industriale per affrontare gli attacchi che hanno origine all'interno della stessa, indirettamente tramite malware, o direttamente per accesso al mezzo fisico con connessione via cavo o wireless. La gestione sicura della rete informatica industriale richiede una serie di accorgimenti che si possono così sintetizzare:
• identificare i flussi delle informazioni in rete e configurare i firewall per permettere il passaggio del solo traffico autorizzato;
• utilizzare soltanto protocolli sicuri (che non trasmettono le password in chiaro) per l'amministrazione dei firewall degli switch. Ovviamente, le password di default fornite dal fabbricante dovranno essere sostituite da password sufficientemente robuste;
• utilizzare firewall con capacità UTM (Unified Threat Management) e quando non è possibile, per garantirne la continua operatività, installare tempestivamente gli aggiornamenti di sicurezza sui PC della rete industriale;
• utilizzare tecnologie wireless che impieghino una crittografia robusta, configurarle nel modo più sicuro ed evitare, per quanto possibile, che il loro raggio di azione raggiunga l'esterno dell'impianto industriale;
• garantire la sicurezza fisica dell'impianto, limitando, tra l'altro, l'accesso ai cavi di trasmissione dati e bloccando l'accesso a porte degli switch non utilizzate;
• gestire la configurazione della rete, mantenendo un catalogo aggiornato di tutti gli apparecchi connessi, verificandolo periodicamente con l'ausilio di strumenti automatici e osservando una procedura per l'autorizzazione e la gestione delle modifiche;
• implementare opportuni processi di autorizzazione all'accesso, fornendo i minimi privilegi necessari agli utenti e revocandoli quando non più necessari;
• implementare i necessari meccanismi di autenticazione, per verificare l'identità del personale autorizzato. Le credenziali devono essere strettamente personali e il loro possessore deve essere responsabile delle attività svolte con il proprio account;
• monitorare il traffico di rete per rilevare eventuali attacchi utilizzando un IDS (Intrusion Detection System).

Non si può prescindere, poi, dalla necessità di sensibilizzare e addestrare il personale alla security.

Né ci si può affidare a una sessione di addestramento 'una tantum': per alimentare una cultura aziendale che promuova la security, l'argomento va ripreso periodicamente, con sessioni di informazione e aggiornamento.

Prevenire è meglio che curare

Prevenire gli incidenti è ovviamente la prima funzione della security. Tuttavia, è parimenti importante essere in grado di reagire a un incidente di security per ripristinare nel più breve tempo possibile l'operatività completa dell'impianto industriale. Per riuscirci bisogna anzitutto fare tutti i preparativi necessari:
• salvare tutte le informazioni (dati, software, sistemi operativi, configurazione) che potrebbero venire corrotte o distrutte in un incidente di security e che sarà quindi necessario ripristinare;
• avere a disposizione ricambi per i componenti più critici o per i quali è conveniente tenere uno stock di ricambi;
• verificare che vi siano i necessari contratti di manutenzione e che prevedano tempi di risposta congrui;
• implementare un processo per gestire gli incidenti di security.

Disporre di un processo per la gestione degli incidenti di security è importante per essere in grado di reagire con prontezza a eventi avversi. Bisogna dunque identificare le categorie di incidente e come reagire in ciascun caso, identificando i ruoli del personale che deve affrontare l'incidente e associando a ciascun ruolo i nominativi o la funzione aziendale delle persone che lo ricoprono.

Nel corso della gestione dell'incidente bisogna poi registrare tutte le azioni compiute, quando e da chi, in modo da disporre di un report che, alla chiusura dell'incidente, potrà essere sottoposto al management e rivisto in modo da valutare l'efficacia delle misure adottate ed eventuali miglioramenti alla procedura da applicare nei casi futuri.

Fonti: IEC 61158 *"Digital data communication for measurement and control - Fieldbus for use in industrial control systems"*; IEC 61784 *"Profile sets for continous and discrete manufacturing relative to fieldbus use in industrial control systems"*; Profibus Nutzerorganisation e. V. (PNO) *"Profinet System Description"; IEC 61508 "Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems"*.

Gfcc (Genoa Fieldbus Competence Center) – www.gfcc.it