Tavola rotonda

Fonte: itrads.com

PARLIAMO DI REVAMPING

INNOVARE SALVAGUARDANDO GLI INVESTIMENTI: COME LA RETE INDUSTRIALE SI PUÒ EVOLVERE MANTENENDO LA COMPATIBILITÀ CON IL PASSATO

a cura di **Ilaria De Poli e Oscar Milanese***

Le previsioni macroeconomiche lasciano intravedere un biennio di crescita nel prossimo futuro, segnando un'inversione di tendenza rispetto agli ultimi anni. Quanto questa previsione potrà portare ad aumentare gli investimenti delle imprese manifatturiere è ancora tutto da verificare, ma le probabilità sono ora maggiori che nel recente passato. Gli impianti esistenti avranno la necessità di essere aggiornati implementando nuove tecnologie, che si dovranno integrare alle precedenti già installate, soprattutto per la parte IT e networking, garantendo nuove funzionalità e maggiori prestazioni. In questo scenario, le reti industriali saranno oggetto di trasformazioni che richiederanno compatibilità con il passato. Vediamo come con l'aiuto di alcuni esperti di primarie aziende del settore manifatturiero.

Come si evolve l'installato

Quali saranno i trend tecnologici del prossimo biennio relativamente all'evoluzione delle reti industriali attualmente installate?

"Sulla base di quanto sta già avvenendo è fin troppo facile prevedere un consolidamento, se non l'accelerazione del trend di crescita e diffusione nel campo delle reti di automazione dei protocolli basati su Ethernet industriale" osserva **Raffaele Esposito**, product manager Safety, I/O & Networking di **Phoenix Contact** (*www.phoenixcontact.it*). "Presto tramontata l'ipotesi di un protocollo a base Ethernet industriale di tipo 'universale', con molta probabilità il mercato si orienterà ora in modo prevalente sui protocolli rappresentati dai Consorzi con maggiori capacità di innovazione, sviluppo e veicolazione/diffusione delle caratteristiche tecniche e delle applicazioni specifiche del protocollo da essi rappresentato".

Altro punto da considerare è la convergenza sempre più spinta tra le tecnologie tipiche del mondo industriale e le soluzioni standard in ambito IT: "Questo trend renderà via via più semplice ed economicamente sostenibile l'approccio a due altri grandi 'filoni' tecnologici, verso i quali i progettisti industriali stanno rivolgendo sempre più spesso la loro attenzione: la teleassistenza (in senso lato) e l'utilizzo di soluzioni di tipo wireless" ha proseguito **Esposito**. Sono disponibili sul mercato svariate tipologie di soluzioni, sia nel campo della teleassistenza, sia del wireless, diverse per aspetti tecnici, architetturali e tecnologici, tutte complementari a un network industriale. L'utilizzatore finale può dunque trovare la soluzione a lui più idonea per soddisfare esigenze specifiche: "La scelta della giusta soluzione tecnologica in base alle proprie necessità permette l'ottimizzazione dei vantaggi ottenibili in termini di flessibilità, diagnostica, semplicità di modifiche/integrazioni, time to market delle applicazioni, oltre che per valutare la convenienza di una soluzione dal punto di vista economico" ha proseguito **Esposito**. "Verrà poi richiesta maggiore attenzione a uno sviluppo e a un'implementazione capaci di garantire il corretto raggiungimento dei livelli di safety e security necessari per la specifica applicazione".

Angelo Candian, head of industrial communication di **Siemens Italia** (*www.siemens.it*), pone invece l'accento sulla diffusione dei sistemi basati su Ethernet: "I tradizionali bus di campo, basati su sistemi di comunicazione seriale, si stanno indirizzando verso nuove tecnologie basate su Ethernet, fra le quali figura Profinet, evoluzione di Profibus, che permette un'agevole integrazione con i dispositivi del mondo IT". Profinet rappresenta la risposta del Consorzio PI (Profibus & Profinet International) per la realizzazione di applicazioni realtime Ethernet nel campo dell'automazione. "Le innovazioni tecnologiche introdotte da Profinet, unite a un'integrazione trasparente dei nodi Profibus installati sugli impianti, fanno sì che Profinet sia destinato a

diffondersi ad ampio raggio" ha proseguito **Candian**. "Con le innovazioni introdotte dalle specifiche v2.3, in particolare, Profinet offre performance elevate, quali un tempo di trasmissione di 31,25 µs per applicazioni isocrone di motion control. Inoltre, Profinet si basa sull'utilizzo di reti Ethernet standard, offrendo numerosi vantaggi in termini di efficienza negli impianti di produzione, quali: utilizzo di pagine web per la diagnostica dei dispositivi, possibilità di impiegare reti WiFi, collegamento via Internet agli impianti per interventi in remoto. Infine, Profinet è liberamente integrabile in rete con dispositivi Ethernet standard (telecamere IP, dispositivi di programmazione, PC gestionali ecc.), senza inserire interfacce o gateway".

Con Candian concorda **Roberto Motta**, solution architect team leader di **Rockwell Automation** (*it.rockwellautomation.com*): "I prossimi trend relativi alla comunicazione industriale sembrano ampiamente definiti da Ethernet sulla base di un installato e di una disponibilità della tecnologia veramente 'globali'. Consolidatosi a livello mondiale con l'utilizzo dei protocolli TCP/UDP/IP, ormai largamente diffusi, Ethernet sta modificando rapidamente anche il volto dell'automazione di fabbrica, trasformando le reti industriali da tecnologie orientate alla mera connessione di dispositivi, a tecnologie indirizzate all'efficienza nella trasmissione delle informazioni". Perché le soluzioni Ethernet possano offrire il massimo in termini di accessibilità e conoscenza per gli utenti del mondo dell'automazione, però, sottolinea **Motta**, sarà fondamentale che Ethernet industriale sfrutti e integri tutte le tecniche di comunicazione divenute, negli anni, degli standard di fatto per gli ambiti aziendale e commerciale. "Servendosi di un'unica rete comune, le infrastrutture di automazione ed enterprise potranno coesistere e condividere i dati in modo efficace, utilizzandoli, per esempio, per definire e creare indicatori aggiornati dell'efficienza delle macchine, gestire i consumi energetici e creare dashboard di controllo delle prestazioni".

Chiude infine **Giancarlo Carlucci**, product manager Plant Solutions - PLC, Networks & I/O per l'Italia di **Schneider Electric** (*www.schneider-electric.it*), ricordando come l'efficientamento e l'ottimizzazione degli asset esistenti, integrando nuovi servizi e tecnologie allo stato dell'arte, costituiscano un'opportunità unica da cogliere per le aziende che intendono ridurre i costi e migliorare la produttività: "Uno degli assi strategici su cui agire nei prossimi anni è garantire ai clienti la continuità produttiva, operando nel contempo al fine di valorizzare i sistemi installati. Ciò può avvenire solamente attraverso un'attenta analisi dell'esistente, seguita da un'azione di modernizzazione, progettata per creare valore percepibile dal cliente grazie a servizi di commodity non solo orientati all'efficienza produttiva, ma anche al ritorno dell'investimento sui costi energetici e manutentivi. Il networking costituisce una parte ineludibile dell'attività di modernizzazione, in quanto, negli attuali sistemi di fabbrica, è determinante per l'integrazione dei dati di processo, nonché di valori energetici acquisiti al fine di attuare un'attività di efficientamento".

Modernizzare o rinnovare… questo è il problema

È preferibile mantenere gli attuali protocolli e software di comunicazione, anche se 'datati', per garantire una più semplice integrazione con i nuovi sistemi, oppure sono auspicabili un deciso e pragmatico rinnovamento e una standardizzazione?

Secondo **Carlucci** è fondamentale che sistemi e impianti siano sempre operativi, senza però rinunciare alla standardizzazione: "L'attività di modernizzazione non deve impattare sulla continuità operativa dei sistemi; tale obiettivo è perseguibile attraverso quella che viene definita 'smooth migration', ossia una graduale modernizzazione dei dispositivi hardware e software. D'altra parte, questa deve andare di pari passo con la standardizzazione dei protocolli di comunicazione, possibilmente a tutti i livelli infrastrutturali. Schneider Electric ha adottato i protocolli standard Ethernet TCP/IP come tecnologia per la trasmissione delle informazioni. Omogeneizzare la tecnologia di comunicazione si traduce in migliori prestazioni, apertura a dispositivi di terze parti e trasparenza in fase manutentiva e predittiva, tutti valori che in genere il cliente riconosce e sui quali è disposto a investire".

Raffaele Esposito, product manager Safety, I/O & Networking di Phoenix Contact

Motta sottolinea invece un diverso aspetto della questione: "Se per protocolli 'attuali' si intendono i fieldbus tradizionali, credo che l'enorme installato a base Ethernet in ogni ambito della vita quotidiana (non a caso si parla sempre più di 'Ethernet of Everything') rappresenti un'attrattiva tale per cui, anche per il mondo industriale, sia facile prevedere che si arriverà, già nei prossimi anni, a un vero e proprio 'ricambio generazionale' per molte installazioni. D'altra parte Ethernet fornisce una tecnologia così universale, che ogni utente può da subito usufruire di una conoscenza e una disponibilità di applicazioni senza precedenti. La quantità di dispositivi industriali e non potenzialmente connettibili alla rete globale sta crescendo esponenzialmente e si prevede che arrivi a 20 miliardi nel 2020 (Internet of Things)".

Per **Esposito**, infine, la risposta non può essere univoca, in quanto occorre valutare le specificità dell'applicazione di fronte alla quale ci si trova: "Sebbene possa sembrare banale, solo un'attenta analisi costi/benefici permette di orientarsi tra le due opzioni ipotizzate… Tutto parte dall'applicazione: su un progetto ex-novo la possibilità di attingere a tecnologie e soluzioni di ultima generazione consente, in termini generali, di ricorrere a tutte le novità tecnologiche introdotte dai nuovi prodotti. Da un punto di vista puramente tecnico, non vi sono normalmente molti dubbi sul fatto che questa sia la soluzione preferibile, escludendo l'utilizzo di soluzioni troppo innovative, ancora in fase di sviluppo e consolidamento. Lo scenario è completamente diverso se si pensa invece a interventi di aggiornamento e integrazione di macchine o impianti già esistenti. Non è però possibile escludere il caso in cui, anche in queste situazioni, un deciso e completo rinnovamento dei prodotti e delle tecnologie in uso possa costituire una soluzione preferibile, sulla base della famosa analisi costi/benefici. In tali casi, d'altronde, quello su cui spesso e volentieri si punta è la parziale introduzione di nuovi prodotti/tecnologie a fronte di un possibile efficace interscambio con l'esistente. Da questo punto di vista, la sempre maggiore diffusione di gateway che consentono la comunicazione tra reti o parte di esse dotate di protocolli diversi costituisce una soluzione ottimale".

Il cambiamento dell'infrastruttura fisica

Quali saranno i maggiori cambiamenti che il rinnovo dell'infrastruttura fisica delle reti comporterà (hardware, gateway, bridge, cavi)?

Con l'introduzione dei protocolli a base Ethernet industriale nelle reti di automazione sarà l'infrastruttura di rete a subire le maggiori modifiche. Afferma **Esposito**: "Nella classica struttura dei bus tradizionali a base seriale i collegamenti tra i vari dispositivi di rete (controllori, accoppiatori di rete, HMI, drive ecc.) avvenivano con 'semplici' cavi dalle caratteristiche tecniche specifiche per ogni singolo protocollo o, nel caso di una connessione in fibra ottica, si utilizzavano conver-

titori ancora una volta specifici per protocollo. Con l'introduzione di Industrial Ethernet tale infrastruttura si modifica assumendo la conformazione ormai da tempo tipica delle applicazioni IT. Si dovranno per esempio utilizzare, in funzione delle caratteristiche del protocollo scelto, dispositivi specifici quali hub o switch, sempre che non siano direttamente integrati nei dispositivi destinati a essere collegati al network, quali gli accoppiatori di rete. La volontà di disporre di caratteristiche tecniche specifiche o più evolute nel network (diagnostica spinta, gestione Vlan, uso di anelli di ridondanza, accesso remoto, comunicazione wireless ecc.) può poi condurre all'uso di componentistica più complessa (switch managed) o addizionale (router, access point, repeater, slave wireless, convertitori rame/fibra, gateway ecc.). Anche i cavi dovranno evolvere per adattarsi a nuove classi di velocità di trasferimento dati o per veicolare, per esempio, anche la tensione di alimentazione per i dispositivi connessi (Power over Ethernet)".

Roberto Motta, solution architect team leader di Rockwell Automation

Secondo **Motta** la struttura fisica della rete di automazione dovrà sempre più essere condivisa con quella del livello enterprise, fino a costituire un'unica entità e questo porterà svariati cambiamenti: "Concetti come Vlan, router, firewall, VPN stanno già entrando a pieno titolo nel mondo della fabbrica. Ora, dalla semplice integrazione fisica stiamo progressivamente passando a quella logica, che prevede l'esistenza di un'unica rete di automazione e aziendale, configurata per soddisfare ai requisiti applicativi di entrambi i mondi. Uno dei fattori di maggiore novità per la struttura fisica delle reti di automazione, determinata dall'avvento di Ethernet, sarà proprio quello di configurabilità a livello logico".

Osserva quindi **Carlucci**: "Negli anni pionieristici dell'automazione abbiamo visto un proliferare di tipi di reti e fieldbus differenti. Questi avevano spesso una base tecnologica comune, ma implementavano ognuno personalizzazioni che impedivano l'integrazione dei sistemi di costruttori diversi se non attraverso l'uso di gateway. Oggi tutte queste esperienze convergono nell'utilizzo del protocollo Ethernet nelle sue varie accezioni. La sfida quindi si pone nel gestire al meglio questa tecnologia senza personalizzarla (limitandone quindi l'integrazione con sistemi terzi), utilizzando dispositivi in grado di sfruttare e massimizzare la tecnologia standard. Per Schneider Electric questo si traduce in un concetto rivoluzionario: portare le funzionalità dei prodotti a connettività Ethernet dentro i componenti di automazione. Così è avvenuto per il controller Modicon M580, un vero e proprio ePAC (Ethernet PAC), che comunica con moduli presenti sul suo stesso backplane via Ethernet, dando la possibilità di creare quella trasparenza e quel tunneling dei dati tra i vari livelli dell'infrastruttura normalmente propri di switch o bridge. A questo possiamo associare moduli per il cambio del media trasmissivo (per esempio rame/fibra o WiFi), creando così soluzioni integrate all'interno del controllore o dell'I/O remoto. In sostanza, diventa possibile progettare architetture più semplici e meno costose, composte da un numero inferiore di firewall, switch, router, gateway, in quanto tali funzionalità sono già integrate nei singoli prodotti intelligenti che compongono la rete".

Fonte: img.gawkerassets.com

"L'evoluzione delle reti industriali verso le nuove tecnologie basate su sistemi Ethernet impatta senza dubbio sulla struttura fisica degli impianti" concorda infine **Candian**. "La diffusione della tecnologia switch e il cablaggio Industrial Ethernet sostituiranno i sistemi seriali: la migrazione verso queste nuove strutture è supportata da prodotti Siemens specifici per uso industriale, quali soluzioni per un'installazione rapida e intuitiva dei cavi Industrial Ethernet (Fast Connect). Per quanto concerne gli switch (unmanaged o managed), i prodotti di Siemens garantiscono funzionalità idonee all'impiego in reti realtime grazie all'introduzione della funzione di priorizzazione dei pacchetti Profinet. Il revamping delle reti fieldbus già installate è garantito dalla disponibilità di gateway che consentono l'integrazione trasparente dei nodi Profibus già presenti sugli impianti, senza bisogno di modificare il software. Il collegamento del livello di campo con la rete Ethernet aziendale è assicurato in maniera controllata, ottimizzando la diagnostica e la gestione dei dati della rete industriale tramite router/firewall layer 3".

Angelo Candian, head of industrial communication di Siemens Italia

Revamping con o senza fili?

Pensate sia importante poter implementare anche le tecnologie wireless industriali in caso di revamping?

Numerose referenze ormai disponibili in ambito industriale mostrano, ricorda **Candian**, come l'uso di prodotti a tecnologia WiFi, "assieme a un adeguato supporto tecnico in fase di progettazione della rete wireless, possono costituire una valida alternativa in termini economici, di affidabilità e sicurezza per applicazioni con dispositivi mobili, dove l'uso di cavi speciali o contatti striscianti implica spesso costi aggiuntivi di manutenzione, costanti nel tempo".

Ugualmente favorevole all'introduzione di soluzioni WiFi è **Carlucci**, che sottolinea come il mercato riconosca in esso una tecnologia con ampi margini di crescita, in grado di supportare soluzioni di sistema che sarebbero molto più dispendiose se sviluppate in altro modo. "In un'ottica di revamping e modernizzazione il WiFi è un 'anello di congiunzione' atto a connettere tra loro apparati del mondo consumer, quali smartphone o tablet, e sistemi o strumentazione industriali".

Più in generale valgono per il WiFi le stesse considerazioni fatte per le nuove installazioni, perciò è consigliabile compiere "un'opportuna analisi del contesto applicativo e dei reali miglioramenti che questa tecnologia può apportare in termini di costi installativi di cablaggio, ma anche di disponibilità e affidabilità del sistema". Illustra quindi Esposito: "Le varie soluzioni wireless per l'ambito industriale oggi esistenti mettono a disposizione dei tecnici delle reali alternative per risolvere situazioni specifiche, quali la comunicazione tra parti in movimento con sistemi di comando centralizzati, o tra parti di macchine o impianti ubicati in ambienti in cui è difficile o economicamente poco conveniente realizzare dei collegamenti fisici, la copertura di ampie aree produttive, la mobilità dell'operatore incaricato della gestione dell'installazione e via dicendo. Le caratteristiche del WiFi posso risultare interessanti sia che si debba procedere a una progettazione ex-novo, sia che ci si trovi di fronte a un'operazione di ammodernamento o integrazione di dispositivi in un'installazione pre-esistente. Si pensi per esempio alla sostituzione per usura di un sistema di comunicazione relativo alle parti mobili di un impianto, realizzato con anelli collettori e contatti striscianti o con cavi flessibili in catene porta-cavi. L'introduzione di una soluzione wireless risolve brillantemente la problematica, rendendo l'intervento più veloce ed economico, senza contare il fatto che l'eliminazione degli effetti dell'usura meccanica rende di fatto superflui i successivi interventi di manutenzione/sostituzione. Oppure si pensi alla possibilità di aggiornare un impianto esteso, che prevede l'uso di sistemi di movimentazione manuale del materiale: la copertura della zona con un'infrastruttura wireless potrebbe consentire l'impiego di AGV con conseguente maggiore flessibilità/scalabilità/produttività dell'impianto stesso, il tutto con pochi e semplici intervenenti sulla parte hardware del sistema di automazione".

In conclusione, **Motta** puntualizza: "Possiamo considerare un dato di fatto che Ethernet commerciale sia diventato wireless, rendendo disponibili soluzioni semplici e affidabili, implementabili a basso costo anche su dispositivi di automazione, ma l'approccio verso i sistemi wireless in campo industriale resta problematico. Prevedibilmente verrà adottato solo dove può portare un effettivo valore aggiunto in termini di semplicità d'uso rispetto a soluzioni alternative al cablaggio già in uso nell'automazione, quali diverse tecniche a induzione o su bandella. Un discorso a parte vale per dispositivi quali iPad, telecamere e lettori portatili RFI o barcode, la cui diffusione in ambito industriale è relativamente recente, ma per i quali ci si aspetta una rapida adozione in un futuro immediato".

La sicurezza non è un optional

Security e safety: quali i trend e quale la reale attenzione che le aziende riservano oggi al tema della cybersecurity?

Risponde **Motta**: "Il concetto di security è relativamente nuovo per le reti di automazione e per quanto ancora si pensi a essa più in relazione a possibili azioni esterne dolose (virus, sabotaggi, accessi non autorizzati) occorre preoccuparsi anche delle eventuali azioni interne, volontarie o meno. Personale e impianti non vanno protetti solo dai rischi connessi alle intrusioni, ma occorre garantire un servizio efficiente, sicuro e sempre disponibile, sia attraverso il controllo della validità e congruità dei privilegi di accesso locali, sia attraverso l'efficienza della rete. Il concetto di security comprende sia l'aspetto della protezione dei dati che transitano in rete, sia quello della sicurezza, ossia che non vi siano guasti in rete tali da causare danni a persone e infrastrutture. Per questo la security si ottiene anche attraverso una pianificazione accurata delle architetture di rete; non solo, è altresì necessaria un'azione a livello culturale finalizzata a limitare i danni derivanti da comportamenti ingenui da parte degli operatori, come una cattiva gestione di username e password, oltre che fornire delle linee guida per evitare la generazione di problemi a livello di rete. Per altro verso, il comparto automazione in genere considera come rischi prioritari contro i quali tutelarsi gli accessi remoti di tecnici e fornitori. Nel contempo, vi è una diffusa consapevolezza dei vantaggi derivanti dalla condivisione delle risorse aziendali con tali soggetti e da una gestione anche in remoto degli asset produttivi. Occorre inoltre ricordare che i danni che possono derivare da una vulnerabilità del sistema informatico non si limitano solo all'accesso a dati sensibili, bensì possono configurarsi come vere e proprie interruzioni della produzione o del servizio con rilevanti perdite economiche". Per quanto concerne l'atteggiamento delle aziende, **Motta** ritiene che "il livello di percezione del rischio informatico è in forte crescita nel campo dell'automazione sia manifatturiera che di processo, data la sempre più diffusa presa di coscienza del fatto che la vulnerabilità dei software costituisce la chiave principale tramite cui gli intrusi riescono ad accedere ai sistemi di automazione, violando la sicurezza informatica aziendale. Un secondo fattore che ha portato a incrementare la percezione del rischio informatico potenziale è la diffusione, anche al livello di fabbrica, di Ethernet, dei protocolli TCP/UDP/IP e di un sistema di cablaggio comune a tutti i layer di comunicazione, dal sensore a Internet: collegare un cavo RJ45 ovunque può creare un reale problema di sicurezza informatica".

Giancarlo Carlucci, product manager Plant Solutions - PLC, Networks & I/O per l'Italia di Schneider Electric

Concorda sulla questione **Carlucci**: "La necessità che i sistemi industriali siano sicuri è sempre più sentita da parte delle aziende. Negli USA queste esigenze sono sfociate in standard come la norma Nerc CIP002, imposta dall'ente regolatore al settore delle infrastrutture elettriche, o linee guida come la ISA-SP99, che indica come sviluppare e misurare i livelli di sicurezza dei sistemi hardware e software. Anche l'Italia ha recepito, con un decreto pubblicato a marzo 2013, quelle che erano raccomandazioni sulla regolamentazione indicate

dalla Comunità Europea. Il decreto definisce un modello organizzativo-funzionale e in sostanza impone agli operatori che gestiscono infrastrutture critiche materiali e immateriali, di dotarsi di meccanismi e procedure da seguire ai fini di prevenire i rischi e ridurre la vulnerabilità. Nello scenario industriale, laddove siano implementati sistemi orientati al controllo da remoto, come negli impianti di gestione dell'acqua o nelle grandi infrastrutture (stradale/ferroviaria), gli utenti devono dotarsi di sistemi atti a isolare le reti, quali firewall". **Carlucci** ritiene che la sensibilità al tema sia in crescita, "spinta anche dalle normative sopra indicate. Va però sottolineato che i clienti spesso si dotano di strumenti atti a bloccare eventuali violazioni che agiscono dall'esterno, sebbene statisticamente gli 'incidenti' non siano provocati intenzionalmente e le maggiori vulnerabilità risiedano piuttosto all'interno del sistema. I casi di rischio maggiore, infatti, derivano da comportamenti errati degli operatori, che involontariamente inseriscono bug o corrompono i firmware e i software dei dispositivi. Una novità è costituita dall'introduzione di controlli di integrità e di proprietà di protezione implementate direttamente dentro i dispositivi collegati in rete. È il caso per esempio delle funzionalità avanzate di cybersecurity disponibili sui PAC di nuova generazione, che permettono di configurare controlli di coerenza sulla memoria, sul firmware e sul codice applicativo, così da correggere istantaneamente errori di processamento o bloccare azioni esterne non autorizzate".

Fonte: www.mobilecloudcode.com

Anche **Candian** ribadisce che, poiché Ethernet e Internet si sono ormai ampiamente diffusi in ambito industriale, "le tendenze di apertura e interconnettività dei sistemi hanno indebolito la protezione degli stessi da minacce esterne, rendendoli più vulnerabili alle intrusioni informatiche da parte di soggetti non autorizzati. È dunque indispensabile implementare una strategia di cybersecurity ottimizzata contro intrusioni e attacchi cibernetici. Nel caso delle reti di fabbrica con collegamenti esterni attraverso Internet, o per reti LAN di fabbrica riservate, è utile implementare delle VPN. Con tale meccanismo si crea un tunnel di collegamento virtuale che sfrutta i normali protocolli di trasporto dati TCP o UDP, nel quale transitano gli stessi criptati. Le chiavi di decodifica risiedono nei due end point router-server. Sono disponibili PLC e PC con funzionalità VPN integrate, in grado di interfacciarsi direttamente con router-server dedicati alle VPN".

Aggiunge quindi **Carlucci**: "L'adozione dei sistemi informatizzati da parte della PA e l'integrazione fattiva delle tecnologie IT nei processi industriali permette una migliore distribuzione delle informazioni lungo gli asset aziendali. Questo si traduce in un costo unitario più basso della produzione, derivante da una maggiore efficienza produttiva data da una migliore gestione dei beni strumentali. Una rete così progettata chiaramente richiede una maggiore attenzione alla gestione dei rischi connessi a safety e security. Spesso l'analisi dei rischi offre alle aziende un'opportunità di miglioramento, soprattutto in un periodo come questo dove la continua pressione sui costi e sui margini impone un consolidamento delle attività. Una sofisticata analisi delle informazioni generate dalla rete è passaggio obbligato per una pianificazione mirata degli investimenti. Sempre più, quindi, in rete passeranno informazioni sensibili da proteggere, affinché la giusta informazione arrivi all'interlocutore più adatto. In questo senso, la protezione e la gestione dei beni strumentali e delle persone è responsabilità dell'utente finale, che deve adottare degli standard di sicurezza validi sul proprio sistema. È invece responsabilità del fornitore di tecnologia fornire le raccomandazioni e le metodologie da seguire per integrare nei prodotti e nelle soluzioni adottate le soluzioni di sicurezza idonee". Non bastano dunque filo spinato e guardie per garantire la sicurezza dei beni strumentali: "Le aziende" prosegue **Carlucci** "devono essere più diligenti nello sviluppare e proteggere il loro business attraverso piattaforme hardware e software in grado di evolversi coerentemente con gli standard di mercato e sfruttando le opportunità di integrazione e sicurezza che le tecnologie IT possono portare ai sistemi di automazione. Sempre più le necessità di business porteranno l'automazione e il networking ad avere un ruolo cruciale nel mettere in comunicazione diretta trasversalmente aree diverse di applicazione anche non propriamente industriali". **Esposito** nota infine come gli aspetti di safety e security, sebbene spesso trattati insieme quando sono oggetto di discussione, vengano ancora troppo spesso "in realtà gestiti in modo autonomo e indipendente, a volte anche proprio da entità e soggetti separati, per esempio il tecnico progettista di automazione industriale per la safety e il responsabile IT per la security. Questa situazione può trovare giustificazione nella storica diversa competenza tecnica tra queste figure e, in una certa maniera, in applicazioni dove non sia previsto l'uso di dispositivi programmabili o soluzioni basate su reti di comunicazione. Pur con la possibilità di continuare a essere gestiti da entità differenti, i safety e security devono sempre essere oggetto di un'analisi congiunta. E proprio nelle applicazioni in cui la safety prevede l'impiego di dispositivi programmabili o soluzioni basate su rete, il giusto livello di security serve a evitare non solo l'accesso a dati sensibili, ma anche ogni possibile intervento di modifica nella logica di funzionamento della macchina o impianto, ben consci del fatto che ogni variazione fraudolenta al funzionamento dell'applicazione può compromettere il funzionamento sicuro della stessa, a maggior ragione se le modifiche vengono eseguite nella parte di automazione deputata alla gestione delle necessarie funzioni di sicurezza". In linea con quanto detto, **Esposito** osserva poi che "l'attenzione alla security è generalmente elevata nelle aziende, quantomeno in tutte quelle applicazioni che si vogliono rendere accessibili da remoto. Ben consci dei potenziali varchi che questo approccio può aprire in ambito cybersecurity, i tecnici di automazione pongono molta attenzione agli strumenti più adeguati per consentire l'accesso solo alle persone autorizzate e per escludere il rischio di corruzione o acquisizione dei dati aziendali sensibili da parte di estranei. Un po' più sottovalutata è invece la protezione di un'installazione non destinata al collegamento con reti esterne, in quanto è ancora fortemente radicata l'errata convinzione che in questo caso non vi siano rischi reali di security. Si trascura così, in modo colpevole, la possibilità da parte dei malintenzionati di accedere comunque alla rete collegandosi per esempio tramite delle porte lasciate libere sugli switch, o la possibilità di introdurre in rete dei malware usando supporti di memoria esterni contaminati. Questa sottovalutazione è oggi sempre meno accettabile, anche alla luce delle soluzioni tecniche disponibili sul mercato: è possibile modulare, anche in modo molto fine, il livello di protezione garantito per l'applicazione specifica, con costi assolutamente accessibili".

*Comitato tecnico Automazione Oggi e Fieldbus & Networks