Hardware e software per l'automazione distribuita

Maggio 2010 • www.ilb2b.it

Fieldbus & Networks

DOSSIER
I fieldbus nel 'green engineering'

PRIMO PIANO
I/O multistandard

Meglio esserci!

PROFIBUS

PI Italia
PROFIBUS • PROFINET

PROFINET

FIERA MILANO EDITORE

Nuove frontiere

Controllare e gestire macchine e apparati senza doversi spostare, accedere in tempo reale ai dati per supervisionare un impianto, intervenire su un allarme da remoto: ecco solo alcuni dei vantaggi offerti dai sistemi di telecontrollo e telegestione. Vediamone prospettive e vantaggi

Carlo Lodari

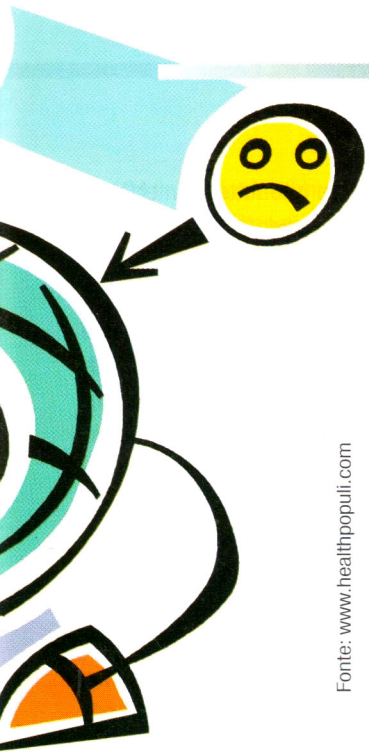
I settori 'promettenti'

Quali sono i settori applicativi più dinamici per le soluzioni di telecontrollo e telegestione?

Parlare di telecontrollo e telegestione oggi vuol dire affrontare uno dei temi più 'caldi' dell'automazione. Da una parte, infatti, in questo momento di relativa stasi del mercato, i costruttori di macchine e impianti si stanno focalizzando sull'offerta di servizi a valore aggiunto alla clientela in essere (quella del telecontrollo è in questo caso un'opportunità da non lasciarsi sfuggire); dall'altra il telecontrollo offre una 'facile' via per ridurre alcuni costi. Gestire a distanza significa infatti risparmiare sul personale 'stanziale' e sulle operazioni di manutenzione, sia da parte di chi offre servizi, che può evitare viaggi onerosi e contenere i tempi degli spostamenti, sia per chi gestisce l'impianto, in quanto consente interventi tempestivi laddove ogni fermo prolungato comporta ingenti perdite finanziarie. Per questo, definire i confini applicativi delle soluzioni di telecontrollo e telegestione è assai complesso: si spazia dall'automazione di macchine e impianti al controllo di distributori automatici. Sottolinea **Vittorio Agostinelli** (Panasonic Electric Works Italia): "Monitorare, gestire e programmare da remoto costituiscono oggi funzionalità irrinunciabili". Oltre alle applicazioni legate alla produzione di energie rinnovabili e al risparmio energetico, **Agostinelli** individua nelle public utility i soggetti più ricettivi e vivaci verso queste soluzioni, soprattutto nei contesti legati al ciclo idrico integrato. Dello stesso parere è **Alberto Poli** (Wago Elettronica), che aggiunge alla gestione acque il mondo della distribuzione elettrica e, genericamente, del controllo della produzione industriale, mentre afferma **Mauro Galano** (Rockwell Automation): "Il settore dei depuratori e potabilizzatori, insieme a quello degli acquedotti sono di gran lunga i più significativi".

Per **Fabio Melegazzi** (Telestar) un ambito dove l'interesse per questo tipo di soluzioni è in crescita è quello del monitoraggio di impianti non presidiati, in un'ottica di teleassistenza: "Costruttori e manutentori hanno sempre più la necessità di acquisire lo stato di funzionamento di impianti quali stazioni di pompaggio, cabine elettriche e ripetitori telefonici e radio, in quanto la presenza in loco di un tecnico comporta costi elevati" e dello stesso parere è **Filippo Cubattoli** (PcVue), soprattutto per supervisionare più siti non presidiati: "Nel campo della gestione di acqua e gas esistono siti remoti di pompaggio, piccole centrali di potabilizzazione, serbatoi, depuratori, riduttori di pressione e gruppi di misura da tenere sotto controllo; oppure nella produzione di energie rinnovabili e nei grandi edifici, in cui la gestione e conduzione degli impianti tecnologici è affidata a ditte esterne, o anche nella gestione di flotte e per la geolocalizzazione di veicoli (logistica, emergenza e soccorso sanitario ecc.)". Con lui concorda **Antonio Augelli** (Siemens): "Gli ambiti della distribuzione e depurazione dell'acqua, dell'irrigazione, dell'oil&gas e delle infrastrutture (tunnel autostradali e ferroviari) sono fra i più recettivi. Vedo poi un ruolo decisivo del telecontrollo nel building management, nella generazione e distribuzione energetica, in combinazione con lo sviluppo delle 'green technology'".

Energia e gestione delle acque sono e saranno ambiti decisivi anche per **Marco Ceriani** (Progea) dal punto di vista della dinamicità e del potenziale di crescita, anche al fine di salvaguardare i consumi. Riassume **Cristian Randieri** (Intellisystem Technologies): "I settori più interessanti sono legati alle reti di distribuzione (acqua potabile, gas, riscaldamento, illuminazione pubblica), poiché proprio per la loro vastità e dislocazione in territori lontani implicano maggiori costi di manutenzione, se la loro gestione è demandata a sistemi 'classici'. La telegestione consente poi di espandere gli impianti in maniera dinamica a costi relativamente bassi". Non solo. Evidenzia **Ivan Mangialenti** (Schneider Electric): "Nei piani di contenimento dei costi delle aziende,



Fonte: www.healthpopuli.com

alla voce energia corrisponde spesso una spesa importante. Nell'ultimo anno, e si tratta di un trend che vediamo in forte crescita, è aumentata la richiesta di sistemi di raccolta delle misure dei consumi sui cinque vettori energetici Wages (Water, air, gas, electricity, steam), integrati con software di analisi dei dati". Costruire un database storico dei consumi costituisce infatti il primo passo per capire dove intervenire per migliorare l'efficienza energetica.

Osserva **Kike Revelli** (Ge.Co.S. - Sistema di Gestione e di Controllo Silos): "Noi ci siamo focalizzati sull'edilizia, in particolare nella gestione di silos per malte e intonaci premiscelati, che sono sparsi sul territorio per periodi più o meno brevi in base alla durata del cantiere e che, proprio perché non 'stanziali', vedono nel telecontrollo o nella telegestione il modo migliore per gestire l'intero ciclo produttivo". Afferma infine **Fabio Masorati** (Movactive): "Dal nostro particolare punto di vista è il fleet management per il trasporto l'ambito applicativo che domina il mercato della telegestione wireless. Per quanto concerne il mondo industriale, non vediamo ancora una tendenza consolidata in un particolare settore, al contrario l'adozione di soluzioni di telecontrollo dipende per lo più dalla sensibilità individuale del management. Più dinamici risultano gli ambiti produttivi più nuovi, in cui i processi non sono ancora strutturati, mentre in quelli consolidati, nonostante gli evidenti benefici (gestione multi-impianto, riduzione dei costi, miglioramento dell'efficienza, sostenibilità ambientale, possibilità di creare nuovi servizi a valore aggiunto), la 'fatica' di ripensare tutti i processi e gestire il cambiamento costituiscono un freno all'innovazione".

Problemi e opportunità

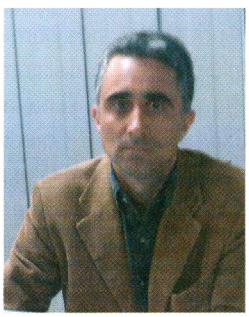
Quali sono le funzionalità più richieste dai clienti e quali le principali criticità da affrontare nella realizzazione di un sistema di telecontrollo e telegestione?

"Le criticità sono solitamente legate alla configurazione hardware dei sistemi, sia per la tipologia di connessione remota offerta (difficoltà a livello di banda, carenza di segnale nelle configurazioni wireless, mancanza di banda larga ecc.), sia per l'architettura locale (condizioni operative estreme, siti non presidiati)" ribadisce **Ceriani**. "Fra le funzionalità richieste, invece, a livello software spicca quella di autogestione". Fare in modo che sia l'impianto, autonomamente, a inviare dai semplici dati alle segnalazioni di malfunzionamento è fra le principali richieste della clientela anche per **Melegazzi**, insieme alla possibilità di monitorare il funzionamento dei sistemi e di modificare/aggiornare da remoto i programmi delle apparecchiature che gestiscono le macchine. "Così" sottolinea **Poli** "si va verso la trasmissione di un sempre più alto numero di dati, il che spinge la ricerca verso nuove tecnologie trasmissive".

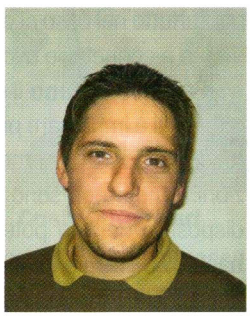
"Dal punto di vista del controllo remoto" prosegue **Ceriani** "è fondamentale consentire agli utenti di accedere al sito sia dalla sede centrale, sia da qualsiasi altro punto via Web. Altra richiesta frequente è la notifica spontanea di eventi significativi, quali allarmi o anomalie, al personale del centro di controllo o a quello reperibile. Inoltre, gli addetti devono essere in grado quanto più possibile di identificare e risolvere i problemi da remoto, senza recarsi in loco. Infine, al sistema di telegestione viene richiesto di tenere una statistica dei dati, sia riferiti alla produzione che ai guasti intervenuti (frequenze, durate, tempi di ripristino)". "Anche noi abbiamo riscontrato la crescente richiesta di accedere a una reportistica raffinata per analisi statistiche e controlli di efficienza" concorda **Masorati**. "A ciò aggiungerei la possibilità di certificare il proprio operato verso i clienti o, per le Pubbliche Amministrazioni, verso i cittadini". **Masorati** conferma poi l'interesse per le segnalazioni di allarmi in relazione a determinati accadimenti. "In tal modo, si possono innescare in maniera automatica o semi-automatica le opportune procedure di gestione dell'evento". Per quanto concerne invece le difficoltà da affrontare nell'implementazione di un sistema di telecontrollo, egli sottolinea come spesso il cliente non abbia una visione chiara né del problema, né delle potenzialità delle tecnologie disponibili. Con lui concorda **Agostinelli**: "L'analisi delle specifiche dell'applicazione e delle esigenze dell'utilizzatore costituiscono uno degli aspetti più critici da affrontare, in quanto ogni applicazione richiede una forte

Vittorio Agostinelli

Alberto Poli



Mauro Galano



Fabio Melegazzi

customizzazione". Il know how acquisito dal fornitore risulta qui determinante, come la sua abilità nel proporre soluzioni innovative, in grado di anticipare i bisogni: "Nell'ambito del nostro progetto di gestione dei silos, i clienti si limitavano a chiedere di poter verificare la quantità di materiale giacente" afferma **Revelli**. "Aver proposto un controllo e soprattutto una gestione da remoto tramite Internet di tutti i silos dislocati sul territorio ha costituito per noi una 'chiave di svolta', sia per la qualità dei servizi offerti, che per l'immediato ritorno economico". Anticipare le esigenze è fondamentale, ma anche garantire alcune funzioni essenziali: "Le funzionalità sono dettate dallo specifico contesto applicativo del sistema, tuttavia alcune peculiarità dovrebbero essere comuni a qualsiasi tipologia di applicazione" ribadisce **Agostinelli**. "Ad esempio, robustezza e affidabilità nelle trasmissioni, con connessioni stabili soprattutto in ambito wireless (in alcuni contesti anche 'always on'); facilità e immediatezza nel recupero delle informazioni; intervenenti rapidi in presenza di anomalie o allarmi; programmazione 'on demand' delle stazioni remote, uso di interfacce semplici e di protocolli standard; indipendenza nella connessione da gestori o server farm esterne". Altro aspetto non trascurabile è la stima dei costi legati alla comunicazione, sia per quanto concerne il traffico generato, sia per la gestione dell'architettura di comunicazione.

"La capacità di utilizzare o riutilizzare i vettori di comunicazione già esistenti e l'apertura verso sistemi wireless (GSM, Gprs, Umts), satellitare e IP based, sono fra le caratteristiche più richieste a un sistema di telecontrollo" ribadisce **Augelli**. "In alcuni casi, si ha la necessità di connettere il centro di controllo alle RTU mediante una connessione ad alta disponibilità, ad esempio usando Internet. Inoltre, nel caso in cui l'ISP (Internet Service Provider), anche solo temporaneamente, non sia disponibile, la RTU deve poter essere raggiunta in modo automatico e trasparente mediante un sistema di comunicazione alternativo. Le criticità sono invece legate all'integrazione di protocolli di comunicazioni diversi, soprattutto nel caso si debba estendere un impianto già esistente o connettere al centro di controllo RTU di vari fornitori". Secondo **Galano** il modo migliore per integrare prodotti differenti è impiegare piattaforme aperte, che utilizzano protocolli standard (Ethernet, Modbus, Profibus ecc.): "Se le stazioni remote non sono raggiungibili con una rete cablata, i dispositivi devono poter utilizzare comunicazioni wireless, basate su TCP/IP. Attraverso modem/router o dispositivi che uniscono le funzioni di router a quelle di Web server, una stazione remota è sempre monitorata dal centro di controllo ed è in grado di storicizzare dati, creare report e inviare messaggi di allarme" conclude **Galano**.

Secondo **Mangialenti** il livello software sta assumendo un ruolo sempre più pregnante: "Qui sono previste funzioni critiche di analisi dei dati (profili di consumo, allarmi, normalizzazione e comparazione dei dati, analisi qualità ecc.) e di accesso diffuso alle informazioni tramite tutte le interfacce disponibili (PC, palmari, Blackberry, cellulari ecc.), con conseguenti criticità".

"Le specifiche funzionali dei sistemi di telecontrollo quasi sempre contemplano il collegamento, la gestione da parte delle periferiche remote di un minimo di memoria storica, per supplire a cadute della comunicazione con il centro di controllo, la gestione della videosorveglianza" afferma **Cubattoli**. "Il problema arriva quando si dispone solo di canali trasmissivi lenti (radio, Gprs, linea commutata o CDA). Da qui l'importanza di scegliere, quando è possibile, il vettore di comunicazione più adatto, nonché le periferiche da usare in rapporto all'applicazione (siti senza rete elettrica o a rischio di esplosione)".

"Interconnessione diretta tra le varie stazioni remote senza passare da un centro di controllo, diagnostica e manutenzione predittiva, interfacce user-friendly, scalabilità e integrazione dei sistemi: sono queste le maggiori richieste dei clienti, insieme alla possibilità di trasferire i dati mediante diversi canali di comunicazione in funzione dalla copertura della rete da parte di operatori diversi" afferma **Randieri**. "Collegato a questo nascono alcune criticità, che vanno risolte in loco in funzione della morfologia dell'impianto e della sua dislocazione sul territorio". La scelta della rete di comunicazione costituisce anche per **Randieri** l'elemento più critico: "Il più delle volte la soluzione ottimale impiega un mix di tecnologie che, a fronte di un servizio affidabile, implicano costi accettabili".

Protocolli emergenti

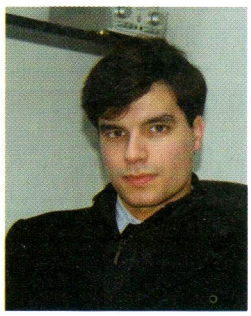
Quali sono i protocolli trasmissivi più adatti e le tecnologie emergenti più valide?

"Non esistono protocolli di trasmissione più adatti di altri in assoluto, in quanto tutto dipende dal tipo e dall'ambito in cui deve agire l'applicazione" afferma **Revelli**. Il punto di partenza è dunque il progetto da realizzare; poi, può accadere che si utilizzino più protocolli di trasmissione per ottenere il miglior risultato possibile in base alla quantità e tipologia dei dati da inviare: "Trasmettere dei fotogrammi non è la stessa cosa che trasmettere una misura di livello o lo stato di una valvola" sottolinea **Randieri**. Secondo quest'ultimo, la migliore scelta è adottare uno standard ampio e diffuso, tipo TCP/IP, con accesso a Internet, poiché "lascia maggiori gradi di libertà e si integra con i più diffusi standard trasmissivi". Sulla stessa linea è **Augelli**: "L'apertura a standard internazionali quali IEC 61850/DNP3 è un 'must'". Interviene quindi **Galano**: "Nello specifico, DNP3 (Distributed Network Protocol) è utilizzato soprattutto in ambito elettrico e di gestione delle acque. Affidabile e a elevate prestazioni, inizialmente mancava dei necessari parametri di sicurezza, lacuna alla quale si è ovviato nel corso degli anni. Nel frattempo però si sono fatti strada IEC 60870-5-101 (seriale) e 60870-5-104 (Ethernet), oggi molto diffusi" specifica **Galano**. "La varian-

te 104, in particolare, è un'estensione della precedente (101) e utilizza un'interfaccia TCP/IP per permettere la connettività a LAN e router". "I protocolli standard permettono di realizzare, in tempi brevi, sistemi aperti, facilmente espandibili e interfacciabili con molteplici apparecchiature" conferma **Agostinelli**. "In caso di applicazioni con esigenze 'spinte', ad esempio quelle per le public utility, adottare IEC 60870 è irrinunciabile, anche se occorrerebbe saper proporre anche protocolli proprietari, per 'ritagliare' la soluzione su misura delle esigenze del cliente". Dello stesso parere è **Poli**: "In futuro, senz'altro, più protocolli, vecchi e nuovi, dedicati al telecontrollo avranno una posizione rilevante sul mercato, come i citati IEC 60870 e 61850, i protocolli proprietari però continueranno a venire usati". "IEC 61850 è ancora in via di affermazione, principalmente nel settore energia" afferma **Ceriani**. "Spesso vengono usati anche protocolli di comunicazione custom, sviluppati da singoli costruttori di RTU, mentre altri protocolli, come Modbus RTU e Modbus TCP, che oltretutto a volte implementano funzioni aggiuntive per il download dei dati da remoto, sono diffusi e utilizzati per la loro semplicità". "L'uso di modem e linee telefoniche analogiche o GSM costituisce la soluzione più facile" suggerisce **Melegazzi**. "Per l'invio/ricezione di semplici comandi o variabili sono validi anche i semplici sms, anche se la necessità di acquisire velocemente un numero sempre maggiore di dati sta spostando le richieste dei clienti verso Ethernet e, quindi, Internet".

"Quando un sistema di telecontrollo/telegestione dispone di una 'presa' RJ45 Ethernet IP, ed è importante che i produttori continuino a muoversi nella direzione di dotare i propri prodotti di questo tipo di connettività, è quasi sempre possibile realizzare il collegamento a un altro sistema di trasmissione dati basato su reti GSM, Gprs, Umts, Adsl, Wifi, Wimax ecc. per centralizzare le informazioni" interviene **Mangialenti**. "Se mai esiste un problema, è legato ai costi". A tale proposito interviene **Cubattoli**: "Non esistono protocolli specifici 'riconosciuti' per il telecontrollo, a eccezione forse di alcune soluzioni proprietarie, che tuttavia si scontrano con le richieste di apertura e interoperabilità del mercato, la soluzione più praticata è 'adattare' al telecontrollo protocolli già esistenti e paradossalmente, quelli 'vecchi', progettati per la trasmissione su linee seriali lente, sembrano essere molto validi". I sistemi di telecontrollo, infatti, lavorano con poche variabili in contesti che non richiedono grandi velocità di trasmissione: "Le apparecchiature necessarie per realizzare un bridge HyperLan affidabile, che a 20 km garantisca vari megabit di larghezza di banda, si acquistano con qualche migliaia di euro" prosegue **Cubattoli**, secondo il quale occorre cercare tecnologie emergenti più a livello di vettori di comunicazione che di protocollo. "Altri sviluppi riguardano l'accessibilità del canale satellitare bidirezionale, alternativa fino a pochi anni fa riservata solo a grandi enti senza troppi problemi di budget. Interessante anche l'utilizzo di gateway intelligenti per adattare periferiche tradizionali (PLC, RTU, controllori Hvac, inverter) in apparati telecontrollabili via Gprs" egli conclude. "Automazione deve sempre essere sinonimo di robustezza e affidabilità" ribadisce **Agostinelli**. "Per cui le eventuali tecnologie emergenti devono essere tecnicamente ben consolidate e collaudate". Su questo prosegue **Masorati**: "Elevata immunità agli errori e un buon grado di riservatezza dei contenuti cosiddetti 'sensibili' sono senz'altro caratteristiche fondamentali nello scambio dati". Occorre poi tenere conto delle specifiche caratteristiche delle informazioni da veicolare. "Il protocollo varia in funzione del tipo di dato" prosegue **Masorati**, che esemplifica: "TPC, ad esempio, usato a livello di trasporto, è adatto per moli considerevoli di dati da scambiare, se non si deve però indagare sulla qualità di ciò che si riceve. Perciò è ideale per trattare dati storici, dove a livello applicativo ci si può affidare a FTP, che garantisce un trasporto robusto.

Per l'invio dello status puntuale del dispositivo, invece, in presenza di quantitativi di dati modesti ma con la richiesta di invii frequenti e immediati, è meglio usare UDP in combinazione con un layer applicativo custom, dotato di caratteristiche quali gestione dell'acknoledge dei dati ricevuti e retry dei dati mancanti, con possibilità d'invio di comandi".


Filippo Cubattoli


Antonio Augelli


Marco Ceriani

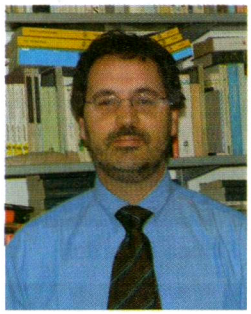

Cristian Randieri

Proteggersi dall'esterno

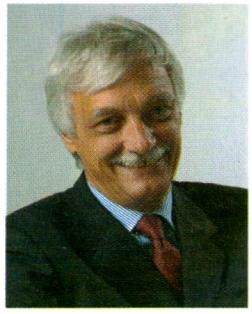
Quali problematiche di sicurezza comporta l'uso di reti Ethernet con accesso a Internet e come si possono efficacemente proteggere i dati e gli accessi?

È forse scontato dire che qualunque transazione di dati, indipendentemente dal mezzo che utilizza, deve essere adeguatamente protetta. "Le connessioni Internet aprono un canale di comunicazione nella rete del cliente verso il mondo esterno; per questo motivo, garantire la sicurezza delle informazioni è molto importante" conferma **Melegazzi**. "Router, firewall e affini fanno da gateway tra il PC remoto

dedicato al telecontrollo e l'apparecchiatura connessa alla rete del cliente, re-indirizzando su un unico indirizzo IP e su un'unica porta la comunicazione tra i due. Le VPN (Virtual Private Network), invece, che stanno prendendo sempre più piede, consentono di creare un canale virtuale protetto tra PC remoto e apparecchiatura da controllare". "Detto ciò" interviene **Revelli** "le strategie di difesa e di protezione devono essere 'congrue' all'importanza e riservatezza dei dati stessi". Ancora una volta, dunque, occorre decidere quali mezzi usare o in quale modo in base all'applicazione. "Per prima cosa, il dato trasmesso deve essere correttamente ricevuto, per cui è essenziale attuare opportune strategie di controllo" prosegue **Revelli**. "Per proteggere gli accessi, di norma, sono sufficienti le impostazioni di sicurezza che si utilizzano per qualsiasi rete (firewall, antivirus, password ecc.); per la protezione dei dati, invece, più sono riservati, più dovrò applicare dei protocolli di sicurezza (criptazione, algoritmi di controllo ecc.,) anche a rischio di compromettere in parte le prestazioni del sistema".



Ivan Mangialenti



Kike Revelli

Fabio Masorati

Dello stesso parere è **Randieri**: "Pensare di proteggere il canale trasmissivo con una VPN crittografata per inviare dati sullo stato di apertura o chiusura di una valvola in un impianto sarebbe eccessivo, mentre diverrebbe ragionevole per l'invio di misure termiche effettuate su centrali nucleari".

"L'accesso ai dati da remoto e la loro pubblicazione sul Web, soprattutto se riferiti a siti che sono 'obiettivi sensibili' per la salute pubblica (produzione energia, acquedotti ecc.) implicano spesso problemi di sicurezza" sottolinea **Ceriani**. "È perciò indispensabile implementare sistemi che offrano elevati requisiti di protezione, usando VPN, quando possibile, firewall opportunamente configurati, sistemi di autenticazione degli utenti e trasmissioni criptate, possibilmente su tecnologie Java e Soap". Le VPN, oltre a richiedere l'autenticazione dell'utente, provvedono a crittografare/cifrare il traffico dati in transito; combinate all'installazione di un firewall fra il PC locale e la rete Internet, per evitare accessi indesiderati, costituiscono le soluzioni di sicurezza migliori e più diffuse anche per **Galano**.

"L'utilizzo del canale wireless per l'invio dei dati risolve in parte il problema della sicurezza, in quanto i dati sono criptati dal canale radio" sottolinea invece **Masorati**. "Se però i due nodi della comunicazione sono distanti, non è possibile affidarsi solo al wireless, perciò nel tratto wired i dati devono essere protetti nel layer applicativo. Per quanto riguarda la consultazione via browser, invece, l'accesso deve essere consentito solo a chi è dotato di opportune credenziali (username e password)".

"Alcuni protocolli, specialmente quelli orientati al telecontrollo come IEC 60870, dispongono già di soluzioni per l'identificazione del nodo in comunicazione, il che garantisce una certa sicurezza" afferma **Agostinelli**. "Certo, l'uso di una VPN e di password specifiche offrono un ulteriore livello di protezione".

"Data la diffusione di diverse modalità di accesso ai dati, penso che il problema della sicurezza si stia spostando sempre più verso il livello software, dove trovano spazio procedure e strumenti tipici del mondo IT" afferma **Mangialenti**. "Del resto, i livelli di trasporto realizzano unicamente il tunneling delle informazioni in arrivo dai sistemi di telecontrollo/telegestione, per cui sono questi ultimi a dover essere già intrinsecamente sicuri". Dello stesso parere è **Cubattoli**: "Gli accorgimenti adottati nel mondo sistemistico, quali VPN, chiavi di cifratura e sistemi di autenticazione, si adattano anche al telecontrollo. Dove invece è necessario intervenire è nella comunicazione fra periferia e centro". Le periferiche remote infatti non hanno grandi possibilità native di protezione. "Nel caso di siti remoti connessi in xDSL si può pensare a una connessione trasparente su VPN" chiarisce Cubattoli. "Con Gprs, invece, la cosa si complica, in quanto l'overhead introdotto dalla connessione VPN è spesso intollerabile. Le alternative possono essere dalle più semplici regole di firewalling, fino a soluzioni più costose, come la richiesta al gestore di telefonia della configurazione di un APN privato". Conclude **Augelli**, sottolineando il concetto di 'zona sicura': "Dal punto di vista topologico, le architetture di rete possono essere strutturate in sottoreti chiuse, definite zone sicure, in grado di connettersi a infrastrutture più ampie mediante un 'entry point' (firewall o router VPN), che garantisce la sicurezza della zona. All'interno di quest'ultima è valido il concetto di fiducia ('trust concept'): tutti i dispositivi appartenenti alla zona possono comunicare senza restrizioni fra loro. La fiducia può estendersi da una zona all'altra solo se l'entry point viene opportunamente configurato, allargando il concetto di zona sicura". ■

readerservice@fieramilanoeditore.it

Ge.Co.S. n. 28 - Intellisystem Technologies n. 29
Movactive n. 30 - Panasonic Electric Works Italia n. 31
PcVue n. 32 - Progea n. 33 - Rockwell Automation n. 34
Schneider Electric n. 35 - Siemens n. 36 - Telestar n. 37
Wago Elettronica n. 38