

Dalla teoria... alla pratica

Si prende qui in considerazione l'implementazione pratica della tecnologia Web nell'ambiente tipico dell'automazione

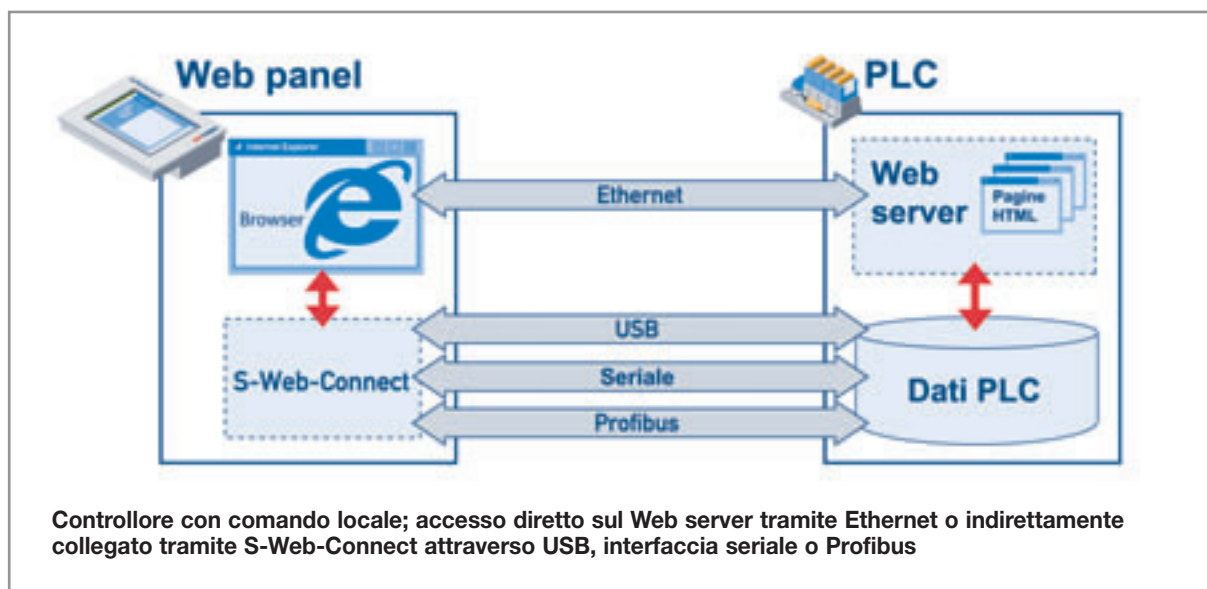
PETER STEIB

Per quanto concerne l'effettiva implementazione delle tecnologie Web in un progetto d'automazione, nella pratica quotidiana occorre confrontarsi con le condizioni reali e con l'insidia dei 'dettagli'. A questo scopo, avere delle conoscenze di base di informatica non costituisce di per sé una condizione necessaria, ma rappresenta un indubbio vantaggio.

La scelta delle apparecchiature

Chi utilizza le tecnologie Web nella tecnica di automazione lavora con PC, pannelli di comando, controllori e componenti infrastrutturali informatiche. Il confine tra PC e

pannello di comando è quanto mai aleatorio: i pannelli di comando di fascia alta si basano spesso su tecniche PC e da questo punto di vista sono considerati dei veri e propri PC. Se si intende con il termine 'PC' esclusivamente il PC da ufficio e quello portatile, escludendo i PC industriali, i panel PC o apparecchiature simili, si può dire che i PC siano normalmente già predisposti all'utilizzo delle tecnologie Web. Il sistema operativo standard e il Web browser sono già installati; anche l'interfaccia LAN, oggi, fa parte della configurazione standard. Se si desidera visualizzare oggetti Java, occorre installare una JVM (Java Virtual Machine), la più diffusa delle quali si può scaricare gratuitamente dal sito dello sviluppatore Java Sun



Microsystems (www.java.com). L'attuale versione 6 offre come novità una funzione 'cache' per la memorizzazione transitoria di file Internet temporanei. In caso di visualizzazione Web con ripetute interrogazioni sui dati, questo potrebbe causare il mancato aggiornamento dei dati di controllo, per cui si consiglia di disattivare questa funzione. In genere, è richiesta la possibilità di eseguire comandi direttamente sulla macchina o sull'impianto, per questo vengono utilizzati pannelli di comando adattati all'impiego diretto sul campo.

Ai fini della tecnologia Web i pannelli di comando non sono altro che dei 'thin client', quindi un 'display' hardware con funzione browser incorporata. A seconda delle esigenze e del caso applicativo sono necessarie diverse esecuzioni; Saia-Burgess Controls offre tre tipi di 'Web panel': pannelli Micro-Browser, pannelli basati su Windows CE e pannelli di comando con Windows XP embedded. La prima tipologia copre il segmento di fascia bassa, più sensibile ai costi. Quando serve unicamente una visualizzazione Web è possibile realizzare, con un pannello Micro-Browser, un comando locale 'Web-based', il tutto al costo di un pannello di comando basato sulla tradizionale tecnica HMI. Oltre ai vantaggi tipici della tecnica Web, i pannelli Micro-Browser offrono un'interfaccia Ethernet, per cui possono essere facilmente collegati in rete. Inoltre, dispongono di un browser in grado di visualizzare pagine Web, non necessitano di una Java Virtual Machine e lavorano risparmiando risorse.

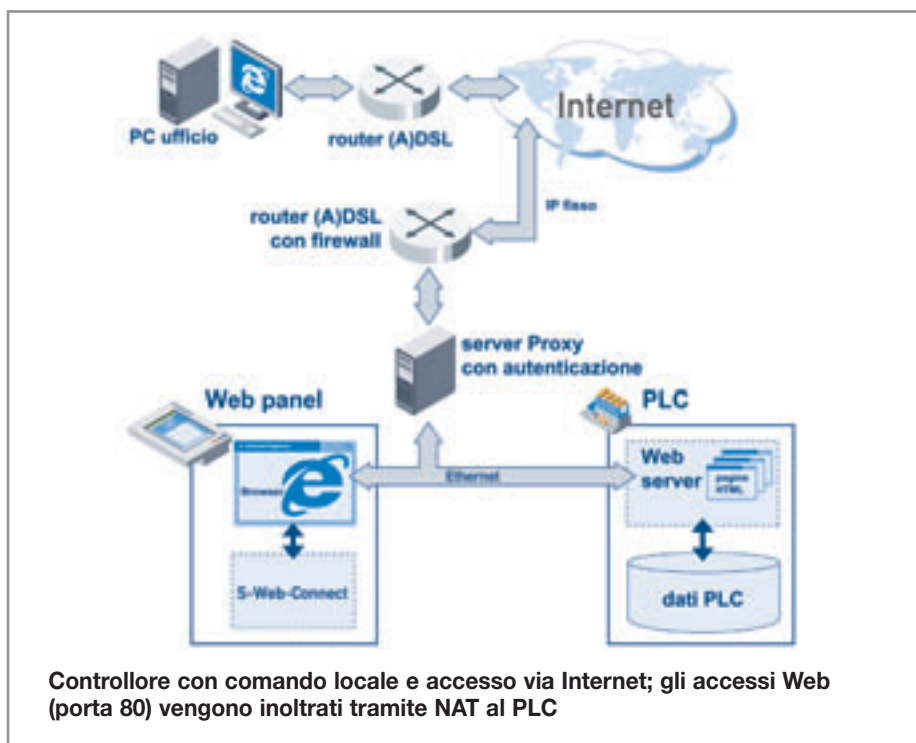
Se le funzioni richieste vanno al di là della semplice visualizzazione Web, per cui si desidera inglobare delle pagine di Web server pubblici, tipo pagine di supporto, oppure applicazioni .NET, entrano in gioco i Web panel Windows CE. In linea di massima, tutti i display basati su Windows CE sono adatti a essere utilizzati come pannelli di comando. Chi, però, crede di poter utilizzare un pannello facilmente reperibile in commercio, si troverà ben presto a dover affrontare elevati costi d'integrazione. Di norma, su un display Windows CE non è installata una Java Virtual Machine, per cui quando si tratta di collegare Java con Windows CE occorre prestare la massima attenzione. In particolare, per gli apparecchi basati su Windows CE, come 'smart-phone' e palmari PDA, vengono proposte delle JVM ridotte, che non offrono funzionalità

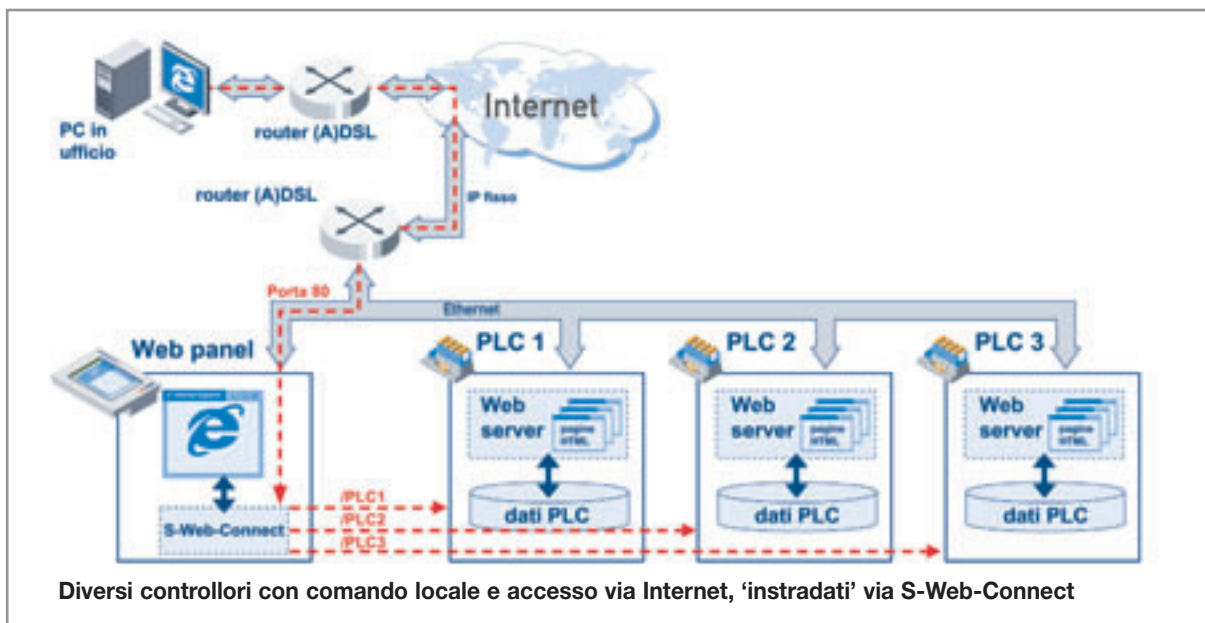
Java complete e non sono adatte alla visualizzazione Web. Inoltre, rispetto ai PC, negli apparecchi basati su Windows CE sono installati processori meno potenti e memorie più piccole. Occorre considerare tutto questo attentamente all'atto della scelta di una JVM: i Web panel basati su Windows CE di Saia-Burgess Controls sono dotati di JVM completa e sono ottimizzati per il sistema Windows CE. Le JVM di norma vengono caricate sotto forma di 'plug-in' all'interno di un browser, ma l'integrazione nel browser, con l'aggiunta della sicurezza relativa, rallenta la visualizzazione. Ecco perché la JVM di Saia può essere avviata come applicazione autonoma sul Web panel Windows CE, anche indipendentemente dal browser, il che comporta un notevole vantaggio in termini di velocità.

Per coloro che hanno esigenze precise in termini di reazione ai comandi, i Web panel Windows CE di Saia-Burgess Controls contengono un 'viewer' per le visualizzazioni Web. Infine, oltre a fornire i vantaggi di un sistema operativo Windows CE, questi Web panel possono essere inseriti in infrastrutture informatiche già esistenti e si possono adattare facilmente agli accessi Internet via 'proxy-server' e autenticazione.

I Web panel più efficienti sono rappresentati dalla classe eXP. Si basano su Windows XP embedded e non si differenziano in termini di funzionamento dai PC; vengono utilizzati dove le esigenze per quanto riguarda l'efficienza del processore e la memoria sono particolarmente severe, oppure quando si devono utilizzare soluzioni software non disponibili per Windows CE.

La condizione di base per l'utilizzo delle tecnologie Web nell'automazione è la disponibilità di controllori con Web server integrato: tutti i controllori (PLC) di Saia-Burgess





Controls sono dotati di Web server e offrono possibilità d'inserimento dati PLC mediante speciali 'tag' sulle pagine Html, oltre a un'interfaccia CGI, con la quale anche applicazioni Java e .NET possono accedere facilmente ai dati PLC.

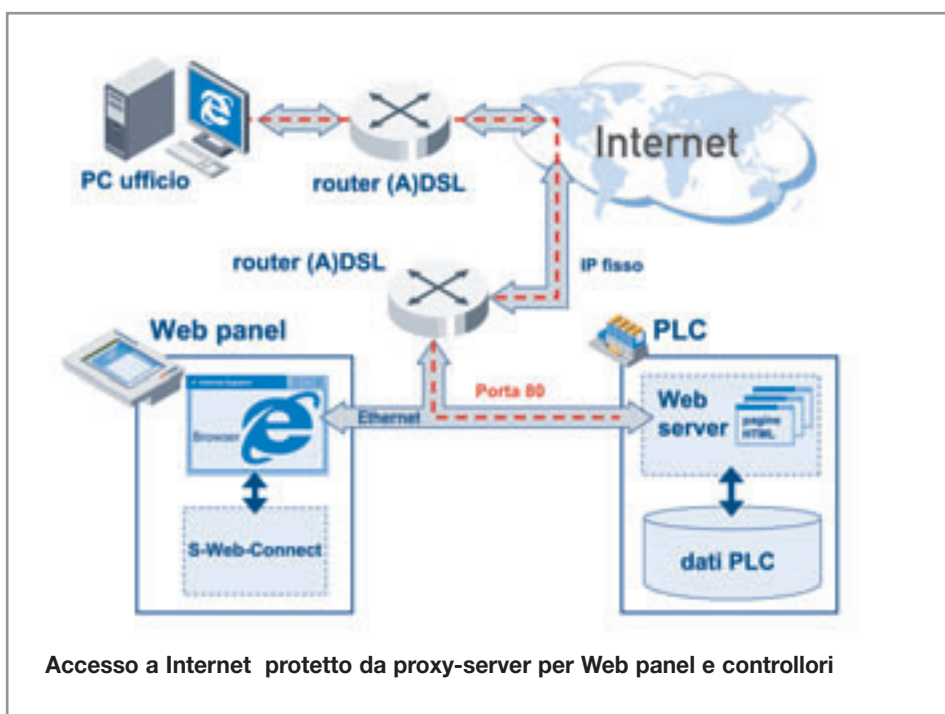
Topologie standard

La topologia più semplice prevede la presenza di un controllore con utilizzo locale; il pannello di comando è collegato direttamente al PLC. Generalmente, un collegamento attraverso Ethernet TCP/IP è preferibile a tutte le altre interfacce, in quanto assicura la massima flessibilità e la possibilità di ulteriori ampliamenti; inoltre, il collegamento temporaneo di un 'Notebook', ad esempio

durante la messa in servizio, diventa un'operazione estremamente semplice. Se non è disponibile un collegamento Ethernet, i controllori Saia possono comunicare con un Web panel tramite interfaccia seriale, USB o Profibus.

La comunicazione avviene tramite browser standard sull'interfaccia LAN, per cui in caso di utilizzo di un'altra interfaccia, gli accessi browser devono essere commutati di conseguenza. A questo scopo si può utilizzare il server di comunicazione S-Web-Connect di Saia-Burgess Controls, che svolge i compiti di un browser inoltrando i dati all'interfaccia desiderata, alla quale è connesso il controllore. Nei Web panel Saia basati su Windows, il tool S-Web-Connect è già incluso, mentre nei PC deve essere installato successivamente. Se, in un secondo momento,

l'interfaccia utente deve essere richiamabile tramite Internet, occorre inserire una connessione LAN, alla quale dovranno essere collegati sia il controllore, sia il pannello. Un router DSL comunemente reperibile può stabilire la connessione a Internet attraverso un comune 'provider'. Di solito, i provider stabiliscono connessioni Internet con un IP dinamico; ciò significa che l'IP del router WAN (Internet) si può modificare. Questo non crea problemi per le connessioni Internet



uscanti, ad esempio quando dal pannello di comando viene aperta una pagina Web. Se invece si desidera accedere al controllore dall'esterno, è indispensabile conoscere l'IP del router. Gli Internet provider offrono perciò a pagamento degli accessi internet con IP fisso, attraverso i quali il router è raggiungibile in qualsiasi momento. La rete interna composta da pannello, unità di comando e router utilizza altri IP rispetto alla connessione DSL del provider. È compito del router fare da intermediario tra i due spazi di indirizzamento IP.

Se, a questo punto, dall'esterno viene effettuato un accesso all'IP fisso del router, quest'ultimo deve sapere a quale partecipante della LAN deve inoltrare l'accesso (pannello o controllore). Nel router questo si può eseguire con l'aiuto della funzione NAT (Network Address Translation). A questo scopo, si può configurare nel router il partecipante al quale devono essere inoltrati gli accessi provenienti dall'esterno. In tale contesto, le porte giocano un ruolo centrale, in quanto costituiscono un tipo di 'sottoindirizzo', in aggiunta all'IP. In altri termini, un IP può essere ampliato con l'indicazione della porta. In questo modo, il router potrà disporre di un criterio di distinzione, quando deve servire nella sua LAN interna più di un partecipante.

La configurazione del NAT avviene tramite una tabella, nella quale si stabilisce l'associazione tra porte e partecipante LAN. I browser comunicano con protocollo http, al quale viene normalmente attribuita la porta 80. Nella tabella NAT si dovrà quindi impostare per la porta 80 l'IP del controllore.

La cosa diventa più difficile quando si vuole accedere a più controllori dall'esterno. Una via percorribile è quella di attribuire diverse porte a ogni singolo controllore, quindi la porta 80 per PLC1, la porta 81 per PLC2 ecc. Tuttavia, per gli accessi browser si sconsiglia di utilizzare sempre la porta 80. In molte aziende, l'accesso Internet di solito è protetto in modo rigido e solo le porte assolutamente indispensa-

bili (tra queste la porta 80) vengono attivate, mentre le altre vengono bloccate tramite 'firewall'.

Se si desidera accedere a più controllori, il tool S-Web-Connect offre una valida soluzione. Gli accessi ai controllori nella NAT vengono deviati sul pannello anziché sui controllori e S-Web-Connect, installato al livello superiore, provvede a inoltrare gli accessi ai singoli controllori in base all'indicazione del percorso indicato nell'URL degli stessi.

Componenti per l'interfaccia operatore



- Web panel con tecnologia Micro-Browser capaci di economizzare risorse per la visualizzazione di pagine Web



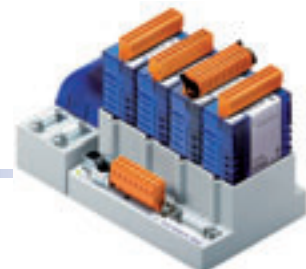
- Web panel basati su Windows CE con Java Virtual Machine completa di viewer per visualizzazioni Web veloci e server di comunicazione S-Web-Connect



- Web panel con Windows XP embedded e Sun Java Virtual Machine con server di comunicazione S-Web-Connect



- PLC con interfaccia operatore con Web server integrato, interfaccia Ethernet e USB, programmabile con Saia PG5 o Step7 Siemens



- Router adatti al settore industriale, dotati di connessioni protette con proxy-server, codifica SSL, VPN e interfaccia Wlan



CCTV LCD



Una famiglia di pannelli LCD state-of-the-art progettata e sviluppata per le applicazioni di videosorveglianza. La qualità superiore dell'immagine viene garantita dalle funzioni De-Interlace e 3D Comb Filter mentre l'accoppiamento con i DVR presenti sul mercato è assicurato dalla completezza degli ingressi. Include PIP/POP personalizzabile.

- SIZE DA 15" A 20,1" RISOL. SXGA 1280X1024
- CONNESSIONI VGA, DVI, SV, AV (BNC), YPBPR
- 3D COMB FILTER: NTSC/PAL; DE-INTERLACE
- RESPONSE TIME 5-12 MS
- FREQ. 38K-80KHZ (ANAL.) 56HZ-75HZ (DIG.)
- LUMINOSITÀ 300-450 CD/M²; CONTRASTO 500:1
- VITA LAMPADE 50.000 H
- ALTOPARLANTI INTERGRATI
- TOUCH SCREEN, VETRO TEMPRATO 3 MM E LOCAL LOOP OPZIONALI

GSM/GPRS

Modem GSM/GPRS perfetti per telecontrollo, teleassistenza, distributori automatici, telelettura, monitoraggio ambientale, localizzazione veicolare e M2M in genere. Nella versione Plus, grazie al microprocessore ARM integrato, è possibile sviluppare un software di gestione della comunicazione via modem in modo che non sia richiesto il controllo da parte dell'apparato tele controllato o per inviare dati già processati, riducendo i costi di comunicazione.



- GSM, GPRS, EDGE 2BAND E 4BAND
- TRASMISSIONE DATI, SMS, FAX, FONIA
- TCP/IP, HTTP / FTP / E-MAIL / TELNET
- VELOCITÀ DATI GSM 9600 BPS GPRS 85,6 KBPS
- INTERFACCIA DB9 RS232
- SUPPORTI PER MONTAGGI SU GUIDE DIN E OMEGA O A MURO
- ALIMENTAZIONE 8V-32V, RANGE TEMPERATURA -20°C/55°C
- VERSIONE CON MORSETTIERA I/O PER 2 INPUT E 2 OUTPUT ESPANDIBILE FINO A 21 SEGNALI
- VERSIONE PLUS CON ARM 7 INTEGRATO (AUTO-CHECK, AUTO-RESET E DOWNLOAD FIRMWARE DA REMOTO, SDK E LIBRERIE API)

AO

automazioneoggi tecnologia web

Questioni di sicurezza

Quando si tratta di tecnologia Web, prima o poi sorgono domande riguardanti il tema della sicurezza: l'intero mercato vive nel timore di attacchi causati da 'hacker' o virus.

Effettivamente, un sistema operativo è il luogo peggiore per costruire una protezione efficace. Da un lato, questo è dovuto alla complessità dei sistemi operativi di oggi, dall'altro il pensiero di una protezione efficace non convince, quando l'intruso ha già raggiunto il calcolatore. Ecco perché negli ambienti professionali il tema della sicurezza viene trattato in modo separato dalla singola postazione di lavoro, ossia dal singolo PC. A questo proposito, esistono componenti dedicati, che svolgono la funzione di protezione 'stand-alone', come i firewall hardware. Per lo più i router (A)dsl comprendono già un firewall, che è in ogni caso da preferire per quanto riguarda l'efficacia a un firewall software installato su PC. Trasferendo questo concetto alla tecnica di automazione, non è consigliabile implementare la sicurezza solo nel controllore. È importante piuttosto che l'ambiente nel quale vengono utilizzati i controllori e i Web panel sia organizzato in modo sicuro. Generalmente, si considerano due ambiti tematici della sicurezza nelle applicazioni IT: l'intrusione nel sistema di calcolatori e reti ('hacking') e i virus. Questi ultimi vengono creati per le piattaforme hardware più ampie possibili, che fanno uso di sistemi operativi standard, tipicamente per i PC Windows. Un controllore è costruito di regola con microcontrollori o processori ottimizzati ed è dotato di sistema operativo proprietario. Questo li rende immuni a tutti i virus prodotti per PC e Windows. La diffusione limitata dei controllori rispetto ai PC rende inoltre molto improbabile la diffusione di virus sui sistemi di controllo. In teoria, i pannelli di comando basati su Windows sono più vulnerabili. Gli sviluppatori di virus vogliono di solito ottenere il massimo effetto possibile e puntano perciò ai sistemi operativi desktop Windows 2000/XP/Vista. Windows CE è già molto meno attraente. Inoltre, occorre considerare che i virus principalmente vengono introdotti e attivati dall'utente. Ciò può accadere anche per un 'clic' di troppo durante la navigazione in Internet, oppure con l'installazione di un programma infettato. I pannelli di comando in applicazioni industriali sono per lo più chiusi, cioè l'interfaccia utente viene automaticamente lanciata durante il 'boot' e l'utente non ha la possibilità di attivare delle pagine Web critiche o di installare dei programmi software. Chi, in particolare per quanto riguarda il pannello basato su Windows eXP, vuole andare sul sicuro, può comunque installare un programma antivirus. In tal caso, dovrebbe scegliere un programma che si aggiorni automaticamente con le ultime 'virus signature' e che svolga i propri servizi in modo discreto in 'background', senza fastidiose finestre 'pop-up' e interazioni obbligate da parte dell'utente. Da questo punto di vista, purtroppo, la maggior parte dei programmi antivirus in commercio risulta carente. La protezione può essere comunque incrementata.



SPECIAL-IND S.P.A.
PIAZZA SPOTORNO, 3 • 20159 MILANO
TEL. +39 02 6074741
FAX +39 02 66800493
readerservice.it n.20454

WWW.SPECIALIND.IT

ta anche in altri modi, come dimostra l'azienda Eset con il suo prodotto Nod32. Quest'ultimo può essere eseguito senza interazione con l'utilizzatore in una modalità 'silenziosa' e invia addirittura delle e-mail quando rileva un'infezione. Nelle applicazioni industriali, però, più che al pericolo dei virus si dovrebbe pensare al problema 'hacking'. In particolare, per quanto riguarda le visualizzazioni Web, nelle quali l'intera interfaccia utente è disponibile 'a domicilio', è necessario un solido controllo degli accessi. Questo si può ottenere tramite un 'proxy server' installato a monte, con funzione di autenticazione. Le richieste inoltrate via Internet vengono in prima analisi dirottate al proxy server. Prima che questo inoltri la richiesta al relativo controllore, l'utente si deve registrare con il proprio nome e la password (autenticazione). In questo modo, si garantisce che solo un determinato gruppo di persone possa avere libero accesso. Per chi desidera anche proteggersi contro le intercettazioni ('sniffer'), il proxy server può eseguire una codifica SSL del traffico di dati. Così si raggiunge lo stesso livello di sicurezza adottato per i 'Web-shop' e l' 'on-line banking'. Un ulteriore metodo per il controllo degli accessi è rappresentato dalle VPN (Virtual Private Network). In questo caso, i dati privati vengono trasmessi tramite Internet in un cosiddetto 'tunnel'. La trasmissione può essere codificata; attraverso un tunnel VPN l'utilizzatore può accedere ai calcolatori

attraverso Internet, come se questi fossero inseriti in una LAN. Per l'accesso a una VPN deve essere installato sul PC un software client utilizzato per stabilire la connessione. Per accedere alle tecniche di sicurezza sopra indicate non è indispensabile impiegare un PC-server particolarmente potente. Sul mercato sono disponibili apparecchi compatti concepiti per l'utilizzo all'interno di un armadio; ad esempio, la ditta Eurogard fornisce un 'service-router' economico, che offre un proxy server con codifica SSL e VPN, compatibile con i controllori PCD di Saia-Burgess Controls.

Il futuro è già iniziato

Negli ultimi anni la tecnologia della comunicazione ha subito drastiche evoluzioni: i telefoni cellulari appartengono ormai alla quotidianità, l'accesso Internet e le tecnologie di rete non sono più il privilegio di una piccola 'élite' di tecnici. Tutto ciò è stato reso possibile anche attraverso l'utilizzo della tecnologia Web. Il lato affascinante di queste nuove tecnologie è la loro totale apertura, che al tempo stesso è garante di sviluppo continuo e di competitività futura. Conoscere questo nuovo mondo è condizione imprescindibile per motivarvi a 'saltare sul treno' del Web. ■

Saia-Burgess Controls readerservice.it n. 99

Jam PAC'd.

Doppia interfaccia Ethernet per connessioni ridondate e segmentazione della rete di controllo

Switch Auto/Manual per test e collaudi

LED di stato e diagnostica per ogni canale

Fusibile facilmente sostituibile

Alimentazione isolata per loop di corrente e celle di carico

Moduli speciali incluso pH/ORP e monitoraggio di segnali in corrente e tensione

Moduli digitali e analogici a 8, 16 e 32 canali per ottimizzare lo spazio nei quadri



Connettori rimovibili per una facile manutenzione e veloce sostituzione dei segnali di campo

Interfacce seriali RS-232 e RS-485/422 per DH+, Modbus®, Profibus®, RFID, lettori barcode, bilance, motion control e altro ancora

Fino a 96 loop di regolazione PID per singolo rack con input analogici o temperature e output analogici o TPO

Cold-junction con terminali compensati per termocoppie

I controllori da rack R-series dispongono di protocolli industriali Ethernet-based quali EtherNet/IP™, Modbus/TCP e OptoMMP™ oltre ai noti protocolli IT come SMTP, FTP, SNMP e altro ancora. Fino a 512 punti di I/O per il controllo, l'acquisizione dati e il monitoraggio remoto.