VALERIO ALESSANDRONI

LE RETI DI SICUREZZA

Nelle reti industriali quello della sicurezza è oggi uno dei requisiti più sentiti. Ne abbiamo discusso con l'aiuto di alcuni esperti

Mentre, in passato, la sicurezza di comunicazione dei dati era affidata alle caratteristiche del protocollo utilizzato, attualmente si stanno diffondendo reti appositamente concepite per garantire una maggiore sicurezza nel trasporto dell'informazione.
Come funzionano queste reti?
E come sono in grado di garantire sicurezza quando vengono interconnesse con reti generiche?
La seguente 'Tavola rotonda' ci ha permesso di delineare meglio i contorni di un segmento del mercato automation che è considerato unanimemente in forte crescita.

Fattori di crescita

Quali sono le esigenze che hanno portato allo sviluppo e alla diffusione delle reti di sicurezza?

Secondo **Raffaele Esposito** (Phoenix Contact) le esigenze che hanno condotto allo sviluppo di reti di sicurezza sono in pratica identiche a quelle che, in passato, sono state alla base dello sviluppo delle reti tradizionali. "Mi riferisco in particolare agli indubbi vantaggi che l'implementazione di una rete introduce nella gestione di una macchina o di un impianto sufficientemente complessi", egli afferma. "Tra questi, il decentramento in campo di I/O con conseguente risparmio sui costi di cablaggio; la diagnostica puntuale senza aggravi di costo con conseguente maggior facilità ed economicità delle operazioni di manutenzione o di riparazione guasti; infine, la flessibilità del sistema con vantaggi legati in particolar modo all'esecuzione di modifiche o integrazioni future della macchina o dell'impianto, in tempi rapidi e con costi contenuti".

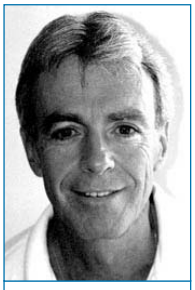
Afferma Raffaele Esposito (Phoenix Contact): "La sicurezza della rete viene gestita e garantita da una molteplicità di fattori, sia relativi al software che all'hardware"

La diffusione odierna delle reti di sicurezza, nettamente minore rispetto a quella delle reti tradizionali, è conseguenza diretta della rigidezza di norme e regolamenti applicabili alla sicurezza del macchinario, che fino a poco tempo fa lasciavano pochissimi margini di manovra circa il possibile uso della logica elettronica per la gestione di funzioni di sicurezza per l'uomo.
L'affinamento delle tecniche di gestione e controllo di tipo elettronico accompagnato da un'evoluzione normativa sull'argomento hanno consentito, nel tempo, a organismi di certificazione riconosciuti competenti a livello internazionale (tra gli altri BG e TÜV) di poter attestare la rispondenza di sistemi basati sulla logica elettronica alle esigenze di sicurezza definite in diverse direttive comunitarie. L'ostacolo maggiore per la diffusione di questa tecnologia viene così ad essere superato.
Afferma **Giacomo Volpe** (Pepperl+Fuchs): "A seguito della massiccia introduzione e dell'ormai consolidato utilizzo delle reti nella gestione dei segnali dal campo, la gestione di una rete di sicurezza differente da quella per la gestione degli I/O tradizionali veniva vista più come un onere che come una necessità. Il bisogno di poter gestire la sicurezza con la stessa filosofia dei dati standard, o addirittura di unificare su un'unica rete la trasmissione dei segnali di sicurezza e di quelli standard, come accade con il sistema AS-i, è stata non solo la molla, ma addirittura la chiave di volta del successo delle attuali reti di sicurezza".

Secondo Giacomo Volpe (Pepperl+Fuchs) nello sviluppo di reti sicure è doveroso partire dall'esperienza già acquisita, facendo tesoro di quanto imparato in precedenza

Secondo **Giancarlo Quintana** (Pilz) l'esigenza principale alla base delle reti di sicurezza è stata quella di portare il livello tecnologico utilizzato per gestire la sicurezza alla pari di quello dell'automazione. "Con l'introduzione delle normative di sicurezza (fine anni '80), a bordo impianto si è assistito a un ritorno della logica elettromeccanica cablata di sicurezza che affiancava l'ormai definitiva soluzione d'automazione standard basata su PLC. Con l'evoluzione della tecnologia,

seguita dalla normazione, già dal 1995 l'avvento dell'elettronica sicura apriva la strada a soluzioni di sicurezza di seconda generazione".
Il PLC di sicurezza, così come già visto vent'anni prima per il primo PLC, permetteva di trasformare la rigidità della logica di sicurezza in flessibilità applicativa grazie al software. Infine, nel 1999 si è assistito al naturale ulteriore passo tecnologico, quello della decentralizzazione su bus di sicurezza. Tra i motivi di questa sempre maggiore diffusione vi è la consapevolezza da parte del cliente/utente di considerare la sicurezza non più come semplice appendice dell'automazione, ma come parte integrante di essa e, quindi, dotata delle medesime caratteristiche funzionali. Inoltre, è pesata la sempre maggiore complessità degli impianti, correlata anche a una più ampia capacità di trasformazione e adattamento, in tempo reale, degli impianti ai processi produttivi. A ciò si aggiunga, infine, la tecnologia, che porta a sistemi sempre più performanti, in grado di gestire tutte le procedure di autotest richieste e di rispondere in modo sempre più completo alle necessità di tempi di reazione veloci di sicurezza e di diagnostica.



Secondo Richard Timoney (Fieldbus Foundation) le reti di sicurezza e quelle tradizionali possono trovare posto in una stessa applicazione

Secondo **Richard Timoney** (Fieldbus Foundation) Foundation Fieldbus è costantemente in ascolto dei propri utenti finali, che ne sostengono l'attività. "Lo scorso anno, l'End User Advisory Council ha raccomandato al nostro comitato direttivo di considerare lo sviluppo di una specifica applicabile ai sistemi a sicurezza critica. Tale Comitato ha quindi lanciato un progetto e sta lavorando con Hima, un noto fornitore di sistemi a sicurezza critica, per assicurarne l'accettazione da parte degli enti normatori". L'elemento chiave è assicurare il mantenimento dell'integrità della tecnologia esistente, evitando di dare inizio a una tecnologia nuova o radicalmente differente. "Riteniamo di avere una metodologia che ci permetterà di farlo", conclude **Timoney**.
"Lo sviluppo delle reti di sicurezza, avvenuto in questi ultimi anni, risulta essere la naturale evoluzione della tecnologia di sicurezza, proprio come negli anni passati lo è stato per l'automazione; infatti la logica cablata si è sviluppata verso quella programmabile proprio come sta accadendo oggi per la tecnologia di sicurezza", sostiene **Enrico Merati** (Rockwell Automation).
Le esigenze che spingono i maggiori produttori di sistemi di sicurezza verso una soluzione di rete sono le medesime che anni fa avevano portato allo sviluppo di reti nell'ambito dell'automazione non di sicurezza, quali una maggiore flessibilità, riduzione dei cablaggi a favore di una migliore 'pulizia' degli impianti, diagnostica integrata, dimensioni d'ingombro ridotte, alte prestazioni.
"Ad oggi, però, la diffusione delle reti di sicurezza stenta a decollare", prosegue **Merati**, "per via sia dei costi eccessivi, non giustificati dai vantaggi indotti, dettati da una ancora ridotta competizione, sia, principalmente, perché le logiche di sicurezza da realizzare sono in genere molto semplici e non vi è l'esigenza, salvo in particolari applicazioni, di trasmettere i segnali 'sicuri' per una loro condivisione tra le diverse zone dell'impianto. Infatti sono molte le applicazioni in cui è sufficiente gestire la sicurezza localmente, per poi trasferire i segnali diagnostici su una rete tradizionale non necessariamente di sicurezza, con costi decisamente inferiori".

"Al fine di garantire i necessari requisiti di sicurezza è essenziale impedire che le funzioni di sicurezza dipendano da segnali non sicuri", ha dichiarato Enrico Merati (Rockwell Automation)

Secondo **Giovanni Bramati** (Siemens) le esigenze sono le stesse che hanno portato allo sviluppo delle reti fieldbus tradizionali; in un settore particolarmente caratterizzato da forti componenti di certificazioni e normative è comprensibile il ritardo rispetto alle soluzioni tradizionali, dovuto ai tempi necessari per la stesura della nuova normativa macchine.

Evoluzione o rivoluzione?

Una rete di sicurezza può risultare dall'evoluzione di una rete tradizionale, o richiede una progettazione ad hoc da zero?

"Schematizzando in modo estremo, le componenti hardware di una rete sono costituite da un'unità centrale d'elaborazione, da I/O decentrati e da un supporto per il flusso dati tra unità centrale e I/O decentrati", afferma **Esposito**. "Sempre parlando in linea schematica, per passare da una rete tradizionale a una di sicurezza si dovrebbe operare sia a livello di unità centrale, implementando un'unità destinata alla gestione dei segnali di sicurezza, sia a livello di I/O decentrati, creandone di particolari specificatamente dedicati all'interfacciamento diretto con i dispositivi di sicurezza in campo".
Fatto questo, nessuna modifica risulterebbe necessaria sul cavo di rete, che è a tutti gli effetti un semplice supporto destinato al trasporto dei dati da/per l'unità centrale e gli I/O decentrati.
Sul fronte software, infine, si dovrebbe modificare il protocollo di rete per consentire l'elaborazione dei segnali

di sicurezza ai soli componenti hardware deputati a tale scopo.
Ovviamente, sia sul fronte hardware, sia su quello software tutte le misure note per la garanzia della sicurezza e dell'efficacia del funzionamento del sistema devono essere messe in opera.
Tale misure possono essere costituite da, per esempio, ricorso a ridondanza, autocontrollo e diversità per i componenti vitali del sistema e utilizzo di software specifici sviluppati anche secondo parametri e concetti già utilizzati in ambiti ove la sicurezza delle persone riveste importanza assolutamente critica (settori quali l'aeronautico, il petrolchimico, l'industria di processo, ecc.).
E' su questa base che vari costruttori stanno operando per creare la versione 'safety' di reti tradizionali già presenti sul mercato. "In conclusione, non risulta necessario prevedere una progettazione ex novo di una rete di sicurezza, ma questa può derivare da un'elaborazione evolutiva di una rete tradizionale già esistente", conclude **Esposito**.
"A mio avviso, data l'importanza della sicurezza del personale durante l'attività di lavoro è doveroso prendere spunto dall'esperienza acquisita in questo campo, facendo tesoro di quanto imparato fino ad oggi", afferma **Volpe**. "Per questo ritengo che partire da zero sia un errore che qualcuno sta anche già facendo. AS-i Safety at Work, cioè la versione AS-i sviluppata per la sicurezza uomo, è stata proprio generata nel 2000 sfruttando le informazioni ricavate dall'esperienza di rete maturata a partire dal 1994".

A parere di Giancarlo Quintana (Pilz) la capacità di rilevare in modo sicuro gli errori sul campo è qualità fondamentale di un sistema di sicurezza

Afferma **Quintana**: "Normalmente si evita di progettare da zero una rete di sicurezza.
E' opinione generale sia meglio partire da fieldbus esistenti e comprovati sul campo e costruire tutti quei meccanismi necessari per trasformare il bus standard in bus di sicurezza andando ad agire su tutti i livelli del sistema ISO/OSI.
La nostra esperienza, non essendo vincolati ad alcun bus standard, ci ha permesso di selezionare sul mercato quello che abbiamo ritenuto il fieldbus con le caratteristiche migliori per essere adattate alla gestione della sicurezza". Quindi si è agito a livello di Safety Data Management, definendo gli aspetti di funzionalità del bus, ossia se si tratta di un bus che trasmette effettivamente informazioni rilevanti per la sicurezza o solo informazioni di monitor.
Questo è fondamentale per valutare e definire quante e quali misure di sicurezza in fase di trasmissione dei dati il bus deve intrinsecamente avere.
Gli interventi hanno riguardato anche il manager della sicurezza, ossia l'elemento che all'interno della rete legge gli input, elabora le funzioni di sicurezza e ne comanda l'intervento, e il numero delle informazioni di sicurezza che devono essere trasmesse che, per tipologia di bus lineare, determina il carico sul bus e quindi il tempo di reazione della sicurezza (notoriamente occorre reagire con tempistiche bassissime).
Secondo **Merati** il cammino che i principali costruttori stanno percorrendo è proprio quello di portare l'evoluzione di reti tradizionali verso la realizzazione di protocolli sicuri in grado di soddisfare le più rigorose richieste in termini di sicurezza. Ne è un esempio l'accordo tra Rockwell Automation, Omron e Sick per lo sviluppo di un protocollo di sicurezza aperto 'CIP Safety', derivante da un'estensione del 'CIP' (Control and Information Protocol), basato su DeviceNet, ControlNet ed EtherNet/IP. Queste tre aziende come membri di Odva (Open DeviceNet Vendor Association) hanno riconosciuto la necessità di un protocollo di sicurezza 'aperto' e compatibile con le reti già oggi esistenti nell'industria.
"Come già detto, intendiamo mantenere l'integrità della tecnologia esistente", afferma **Timoney**. "Allo stesso tempo, riconosciamo la natura critica dei sistemi di sicurezza e la necessità di rispettare le normative. Stiamo lavorando con alcuni dei migliori tecnici di società leader per sviluppare una metodologia in grado di soddisfare entrambi i criteri e riteniamo di avere trovato un approccio corretto".
"Una rete dedicata anche alla sicurezza deve permettere la trasmissione di dati esenti da errori, al fine di garantire il necessario intervento in caso di guasto", sostiene **Merati**. "A tale proposito è possibile arrivare partendo da una rete tradizionale dopo opportune modifiche al protocollo di comunicazione, così da garantire i livelli di sicurezza richiesti dalle normative, che, è bene precisare, sono ad oggi ancora in corso di sviluppo per i dispositivi a logica programmabile e le reti di sicurezza". Ovviamente una progettazione ad hoc da zero potrebbe portare agli stessi risultati, in termini di sicurezza, ma darebbe luogo a una soluzione dedicata, quindi poco aperta e in contrasto con le esigenze e le richieste del mercato.
Sostiene **Bramati**: "La tecnica di sicurezza (Safety Integrated) è parte integrante di Totally Integrated Automation. Siemens integra infatti la tecnica di sicurezza nell'automazione standard e in modo omogeneo in tutto il sistema". Dove l'automazione standard (classici PLC) e quella di sicurezza (elettromeccanica) sono oggi ancora divise, i due mondi crescono insieme per fondersi in un sistema globale integrato e omogeneo. "Per Siemens la tecnica di sicurezza è parte dell'automazione standard ed è fondamentale mantenere l'omogeneità del sistema".

Internetworking fra reti sicure e non

L'interfacciamento di una rete di sicurezza con una rete tradizionale può portare a una diminuzione delle caratteristiche di sicurezza? In caso affermativo come si può ovviare a questo?

"La risposta è: 'non deve'", interviene **Quintana**.
"Qualsiasi elemento inserito in un contesto di sicurezza va a incidere sull'equilibrio del sistema di sicurezza". Nella classica catena di sicurezza sensore-logic solver-attuatore, un semplice relè d'interfaccia prima dell'attuatore costituisce un elemento di possibile perdita della funzione di sicurezza e, cita la norma, in quanto tale deve essere controllato dalla logica stessa. Così avviene all'interno del logic solver, quanto più complesso esso risulta essere. "Nel nostro caso il logic solver, costituito dal manager, dal bus e dai nodi di sicurezza deve considerare il semplice gateway d'interfacciamento come qualcosa che non rientra nel contesto di sicurezza e come tale non deve interferire con essa", aggiunge **Quintana**. "E' necessario che vi sia il più possibile una barriera tra dati safe e non-safe; le possibili soluzioni tecnologiche vanno dalla diversificazione o separazione dei bus e/o dei master device, all'utilizzo di gateway di sicurezza safe/non-safe. Non sempre semplici algoritmi software o filtri sui telegrammi bus sono sufficienti per mantenere i due mondi completamente separati".
Secondo **Esposito** la commistione di segnali dedicati alla sicurezza e dedicati all'automazione tradizionale può rappresentare un pericolo potenziale che potrebbe condurre alla mancata affidabilità della gestione della sicurezza della macchina o dell'impianto. Risulta quindi fondamentale che segnali generati, elaborati, trasmessi o acquisiti da componenti basati su logica elettronica tradizionale non influenzino quella parte di rete globale che è deputata alla gestione della sicurezza.
"Questo perché la logica tradizionale non offre sufficienti garanzie, soprattutto in caso di guasti", sottolinea **Esposito**. "Svariati sono i sistemi che possono permettere una separazione affidabile tra i due mondi", egli prosegue.
"In linea di principio, comunque, l'elemento cuore per la gestione di questo tipo di problematica è rappresentato dal protocollo di rete".
Ai segnali di sicurezza viene attribuito un protocollo particolare che potrà poi essere riconosciuto e gestito solo dai componenti hardware specificatamente dedicati alla gestione di funzioni di sicurezza a livello sia di unità centrale, sia di periferia (I/O decentrati destinati all'acquisizione o alla distribuzione di segnali di sicurezza).
Ovviamente tali dispositivi hardware specificatamente dedicati alla gestione delle funzioni di sicurezza non terranno conto di tutti i segnali che non presenteranno quella parte di protocollo che li caratterizza come segnali di sicurezza.
Sostiene **Volpe**: "La sicurezza riveste un'importanza nel design della macchina così elevata che va analizzata a fondo prima di essere collaudata e certificata. Solo una rete di sicurezza ben fatta può evitare proprio questa paventata evenienza, mischiando reti con differente grado di sicurezza. Per questo ci vuole chiarezza e reti che hanno un grado di conoscenza più elevato possibile da parte di un qualunque operatore del settore, che poi è quello che si è proposto AS-i Safety at Work con la certificazione europea EN 954-1".
Afferma **Merati**: "Al fine di garantire i necessari requisiti di sicurezza è sempre necessario impedire che funzioni di sicurezza dipendano da segnali non sicuri. Nel caso delle reti di comunicazione, il protocollo deve ovviamente garantire questo comportamento ed è in tale direzione che si tende a implementare un protocollo esistente con requisiti orientati alla sicurezza, anche se il mezzo fisico di trasmissione risulta il medesimo. A dimostrazione di ciò possiamo notare che anche nel caso di reti di sicurezza dedicate il mezzo fisico di trasmissione non è né ridondante né sicuro, ma semplicemente la sicurezza della comunicazione si basa principalmente sulla sicurezza offerta dal protocollo di comunicazione". Secondo **Merati** l'utilizzo di un'unica rete in grado di soddisfare sia i requisiti di sicurezza che le altre funzionalità richieste, non può essere motivo di diminuzione delle caratteristiche di sicurezza, proprio perché non è il mezzo fisico a garantire il comportamento sicuro di una rete di sicurezza. L'accorgimento ulteriore che deve essere preso nel caso di una rete 'estesa alla sicurezza' consiste nel garantire che non vi siano rischi di ricevere o inviare dati corrotti al fine di assicurare una comunicazione esente da errori.
Dichiara **Bramati**: "La soluzione proposta da Siemens ha proprio il vantaggio d'integrare in un unico supporto dati standard e dati sicuri, senza una diminuzione delle caratteristiche. In casi particolari, come le partenze motore fail-safe montate sulle stazioni di periferia decentrate di tipo sicuro, vengono utilizzate delle centraline esterne per aumentare la sicurezza del sistema ai massimi livelli".
Secondo **Timoney** le reti di sicurezza e quelle tradizionali possono essere interfacciate all'interno della stessa applicazione. "Poiché Foundation Fieldbus utilizza un approccio a blocchi funzionali al controllo, pensiamo che il proble-

Giovanni Bramati (Siemens) ha sottolineato come Siemens integri la tecnica di sicurezza nell'automazione standard, creando sistemi omogenei

ma possa essere risolto da un particolare blocco. Il blocco di sicurezza introduce semplicemente un altro blocco, con una specifica procedura di esecuzione".

Veniamo alle tecnologie

Quali sono le tecnologie più consolidate per garantire la sicurezza della rete?

"La sicurezza della rete viene gestita e garantita da una molteplicità di caratteristiche che ricoprono sia l'ambito software che quello hardware", sostiene **Esposito**.
Limitandosi a fornire semplicemente qualche cenno senza alcuna pretesa di esaustività, è possibile indicare come per quel che riguarda gli aspetti hardware di solito si privilegi la configurazione multi-microprocessore, sia a livello di unità centrale di elaborazione, sia di I/O decentrati. Ciò consente la presa in considerazione del concetto di ridondanza, che è uno dei cardini tecnologici utilizzati per prevenire perdite di affidabilità in caso di guasti di componenti. "Spesso i microprocessori sono di marche differenti, in ossequio al principio della diversità", sottolinea **Esposito**. "Altro elemento importante è la costante autodiagnosi dei componenti interni secondo tempistiche e modalità che variano da costruttore a costruttore. Per quel che riguarda gli aspetti software si è già accennato alla presenza di protocolli di rete particolari per la differenziazione certa e affidabile tra segnali di sicurezza e d'automazione tradizionale".
Altre precauzioni vengono prese a livello di compilazione dei programmi software, così come vengono creati dei pacchetti software specifici chiusi che non possono essere modificati dall'utente. Molti altri aspetti vengono tenuti in conto, non ultimo la valutazione delle influenze esterne sui vari componenti del sistema (vibrazioni, EMC, ecc.). "TÜV e BIA, due enti certificatori di sicurezza di fama mondiale, hanno dato la loro approvazione al sistema AS-i Safety at Work dichiarandolo sistema di collegamento intelligente di sicurezza fino a Categoria 4, il massimo", interviene **Volpe**.
Come spiega **Bramati**, nel caso di Siemens al protocollo standard Profibus-DP è stato sovrapposto un profilo di comunicazione in sicurezza con frame fail-safe verso gli slave sicuri. In ogni caso, diversi tipi di configurazione consentono anche il controllo locale delle parti d'impianto sicure, integrando una piccola CPU di tipo fail-safe direttamente sulla periferia remotata.
Secondo **Quintana** uno dei fattori fondamentali di qualsiasi elemento di sicurezza è la capacità di rilevare in modo sicuro gli errori sul campo per definire, di conseguenza, il profilo di recovery e le condizioni di sicurezza da attuare a bordo macchina o impianto. "Una forte error detection garantisce la sicurezza, una flessibile error avoidance rende disponibile il bus", egli precisa. "Condizione necessaria per rendere sicuro un bus è che i meccanismi di rilevamento, correzione ed eventuale ripetizione del telegramma e di ripristino degli errori siano ridondati, affinché il singolo errore venga sempre diagnosticato (ed eventualmente corretto) e non costituisca una potenziale fonte di perdita del controllo". Se per un bus standard tali meccanismi esistono naturalmente, non è richiesto che vengano necessariamente resi sicuri. Un bus di sicurezza deve, invece, instaurare la procedura minima di raddoppio diversificato dei meccanismi di error detection già al Layer 2 del modello ISO/OSI.
L'accesso al bus da parte di un nodo safe deve essere prioritario rispetto a qualsiasi altra informazione e, soprattutto in sistemi bus lineari multi-master, l'accesso non deve collidere con le informazioni che stanno occupando in quel momento la linea. Il Csma/CD+CR (carrier sense, multiple access/collision detection + collision resolution) permette di incanalare le informazioni sul bus in modo ordinato, evitando le possibili collisioni e sincronizzando tutti i partner.
L'aspetto di priorità e velocità delle informazioni di sicurezza si riflette anche sulla modalità con cui tali informazioni sono guidate sul bus; se un'informazione di sicurezza viene trasferita non appena si verifica (event-oriented drive), abbiamo la garanzia che i tempi di risposta dell'impianto siano pressoché immediati senza dover attendere l'interpretazione della priorità del messaggio o il polling di tutti i partecipanti. "La condizione ottimale di un bus di sicurezza è quella di avere una rete il più possibile libera da informazioni di qualsiasi tipo in transito e guidata sulla base degli eventi di sicurezza che devono essere trasferiti", conclude **Quintana**.
A parere di **Merati**: "Ad oggi, anche se la diffusione delle reti di sicurezza è ancora molto limitata, le tecnologie più comuni spaziano da un approccio dedicato solo alle funzioni di sicurezza, con anche separazione hardware del bus, con tutte le complicazioni che una tale scelta comporta, a un approccio molto più aperto, con bus condiviso sia per la sicurezza che per l'automazione, con evidenti vantaggi di flessibilità, riduzione costi, semplicità di utilizzo e manutenzione, oltre a una totale apertura del sistema". La tecnologia di base è la stessa, ma con orientamenti completamente differenti; il primo, con separazione totale della sicurezza, ricalca la metodologia utilizzata nell'approccio elettromeccanico, mentre il secondo, più innovativo, vuole eliminare ogni barriera al fine di semplificare la coesistenza di sicurezza e produttività.
Afferma, infine, **Timoney**: "British Nuclear Fuels e altri utenti stanno conducendo studi su applicazioni a elevata affidabilità basate sull'uso di Foundation Fieldbus. L'affidabilità è diventata molto superiore a quella indicata dalle prime stime. Ritengo quindi che il nostro protocollo fieldbus si dimostrerà una delle implementazioni a maggiore affidabilità nel campo delle reti". ■