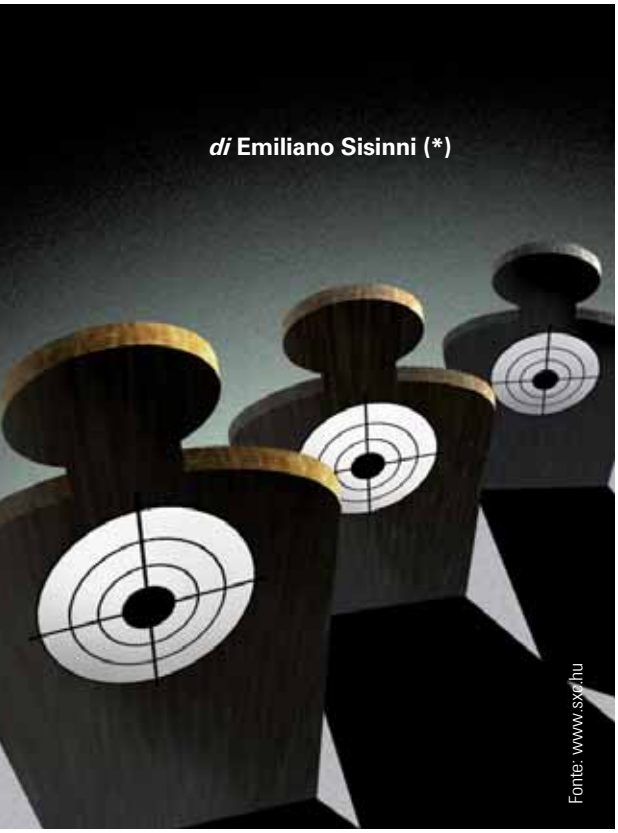

Sicurezza

SOLUZIONI DI COMUNICAZIONE INDUSTRIALE PER AREE PERICOLOSE

di **Emiliano Sisinni (*)**

APPARSI SUL FINIRE DEGLI ANNI '80, I BUS DI CAMPO SONO STATI AMPIAMENTE ADOTTATI E ACCETTATI NELLE APPLICAZIONI DI CONTROLLO E MONITORAGGIO SOLO A PARTIRE DA UNA DOZZINA D'ANNI A QUESTA PARTE MA CON MOLTE RISERVE RIGUARDO AL LORO IMPIEGO IN AREE PERICOLOSE

La stragrande maggioranza degli impianti di processo e delle soluzioni per l'automazione industriale ha requisiti unici per quanto riguarda l'infrastruttura di comunicazione, che differiscono profondamente da quelle di una rete per applicazioni home/office.

In particolare, i nodi di una rete industriale devono resistere alle più severe condizioni ambientali, quali intervalli di temperatura estremi, sollecitazioni meccaniche gravose, sovratensioni di alimentazione e in alcuni casi anche scariche di fulmini, interferenze elettromagnetiche e, non ultimo, necessità di operare in aree pericolose. La risposta a questi requisiti è arrivata con la comparsa dei cosiddetti bus di campo. I vantaggi che derivano dal loro uso sono ormai evidenti a tutti; tanto per citarne qualcuno si ricordi il minor costo per i cablaggi, il risparmio nella stesura dei progetti e della documentazione (dovuto ai layout più semplici e uniformi), la riduzione dei costi e dei tempi di avvio e di messa in servizio, e la richiesta di meno risorse al sistema di supervisione, capacità che possono essere sfruttate per evoluzioni future dell'applicazione.

Tuttavia, pur essendo apparsi sul finire degli anni '80, i bus di campo sono stati ampiamente adottati e accettati nelle applicazioni di controllo e monitoraggio solo a partire da una dozzina d'anni a questa parte e, comunque, con molte riserve riguardo al loro impiego in aree pericolose.

È stata la disponibilità di soluzioni standard e chiaramente multivendor (che ha permesso l'interoperabilità tra prodotti differenti) a capovolgere drasticamente la situazione. I vantaggi di un approccio distribuito sono oggi chiaramente compresi da tutti tanto che, ad esempio, sta prendendo sempre più piede l'ipotesi di spostare la strategia di controllo dal PLC al livello di campo. Anzi, la frontiera attuale, dietro alla quale è in corso un acceso dibattito, è l'adozione di un bus di campo wireless (ovviamente ottimizzata per l'impiego industriale) anche per il trasferimento di dati critici ed eventualmente per applicazioni di controllo.

Sono in molti a sostenere che un enorme stimolo all'introduzione delle tecnologie di comunicazione digitali nel mondo industriale sia stata l'enorme diffusione (e i conseguenti vantaggi derivanti dall'economia di scala) di Ethernet che, inizialmente 'disprezzato' e considerato come una tecnologia non applicabile perché non deterministica, è ora accettata e utilizzata in tutto il mondo grazie anche all'avvento delle architetture basate sugli switch. Anzi, il suo impiego cresce a ritmi insperati, tanto che una recente analisi di Frost e Sullivan stima che, a livello globale, l'incremento dei nodi installati viaggia al ritmo del 50% annuo a partire dal 2000. Tuttavia, se Ethernet è riuscito a divenire un chiaro riferimento per le comunicazioni industriali, c'è comunque preoccupazione sul modo migliore di applicare i bus di campo all'interno delle zone pericolose (ad esempio perché a rischio esplosione).

È un dato di fatto che nel recente passato (si veda il 'The Industrial Wireless Book', VDC Survey 2006) vi è stata una notevole crescita nella domanda e nell'uso dei dispositivi a sicurezza intrinseca, non solo in Europa, storicamente più coinvolta in queste problematiche, ma anche in tutto il Nord America. Lo stesso sondaggio ha anche evidenziato che la maggior parte degli strumenti a sicurezza intrinseca oggi utilizzati è basato sulla tecnologia Profibus, a differenza di quelli convenzionali, per i quali Hart è di fatto leader per gli strumenti per il processo. Nel dettaglio, la crescita più elevata per la strumentazione cablata (9% annuo) è relativa all'I/O remoto, mentre i trasmettitori wireless registrano una crescita pari al 35% annuo. A corollario di ciò va detto che tuttora, le soluzioni proprietarie dominano invece il mercato delle soluzioni per il controllo.

Le strategie applicate nelle aree pericolose

Può essere a questo punto utile una piccola digressione sulle tecniche di 'prevenzione' comunemente utilizzate nelle aree a rischio, il cui scopo è di eliminare una delle tre parti del triangolo della combustione, ovvero: combustibile, comburente e calore.

Nel passato, il tipico approccio per la protezione dalle esplosioni prevedeva l'uso di custodie a prova di esplosione, che tollerano che l'esplosione avvenga ma ne limitano l'impatto tramite un apposito 'contenitore' all'interno del quale viene alloggiata l'apparecchiatura; è necessario ovviamente prevedere l'uso di speciali boccole per l'accesso dei cavi, la cui installazione può essere alquanto complessa e costosa e rendere gravose le operazioni di manutenzione. Va detto però che esistono anche alcuni sistemi di connessione che possono essere utilizzati in zone pericolose ed eventualmente anche adatti a inserzioni hot-plug.

Nel caso della sicurezza intrinseca, la premessa è di mantenere l'energia immessa nell'ambiente al di sotto di quella necessaria a innescare un'atmosfera esplosiva. È la tecnica normalmente usata, per esempio, con i tradizionali segnali analogici 4-20 mA e, nel caso dei bus di campo, con le tecnologie Profibus PA e Fieldbus Foundation H1. Purtroppo, tale approccio limita chiaramente le distanze massime che i nodi possono tollerare.

Una soluzione alternativa prevede il ricorso a un cavo a fibra ottica, che permette di superare il limite sulla lunghezza dei cavi, portandolo in generale a più di un chilometro. Va comunque detto che anche la luce può provocare un'esplosione e opportuni accorgimenti devono essere presi. In questo caso, seguendo quanto riportato dalla normativa IEC60079-28, ci sono tre tipologie di protezione, ovvero 'op is = inherently safe optical radiation', 'op pr = protected optical radiation' e 'op sh = optical radiation interlock'.

Rispetto al doppino in rame, la fibra è più robusta rispetto alle condizioni ambientali estreme, ma questo vantaggio è associato ad altre limitazioni, derivanti essenzialmente dal costo più elevato e dalle proprietà meccaniche non eccellenti, relative soprattutto alla fragilità della fibra e a vincoli sul raggio del cavo.

I bus di campo wireless e le aree pericolose

Un discorso a parte deve essere fatto per i sistemi di comunicazione industriale wireless, i cui molti vantaggi sono da più parti continuamente richiamati. Uno di questi è la potenziale riduzione dei costi, tenuto conto del fatto che i costi di cablaggio aumentano drasticamente al crescere della lunghezza. Non meno importante è la flessibilità che tali soluzioni promettono, poiché i dispositivi possono essere posizionati, almeno in linea di principio, ovunque e senza la necessità di uno scavo. La loro sempre maggior diffusione ha quindi portato in evidenza anche l'esigenza di prendere in considerazione le implicazioni derivanti da un loro uso in aree pericolose. Chiaramente, l'utilizzo di contenitori a prova di esplosione può non essere una strategia di facile attuazione; infatti i dispositivi wireless emettono radiazione elettromagnetica che rappresenta una potenziale fonte di innesco per un'atmosfera esplosiva. Il rischio principale risiede nella creazione di correnti indotte negli oggetti metallici e nei circuiti elettronici non adeguatamente schermati rispetto alle interferenze elettromagnetiche. Tali correnti possono causare un surriscaldamento dell'oggetto metallico stesso e innescare la formazione di scintille.

La situazione non è attualmente ben definita; ad oggi non ci sono standard che includono un riferimento esplicito ai rischi connessi all'uso del wireless, poiché le norme internazionali riguardano solamente i livelli di esposizione alla radiazione a radio frequenza sul corpo umano. Gli stessi standard protocollari quali ISA100 e WirelessHart, per i quali già oggi esistono dispositivi commercialmente disponibili, non forniscono particolari indicazioni riguardo la loro installazione in aree pericolose. La normativa IEC60079-0 include delle tabelle riguardanti i livelli di potenza e di energia che sono ammessi in aree pericolose, mente il British Standard BS6656, relativo alla valutazione della combustione accidentale di aree infiammabili a causa di radiazioni a radiofrequenza fornisce delle raccomandazioni d'uso, limitandosi però a discutere del caso in cui una sorgente e a radio frequenza esterna si trova a dover trasmettere verso un'area pericolosa.

Un'altra potenziale fonte di rischio è connessa all'impiego delle batterie che vengono utilizzate per l'alimentazione di dispositivi portatili. Ad esempio, in funzione dei criteri con cui sono stati progettati, alcuni dispositivi cessano di essere a sicurezza intrinseca quando vengono aperti per la sostituzione della batteria, il che implica la necessità di mettere il dispositivo fuori servizio. Alcuni produttori hanno pertanto deciso di ricorrere a batterie a sicurezza intrinseca che permettono la loro sostituzione in campo; le batterie sono alloggiate in custodie sigillate, così da prevenire eventuali scintille. Ulteriori problematiche nascono dall'adozione di nodi il cui ruolo è quello di adapter, ovvero connettere tramite comunicazione wireless della strumentazione tradizionale e quindi cablata, ad esempio per estrarre da un dispositivo non solo i dati di processo ma anche le informazioni relative alla diagnostica. Non è ancora ben chiaro se questo 'adattatore' sia parte del loop di acquisizione esistente o sia da considerarsi come un nuovo strumento con la propria certificazione. Se deve essere considerato parte del loop esistente, ne cambia la dinamica e quindi richiederebbe una nuova certificazione dell'intero sistema. Un'altra potenziale fonte di rischio è che alcuni strumenti sono alimentati direttamente dall'adapter, pertanto è necessario prestare le opportune precauzioni in fase di progettazione dell'impianto. L'antenna stessa, essendo la fonte di emissione della radiazione, deve essere tenuta in considerazione, ad esempio valutando il suo EIRP (Effective Isotropic Radiated Power, ovvero l'indicazione della potenza effettivamente irradiata rispetto a un'antenna isotropica, cioè ideale). La norma IEC60079 prima citata tuttavia non fornisce alcuna indicazione dei limiti di energia Eirp per i dispositivi posti in aree pericolose. Va comunque detto che, convenzionalmente, si ritiene che radio con potenze di trasmissione inferiori a 100 mW Eirp nelle bande ISM centrate attorno a 2.4 e 5 GHz non dovrebbero porre alcun rischio. Pertanto, finché non verrà comunemente accettato l'utilizzo della tecnologia wireless anche in ambienti pericolosi e, soprattutto non verranno rilasciate normative che ne regolamentino l'impiego, la raccomandazione è di seguire le procedure atte a verificare e garantire che la potenza irradiata rientri nei livelli di energia di accensione della zona pericolosa.

(*) Comitato tecnico Fieldbus & Networks