Il wireless per **l'automazione di fabbrica e di processo**

L'uso delle tecnologie wireless nel campo dell'automazione industriale è tuttora avvolto da un alone di mistero e soprattutto di diffidenza. Scopo di questo articolo è chiarire i requisiti del sistema di comunicazione a fronte di una distinzione tra automazione di fabbrica e controllo di processo. Viene inoltre fornito qualche cenno al problema della coesistenza, destinato a diventare predominante in un futuro prossimo sicuramente contraddistinto da un impiego sempre maggiore di soluzioni "senza filo".

Emiliano Sisinni

Keyword

Reti di sensori wireless, sistemi distribuiti, Wireless Hart, WSan

Parlando di wireless per l'industria, occorre innanzitutto tenere presente che non solo non è possibile identificare un'unica soluzione per tutte le possibili applicazioni, ma che, più in generale, è impensabile, almeno oggi, una totale eradicazione dei cavi a favore di una soluzione totalmente wireless. Bisogna invece ipotizzare l'implementazione di una rete ibrida che sostituisca le tradizionali connessioni cablate solo laddove ne può emergere un effettivo vantaggio.
Un utile distinguo può essere fatto tra automazione di fabbrica e controllo di processo, come evidenziato nella ►**tabella 1**. Pur dovendo soddisfare requisiti apparentemente simili, le due diverse aree pongono requisiti decisamente differenti. In particolare, tipicamente la latenza introdotta dal sistema di comunicazione non è un problema nel secondo caso mentre è di fondamentale importanza nel primo. Altra peculiarità del controllo di processo è di dover coprire aree molto estese, spesso pari anche a diversi chilometri quadrati, mentre le dimensioni di una cella di lavorazione sono ridotte. Infine, va notato che gli strumenti intelligenti (dotati cioè di una comunicazione basata su un bus di campo) presenti nell'industria di processo hanno costi elevati, al contrario dei dispositivi semplici e poco costosi dell'automazione discreta. Diverso è quindi l'impatto economico della circuiteria aggiuntiva necessaria all'implementazione dell'interfaccia radio.
Questa, seppur grossolana, classificazione permette di giustificare le scelte tecnologiche implementate nei diversi fieldbus wireless oggi disponibili, come meglio chiarificato nel paragrafo successivo.

Caratteristica	Controllo di processo	Automazione discreta
Tipologia del sensore/dato di misura	Essenzialmente analogica	Essenzialmente discreta/digitale
Numero di sensori per unità	1000	100
Dimensioni dell'impianto/cella	1000 metri	10 metri
Unità per impianto	Decine	Centinaia
Durata del ciclo produttivo	100 giorni	1 giorno
Tempo di avvio	Ore	Minuti
Control Loop Time	0.1-1000 s	0.001-0.5 s
Costo dei dispositivi	$1000	$100
Costo di installazione / Costo di un dispositivo	10 X	4 X
Architettura	DCS	PAC/PLC
Soluzioni correnti	HART, Foundation Fieldbus, Profibus-PA, Ethernet	Profibus-DP, DeviceNet, Interbus, AS-I, Ethernet

Tabella 1 - Diversi requisiti dell'automazione di fabbrica e del controllo di processo

L'AUTORE
E. Sisinni, Dipartimento di Ingegneria dell'Informazione, Università di Brescia

Le scelte protocollari

Un qualunque sistema di comunicazione digitale è normalmente descritto in funzione dei protocolli, ovvero delle regole che devono essere seguite per rendere possibile lo scambio delle informazioni dalla sorgente alla destinazione. Un modello ampiamente accettato e universalmente utilizzato è quello proposto dall'ISO, l'International Organization for Standardization, nel 1978. In particolare tale modello è costituito da strati (o livelli), i cosiddetti layer, che racchiudono uno o più aspetti fra loro correlati della comunicazione fra due nodi di una rete. I layer sono in totale 7 e vanno dal livello fisico (quello appunto del mezzo fisico, ovvero nel nostro caso delle onde radio) fino al livello dell'applicazione.
Una rappresentazione schematica di questo modello, nella sua versione semplificata che ignora i livelli di trasporto, sessione e presentazione spesso non presenti nei sistemi di comunicazione industriali, è fornita nella ►**figura 1**.

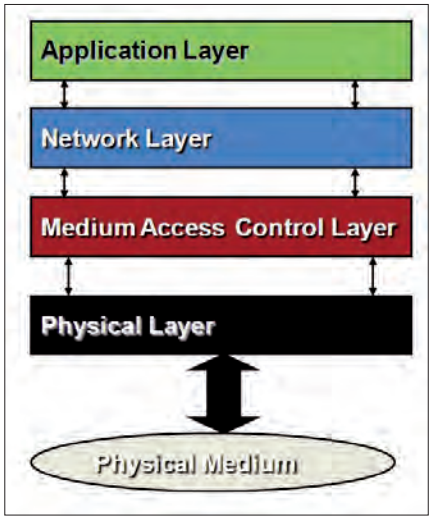

Figura 1 - Il modello ISO/OSI, versione semplificata

Partendo dal **livello fisico**, una prima considerazione riguarda l'uso quasi esclusivo di una banda di circa 80 MHz nell'intorno dei 2.4 GHz, normalmente conosciuta come banda ISM (acronimo di Industrial, Scientific and Medical, ovvero i campi d'uso per i quali è stata ideate dagli enti normatori). Tale scelta ovviamente pone dei severi limiti alla coesistenza di più reti co-locate, ma è dettata dalla necessità di poter disporre di una porzione di spettro che sia:
- sufficientemente ampia da garantire un data rate elevato oltre alla possibilità di allocare reti differenti su canali differenti;
- liberamente disponibile, ovvero, utilizzabile senza il rilascio di alcuna licenza particolare;
- utilizzabile in tutto il mondo, per evitare di dover approntare apparati differenti in funzione del mercato di destinazione.

La regolamentazione è differente da nazione a nazione, ma in Europa si fa riferimento alle specifiche emanate dall'ETSI, in particolare la norma EN 300 328. Inoltre, la necessità di adottare dispositivi originariamente pensati per le applicazioni consumer per ridurre i costi di fatto riduce a due le tecnologie più utilizzate, ovvero IEEE 802.15.4-PHY [1] e IEEE 802.15.1-PHY [2], vale a dire i livelli fisici che sono ad esempio impiegati in ZigBee, nel primo caso, e in Bluetooth, nel secondo. All'interno della stessa banda operano anche le reti WiFi (basate su IEEE 802.11), utilizzate da diverse soluzioni oggi esistenti, anche se la maggior complessità che caratterizza queste soluzioni pone alcuni limiti in termini di costo e consumo.

> *I tempi sono ormai maturi per l'introduzione dei fieldbus wireless, specie per le tipiche applicazioni dell'industria di processo*

Il livello che si incontra successivamente è quello del **collegamento dati**, che si preoccupa di garantire l'affidabilità della comunicazione tra vicini. In particolare, sono i protocolli di questo livello che hanno il compito di garantire un accesso al mezzo equo per tutti i dispositivi (nodi) che partecipano alla rete. A partire da questo livello emergono le profonde differenze delle soluzioni industriali rispetto alle applicazioni del mondo consumer sopra citate. Se queste ultime tollerano possibili collisioni derivanti da comunicazioni contemporanee di due o più nodi, una tale situazione non è accettabile in un contesto industriale, dove è richiesto il determinismo. Per questo motivo, la tecnica di accesso al mezzo convenzionalmente impiegata è quella della divisione di tempo. Mantenendo il discorso il più generale possibile, i fieldbus wireless ricorrono a un'architettura centralizzata che provvede a dividere il tempo in pattern ripetitivi (noti anche come frame, la cui durata coincide tipicamente con il tempo di ciclo richiesto) costituiti da un insieme di time slot, all'interno dei quali può effettivamente avvenire la comunicazione tra un nodo sorgente ed un nodo destinazione. Appare evidente che la strategia appena presentata richiede inoltre che i nodi condividano tutti lo stesso senso del tempo, ovvero che in qualche modo siano disponibili dei meccanismi di sincronizzazione.

È comunque ben diverso dover garantire tempi di ciclo di millisecondi o di secondi. Tempi di comunicazione brevi possono essere ottenuti grazie ad un elevato bit rate, ma questo pone seri, e spesso invalicabili, limiti sul costo (dettati dalla complessità della radio) e sui consumi (dettati dall'impossibilità di implementare strategie a basso duty-cycle). In base a questa grossolana analisi si spiega come mai le soluzioni wireless sono da tempo disponibili per l'industria di processo ma stentano ad emergere, almeno come soluzioni standard, per l'automazione di fabbrica.
Per quanto riguarda il **livello di rete**, è di nuovo necessario fare una distinzione in funzione dell'area di applicazione. E' già stato sottolineato che, in termini generali, le soluzioni wireless per l'industria ricorrono a strutture centralizzate, che richiedono pertanto la presenza di un gestore della rete noto anche come Network Manager. Esso stabilisce, tra le altre cose, i percorsi che devono seguire i pacchetti di informazione per giungere a destinazione. L'automazione di fabbrica, caratterizzata da latenze ridotte, da una densità dei nodi molto elevata e da un'area coperta ridotta, ben si presta ad una topologia di tipo a stella, nella quale tutti i nodi sono connessi, tramite un tratto dedicato (connessione punto-a-punto), ad un nodo centrale (centro stella, coordinatore della rete). Al contrario, il controllo di processo, che deve coprire aree molto vaste, si affida a una connessione di tipo magliata o mesh, nella quale tutti i nodi non sono necessariamente i destinatari di una transazione, ma ci possono essere dei

router intermedi il cui compito è instradare l'informazione verso la destinazione finale. Oltre ad un'intrinseca robustezza della rete derivante dalla possibilità di utilizzare percorsi ridondati, tale topologia permette di utilizzare basse potenze di trasmissione pur potendo coprire vaste aree grazie a salti multipli (hop) di router in router. Purtroppo, proprio la necessità di una molteplicità di salti aumenta notevolmente la latenza della comunicazione, rendendo inattuabili tempi di ciclo molto brevi (nell'ordine dei millisecondi).
Una rappresentazione grafica dei concetti appena esposti è data dalla ►figura 2 che mostra come all'interno dei time slot siano allocate le comunicazioni tra nodo sorgente A e destinazione B (nel caso di topologia a stella) o tra i diversi router A1, A2, A3.

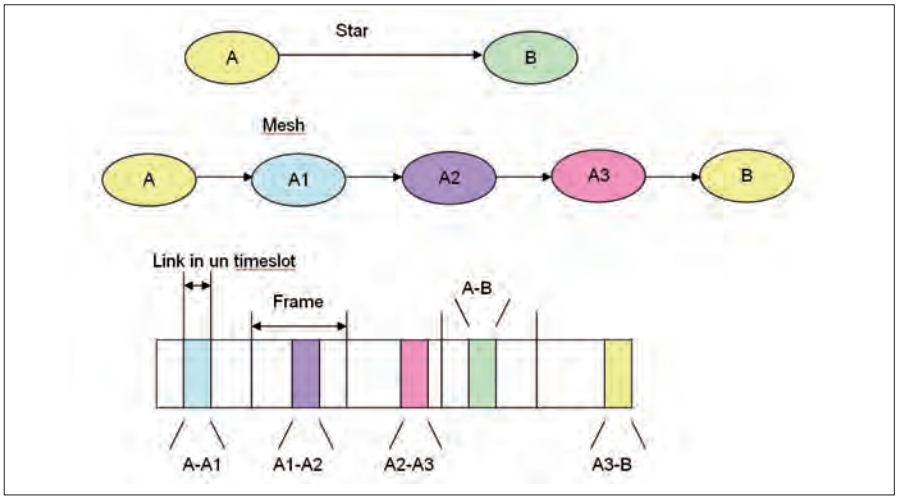

Figura 2 - Accesso a divisione di tempo, star e mesh routing

Infine, è già stato anticipato che l'uso del wireless è, almeno ad oggi, da intendersi integrato all'interno di una soluzione di interconnessione cablata, a realizzare una rete di reti, ognuna delle quali è in grado di soddisfare particolari requisiti di una ben specifica applicazione. Ciò richiede la presenza di un gateway che, tramite uno (o più) Access Point (AP), vada ad interfacciare il coordinatore della rete wireless con quella cablata; una schematizzazione di questo approccio è data dalla ►figura 3.
Un esempio di reti wireless commerciali per l'automazione industriale è dato da WirelessHart, originariamente proposto dal Consorzio HCF e oggi standard IEC 62591, per il controllo di processo, e dal WSan-FA (Wireless Sensor and Actuator Network for Factory Automation), per l'automazione di fabbrica, che si rifà alla soluzione WISA proposta da ABB.

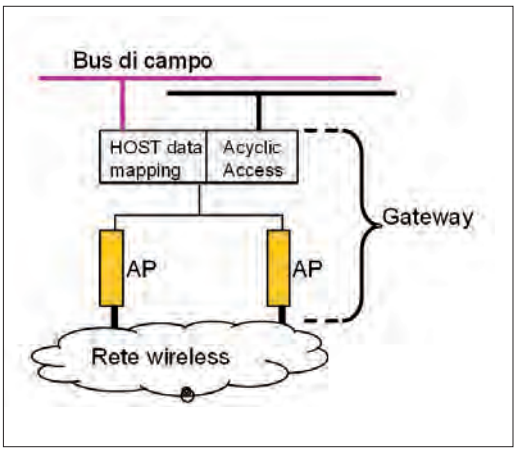

Figura 3 - Uso di un gateway per l'interfacciamento verso una rete cablate

WirelessHart per il controllo di processo

L'architettura di una rete WirelessHart IEC 62591 [3] è rappresentata nella ►figura 4.

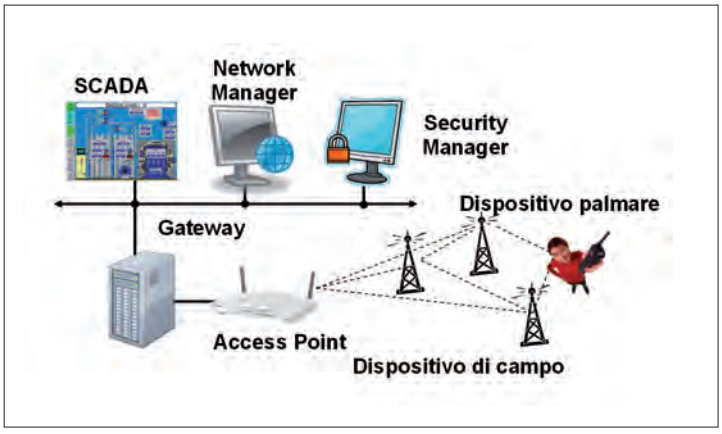

Figura 4 - Architettura di una rete WirelessHart

Un unico Network Manager (NM), ovvero un'entità logica centralizzata che sovraintende al funzionamento della rete stessa, è sempre presente. Ad esso spetta la valutazione della qualità del servizio offerto dalla rete, l'affiliazione di nuovi nodi e la pianificazione dei percorsi (route). In particolare, è proprio la pluralità di route (almeno due) che collegano un qualunque nodo della rete ad un qualunque altro nodo a garantire l'affidabilità del collegamento. Un Security Manger (SM) affianca il NM nella gestione delle chiavi di cifratura.
Lo standard prevede ben tre diversi **livelli di cifratura** (comunque obbligatoria); particolarmente critica è la fase di affiliazione, che deve garantire l'affidabilità del nuovo nodo che sta per entrare a far parte della rete. Proprio per questo motivo lo standard prevede che lo scambio della cosiddetta Join Key avvenga tramite un dispositivo di programmazione cablato (handheld device, ovvero un dispositivo palmare), ritenuto più sicuro. Esiste poi un Gateway, il cui compito è di essere il tramite tra i nodi wireless presenti sul campo e il resto dell'automazione di impianto. La **connessione fisica** è invece implementata da un Access Point.
Per quanto riguarda lo stack protocollare, il **livello fisico** è conforme allo standard IEEE802.15.4. Per l'accesso al mezzo, WirelessHart implementa una rete sincronizzata basata sulla divisione di tempo con time slot di durata fissa e pari a 10 ms, organizzati dal NM in superframe. All'interno di ognuno dei time slot può essere allocato un link, ovvero un'opportunità di comunicazione tra due nodi. Più superframe possono essere gestiti nella stessa rete, ad esempio per garantire tempi di scansione dei nodi differenti. L'organizzazione dei superframe può variare dinami-

camente nel corso della vita delle rete in base a valutazioni statistiche sullo stato di salute dei collegamenti tra i diversi nodi. È sempre il NM che, basandosi su queste stesse valutazioni, decide quali canali a RF utilizzare in ogni link e può decidere di adottare strategie di blacklisting per "aggirare" porzioni dello spettro già occupate da altri interferenti.

Per quanto riguarda il **livello rete**, WirelessHart ha una topologia di tipo mesh; questo implica che ogni dispositivo deve essere capace di inoltrare un pacchetto all'interno della rete (deve cioè poter svolgere il ruolo di un router). La latenza della risposta, è quindi tipicamente nell'ordine del secondo o più. Tale scelta ben si adatta a quelli che sono i tipici requisiti di determinismo delle tipiche applicazioni dell'industria di processo.

Il livello più alto dello stack protocollare, il **livello applicazione**, replica il meccanismo command-response proprio della controparte cablata Hart, conservandone anche le strutture dati, così da garantire una totale trasparenza all'utente finale.

WSan-FA per l'automazione discreta

La soluzione denominata WSan-FA trova spunto nel sistema di comunicazione proprietario di ABB noto come Wisa. Purtroppo il processo di standardizzazione non è ancora del tutto completo, motivo per cui ad oggi non esistono prodotti commerciali WSan, ma, solo Wisa [4,5].

L'architettura alla base di ogni rete WSan-FA è una rete con una **topologia a stella**; questa scelta è giustificata dalle dimensioni tipiche di una cella di lavorazione. L'accesso al mezzo avviene grazie ad un meccanismo a divisione di tempo e un uso efficiente e diversificato nel tempo dei canali a radio frequenza disponibili (grazie al **channel hopping e blacklisting**) ne aumenta l'immunità ai disturbi e ne garantisce la coesistenza con altre reti eventualmente presenti. Le radio operano nella banda libera ISM @ 2.4 GHz e condividono lo stesso livello fisico di Bluetooth, ovvero un transfer rate grezzo di 1 Mbps e una modulazione GFSK con un canale di 1 MHz. I rimanenti livelli dello stack protocollare sono comunque totalmente differenti e sono infatti ottenibili **tempi di ciclo** nell'ordine dei 2 ms con più di 100 nodi presenti. Tali prestazioni sono possibili grazie alla necessità di trasferire piccole quantità di dati per ogni transazione (non più di 10 byte, più spesso un solo byte per sensori semplici come un interruttore di prossimità). In ogni cella sono poi attivi contemporaneamente un unico canale di down-link, dalla stazione base verso i nodi, e ben quattro canali di up-link, dai nodi verso la stazione base. Per ottimizzare i consumi, la comunicazione avviene normalmente su evento, ovvero i canali di up-link sono utilizzati solo in caso di effettiva necessità. Un meccanismo di acknowledgement e di eventuale riprova automatica consente di incrementare l'affidabilità della rete.

La ►**figura 5** mostra un tipico esempio di architettura di una rete WSan-FA.

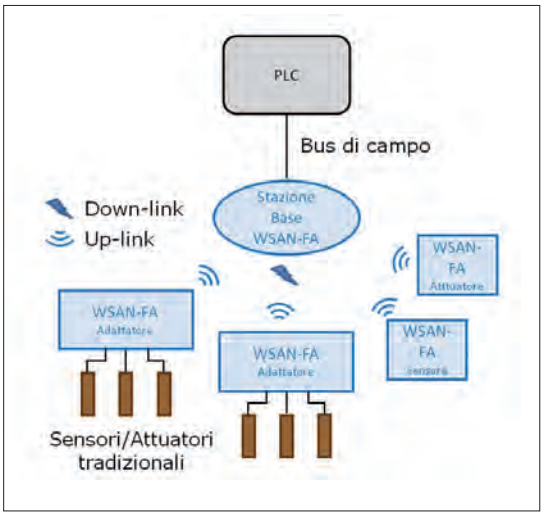

Figura 5 - Architettura di una rete WSan

Il problema della coesistenza

La coesistenza è solitamente definita come quello stato del sistema in cui tutti i sistemi di comunicazione wireless operanti all'interno della stessa area sono in grado di soddisfare le loro specifiche di funzionamento. Per poterla garantire occorre "ortogonalizzare" le comunicazioni radio, cosa che può essere fatta nel dominio dello spazio, del tempo e/o della frequenza.

Tipicamente è garantita ricorrendo a tre approcci definiti come:

- "autonomo", perché non supervisionato in alcun modo;
- "cooperativo", perché le diverse reti includono nella loro organizzazione protocollare meccanismi di adattamento all'ambiente e collaborano in maniera spontanea per coesistere;
- "pianificato", perché basato sull'intervento di un operatore umano.

Mentre la normativa europea sembra decisa ad adottare soluzioni basate sul "listen-before-talk", che si scontrano con la necessità di garantire determinismo, il gruppo WG17 del comitato 65C dell'IEC sta lavorando alla definizione di regole mirate all'impiego industriale. Tali sforzi sono confluiti nel documento IEC 62657-2 TS Ed1.0 "Industrial communication networks - Wireless communication network and communication profiles – Coexistence". In particolare, seguendo l'ultimo approccio dei tre elencati sopra, viene definita la figura del "**coexistence manager**" che, dovendosi fare carico della scelta dei sistemi di comunicazione che devono essere presenti nell'impianto, è in grado di armonizzarne le richieste. Il suo ruolo è quindi quello di una sorta di "arbitro" che vada ad agire sui parametri di configurazione delle reti wireless in modo da evitare a priori la nascita di collisioni, massimizzando il throughput complessivo.

Bibliografia

[1] IEEE Std 802.15.4-2006, *Wireless Medium Access Control(MAC) and Physical Layer(PHY) specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*.

[2] IEEE Std 802.15.1-2005 – Part 15.1, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)*. IEEE Standards Association. doi:10.1109/IEEESTD.2005.96290. ISBN 0-7381-4707-9

[3] IEC 62591:2010 Ed 1.0, *Industrial communication networks. Wireless communication network and communication profiles - WirelessHART*

[4] J.-E. Frey, J. Endresen, A. Kreitz, G. Scheible, "Unplugged but Connected", *ABB Review*, Issue 3 and 4 2005 (2 parts).

[5] G. Scheible, R. Disselnkoetter, "Wireless Power for Wireless Devices", *ABB Review*, Issue 2 2006