INTRODUZIONE ALLE RETI DI CONTROLLO

a cura di

Giacomo PISCITELLI
Dipartimento di Elettrotecnica ed Elettronica
Politecnico di Bari

Questa introduzione alle reti dicontrollo è stata ricavata dalla Tesi di Laurea del dott. Ing. Michele RUTA dal titolo "Studio e sviluppo di una applicazione di telecontrollo su IP"

Bari novembre 2003

INDICE

1 LE RETI DI CONTROLLO

1.1 Introduzione.

Il concetto di rete nella sua accezione più generale si può ritenere ormai ampiamente acquisito. Le applicazioni più diffuse hanno riguardato in maniera quasi esclusiva i cosiddetti *computing system*, vale a dire le reti di calcolatori; molto meno comuni sono invece i sistemi per il controllo di dispositivi. I protocolli di comunicazione impiegati potevano essere adoperati sia per la semplice condivisione di informazioni tra workstation fisicamente non adiacenti che per costituire sistemi distribuiti. In entrambi i casi essi dovevano essere progettati ed ottimizzati per consentire il transito di grandi quantità di dati su mezzi trasmissivi opportuni e con sufficienti garanzie di affidabilità e sicurezza. Con il passare del tempo sono state migliorate una serie di funzionalità ed è stata aumentata la loro flessibilità.

Solo quando il costo dei microprocessori ha raggiunto un livello talmente basso da consentire la loro incorporazione all'interno di controllori e dispositivi, sono stati progettati e poi realizzati i primi protocolli di comunicazione per reti di controllo. Tuttavia soltanto in pochi casi si può dire che sia stato eseguito un vero e proprio *tuning* delle specifiche progettuali allo scopo di garantire delle performance ottimali; inoltre non esistono – a differenza di quanto accade per le reti di calcolatori – degli standard universalmente riconosciuti, accettati ed adoperati.

In un certo qual modo le *control network* ampliano le funzionalità delle *data network* (ad esempio una LAN potrebbe sicuramente costituire una delle componenti di una rete di controllo complessa) per cui almeno dal punto di vista teorico si tratta di entità più generali.

Oltre a questo le reti di controllo rappresentano in certo senso un'estensione in direzione dei sistemi distribuiti delle reti di calcolatori tipo *area network*. Sono infatti parecchie le analogie che le avvicinano a questo tipo di strutture, caratterizzate dalla totale trasparenza degli eventi rispetto all'utente e da una gestione interna completamente autonoma; si tratta in altre parole di veri e propri organismi complessi unitari costituiti da un insieme di enti che non si limitano a condividere delle risorse comuni, ma che partecipano in maniera attiva e sostanziale al flusso di elaborazione in uscita.

1.2 Caratteristiche delle reti di controllo.

Cominciamo col dire che il mercato delle reti di controllo vive di una serie di anime: dall'industria del controllo degli edifici (monitoraggio degli accessi, gestione dell'energia, gestione dei sistemi luce e dei sistemi di sicurezza) alla domotica, dalle molte applicazioni in campo industriale a quelle inerenti i servizi di pubblica utilità fino ad arrivare all'industria dei trasporti.

Esistono oggi numerosi protocolli utilizzati in ciascuno di questi campi, e probabilmente, uno dei fattori che maggiormente vincola la crescita di questo settore é proprio l'incertezza su quale di essi prevarrà e diventerà lo standard di mercato. E' chiaro che un primo importante discriminante sarà proprio la capacità di una tecnologia di soddisfare esigenze molto dissimili tra loro.

Una control network recupera informazioni in ingresso (ricevendole da sensori di caratteristiche e generi diversi) le elabora opportunamente e ne fa seguire delle azioni in uscita in tutto e per tutto dipendenti dall'ingresso e dallo stato del sistema.

Abbiamo già detto di come in qualche modo le reti i controllo somiglino a quelle di dati. Le data network si compongono di una serie di computer connessi ad una serie di mezzi di comunicazione differenti, collegati tra loro per mezzo di router e che comunicano l'uno con l'altro utilizzando un protocollo di comunicazione comune come può essere ad esempio TCP/IP. Le reti di dati vengono ottimizzate per movimentare grandi quantità di informazioni ed il progetto del loro protocollo di comunicazione prevede come accettabili ritardi occasionali nelle risposte e nelle consegne dei pacchetti. Le reti di controllo contengono componenti simili ottimizzate in base al costo, alle prestazioni, alle dimensioni ed alle caratteristiche delle risposte di controllo.

Inoltre le reti di controllo permettono di creare sistemi in rete che estendono le loro applicazioni in campi ove la tecnologia per reti di dati non consente di arrivare.

Possiamo riassumere le principali differenze tra *control network* e *data network* nel seguente elenco:

- il flusso informativo tra dispositivi deve necessariamente essere regolare, affidabile e robusto.
- i dati in transito vengono incapsulati in formato di brevi messaggi (*short messages*).
- la comunicazione fra dispositivi è di tipo paritetico (*peer to peer*).

1.3 Architetture di rete master/slave.

Fino ad alcuni anni fa le logiche di controllo venivano realizzate per mezzo di pannelli a relè elettromeccanici o utilizzando controllori pneumatici. E' stato poi l'avvento della tecnologia dello stato solido ad offrire il mezzo per ridurre i costi e aumentare nel contempo la flessibilità utilizzando circuiti logici per rimpiazzare cavi, tubi e relè. Quello che nel tempo ha fatto la differenza è stata la sempre maggiore potenza degli algoritmi di governo che potevano così consentire un controllo sempre più stringente sui processi.

Il problema della flessibilità non è stato tuttavia completamente e definitivamente risolto. Restano le difficoltà legate all'aggiornamento delle componenti di comando in seguito ad eventuali modifiche della configurazione del sistema. In alcuni casi questi impedimenti sono addebitabili alla natura proprietaria di hardware e software. E' molto diffusa infatti la consuetudine di costruire sistemi "chiavi in mano" in cui si provvede a fornire al cliente finale tutto quanto è necessario al funzionamento dell'impianto nel suo complesso, a partire dai protocolli di comunicazione fino ad arrivare alle logiche. Questo approccio da un lato garantisce un riferimento unico per l'intero sistema per quanto riguarda le responsabilità sul funzionamento e la risoluzione dei problemi ad esso relativi. Dall'altro forza l'utente finale a perpetuare il rapporto con il costruttore del suo impianto per la durata dell'intera vita del sistema limitandone pesantemente scelte e possibilità di intervento autonome.

Per giunta l'esigenza di progettare e nel contempo ingegnerizzare oltre che commercializzare sistemi così complessi ad opera di un unico autore restringe fortemente l'insieme dei possibili costruttori ad un piccolo gruppo di grandi compagnie con il rischio di formazione di *trust* e con la ovvia conseguenza di limitare le potenzialità di sviluppo dell'intero settore. E' sufficiente confrontare l'incremento del rapporto prestazioni/prezzo relativo al mercato delle reti di personal computer con quello delle reti di controllo (si veda il grafico), perché venga alla luce il forte divario dovuto ad una diversità di impostazioni generali e ad una differente politica di investimenti.

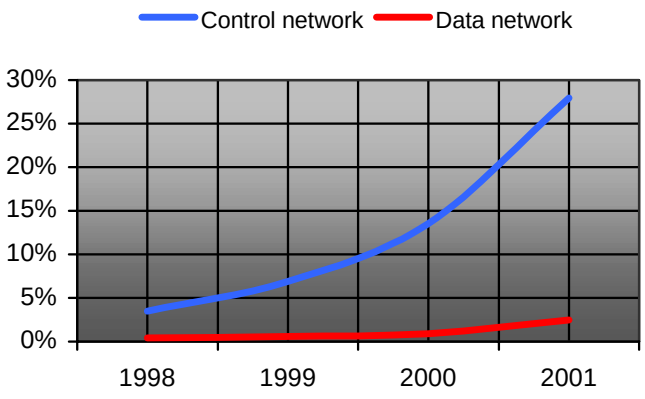


Figura 1. : Rapporto prestazioni/prezzo per reti di dati e di controllo (fonte AssInform).

Tra l'altro tutti i tentativi di realizzare sistemi che potessero essere compositi si sono scontrati contro difficoltà tecnologiche piuttosto serie. Infatti l'incompatibilità dei protocolli di

comunicazione relativi a componenti diversi obbliga all'utilizzo di porte RS-232 programmabili, di gateway appositamente strutturati e in generale vincola il progettista a soluzioni di natura per la verità abbastanza precaria. Le informazioni di controllo vengono veicolate lungo percorsi fissi che in genere finiscono per interessare tutti i sottosistemi, gli eventuali problemi di funzionamento non possono essere circoscritti con facilità e magari riferiti a specifiche componenti del sistema complessivo, le rilevazioni relative a sensori differenti spesso non sono singolarmente accessibili. In ultimo ciascuna parte riesce difficilmente ad adattare in tempo reale le proprie risposte in rapporto allo stato di tutto il sistema (e questo implica un sensibile decremento delle prestazioni di punta).

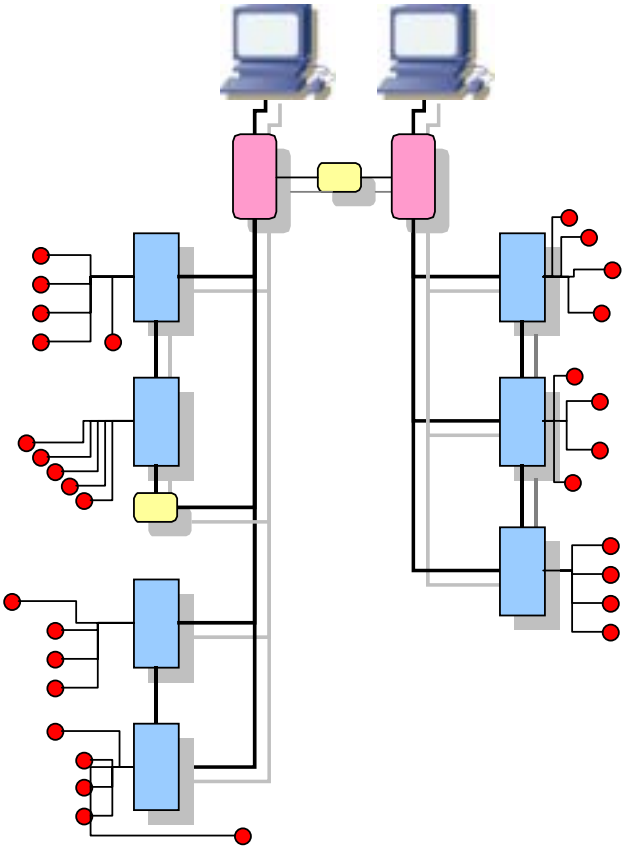


Figura 2 : un esempio di architettura centralizzata.

La figura precedente mostra la topologia caratteristica di una rete di controllo ad architettura centralizzata, esempio tipico della maggior parte di sistemi di controllo per applicazioni industriali e commerciali.

Sensori e attuatori sono connessi ad un quadro di comando che a turno li collega ad un controller generale per mezzo di un bus di comunicazione master/slave di tipo proprietario. A sua volta il controller monta un microprocessore ad alte prestazioni che

provvede al lancio degli applicativi specifici per il governo di tutti i punti di input e di output ad esso legati. Nella maggior parte dei casi questo macro-controller può dialogare con altri di pari dignità attraverso un nuovo bus di comunicazione proprietario. In queste architetture sensori e attuatori sono tipicamente dispositivi di I/O "stupidi" essendo privi di ogni capacità di comunicazione e non disponendo a bordo di alcun tipo di intelligenza.

Le architetture di questo genere hanno tipicamente una HMI (Human Machine Interface) proprietaria così come è proprietario l'applicativo di gestione sviluppato e testato tramite appositi tool di programmazione che ciascuna azienda mette a punto in base alle proprie esigenze.

1.4 Architetture di rete aperte.

Una **open control network** è una rete di controllo con una struttura profondamente diversa rispetto alle architetture di tipo centralizzato. Si tratta di un sistema nel quale possono confluire una serie di dispositivi intelligenti in grado di comunicare autonomamente l'uno con l'altro. Dunque non è richiesto l'intervento di alcun controller di supervisione che raccolga le informazioni dei dispositivi in fase di trasmissione, ne rilevi provenienza e destinazione per poi successivamente provvedere all'instradamento. Allo stesso modo nessun componente di rete si deve far carico di algoritmi di controllo responsabili del governo del sistema nella sua totalità.

Questo consente a ciascun dispositivo di diffondere informazioni all'interno della rete senza passaggi intermedi; il flusso informativo viene suddiviso in pacchetti e inviato da un mittente a uno o più destinatari. Non occorre altro. Questa impostazione si discosta in maniera sostanziale da quella tradizionale; la novità sta proprio nella tendenza a distribuire l'intelligenza in direzione della periferia, ad eliminare la gerarchia e a semplificare i meccanismi tecnici di scambio delle informazioni. La successiva fase è poi rappresentata dallo sforzo di universalizzare questo orientamento sì che esso possa poi divenire uno standard de facto.

Lo schema mostrato nella figura che segue è relativo ad una rete di controllo aperta distribuita e paritetica .

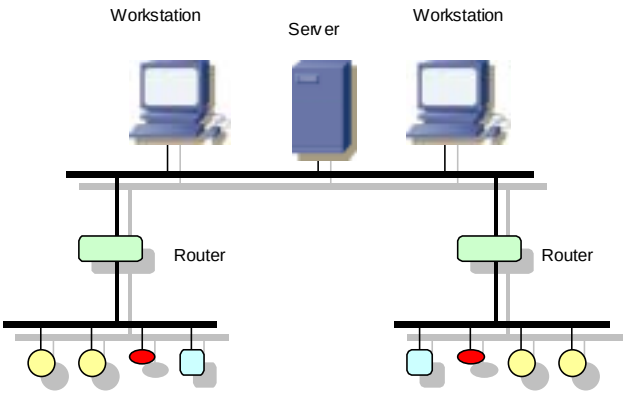


Figura 3 : un esempio di open control network.

1.5 Ma come è fatta una rete di controllo?

In questo paragrafo si illustrano i costituenti chiave di una rete di controllo aperta. Come si è detto essa consiste di una serie di *device* intelligenti (**nodi**) in grado di dialogare l'uno con l'altro adoperando un protocollo di comunicazione comune su uno o più canali di trasmissione. Ciascuno di essi include uno o più processori che ne costituiscono la… "mente" e che servono ad implementare il protocollo. Inoltre ogni dispositivo monta un ricetrasmettitore (o ***transceiver***) che funge da interfaccia elettrica con il mezzo trasmissivo.

I device diffondono liberamente in rete informazioni specifiche relative all'applicazione che stanno eseguendo. Tuttavia le diverse applicazioni non sono sincronizzate l'una con l'altra e questo potrebbe implicare che dispositivi differenti tentino di trasmettere allo stesso istante generando delle collisioni. Il protocollo di comunicazione fornisce l'insieme di norme e procedure per la regolamentazione dell'accesso al mezzo e cioè definisce la lunghezza e il formato dei messaggi tramite i quali avviene lo scambio di informazioni, stabilisce le azioni da intraprendere in fase di trasmissione, a ricezione avvenuta ed in caso di collisione. Solitamente il protocollo di comunicazione è inglobato nel firmware del chip di ciascun dispositivo in rete.

Figura 4. : Caratteristiche del protocollo di comunicazione di una rete di controllo.

Per quel che riguarda i canali di comunicazione, si può dire che ne esistono di diversi tipi e ciascuno con differenti caratteristiche costruttive; in base alla tipologia del mezzo di trasmissione da adoperare occorrerà scegliere un opportuno ricetrasmettitore. Esistono anche ricetrasmettitori idonei al funzionamento su più mezzi e quindi solitamente la scelta di un transceiver verrà effettuata in base al canale o ai canali che esso supporta. D'altra parte si preferirà un mezzo piuttosto che un altro a seconda delle velocità di trasmissione che si vogliono raggiungere, della topologia scelta per la rete e delle distanze che si intendono coprire.

1.6 Nuove tecnologie e progetti datati.

Possiamo affermare senza tema di smentita che ancora oggi non tutti i costruttori di sistemi di controllo sono effettivamente pronti allo sviluppo integrale di piattaforme che siano realmente e completamente aperte. Lo dimostra il fatto che fra i sistemi attualmente più diffusi ci siano quelli cosiddetti gerarchici. In essi abbiamo una struttura di tipo piramidale (si veda la figura che segue) nella quale è determinante la funzione di supervisione dei vertici sulla base.

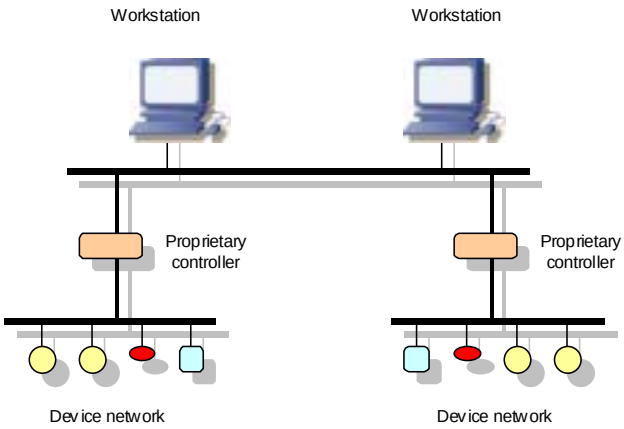


Figura 5. : un esempio di sistema ad architettura gerarchica.

Al livello più basso abbiamo sensori e attuatori chiusi in una serie di sottoreti (magari anche aperte) detti device network; tuttavia l'accesso ad esse non può avvenire a partire da un punto qualsiasi della rete. Esistono infatti al livello immediatamente superiore dei controller con funzioni di gateway i quali in maniera proprietaria filtrano il flusso informativo da e verso i dispositivi. Gli algoritmi per questi controller non hanno caratteristiche e interfacce standardizzate, per cui non è garantito il loro funzionamento con apparati di altri costruttori. Quindi per quanto la tecnologia del gateway possa essere moderna, per quanto la tipologia della rete possa far pensare ad una architettura aperta, il risultato complessivo è in realtà un sistema proprietario e quindi tutto sommato abbastanza rigido.

E' evidente che strutture di questo genere rappresentano comunque un passo in avanti rispetto a sistemi completamente proprietari, che un tempo erano l'unica alternativa possibile, ma se si pongono dei vincoli così stringenti sul solo veicolo di comunicazione tra l'ultimo livello e le rimanenti parti della gerarchia, nella sostanza si è ancora lontani da sistemi realmente aperti.

Ma analizziamo più in dettaglio le caratteristiche dei controller di supervisione. Essi consentono la gestione della maggior parte delle funzionalità di controllo di dispositivi di I/O, di unità terminali e di altri controllori. Questi complessi "pannelli di comando" fungono poi anche da gateway per le informazioni che provengono dalle varie reti di dispositivi provvedendo all'adeguamento del loro protocollo di comunicazione con qualsiasi altro meccanismo di trasporto delle informazioni operante ai livelli più alti della gerarchia. Spesso questi controller vengono adoperati allo scopo di fungere da driver appositi per la connessione con altri bus proprietari o all'atto dell'ammodernamento di un sistema, per incorporarvi vecchie apparecchiature. Questo da un lato garantisce una soluzione al

problema dell'integrazione di apparati diversi, dall'altro implica un forte aumento della complessità del sistema. Per rendersene conto basti pensare alle difficoltà ingenerate dalla diversità dei tool per la configurazione e la gestione della rete che ciascun costruttore possiede ed adopera. Per di più ognuno di essi produce una HMI proprietaria per cui chi si occupa dell'integrazione dovrebbe impiegare tempo e risorse per imparare ad adoperare una moltitudine di interfacce prive di standard e con caratteristiche spesso contrastanti.

Quindi possiamo riepilogare le ragioni per cui i sistemi ad architettura gerarchica non rappresentano la soluzione ottimale per una rete di controllo:

- *Sono inutilmente complesse.* Se si implementasse il sistema con una struttura realmente peer to peer si potrebbe eliminare con certezza il primo livello della gerarchia (supervisione sui controllori) senza alcuna perdita in termini di funzionalità. Non vi sono infatti benefici per l'utente finale derivanti dalla presenza di questo ulteriore layer che apporta costi accessori oltre che un sicuro aumento della complessità legato all'installazione, alla configurazione e alla manutenzione di un secondo aggiuntivo livello di controllo nella stessa rete, basato per altro su una differente tecnologia rispetto a quello inferiore.

- *Sono sostanzialmente di tipo proprietario.* Per quanto il livello più basso della piramide possa essere progettato e realizzato in maniera aperta, la presenza di controller proprietari implica la perdita di quasi tutti fra i più importanti benefici derivanti dall'adozione di un open standard; vale a dire la libertà per l'utente finale di modificare, aggiungere, scegliere e implementare nuove funzionalità e la facilità di gestirle e manutenerle.

- *Non è possibile comunicare con qualsiasi punto, in qualsiasi momento, da ovunque nella rete.* Visto che l'architettura consta di una serie di layer di controllo non è possibile la comunicazione diretta tra dispositivi appartenenti a canali separati. La procedura di acquisizione dei dati rallenta molto la comunicazione: essa prevede la traduzione tra almeno due protocolli diversi e la memorizzazione in un database globale. Questo spesso significa ritardi inaccettabili. Inoltre in generale le caratteristiche architetturali strozzano il flusso informativo tra i dispositivi, riducono la facilità di implementazione degli algoritmi di controllo e dilatano i tempi per l' installazione e la manutenzione dei sistemi.

Dunque nel caso di sistemi gerarchici si può erroneamente credere di disporre delle funzionalità di una open network in quanto il sistema si fonda su una tecnologia di base

concepita per essere tale; in realtà è il progetto di rete datato ad inibire queste aspettative. Appare quindi chiara la necessità per una nuova tecnologia di accompagnarsi ad un progetto della rete che consenta di esplicarne appieno le potenzialità.

2 Il mercato

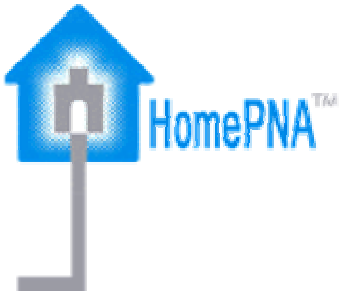
E' di seguito riportato un elenco dei protocolli per reti di controllo maggiormente diffusi. Il criterio con il quale sono stati suddivisi è rappresentato dal o dai mezzi trasmissivi che supportano. Segue poi una panoramica dei principali canali di comunicazione per control network con indicazione degli standard di mercato più comuni che ne consentono l'utilizzo. Parleremo di twisted pair telefonici, fibre ottiche, cavi coassiali RG-6, per quel che riguarda mezzi che richiedono una messa in posa e quindi l'inserimento "invasivo" di cavi all'interno di edifici; di onde convogliate su linea elettrica (Power Line Communication), di radiofrequenza e di raggi infrarossi, per quanto concerne, invece, mezzi che non richiedono nuova posa di cavi.

2.1 Linee telefoniche.

Le linee telefoniche attuali, costruite essenzialmente per il segnale vocale e ottimizzate per tale scopo, non sono adatte per trasmissioni dati ad alta velocità in quanto le loro caratteristiche di impedenza e attenuazione non possono essere ben controllate. La prima compagnia che ha cercato di risolvere questi problemi è la **Tut** Systems Inc. di Pleasant Hill in California. Essa ha impiegato un multiplexing a divisione di frequenza per creare tre canali ognuno dei quali con un differente scopo: servizio telefonico normale (fino a 3400 Hz), segnale ADSL per il collegamento ad Internet (da 25 KHz a 1.1 MHz), gestione del traffico di controllo (da 5.5 a 9.5 MHz).

Sul canale deputato al controllo, Tut riversa dati a 1 Mbit/s con 7.5 MHz di frequenza portante. All'interno della banda prevista, viene adoperato lo standard IEEE 802.3 CSMA/CD, che è solitamente utilizzato per Ethernet, ma si incapsulano i frame Ethernet in pacchetti più grandi. Infatti per il trasferimento ad alta velocità, viene utilizzata una tecnologia proprietaria di pulse modulation, codificando più bit nello stesso impulso.

La tecnologia Tut è stata utilizzata nella prima versione (la 1.0) dello standard **HomePNA** (Home Phoneline Networking Alliance), un sodalizio formato da compagnie quali *3Com*, *Advanced Micro Devices*, *AT&T*, *Compaq Computer*, *Hewlett-Packard*, *Intel*, *IBM*, *Lucent Technologies*, pensato esplicitamene per applicazioni domotiche.



Il trasferimento a 1 Mbit/s si rivela estremamente lento qualora lo si voglia impiegare per la trasmissione video (ricordiamo che MPEG-II richiede una banda di 2-4 Mbit/s, mentre

per la trasmissione DVD saliamo a 3-8 Mbit/s ed addirittura nel caso di HDTV arriviamo a 19 Mbit/s). Dunque, stante il crescente peso che l'entertainement andava assumendo all'interno del mercato, sono state studiate soluzioni per incrementare la velocità di trasferimento dati (in linea teorica il limite sostenibile era dell'ordine di 100 Mbit/s sfruttando porzioni di banda tra 2 e 30 MHz). Nasceva sotto questi auspici la seconda release di HomePNA proposta da *Epigram Inc*. *e Lucent Technologies Inc.*. Essa supporta pienamente la versione precedente, incrementa la velocità di trasferimento dati fino a 10 Mbit/s utilizzando una banda tra 4 e 10 MHz con frequenza portante a 7 MHz. La versione 2.0 impiega una modulazione di ampiezza in quadratura a divisione di frequenza (FDQAM), nella quale ogni singola informazione QAM è ripetuta in due regioni di banda per aumentare la robustezza del trasferimento dati nel caso in cui parte dell'informazione venga attenuata o corrotta.

2.2 Onde convogliate su linea elettrica.

Mentre le linee telefoniche non sono sempre a disposizione, le linee elettriche lo sono in quasi tutti i casi. Quindi sono già maturi sforzi per far comunicare diverse aree di un sistema di controllo tramite onde convogliate.

La prima in ordine di tempo e di diffusione tra queste tecnologie è stata **X-10**, sviluppata nel 1976 e largamente diffusa negli Stati Uniti. La commercializzazione di prodotti compatibili è effettuata prevalentemente dall'azienda X-10, ma esistono anche altre aziende che sviluppano apparecchi per questo standard semplice e di basso costo. Vediamo in che cosa consiste.

C'è un pannello di controllo e vari moduli che si connettono ad esso direttamente tramite linea elettrica; poi ogni apparecchio deve essere collegato ad uno specifico modulo ed in questo modo viene ad assumere un particolare ID da 0 a 255 (le dimensioni della rete che ne risulta sono ampiamente sufficienti per le esigenze di un'abitazione o di una piccola industria). Dal pannello di controllo oppure da un computer ad esso collegato, è possibile mandare segnali di accensione/spegnimento ad ogni modulo sotto forma di impulsi.

Un impulso di controllo consiste in un picco di 120 KHz lungo al massimo 1 millisecondo (uno logico), mentre la sua assenza rappresenta lo zero logico. La sincronizzazione avviene inviando impulsi nell'intorno (200 μs) dello zero della frequenza della corrente alternata (60 Hz negli USA). Inoltre ogni modulo può essere messo in polling dall'unità di controllo e indicare il proprio stato. La velocità di trasmissione supportata arriva a 50 bit/s. L'inconveniente di sistemi di questo tipo è che ci sono problemi se il bit rate

aumenta oltre pochi bit per secondo: si generano rumore, interferenze, attenuazione e variazioni di impedenza della linea per cui il comportamento non è più prevedibile.

CEBus (EIA 600) è uno standard aperto che fornisce specifiche per utilizzare le linee elettriche, ma anche TP5 (doppino telefonico), cavi coassiali, infrarossi e radiofrequenza. Il sottolivello MAC del livello 2 del sistema CEBus implementa una tecnica CSMA/CDCR (Collision Detection and Resolution). Questo permette ad ogni dispositivo sulla rete di accedere al mezzo in ogni istante grazie alla possibilità di risolvere le collisioni; tuttavia un nodo che voglia mandare un pacchetto dati, deve prima "ascoltare" affinché non ci siano altri pacchetti in transito sulla linea e solo quando questa è libera, può intraprendere una trasmissione (ed in questo sono forti le somiglianze con il protocollo IEEE 802.3).

CEBus, inoltre, specifica un linguaggio (CAL, Common Language Application) che permette alle varie unità di comunicare tra loro. Ogni unità componente il sistema è definita come un *contesto* in CAL; un sensore oppure un videoregistratore sono esempi di contesti. Ogni contesto è poi diviso in oggetti (esempi di oggetti sono lo stato per il sensore, il volume di registrazione per il VCR). I segnali di comando possono identificare il contesto e attivare funzioni sugli oggetti, così come modificare lo stato di un sensore. I ricevitori di cui ogni unità deve essere dotata captano i segnali di comando e provvedono alla loro attuazione.

Utilizzando la tecnica OFDM, simile alle tecniche di modulazione per la radiofrequenza, è possibile inviare una grande quantità di dati sulla linea elettrica. Questa tecnica, infatti, risolve il problema delle riflessioni multiple, che è la principale causa di interferenza nelle comunicazioni su linea di potenza. In teoria è possibile arrivare a trasmettere ad una velocità di 100 Mbit/s, secondo la compagnia *Intellon Inc.* che implementa questa tecnologia.

La *Intelogis Inc.* utilizza una tecnologia che trasmette i dati in una banda di frequenza superiore rispetto a quella dove si registrano i più ampi picchi di rumore; si chiama *Plug-in PLX* ed è conforme allo standard CEBus-CAL. Essa opera in modo simile al polling tra più nodi in una rete Ethernet. Ciascun device, quando entra nella rete per la prima volta, "sente" il passaggio di altri pacchetti sulla linea e manda i propri pacchetti solo se è permesso farlo. Una volta che tutti i nodi si conoscono tra loro, viene ad instaurarsi uno schema dinamico di distribuzione di token. Questo riduce il rischio di collisioni, evita di ricorrere continuamente al polling ed aumenta l'effettivo throughput di rete. La versione corrente arriva fino a 350 Kbit/s, ma è previsto che la prossima arrivi a 2 Mbit/s.

Sempre nel campo delle onde convogliate la *High Tech Horizon* ha commercializzato una specifica scheda di comunicazione per PC che consente un discreto bit rate (2.4 Mbit/s); questa scheda può essere utilizzata sia per scambiare messaggi e dati tra PC e periferiche,

sia, tramite un software per il riconoscimento vocale in dotazione, per “parlare” al computer da ogni punto, per esempio, di una casa.

Un'altra serie di compagnie si è riunita in una organizzazione, la **HomePlug Powerline Alliance**, che utilizza una tecnologia sviluppata dalla *Intellon* e prevede l’installazione di alcuni tool in ogni computer o su un apposito chip in ogni apparecchio che si voglia collegare in rete. La tecnologia utilizzata trasmette in bande al di sopra dei 4 MHz (zona ove si verificano i maggiori fenomeni di interferenza nella rete elettrica a 60 Hz) fino a 21 MHz utilizzando canali di comunicazione multipli in modo dinamico: in pratica si determina di volta in volta qual’è il canale meno rumoroso e a degradazione minore. La velocità di trasmissione arriva a 8 MBit/s e l’utilizzo principale di questo standard rimane quello di poter condividere informazioni tra nodi e utilizzare un comune accesso ad internet.

2.3 Radiofrequenza (wireless).

La radiofrequenza è la tecnologia per la trasmissione di dati e voce attualmente più studiata. In molte situazioni essa fornisce una soluzione conveniente ed economica per la costruzione di reti di dimensioni contenute. La tabella seguente riassume i concetti salienti:

Tabella I: Tecnologie wireless per reti di controllo

Nome	Applicazione	Caratteristiche	Banda di frequenza (GHz)	Tipo di modulazione	Bit rate (Mbit/s)	Organizzazione di specifica	Agenzia di certificazione
802.11 FH	Rete dati wireless	Opzione per la crittografia	2.4	FH (Frequency Hopping)	2	IEEE	WLIF (Wireless LAN Interoperability Forum)
802.11 DS	Rete dati wireless	Opzione per la crittografia	2.4	DS (Direct Sequenze)	2	IEEE	WLIF
High-speed 802.11	Wireless LAN ad alta velocità	Broadband	5	DMT/OFDM (Discrete MultiTone/ Orthogonal FDM)	6-54	IEEE	WECA (Wireless Ethernet Compatibility Alliance)
			2.4	DS	11		WLIF-WECA

HiperLAN BRAN (Broadband Radio Access Networks)	Wireless LAN multimediale ad alta velocità	Supporta voce, dati e video; può coesistere con WLAN a 2.4 GHz; certificabile in USA ed in Europa	5	GPSK (Gaussian Phase Shift Keying)	24	ETSI (European Telecommunications Standard Institute)
DECT (Digital Enhanced Cordless Telecomm.)	Voce e dati per case e piccoli uffici	Integra voce e dati	1.88-1.90	GFSK (Gaussian Frequency-Shift Keying)	1.152	ETSI
Shared Wireless Access Protocol	Comunicazione wireless per case e piccoli uffici	Basso costo	2.4	FH	2	HomeRF Working Group
Bluetooth	Standard per la radiofrequenza	Basso costo, corto raggio, supporta solo voce e dati	2.4	FH	1	Bluetooth Consortium

L'infrastruttura radiomobile attuale (TACS/ETACS e AMPS per la telefonia di prima generazione, GSM/DCS/PCS per quella di seconda generazione) dispone di un servizio dati a velocità molto basse, inutilizzabile per una rete di controllo; per questo sono stati studiati standard alternativi. Si tratta di HomeRf, Wi-Fi (altrimenti detto IEEE 802.11B) e Bluetooth.

HomeRf (sostenuto da *IBM*, *Motorola* e *Proxim*) usa una modulazione a *frequency hopping* e viaggia a 2 Mbit/s.

Wi-Fi (sostenuto da *Cisco System*, *3Com* e *Lucent Technologies*) usa la *direct sequence* dei dati, viaggia a 11 Mbit/s ed è più costoso rispetto ad HomeRf.

Infine **Bluetooth** (chiamato così per ricordare un re scandinavo vissuto nel decimo secolo che unificò sotto di sé numerosi reami danesi) è uno standard che si prefigge di conglobare tutta la radiofrequenza a corto raggio (reti di piccole e medie dimensioni) e far colloquiare tra loro dispositivi anche non connessi sulla stessa rete. In pratica si occupa di fare da bridge tra reti diverse tutte a radiofrequenza. E' sostenuto da *Intel*, *Ericsson* e *Nokia*).

Lo standard **IEEE 802.11** permette sia l'utilizzo di una modulazione DS che FH e con entrambe le tecniche si arriva ad un massimo bit rate di 2 Mbit/s. Tuttavia con la nuova release, che utilizza la codifica numerica CCK (Complementary Code Key), si può arrivare fino a 11 Mbit/s; resta però il problema che questo standard, inizialmente pensato per la telefonia cellulare, ha overhead molto alti.

Se poi si adopera la tecnologia LST (Layered Space-Time processing) si possono ottenere bit rate fino a 50-100 Mbit/s nella stessa banda di sistemi che prima al più potevano arrivare a 11 Mbit/s, e così si potrebbe pensare di utilizzare IEEE 802.11 per trasmissioni video e TV High Definition (HDTV). Utilizzando invece DMT (Discrete MultiTone) assieme a FDM si può arrivare a bit rate intorno a 6-54 Mbit/s. Queste due ultime soluzioni comunque sono ancora in fase di studio.

ETSI supporta due protocolli: HiperLAN, per il traffico ad alta velocità e DECT che invece opera a velocità inferiori.

HiperLAN, che in futuro si chiamerà **BRAN**, altro non è che una collezione di specifiche per reti operanti a 5 GHz con bit rate fino a 24 Mbit/s (sufficienti per la televisione ad alta definizione). Non è ancora certa l'applicabilità di questo standard agli Stati Uniti in quanto la sua frequenza di lavoro è già occupata.

DECT opera invece tra 1.88 e 1.99 GHz, ha un bit rate di 1.152 Mbit/s ed è stato progettato principalmente per la voce umana; *British Telecommunications* sta cercando di adattarlo alla trasmissione dati.

2.4 Standard di trasmissione per mezzi eterogenei.

EIB è uno standard europeo risalente ai primi anni novanta ed è proprietà della European Installation Bus Association cui sono associate o affiliate più di cento aziende europee (tra cui *ABB*, *Siemens*, *Vimar*, *Gewiss*, *Philips*). I prodotti di recente sviluppo vengono certificati da appositi laboratori. Sono supportati vari mezzi trasmissivi: il doppino, le onde convogliate, la radiofrequenza e Ethernet; possono essere collegati in rete fino a 61455 dispositivi.

EHS è l'acronimo di European Home System, uno standard sviluppato a partire dal 1987 nell'ambito dei programmi europei Eureka ed Esprit. È aperto e prevede una certificazione dei nuovi prodotti. Supporta vari mezzi trasmissivi: il doppino, le onde convogliate, il cavo coassiale, la radiofrequenza, i raggi infrarossi. Un unico sistema può gestire fino a 1012 indirizzi.

Poi abbiamo **BAtiBUS**, uno standard europeo che comprende più di 80 aziende (tra cui *Merlin Gerin*, *Airlec*, *EDF*, *Landis&Gir*). Esso implementa un protocollo di comunicazione

aperto diffuso nel 1989 e supporta vari mezzi trasmissivi: il doppino, la radiofrequenza e i raggi infrarossi. La velocità di trasmissione è di 4800 baud.

Anche **KONNEX** è uno standard tecnologico europeo. Mira ad integrare tutti i sistemi bus per la home and building automation. Nasce dalla convergenza di EIB, Batibus ed EHS. Permette la gestione di oltre 40.000 dispositivi "intelligenti" all'interno di un unico impianto.

LONWORKS è uno standard nato nel 1990 (a partire da X-10 e da EIA 709) di proprietà della americana *Echelon*. Chiunque può sviluppare prodotti che utilizzino LONWORKS, ma questi dovranno poi essere certificati. Si tratta di uno standard diffuso a livello mondiale e utilizzato da più di 4000 aziende (tra cui anche le italiane *Merloni* ed *ENEL*). I moduli sparsi in tutto il mondo sono 9 milioni, di cui il 20% utilizzato nelle case. Tra i mezzi trasmissivi che si possono utilizzare abbiamo il TP5, le onde convogliate, il cavo coassiale, la radiofrequenza, i raggi infrarossi e le fibre ottiche. Attraverso LONWORKS è anche possibile controllare il consumo energetico di ogni singolo apparecchio, permettendo risparmi anche dell'ordine del 10-30% e la gestione di scenari di sovraccarico elettrico e blackout.

Infine **HAVi** (Home Audio Video interoperability) è un middleware sviluppato da un insieme di aziende per facilitare l'interoperabilità fra apparecchi realizzati da industrie diverse, in modo da costruire più facilmente applicazioni distribuite per reti di controllo.

E' costituito dall' insieme di API e servizi e dal protocollo di rete IEEE 1394 (high performance serial bus). Realizza un ambiente peer to peer, dove ogni device può scoprire, interrogare e controllare ogni altro apparecchio, inoltre gruppi di dispositivi possono anche cooperare tra loro. HAVi riconosce quattro categorie di apparecchi elettronici: FAV (Full AV), IAV (Intermediate AV), BAV (Base AV), LAV (Legacy AV). FAV e IAV fungono da controllori, mentre BAV e LAV possono essere solamente controllati. I servizi di sistema supportati sono i seguenti:

- *Discovery*. Segnala quando i device sono aggiunti o rimossi dalla rete.
- *Messaging*. Stabilisce uno schema di indirizzamento e si occupa del trasferimento di messaggi.
- *Lookup*. Fornisce il servizio di ricerca di informazioni per applicazioni e device.
- *Events*. Implementa un sistema di eventi distribuiti in grado di scatenare specifiche azioni software.
- *Streaming*. Fornisce il servizio di data stream.

- *Reservation*. Permette alle applicazioni di riservare dei device; inoltre si ha la possibilità di realizzare azioni programmate, come per esempio sintonizzarsi e registrare un programma televisivo ad una specifica ora.
- *User interaction*. Permette la realizzazione di interfacce utente.

Infine **JINI** è una tecnologia basata su Java. Permette di ottenere un vero ambiente Plug & Play. Infatti mediante una specifica procedura di registrazione ogni dispositivo che si affacci alla rete per la prima volta si annuncia agli altri già presenti e pone in condivisione le proprie risorse. Ogni procedura è supervisionata da un servizio di look up che risponde a criteri di sicurezza. Altro importante vantaggio è il ridotto impegno di memoria che permette a Jini di essere installato a bordo dei microchip di quasi tutti i dispositivi elettronici di uso comune.

2.5 Reti di controllo e Internet.

Si è fatto molto parlare, dopo la “rivelazione” di internet, della sua applicabilità alle nostre azioni quotidiane. Effettivamente la potenza di questo strumento non è nella reale innovazione tecnica (intesa in senso puro) apportata, ma riguarda piuttosto il modo di re-interpretare i contorni tradizionali della comunicazione, in quanto esso consente nuove possibilità per gli utenti (non tecnici) medi.

Posto che la tecnologia alla base di internet è conosciuta da oltre venticinque anni, cosa ha allora innescato il processo esplosivo di espansione avvenuto negli ultimi anni? La risposta a questa domanda è importante per capire in che direzione si sta andando e quali campi saranno interessati in questo percorso nel prossimo futuro. Sono in molti a credere che il potenziale di internet sia stato sfruttato solo in minima parte finora.

Il “sogno” del *World Wide Web* ha essenzialmente permesso alla gente di raggiungere facilmente ed a basso costo altra gente. La posta elettronica, discutibilmente l'applicazione più popolare di internet, si è trasformata in uno strumento indispensabile per molte attività commerciali ma anche per molte famiglie. Ma senza andare molto lontano, basta dire che il numero di nuove aziende e di nuovi individui in qualche modo in grado di affacciarsi al Web sta incrementandosi ad un ritmo stupefacente e tutto ciò grazie alla facilità di entrare in contatto e rimanervi. E’ una rivoluzione della comunicazione senza precedenti.

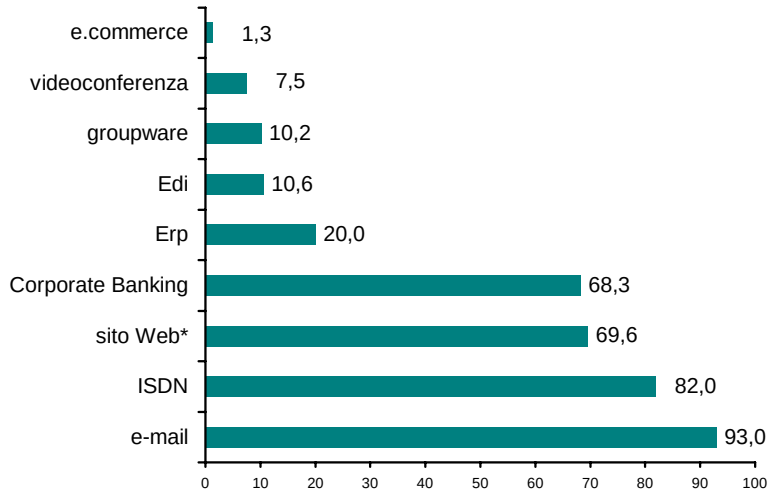


Figura 6. : Alcuni "numeri" di internet (fonte osservatorio TeDIS).

Nell'ultimo periodo, dunque, l'attenzione si sta spostando su quello che è possibile fare sfruttando le enormi potenzialità di questo strumento così versatile.

L'idea è che applicazioni piccole, che eseguono operazioni specifiche, possano connettersi ad internet per svolgere alcune particolari task. Alla base c'è sostanzialmente un concetto analogo rispetto a quello di accedere ad internet per mettere in contatto persone tramite un personal computer, ma è necessaria una quantità di hardware di gran lunga inferiore e quindi i costi per l'utente finale risultano ben più contenuti.

E' possibile seguire un ragionamento semplice. Visto che le potenzialità di internet sono in grado di sostenere senza difficoltà ulteriori carichi informativi, è certamente proponibile la possibilità di andare oltre i personal computer e coinvolgere in qualche modo gli apparecchi intorno a noi. I dispositivi di uso giornaliero, luci, interruttori, termostati, TV, condizionatori d'aria, sistemi di sicurezza, segnalatori di incendio, possono tutti essere pensati come futuri client per internet.

In linea di principio questa idea può essere realizzata semplicemente assegnando degli indirizzi IP unici a tutti questi dispositivi resi appena un po' più intelligenti con l'ausilio di un chip e dotandoli anche di un piccolo web server integrato. Così facendo, per mezzo di un semplice browser sul www, si potrebbero monitorare i dispositivi controllandone i parametri.

In realtà questa idea apparentemente semplice ha molti limiti pratici. La tecnologia alla base di internet non è nata per collegare insieme degli apparecchi. Dispositivi di controllo piccoli e a basso costo hanno un proprio insieme unico di caratteristiche molto differenti da quelle del mondo dei calcolatori. E' necessario, dunque, introdurre delle variazioni nell'architettura di rete al livello più alto della gerarchia OSI, quello applicativo.

Noi sappiamo, in base a quanto detto nei paragrafi precedenti, che le reti di controllo connettono insieme dispositivi intelligenti per implementare sistemi attivi e distribuiti fornendo una piattaforma a basso costo, affidabile e flessibile, ottimizzata in base alle specifiche di controllo. Ora, però, bisogna fare un passo avanti.

Dunque sembra abbastanza naturale estendere il paradigma alla base del web ai dispositivi di controllo, ma è inutile nascondere che l'obiettivo ultimo è la fusione di reti dati e reti di controllo a formare un sistema organico, omogeneo ed universale. Così come le varie intranet si sono trasformate in una serie di propaggini di internet, le reti di controllo locali, le cosiddette ***infranet***, potrebbero seguire lo stesso destino per permettere alle informazioni (dati e controllo) di fluire in maniera bidirezionale da qualcuno a qualcosa. Sarebbe una vera rivoluzione poter raggiungere gli oggetti così come oggi si raggiungono dei soggetti. La realtà mostra già i primi segni di uno sviluppo in questa direzione, tuttavia si è ancora molto lontani da una diffusione e da una accettazione universale di questo genere di idee.

La figura che segue sintetizza questi concetti. Essa mostra l'infrastruttura completa delle informazioni.

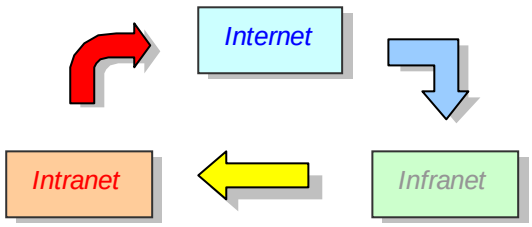


Figura 7. : Infrastruttura delle informazioni completa.

L'idea che gli apparecchi di uso quotidiano potessero essere collegati ad internet è sembrata logica a molti analisti. Siamo circondati di dispositivi "carichi" di elettronica e, d'altra parte, visto il trend con cui sta aumentando il numero di utenti del World Wide Web, legare insieme questi mondi sembrerebbe quasi una misura naturale. Bene, è certamente così, tuttavia la fusione di questi due universi è stata rallentata negli anni passati da alcuni ostacoli tecnici.

Oltre a questo internet e le intranet hanno cominciato ad essere accettati in maniera universale e a subire uno sviluppo e una larga diffusione solo quando c'è stato uno standard universale e di facile impiego per il loro utilizzo. La crescita in termini di aumento dei contenuti (aumento dei siti web), ha avuto poi un effetto promozionale ulteriore. Il www e la diffusione capillare dei browser commerciali (oggi parte integrante del pacchetto software di un sistema operativo) hanno fornito lo slancio per consentire di iniziare a risolvere i limiti tecnici e studiare soluzioni alternative.

Le reti di controllo, dal canto loro, sono relativamente nuove. E nel loro caso, prima di ogni altra cosa, esiste l'esigenza di normalizzare la comunicazione tra dispositivi e rispettive applicazioni. Gli standard per il World Wide Web si appoggiano sul protocollo di TCP/IP, sul protocollo HTTP e sul linguaggio HTML; ogni componente lavora insieme agli altri in maniera organica e armoniosa. Il mondo dei controlli, invece, sta ancora stabilendo norme e tecnologie standard per cui solo quando questa fase sarà ultimata si potrà andare oltre.

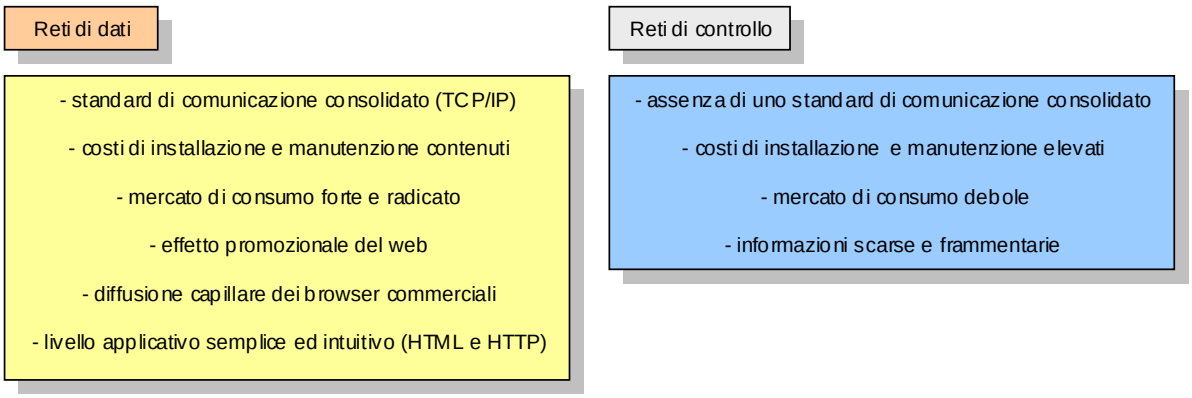


Figura 8. . Punti di forza delle reti di dati e di debolezza delle reti di controllo.

Nella analisi che segue si tenterà di gettare un ponte virtuale fra internet ed il mondo dei controlli valutando i requisiti necessari ad una unione che mantenga un successo duraturo.

2.6 Integrazione tra dati e controllo.

I sistemi integrati dati-controllo (che da ora in avanti chiameremo semplicemente sistemi integrati) sono stati usati tradizionalmente in applicazioni quali l'automazione di processi di controllo all'interno di industrie ove era necessaria una unità centrale dotata di elevata potenza computazionale per fare funzionare il processo o alcune parti di esso. Nella maggior parte dei casi, i requisiti operativi, quali l'interfaccia grafica per l'utente (la cosiddetta *Graphical User Interface* o *GUI*) o le prestazioni in tempo reale del sistema, erano talmente specifici da non consentire per questi scopi l'uso di un PC desktop generico.

Nucleo centrale di elaborazione in sistemi integrati è il *microcontroller* e i maggiori costruttori di circuiti integrati hanno dedicato intere famiglie di prodotti a questo tipo di chip. Lo sviluppo dei microcontrollori dal punto di vista tecnologico è stato significativamente più veloce rispetto a quello dei microprocessori tradizionali, ma il volume d'affari complessivo di

questi ultimi ha letteralmente fagocitato il mercato dei primi. Dal punto di vista delle vendite, le applicazioni per sistemi integrati possono appartenere ad una delle due categorie seguenti: ***consumer*** o **commerciale**.

I sistemi integrati commerciali vengono adoperati in applicazioni come l'automazione degli edifici, il controllo dei processi e l'automazione nelle industrie. Tipicamente, questi apparati sono composti da una stazione centrale di elaborazione che mantiene il collegamento con un gran numero di sensori e attuatori fisici durante tutta la fase di funzionamento. Si può dire che il mercato dei sistemi integrati per applicazioni commerciali sia diventato ragionevolmente maturo negli ultimi dieci anni. Se si volesse impiantare un sistema, si avrebbe a disposizione una vasta gamma di microcontrollori con requisiti di calcolo differenti (8, 16 e 32 bit) equipaggiati con banchi di memoria, timer, sezioni di I/O e molto altro. Oltre a questo, poi, la complessità di tali sistemi insieme alle necessità di affidabilità ed ai requisiti operativi per il *real time* ha generato un mercato parallelo per i sistemi operativi (i cosiddetti *Real Time Operating System* o *RTOS*).

Per quanto riguarda invece il mercato di consumo, solo recentemente si stanno comprendendo le reali possibilità dei sistemi integrati dati-controllo. L'impulso alla costruzione di dispositivi di controllo consumer è stato il pesante abbassamento dei costi e la straordinaria miniaturizzazione dei componenti. I microcontrollori di bassa e media capacità computazionale (4, 8 e 16 bit) sono riusciti a fare il loro ingresso all'interno di forni a microonde, termostati, videocamere e di molti altri apparecchi di uso comune.

Diversamente da quanto accade per il mercato commerciale, il processo di sviluppo del software per i dispositivi consumer non risulta ancora standardizzato. Le applicazioni relative, infatti, mancano di un sistema operativo organico a causa della forte richiesta di prodotti sempre più piccoli e sempre meno costosi; questo spinge a rivedere e modificare a scadenza regolare gli standard costruttivi a detrimento di una impostazione comune.

Passando dai problemi strutturali all'aspetto applicativo, dovremo porre una distinzione di massima tra applicazioni integrate centralizzate (o *standalone*) e applicazioni distribuite.

Le **applicazioni dati-controllo centralizzate** vengono allocate in maniera statica e svolgono funzioni molto precise. Esse non sono in grado di comunicare in maniera flessibile con applicazioni di altri dispositivi, ma possono impartire ordini a distanza a sensori ed attuatori collegati ad una unità centrale principale. Un sistema di sicurezza domestica e un sistema centralizzato per il controllo di processi sono da considerarsi esempi di sistemi integrati standalone. La maggior parte di queste applicazioni si basa solitamente su RTOS commerciali (per esempio Microsoft Windows CE).

Al contrario le **applicazioni dati-controllo distribuite** si basano su di una infrastruttura orizzontale che rende la loro impostazione interna profondamente diversa. Non

è richiesto alcun nucleo di intelligenza centralizzato che sovrintenda al funzionamento del sistema, ma esiste solo un canale fisico ed una serie di nodi intelligenti che lo utilizzano per la comunicazione.

La Figura seguente riassume in una rappresentazione bidimensionale il mondo dei sistemi integrati.

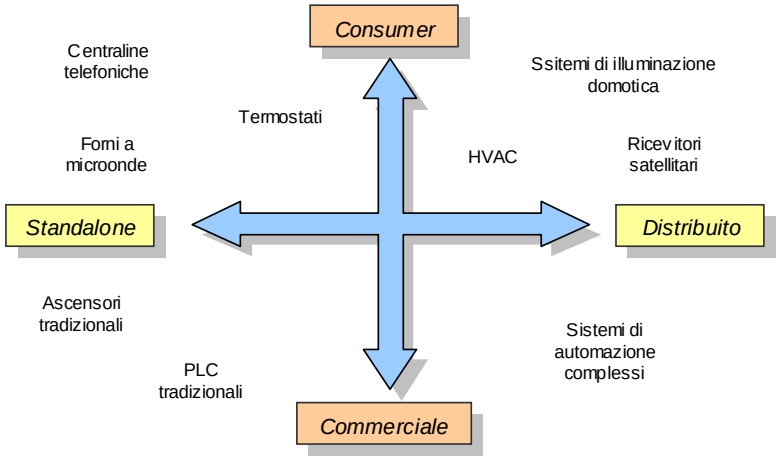


Figura 9. : Il mondo dei sistemi integrati

Come si può vedere dalla figura, il mercato dei sistemi integrati a destinazione commerciale è stato il cuore della transizione tra le architetture standalone e le architetture distribuite. I progressi nelle tecnologie per il control networking hanno notevolmente accelerato la transizione dai sistemi centralizzati basati su RTOS a quelli distribuiti in rete.

Le applicazioni centralizzate e quelle distribuite sono di solito mutuamente esclusive nel senso che ciascuna possiede un proprio set di tool e si basa su tecnologie proprie. Sebbene sempre più prodotti consumer stiano scoprendo l'impostazione distribuita, ci sono ancora molte applicazioni che invece non sono affatto distribuite. Un sistema domotico moderno per il trattamento dell'aria consiste in una serie di nodi intelligenti (termostati, caldaie, condizionatori, convettori, ecc.) che comunicano a vicenda utilizzando ad esempio la linea elettrica e rappresenta un caso di impostazione distribuita, mentre i più utilizzati sistemi per il governo di catene di montaggio sono sicuramente standalone.

Figura 10. : Le reti integrate dati - controllo contengono una componente di comunicazione una di computazione ed una di controllo.

Tuttavia possiamo dire senza tema di smentita che, a parte quelle applicazioni consumer integrate che non possono essere distribuite per loro natura (ad esempio quelle che sono fisicamente centralizzate), quasi tutte le applicazioni che in precedenza erano implementate per mezzo di architetture centralizzate possono essere reimpostate in modo orizzontale, con costi di sistema più bassi, con un miglioramento delle funzionalità e con un aumento della flessibilità. Così come avviene nel caso dei calcolatori, ci sono una serie di vantaggi nel risolvere problemi di controllo utilizzando le reti; in particolare ricordiamo i più significativi:

- eliminazione dei *single point of failure*
- riduzione dei costi di cablaggio
- riduzione dei costi di installazione e manutenzione del sistema
- interoperatività tra dispositivi di costruttori differenti

E' evidente dunque che i benefici del networking non sono limitati al solo mondo dei calcolatori. Quando avremo reti di controllo ovunque intorno noi, posto che internet e le intranet rappresentano delle realtà ampiamente consolidate, la cosa che sembrerà più logica da fare sarà pensare ad aggregare queste strutture a costituire un unico sistema globale di dati e controllo.

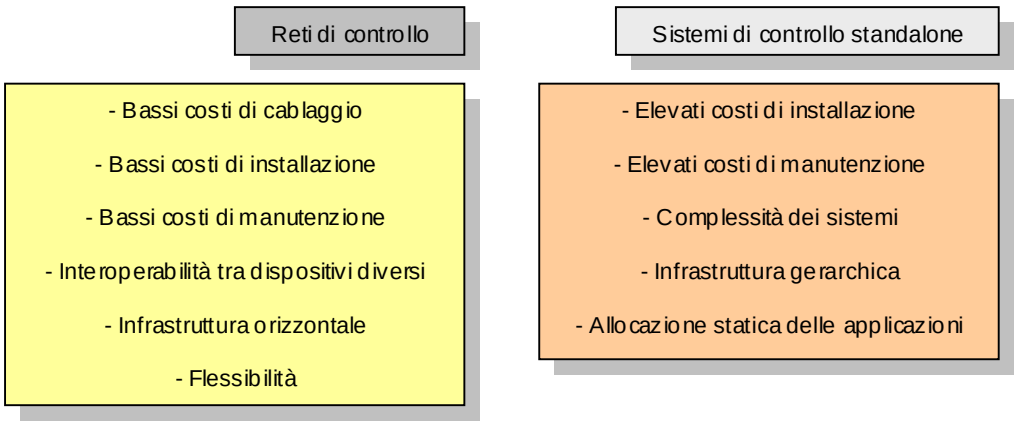


Figura 11. : Confronto tra reti di controllo distribuite e sistemi standalone.

2.7 Conclusioni.

Visti i progressi delle tecnologie di networking degli ultimi anni e la riduzione dei costi connessi alla produzione dei circuiti integrati, è oggi tecnicamente matura la creazione di generiche reti di informazioni atte a veicolare senza distinzioni dati puri e messaggi di controllo.

Così come è successo alcuni anni fa per i sistemi di dati, anche per quelli di controllo la tendenza è verso la decentralizzazione. Ma c'è di più. Quando entrambi i sistemi saranno pronti (e uno dei due lo è già) la loro fusione sarà l'evoluzione naturale. Internet, le intranet e le infranet dispongono dei mezzi tecnologici per operare insieme; l'obiettivo finale dovrà essere quello di permettere alla gente di mantenersi in contatto con oggetti altrettanto facilmente di come oggi può mantenersi in contatto con altra gente.

Così come è accaduto per il mondo dei calcolatori, i benefici derivanti dall'approccio di rete (vale a dire ridotti tempi di sviluppo, aumento delle funzionalità e dell'affidabilità di calcolo, interoperabilità, semplificazione dell'aggiornamento e della manutenzione dei sistemi e molto altro) hanno soltanto aperto le porte ad un progetto a lungo termine che vedrà una gerarchia logica di reti. L'interconnessione di esse genererà un sistema globale di dati e controllo - qualcosa di molto più complesso e organico della somma di parti diverse.