Integrazione e controllo nella Domotica

Introduzione

I primi bus, intesi come connettori per i componenti di un sistema complesso, risalgono agli anni '60, quando venne sviluppato il primo computer e sorgeva così il problema della connsessione dei sui componenti elettronici interni mirato allo scambio di dati. In seguito il concetto fu esteso al collegamento esterno fra più computer per condividere risorse o scambiare informazioni.
La domotica intesa come integrazione di servizi atti a migliorare l'esperienza di vita degli utenti nell'ambiente che in cui vivono (che sia abitativo o lavorativo), soffre del classico problema di cui soffrono tutte le tecnologie che hanno vissuto una adozione a singhiozzo, come eterne speranze che faticano a trovare un posto, vuoi per problemi di costo, di non comprensione da parte delle masse per una adozione su larga scala (comunque legato alla questione monetaria) o per problemi di carattere tecnico. In questo gruppo di problemi se ne può facilmente individuare uno che rende di importanza fondamentale l'integrazione fra diversi protocolli: il sovraffollamento di standard.
Avere troppi standard è come non averne nessuno, la gestazione prolungata del processo di adesione alla domotica da parte del mercato ha fatto si che a più riprese venissero presentati come standard universali protocolli che non lo erano affatto, che si sono, col tempo, ritagliati si una piccola fetta, la propria nicchia nel mercato, finora piccolo, dell'automazione per la casa, ma che non permettevano in maniera semplice l'integrazione dei propri dispositivi con quelli di altri costruttori, rendendo così molto confuso, costoso e poco appetibile la soluzione automatizzata rispetto a quella classica.
La poca sensibilità riscontrata nell'utenza, figlia della scarsa interoperabilità fra i diversi protocolli e dispositivi disponibili sul mercato, sembra tenere ancora lontano il momento dell'esplosione di questo mercato che avrebbe già ora le potenzialità di rendere sempre migliore il vivere la propria abitazione, innalzando il livello di qualità della nostra vita attraverso i tre obiettivi principali qui riassunti:

- Innalzamento del livello di comfort: fondamentale nel caso di utenti disabili
- Ricerca del risparmio energetico: bilanciamento del carico
- Maggiore sicurezza: incolumità dell'utente

L'utente finale però non comprende, vuoi per la difficoltà dei temi trattati, la necessità di acquistare prodotti domotici rispetto a quelli tradizionali. “Infatti i potenziali benefici che deriverebbero dall’acquisto di questi prodotti non riescono a giustificare uno sforzo economico maggiore, per quanto l’introduzione di intelligenza, intesa come capacità di calcolo, all’interno di un qualsiasi dispositivo, comporti costi aggiuntivi sempre più esigui.
Inoltre, a causa della scarsa interoperabilità tra i vari standard, per sfruttare a pieno i benefici della domotica, l’utente sarebbe costretto ad acquistare solo i prodotti conformi ad un particolare sistema. Ciò potrebbe verificarsi solo in due condizioni: l’acquisto contemporaneo di tutti i dispositivi presenti nell’edificio, oppure una cognizione tecnica dello standard utilizzato mirata all'acquisto di ulteriori dispositivi conformi ad esso. Entrambe le condizioni sono però di difficile realizzazione, dal momento che nella maggior parte dei casi, l’ambiente domestico è molto dinamico: la topologia e la dislocazione dei suoi elementi cambiano frequentemente e i dispositivi vengono acquistati in momenti diversi. Si pensi, ad esempio, agli elettrodomestici: è quantomeno raro che tutti quelli presenti in una abitazione siano acquistati contemporaneamente, e comunque si tratta di oggetti che nel tempo finiscono con il deteriorarsi, usurarsi e diventare obsoleti.
Per comprendere meglio queste limitazioni è di aiuto un esempio classico di applicazione domotica: si supponga di avere una caffettiera che possa essere accesa tramite una radiosveglia ad un’ora prestabilita. Se la radiosveglia e la caffettiera parlano la stessa lingua, ossia sono entrambe conformi al medesimo standard, ogni mattina sarà possibile avere il caffè pronto appena svegli. Tuttavia, se per qualsiasi motivo, uno dei due dispositivi deve essere cambiato, sarà necessario rimpiazzarlo con un altro conforme allo stesso standard.
Sarebbe invece auspicabile permettere all’utente di scegliere i dispositivi indipendentemente dallo

standard cui appartengono: in questo modo l'utente non dovrebbe minimamente conoscerne le specifiche tecniche, ma potrebbe esclusivamente trarne tutti i possibili benefici.
Lo sforzo di quella parte della comunità scientifica che si occupa di domotica è teso, dunque, a infondere la necessaria sensibilizzazione affinché si affermi definitivamente l'impiego di queste tecnologie." (cit. Tesi Domonet, Dario Russo)
In questi anni si è così aperta una nuova via che potesse permettere l'adozione della domotica nelle case, alcuni produttori hanno iniziato a collaborare per portare una maggiore integrazione fra dispositivi di diverse marche, dando così l'impressione di aver compreso quanto fosse inutile ai fini dell'adozione di massa continuare sulla strada del farsi il proprio piccolo, magari anche perfetto, standard in casa. Uno dei maggiori esempi di questa visione è dato dallo standard EIB/KNX, in cui alcuni grossi produttori di materiale elettrico (Siemens, ABB, bticino, insomma i favoriti dagli elettricisti che, ricordo, sono i primi a poter scegliere e proporre ai loro clienti, che siano utente finale o costruttore di immobili, soluzioni basate sulla domotica piuttosto che sul classico impianto elettrico, gli architetti tendono ancora a percepire l'automazione casalinga come un giocattolone da suggerire solo ai clienti più facoltosi) si sono trovati per collaborare e definire uno standard che una intera linea di loro prodotti, in questo modo completamente intercambiabili, possa usare. Nacque così il consorzio Konnex, anche se a mio avviso un po' troppo in ritardo sui tempi ed ora in rincorsa rispetto alla moltitudine di standard di nicchia che si sono affermati nel tempo nelle diverse aree che costituiscono l'ambiente casa (riscaldamento e climatizzazione, luci, sicurezza, etc...).
Proprio per evitare questa rincorsa, si è aperta un'ulteriore strada: lo sviluppo di piattaforme per l'integrazione di diversi standard. Un primo input è stato fornito direttamente dai creatori della miriade di standard che si stavano producendo, questi, capendo che un mondo cieco, sordo e muto verso il resto della casa era, oltre che un errore progettuale, anche un forte stop alla adozione di massa dei loro prodotti (parallelamente a quello che successe nel mondo dei computer negli anni ottanta, in cui la proposta di hardware compatibile in maniera intercambiabile, l'ormai classico hardware per pc, favorì l'adozione del personal computer nelle case degli utenti, se l'informatica si fosse chiusa nel mondo dei mainframe, i prezzi non si sarebbero abbassati e saremmo ancora qui a comprare pezzi da un unico produttore a prezzi troppo alti), iniziarono a creare interfacce hardware verso altri standard, che collegano fisicamente diversi bus preoccupandosi dell'accoppiamento dei livelli elettrici e delle altre grandezze fisiche, in modo da poter inviare comandi del protocollo giusto per far eseguire ai dispositivi degli altri bus i loro compiti. In questa architettura mista diventa sempre più importante l'apporto dei programmatori intesi non solo come configuratori dei dispositivi che compongono il bus, ma anche come integratori e supervisori, in questo scenario diviene cosi importante avere una chiara visione di insieme del progetto e del sistema in modo da poter creare scenari e semplificazioni nella vita dell'utente anche in sistemi eterogenei.
I bus tendono sempre più ad assumere una conformazione distribuita, con ogni dispositivo che sa cosa deve fare e come relazionarsi con gli altri dispositivi sulla stessa maglia, distinguendosi così, in maniera diametralmente opposta dalle prime architetture domotiche, completamente centralizzate e controllate da un processore, un server, che mantiene al suo interno tutta la logica dell'applicazione. Il punto di contatto fra le due visioni sembra diventare sempre di più lo scenario preferito per l'integrazione delle varie tecnologie fino a quando un vero standard unitario verrà seguito, forse in una visione troppo utopistica, da tutti i produttori. In questa situazione l'informatico può facilmente inserirsi sviluppando software di supervisione che possono essere semidistribuiti su alcuni controllori che gestiscono in maniera coesa e unitaria gli eventi intra e interbus. I dispositivi vengono così programmati logicamente per vivere all'interno del proprio microcosmo/bus, interagendo gli uni con gli altri, ma non potendo, per limitazioni intrinseche alla pochezza dell'hardware che ne fornisce intelligenza, interloquire direttamente anche con dispositivi che parlano una lingua diversa, questo fa si che, a maglie, il sistema sia completamente autogestito, ma non concertato con gli altri sistemi. Per fornire un livello di integrazione maggiore si inseriscono così i controllori multiprotocollo che sfruttano le interfacce che i vari creatori dei bus hanno reso disponibili per dialogare con infrastrutture standard (in questo caso veramente riconosciute e accettate dalla comunità intera, siano esse reti ethernet, rs232 o usb), per fornire un livello di

gestione superiore, che si preoccupa di monitorare i livelli inferiori e comandarli, dando una parvenza di unità fra i diversi sistemi. L'informatico deve così conoscere tutti i supporti di trasmissione e i protocolli di comunicazione dei diversi dispositivi così come le interfacce fra i bus ed infine progettare tenendo bene a mente le interazioni fra i sistemi, questo potrà farlo in accordo con i progettisti della parte elettrica, da cui ci si aspettano schemi dettagliati delle connessioni logiche fra i dispositivi, le quali porteranno alla naturale creazione di scenari ed altre facilitazioni per l'utilizzatore finale.
Proprio ad esso deve poi essere rivolta la cura maggiore nella progettazione usabilità delle interfacce utente. Come l'ingegneria del software insegna, la progettazione della vista è importante quanto la logica che viene poi mossa dalle azioni che la innescano, lo studio di usabilità deve essere centrale per evitare che i sistemi installati divengano più un problema che un aiuto e questo è tanto vero nelle installazioni che fanno largo uso di pannelli touchscreen, quanto in quelle in cui l'utente interagisce semplicemente attraverso pulsantiere, il progettista deve così avere una grande capacità di sublimare le molte azioni che possono tornare utili nella fruizione dell'impianto in pochi e intuitivi movimenti dell'utente, qui sta la maggiore difficoltà nella progettazione, la logica dei singoli dispositivi è fredda e non deve trasparire nuda e cruda nel normale utilizzo, è impensabile che un uomo utilizzi la casa in questo modo. Il progettista deve caricarsi della complessità del sistema individuando, quindi, quali funzionalità esporre e come raggruppare sensatamente molte funzioni in pochi gesti.
Si arriva così dalla completa integrazione dei moduli ed alla gestione integrata dei servizi.
Oggi l'automazione si rivolge a due mercati, gli edifici e gli impianti industriali, mentre nella seconda la produzione è il fine ultimo, la prima è rivolta all'uomo.
Tutte queste considerazioni portano intrinsecamente a un cambiamento nel modo di progettare gli impianti, riducendo al minimo i cablaggi e spostando la complessità a un livello superiore.
Il bus di controllo, un semplice mezzo per interconnettere funzionalmente i dispositivi, sostituirà i cavi ed il progettista dovrà possedere una conoscenza di base dei principi e delle caratteristiche di trasmissione dei dati, in modo da poter scegliere tra i diversi supporti di comunicazione.
Inoltre, il cablaggio manuale sarà sostituito da una fase di indirizzamento e di programmazione che richiederanno la conoscenza dei dispositivi hardware e software. Infine, nei sistemi più estesi, potrà essere necessaria la connessione tra diversi sistemi bus richiedendo l'installazione di opportune interfacce e, di conseguenza, la familiarità con i problemi relativi.
L'automazione degli edifici può connettere i sistemi di illuminazione, telecomunicazione, riscaldamento, aria condizionata, sicurezza, gestione dei carichi ed intrattenimento in un unico sistema di controllo. In più, consentendo alla rete di controllo dell'edificio di estendersi al di fuori dei limiti dell'edificio, possono essere offerti nuovi servizi a valore aggiunto e nuove funzioni.
La comunicazione sta progressivamente diventando diretta, disposta orizzontalmente al livello del campo e nello stesso tempo verticalmente attraverso tutti i livelli gerarchici.
I middleware domotici si possono dividere in due grandi classi che differiscono sostanzialmente per il sistema di comunicazione usato: una, più tradizionale, fa uso di un sistema bus, l'altra, più recente, si basa su un insieme di protocolli più evoluto come TCP/IP. Del primo tipo fanno parte standard oramai consolidati nel mondo della domotica, quali ad esempio X10, EIB, BatiBus, EHS, Konnex, LonWorks, CEBus, C-Bus, la seconda tipologia invece include, tra gli altri, standard come UPnP, Jini, OSGi.
A fianco di un particolare sistema di comunicazione, è disponibile un numero sempre maggiore di standard che si basano su mezzi trasmissivi diversi, come IEEE 802.11b (Wi-Fi), Bluetooth, IEEE 1394 (Firewire), IrDA, ZigBee, etc.

Tecnologie e protocolli dello strato fisico

La direzione che verrà intrapresa nel mondo della domotica non potrà comunque prescindere dall'esistenza dei protocolli che oggi vengono installati, ovviamente stilare una lista di caratteristiche e funzionalità di tutti quelli rintracciabili sul mercato non è di nessuna utilità, molti di essi vengono presentati e usati solo a livello locale da piccole aziende che, sfruttando l'onda della novità e sperando di guadagnare dal marasma iniziale si sono buttate nella realizzazione di propri progetti di domotica dalla breve vita e dall'applicazione e installazione spazialmente circoscritta alla zona di appartenenza della ditta stessa.
In questo capitolo si cercherà di fornire una panoramica dei protocolli e delle tecnologie più utilizzate oggi o dalle maggiori potenzialità di impiego futuro, spiegandone, ove individuabile, l'area di maggiore implementazione.

Infrarossi

Questa versatile tecnologia viene utilizzata in moltissimi campi, quello di interesse per la domotica è l'ambito della comunicazione.
I dispositivi che possono essere comandati via infrarossi devono sottostare allo standard definito e mantenuto dalla IrDA.
La trasmissione dell'informazione avviene per modulazione, per esempio la codifica del dato potrebbe essere fornita dalla presenza (ON) o assenza (OFF) della radiazione emessa dal LED, il ricevitore trasforma la radiazione in corrente elettrica attraverso un fotodiodo. Il ricevente filtra le lente radiazioni naturali e risponde solo a veloci pulsazioni.

Ethernet

Questo protocollo per reti locali vanta il maggior installato fra tutti quelli che verranno presentati in questa trattazione, divenendo di fatto uno standard per la comunicazione universalmente riconosciuto. Il nome deriva dal concetto fisico dell'etere.
Le tecnologie nel loro insieme definiscono una serie di standard di cablaggio e di segnale e vari protocolli dello strato fisico e data link ed un formato di indirizzamento comune.
Venne studiato un gruppo di imprese, costituito da Xerox Corporation, Intel Corporation e Digital Equipment Corporation, che nel 1978 portarono alla standardizzazione 802.3 e il 30 settembre 1980 a pubblicare la versione 1.0 dello standard Ethernet.
Successivamente, l'interesse delle imprese del settore aumentò al punto che l'IEEE costituì alcuni gruppi di studio finalizzati a perfezionare e consolidare Ethernet, nonché a creare numerosi altri standard correlati. Uno dei risultati raggiunti fu la pubblicazione, nel 1985, della prima versione dello standard IEEE 802.3, basato sull'originale specifica Ethernet, ma non completamente identificabile con essa. In seguito, lo standard Ethernet come tale non è più stato mantenuto, ma il termine continua ad essere usato quasi come fosse un sinonimo di IEEE 802.3, sebbene i due standard non coincidano affatto.
Ethernet attualmente è il sistema LAN più diffuso per diverse ragioni:

- È nata molto presto e si è diffusa velocemente per cui l'uscita di nuove tecnologie come FDDI e ATM hanno trovato il campo occupato;
- Rispetto ai sistemi concorrenti è più economica e facile da usare e la diffusione delle componenti hardware ne facilitano l'adozione;
- Funziona bene e genera pochi problemi (cosa rara nel campo informatico);
- È adeguata all'utilizzo con TCP/IP;
- Nonostante i suoi concorrenti fossero più veloci nella trasmissione dati, la Ethernet era comunque sufficientemente appetibile per essere adottata su larga scala.

Nonostante Ethernet abbia diverse tipologie, l'elemento comune è nella struttura del frame, ricevuto dallo strato fisico della pila ISO/OSI, che viene definito DIX (DEC, Intel, Xerox) ed è rimasto fedele alla versione originale i cui elementi sono:

- Preamble - Preambolo (8 byte): I primi 7 byte hanno valore 10101010 e servono a svegliare gli adattatori del ricevente e a sincronizzare gli oscillatori con quelli del mittente. L'ultimo byte ha valore 10101011 e la serie dei due bit a 1 indica al destinatario che sta arrivando del contenuto importante;
- Destination MAC address - Indirizzo di destinazione (6 byte): Questo campo contiene l'indirizzo LAN dell'adattatore di destinazione, se l'indirizzo non corrisponde il Livello fisico del protocollo lo scarta e non lo invia agli strati successivi.
- Source MAC address - Indirizzo sorgente (6 byte);
- EtherType - Campo tipo (2 byte): Questo campo indica il tipo di protocollo in uso durante la trasmissione e la lunghezza del campo dati;
- Payload Campo dati (da 46 a 1500 byte): contiene i dati reali e possono essere di lunghezza variabile in base al MTU (Maximum Transmission Unit) della Ethernet. Se i dati superano la capacità massima, vengono suddivisi in più pacchetti;
- FCS Controllo a ridondanza ciclica (CRC) (4 byte): permette di rilevare se sono presenti errori di trasmissione, in pratica il ricevente calcola il CRC mediante un algoritmo e lo confronta con quello ricevuto in questo campo.

Gli indirizzi sono tutti a 6 byte in quanto Ethernet definisce uno schema di indirizzamento a 48 bit: ogni nodo collegato, quindi, ha un indirizzo Ethernet univoco di questa lunghezza. Esso corrisponde all'indirizzo fisico della macchina ed è associato all'hardware.
Sono anche detti indirizzi hardware, indirizzi MAC (o MAC address) o indirizzi di livello 2.
La codifica usata per i segnali binari è la codifica Manchester.
Ethernet è una tecnologia che fornisce al livello di rete un servizio senza connessione, in pratica il mittente invia il frame nella LAN senza alcun handshake iniziale, questo frame viene inviato in modalità broadcast (o a bus condiviso) e attraversa tutta la LAN. Quando viene ricevuto da tutti gli adattatori presenti sulla LAN quello che vi riconoscerà il suo indirizzo di destinazione lo recepirà mentre tutti gli altri lo scarteranno.
Il frame ricevuto può contenere errori, la maggior parte dei quali sono verificabili dal controllo CRC. Un frame che non supera il controllo CRC, viene scartato. Ethernet non prevede la ritrasmissione del frame scartato, né una notifica della sua perdita agli strati superiori. Ethernet è quindi inaffidabile, ma anche semplice ed economica.
Sarà compito degli strati superiori (ad esempio TCP) provvedere alla ri-trasmissione.
La gestione delle collisioni e dell'occupazione simultanea del canale di trasmissione viene gestita mediante il CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Anche da questo punto di vista, Ethernet non è in grado di garantire la consegna di un frame, e men che meno che il frame sia consegnato entro un tempo prevedibile.
Nei sistemi Ethernet recenti, il problema non si presenta in quanto con gli switch e la crescita della capacità (vedi Gigabit Ethernet) si eliminano le collisioni e si rende molto più improbabile la congestione.
Ethernet tende a crescere ma il cavo Ethernet ha una capacità limitata sia in lunghezza sia in capacità di traffico, per cui le LAN di grosse dimensioni vengono suddivise in reti più ridotte interconnesse tra loro da particolari nodi tra i quali possiamo trovare dei ripetitori, degli hub o elementi più sofisticati come bridge o switch.
Il ripetitore semplicemente replica il segnale ricevuto. Il cavo Ethernet può quindi assumere lunghezze molto maggiori alle sue capacità. L'unico vincolo è che tra due computer ci devono essere al massimo due ripetitori per salvaguardare la temporizzazione di CSMA/CD.
Il bridge è un elemento di interconnessione più sofisticato dell'hub perché opera sui pacchetti e non sui segnali elettrici. Con questo sistema si possono creare segmenti di LAN indipendenti in cui le collisioni e i ritardi restano limitati.
Molti bridge sono adattativi o ad apprendimento per cui sono provvisti di un software con elenchi di indirizzi per ogni scheda ethernet che posseggono. In questo modo quando arriva un pacchetto, estrapolano l'indirizzo di destinazione, e inviano lo stesso pacchetto nel segmento giusto in base agli elenchi associati alle schede.

Molto più sofisticati sono gli switch composti da un numero elevato di schede ethernet che consentono ad ogni host di essere connessi direttamente. Allo switch vengono poi collegati uno o più cavi Ethernet ad alta velocità che collegano altri segmenti di LAN.
In questo modo lo switch intercetta i pacchetti e li ridireziona ad un host oppure sui segmenti Ethernet. La gestione dei pacchetti, quindi, è ottimizzata perché questi sono subito reindirizzati alla destinazione evitando, per quanto possibile, collisioni. In questo modo ogni scheda ha un suo dominio di collisione.

Wi-Fi

Tecnologia alla base delle WLAN basata sulle specifiche IEEE 802.11. Originariamente nato per collegare dispositivi mobili come laptop e PDA nelle LAN, ora è sempre più utilizzato da altri servizi come terminali per il VoIP, televisioni e lettori DVD e sono in studio standard che permettano una implementaione del Wi-Fi nel mercato del controllo e automazione automobilistica per aumentare la sicurezza nelle autostrade.
I dispositivi, oltre a potersi agganciare a un hotspot, possono essere configurati in una configurazione peer-to-peer per poterli collegare direttamente uno all'altro (network ad-hoc).
Una tipica installzione wi-fi è composta da uno o più access point e da uno o più client, l'AP manda in broadcast il proprio identificativo chiamato SSID o nome di rete attraverso pacchetti chiamati beacon ogni 100ms, i beacon hanno breve durata e pochissimo impiego di banda in modo da non avere impatto sulla banda disponibile nella rete. Se il client si trova nel range di due AP con lo stesso SSID il suo firmware sceglie a quale connettersi valutando alla forza del segnale. La trasmissione aerea si comporta come una rete ethernet cablata non switchata, quindi non gestisce le collisioni, ma si affida ad uno scambio di pacchetti RTS/CTS per cercare di evitarle.
Vantaggi del Wi-Fi:

- Permette di creare reti LAN senza stendere cavi (meno costoso)
- Prezzi dei chip in continuo calo
- Grande interoperabilità fra i dispositivi presenti sul mercato
- Standard Globale, a differenza per esempio della rete cellulare, un dispositivo comprato in una zona del mondo può funzionare ovunque.
- WPA e WPA2 rendono molto sicuro l'encripting delle informazioni
- Nuovi protocolli nati per il QoS e il risparmio energetico rendono il Wi-Fi sempre più adatto ad applicazioni sensibili alla latenza come lo streaming di Audio e Video e l'inclusione in dispositivi small form factor.

Svantaggi del Wi-Fi:

- La potenza isotropica irradiata è limitata in europa a 20dBm
- Altri standard consumano e scaldano meno
- WEP è lo standard di crittazione più usato, ma è facilmente crackabile.
- Gli AP generalmente, per semplicità di uso per i novizi, partono di default senza nessun tipo di crittazione.
- La maggior parte degli AP a 2,4GHz partono di default sullo stesso canale, congestionandolo e rendendo difficile l'accesso, in aggiunta in alcuni stati certi canali non sono disponibili.
- Il range non è molto ampio, indoor 45m, outdoor 90m

Per i bassissimi costi della tecnologia, il wi-fi è la soluzione principale per il digital divide, che esclude ben 10 milioni di italiani dalla banda larga. Le antenne wi-fi generalmente sono parabole poste sui tralicci della corrente elettrica e dietro i campanili che tipicamente sono i punti più alti nel paesaggio nazionale. Ciò evita un onere elevato per la costruzione di torrette dedicate. Le antenne delle singole case sono poste sui tetti.
È importante porre in alto i trasmettitori perché in assenza di barriere in linea d'aria il segnale dell'access point copre distanze di gran lunga maggiori.

Bluetooth

Bluetooth è un termine che identifica l'aderenza di un prodotto a uno standard industriale per una WPAN sviluppata da Ericsson e in seguito formalizzata dalla Bluetooth Special Interest Group (SIG). SIG è stata formalmente annunciata il 20 maggio 1999. È un'associazione formata da Sony Ericsson, IBM, Intel, Toshiba, Nokia e altre società che si sono aggiunte come associate o come membri aggiunti.
Bluetooth fornisce un metodo standard, economico e sicuro per scambiare informazioni tra dispositivi diversi utilizzando onde radio. Questi dispositivi possono essere personal digital assistant (PDA), telefoni cellulari, portatili, computer, stampanti, macchine fotografiche, ecc.
Bluetooth cerca i dispositivi coperti dal segnale (10 metri in ambienti chiusi) e li mette in comunicazione tra di loro.
Nel mondo del controllo possono prendere il posto degli infrarossi per comandare i classici dispositvi casalinghi, in futuro sarà usato anche per i terminali wireless VoIP.
Un dispositivo Bluetooth può comunicare con un massimo di altri sette in una configurazione di rete ad-hoc. Altri 255 dispositivi possono essere in uno stato inattivo e attivati dal master in qualsiasi momento. Il master device dialoga con un solo dispositivo alla volta, ma può switchare velocemente fra i dispositivi usando una politica round-robin (no priorità, slice di tempo uguali a tutti i dispositivi). Ogni dispositivo può essere promosso a master in ogni momento.
Esistono bridge che possono collegare due reti.
Ogni dispositivo, sotto richiesta, può inviare le seguenti informazioni:

- nome
- classe
- servizi
- informazioni hardware

L'utilizzo di alcuni servizi può avvenire solo dopo il pairing che crea una relazione di fiducia e insieme un sistema di crittazione delle informazioni scambiate.

Firewire (IEEE 1394)

Questa tecnologia sviluppata da Apple è uno standard che definisce un bus seriale e le sue interfacce. Viene principalmente utilizzato nelle applicazioni audio video e trasferimento di dati, offrendo comunicazioni ad alta velocità. Supporta due diverse modalità di trasferimento dati: asincrona e isocrona. La modalità asincrona avviene quando il dato spedito viene ricevuto dall'altra parte del cavo. Nel caso in cui la linea fosse libera, viene nuovamente inviato. La modalità isocrona garantisce, riservando una certa banda sul bus, che il trasferimento dati avvenga sempre in un certo intervallo di tempo, caratteristica fondamentale nei sistemi realtime. In questa modalità si possono acquisire dati dagli apparecchi digitali come videocamere e macchine fotografiche. E' stata adottata dalla HANA (l'Alleanza per l'alta definizione audio video nei network) come interfaccia standard per il controllo e la comunicazione. Oltre che nella versione che vediamo abitualmente nei computer il IEEE 1394 esiste anche in versione Wireless, in fibra ottica e su cavo coassiale sempre utilizzando il protocollo isocrono.
Nelle intenzioni iniziali della Apple il firewire doveva essere un rimpiazzo per il parallel SCSI con aggiunta connettività verso dispositivi per l'audio/video.
Al giorno d'oggi lo standard è stato rivisitato più volte, presto verrà presentata una nuova versione (1394c) che supporterà il trasferimento dati a 800Mbit/s lungo un cavo ethernet CAT5 di 100m non schermato.
Dal punto di vista fisico lo standard firewire si compone di 4 fili per i dati e 2 per l'alimentazione da portare ai dispositivi (nella implementazione Sony mancano i due cavi per l'alimentazione).
La tecnologia può collegare fino a 63 periferiche senza bisogno di un PC di supervisione (a differenza di USB) in una topologia aciclica (a differenza dallo SCSI parallelo).
I dispositivi firewire implementano uno standard ISO per la configurazione e identificazione chiamato “configuration ROM” che fornisce le funzionalità di plug and play, in più tutti i dispositivi

sono identificati univocamente da una estensione del formato del MAC address e mettono a disposizione codici standardizzati e conosciuti che indicano il tipo di dispositivo e i protocolli che supporta.
I box per la decodifica della TV via cavo possono contenere una interfaccia firewire utilizzata per la visualizzazione e registrazione dei programmi.
I dispositivi Firewire sono organizzati gerarchicamente sul bus seguendo una topologia ad albero, uno dei nodi viene eletto a radice nella fase iniziale in cui i dispositivi si assegnano degli id univoci sulla rete, l'assegnamento dell'id avviene sempre e solo dopo un reset del bus.
Attraverso il firewire si possono anche creare reti di computer ad hoc e non routed sia su Ipv4 che su Ipv6, i maggiori OS moderni supportano la creazione di reti attraverso il firewire.

RS-232

E' uno standard seriale per scambio di dati binari fra una DTE (Data terminal equipment) e una DCE (Data circuit-terminal equipment).
Venne standardizzato nel 1963 dalla EIA definendo le caratteristiche elettriche dei segnali, le caratteristiche meccaniche delle interfacce, la funzione di ogni circuito presente nel connettore e un sottoinsieme standard di circuiti di interfaccia per le applicazioni di telecomunicazione più importanti.
Lo standard non definisce algoritmi di compressione dei dati o meccanismi di correzione degli errori, così come la codifica dei caratteri o la struttura dello stream dei dati (bit di parità, bit di start e stop, bit per il dato, etc.).
L'interfaccia RS-232 ridotta utilizza un protocollo di trasmissione seriale di tipo asincrono.
Seriale significa che i bit che costituiscono l'informazione sono trasmessi uno alla volta su di un solo "filo". Questo termine è in genere contrapposto a "parallelo": in questo caso i dati sono trasmessi contemporaneamente su più fili, per esempio 8, 16 o 32.
Parlando astrattamente si potrebbe pensare che la trasmissione seriale sia intrinsecamente più lenta di quella parallela (su di un filo possono passare meno informazioni che su 16). In realtà questo non è vero in assoluto, soprattutto a causa della difficoltà di controllare lo skew (disallineamento temporale tra i vari segnali) dei molti trasmettitori in un bus parallelo, e dipende dalle tecnologie adottate: per esempio in una fibra ottica, in un cavo ethernet, USB o FireWire (tutti standard seriali) le informazioni transitano ad una velocità paragonabile a quella di un bus PCI a 32 fili. In questa voce si parlerà solo di interfacce seriali "lente" cioè gestibili da PC e microcontrollori "normali".
Asincrono significa, in questo contesto, che i dati sono trasmessi senza l'aggiunta di un segnale di clock, cioè di un segnale comune che permette di sincronizzare la trasmissione con la ricezione; ovviamente sia il trasmettitore che il ricevitore devono comunque essere dotati di un clock locale per poter interpretare i dati. La sincronizzazione dei due clock è necessaria ed è fatta in corrispondenza della prima transizione sulla linea dei dati.
Limitazioni dello standard:

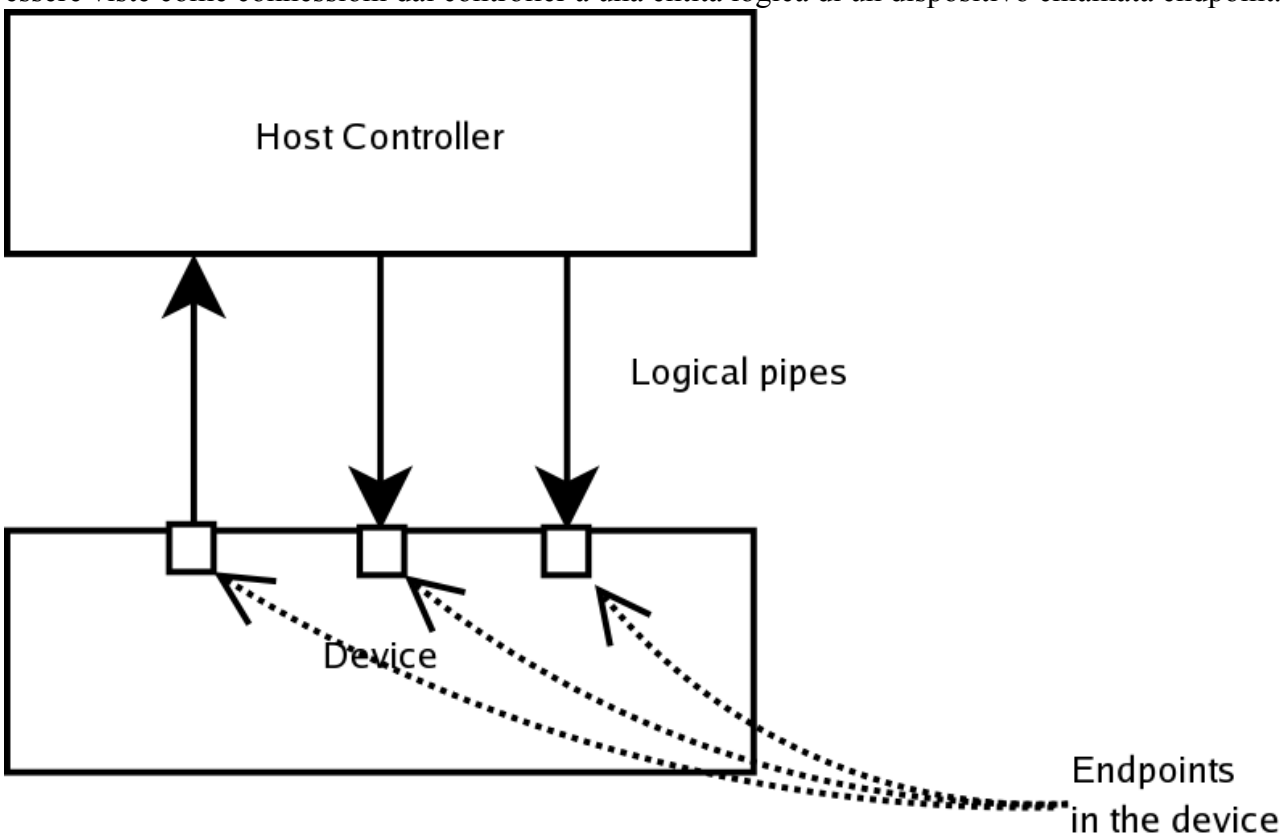
- Alto consumo di potenza rispetto a tecnologie più moderne come USB
- Poco immune al rumore
- Nessuna definizione per le connessioni multi-drop
- Asimmetria dei ruoli ai due capi del cavo, i dispositivi devono essere o DCE o DTE
- Controllo di flusso non affidabile, i protocolli di handshaking era stato pensato limitatamente a collegamenti dial-up

La seriale o rs232 sta piano piano lasciando il posto all'USB, anche se per il controllo di dispositivi come luci, relay, etc. la semplicità e immediatezza di manipolazione delle linee di controllo lo rende comunque più appetibile, infatti lo USB è un protocollo più complesso, non permette un dialogo diretto con i dispositivi seriali e ha bisogno, lato ricezione, di un software che possa decodificare i dati seriali inviati.
Half-duplex indica che la trasmissione è bidirezionale, ma non avviene contemporaneamente nelle due direzioni: un dispositivo (ricevitore, listener o Rx) ascolta e l'altro (trasmettitore, talkner o Tx) emette segnali. Quando è necessario si scambiano i ruoli.

La trasmissione full-duplex indica che la trasmissione è bidirezionale e contemporanea. In questo caso sono necessari ovviamente due fili oppure qualche altro sistema per distinguere i due messaggi contemporanei nelle due direzioni.
Lo standard RS232 permette una trasmissione full-duplex in quanto è utilizzato un conduttore separato per ciascun verso di trasmissione delle informazioni. Il vincolo è in genere la necessità che trasmissione e ricezione abbiano lo stesso formato e, ovviamente, che ciascuno dei due nodi abbia sufficiente potenza di calcolo per la gestione del duplice flusso di informazioni.
Se la trasmissione è sempre in un solo verso, si parla di simplex.
Supporta l'invio di dati sia sincrono che asincrono.

Universal Serial Bus (USB)

Standard seriale nato per i PC, ma col tempo evoluto in molti altri campi, nato per soppiantare sia le interfacce parallele che seriali classiche a causa della poca standardizzazione di quei protocolli. Il design di un sistema USB è fortemente asimmetrico con un controllore e molti dispositivi (funzioni) collegati in daisy chain (dispositivo A collegato al B collegato al C, il C non può essere collegato direttamente ad A così come non è prevista la chiusura dell'anello in nessuna punto ne la formazioni di sottoanelli). Grazie all'utilizzo di Hub si può raggiungere una topologia ad albero con un limite di 5 livelli di rami per ogni controller. Ogni controller può gestire un massimo di 127 dispositivi, hub compresi.
Ogni funzione e hub ha associata una pipe o canale logico, un po' come le pipe di Unix, possono essere viste come connessioni dal controller a una entità logica di un dispositivo chiamata endpoint.



Questi endpoint e le relative pipe sono numerate da 0 a 15 in ogni direzione, così una funzione può avere fino a 32 pipe attive, 16 nel controller, e 16 fuori dl controller. Ogni pipe è unidirezionale ed esiste un endpoint particolare, il numero 0, che serve per la gestione del bus. Le pipe sono divise in 4 categorie basate sul tipo di trasferimento:

- Trasferimenti di controllo: tipicamente usato per corti, semplici comandi al dispositivo e le risposte, normalmente sono trasferimenti associati all'endpoint 0.
- Trasferimenti isocroni: solo a certe velocità garantite (non necessariamente alla massima velocità disponibile), possono portare a perdita di dati, usato per audio e video in realtime.

- Trasferimenti a interrupt: per dispositivi che richiedono una risposta veloce, che hanno una costrizione nella latenza di risposta (dispositivi di puntamento come mouse e tastiere).
- Trasferimenti di massa: larghi trasferimenti che usano tutta la largheza di banda disponibile come i trasferimenti di file.

I dati inviati via USB sono codificati usando NRZI (se il livello logico è zero non si ha transizione, se il livello logico è 1 si avrà una transizione).
Lo standard prevede che il connettore porti anche un segnale per alimentare le periferiche a basso consumo. Le periferiche che hanno richieste energetiche elevate vanno alimentate a parte. I limiti energetici dello standard vanno seguiti scrupolosamente pena il probabile danneggiamento del gestore dato che lo standard USB non prevede nelle specifiche minime la disconnessione in caso di sovraccarico.

DAAP

E' il protocollo introdotto dalla Apple per permettere la condivisione della musica in una rete LAN sia cablata che wireless. E' un protocollo protetto da licenza e solo recentemente la Apple ha iniziato a fornirne le specifiche per applicazioni commerciali, tuttavia è stato studiato talmente a fondo con le tecniche del reverse engineering che sue implementazioni per diverse piattaforme sono di facile individuazione. Viene utilizzato nella fase iniziale dello streaming di risorse audio, in cui le sorgenti di contenuti multimediali usano questo protocollo per annunciare ai client quali contenuti possono mettere a disposizione.
Un server DAAP è un server HTTP che invia la lista di canzoni che possiede e ne gestisce lo streaming verso i client richiedenti.
Le richieste vengono effettuate sotto forma di URL inviati al server che risponde con dati di tipo MIME application/x-dmap-tagged, che il client può poi trasformare in XML. Di solito viene utilizzato Zeroconf o le sue specializzazioni Avahi o Bonjour per annunciare e scoprire in maniera automatica e trasparente i contenuti DAAP in una sottorete. La porta utilizzata dal servizio o demone DAAP è la 3698.

Universal Plug And Play (UPnP)

Nasce come set di protocolli per reti di computer, gli obiettivi dichiarati dal UPnP Forum, propositore del protocollo, sono quelli di rendere semplice e automatica la condivisione di dati, comunicazioni e multimedia negli ambienti casalinghi o lavorativi. UPnP utilizza standard di comunicazione via internet aperti per definire e pubblicare i protocolli di controllo di cui si compone.
Questo set di protocolli permette networking di tipo peer to peer fra PC, applicazioni in rete e dispositivi wireless. L'architettura è di tipo distribuito, aperta e basata su UDP, TCP/IP e HTTP.
Le caratteristiche di UPnP sono:

- Indipendenza dai dispositivi e dal media utilizzato. Non vengono usati device driver, ma protocolli comuni ed è stato progettato per poter funzionare su qualsiasi tecnologia fisica o media come: linee telefoniche, linee di potenza, IR, RF, ethernet, WiFi, Bluetooth e firewire.
- L'architettura permette controllo e interazione con i dispositivi via interfaccia web.
- Indipendenza dai sistemi operativi e dai linguaggi di programmazione. Non vengono fornite ristrettezze nelle possibili API fornibili dai produttori delle interfacce di controllo, viene lasciato completa libertà di adattarsi a ogni installazione. UPnP quindi fornisce la possibilità di avere il controllo e interazione sui dispositivi sia via interfacce web, che attraverso la programmazione classica.
- Basata su tecnologie internet.
- Estensibilità. Ogni prodotto può avere servizi specifici disposti in layer superiori alla architettura di base.

L'architettura UPnP supporta zeroconf, networking invisibile e auto scoperta dei servizi per una discreta quantità di dispositivi prodotti da svariati produttori. Ogni dispositivo che venga inserito

nel network, riceverà un indirizzo IP, annuncerà il proprio nome, e su richiesta le proprie capacità, richiedendo a sua volta quelle degli altri dispositivi. I server DHCP e DNS non sono necessari e vengono usati solo se presenti nella rete, in più, se il dispositivo venisse scollegato non lascerebbe traccia della sua presenza.
L'architettura si basa sull'IP, ogni dispositivo deve contenere un client dhcp e, previo inserimento nella rete, deve cercare un server DHCP per ottenere un ip, se il server non venisse trovato, il dispositivo deve riconoscere la rete come unmanaged e assegnarsi un indirizzo arbitrario, se nella ricerca un DN server gli fornisse un dominio, il dispositivo dovrebbe sempre usare il proprio nome nelle successive operazioni.
Segue una descrizione operativa delle fasi che compongono il protocollo:

1. Scoperta: assegnato un indirizzo IP, il primo passo nel networking UPnP è quello di annunciare ai punti di controllo i servizi che il dispositivo può fornire, analogamente, quando un punto di controllo viene inserito nella rete, esso cercherà i servizi disponibili. Lo scambio avviene attraverso messaggi che indicano poche, essenziali informazioni per ogni dispositivo o singolo servizio, per esempio: il tipo, l'id, e un puntatore a informazioni più dettagliate.
2. Descrizione: dopo che il punto di controllo ha scoperto un nuovo servizio o dispositivo deve, attraverso l'url fornito nella fase precedente, ottenere maggiori informazioni su come interagire e quali capacità deve attendersi dal dispositivo, queste sono espresse sotto forma di dati XML in cui sono presenti: nome, modello, casa costruttrice, numero seriale, sito web del costruttore e la lista dei dispositivi o servizi forniti con gli url per controllarli così come la lista dei comandi, e parametri a cui il servizio risponde con azioni ben determinate. Lo stato durante il funzionamento viene mantenuto in una serie di variabili anche esse descritte nel file XML attraverso il tipo di dato, il range e gli eventi che possono caratterizzarle.
3. Controllo: ora un punto di controllo può inviare azioni da far compiere al dispositivo o servizio attraverso i messaggi di controllo definiti al punto 2 e presenti all'URL di controllo. I messaggi sono espressi in XML usando il protocollo SOAP. La fase di controllo può essere vista come una chiamata di funzione che restituisce o meno il risultato dell'operazione richiesta. Gli effetti dell'azione possono anche non essere la semplice restituzione del risultato, ma più probabilmente un cambio dello stato run time del dispositivo monitorabile attraverso le variabili definite nel punto 2.
4. Notifica di evento: quando le variabili interne cambiano, modificando così lo stato modellato, il dispositivo pubblica le modifiche avvenute, un punto di controllo può essere sottoscritto alla ricezione di queste informazioni (un po' come per un RSS Feed). La pubblicazione avviene per invio di messaggi di evento che racchiudono il nome della variabile e il valore attuale. Ovviamente anche questa comunicazione sfrutta lo standard XML attraverso l'architettura GENA. Quando un punto di controllo si sottoscrive per la ricezione dei messaggi da un dispositivo, riceve un primo messaggio di evento contenente tutte le varibili e i loro valori istantanei dando così la possibilità al controllore di inizializzare il proprio modello interno della risorsa. Ovviamente questa notifica viene sempre inviata contemporaneamente a tutti i controllori sottoscriventi.
5. Presentazione: è il passo finale del protocollo, se il dispositivo ha dichiarato al punto 2 un URL per la presentazione, il punto di controllo apre questo URL in un browser web dando all'utente la possibilità di monitorare e controllare il dispositivo.

Una estensione di UPnP, chiamata UPnP AV, viene mantenuta e sviluppata da un consorzio di aziende produttrici di dispositivi per l'intrattenimento mirata alla distribuzione di contenuti multimediali all'interno della casa o ufficio.
La UPnP AV si compone di:

- MediaServer DCP: è il server (dispositivo slave) che condivide e gestisce lo streaming dei dati (audio, video, immagini e file) verso i client nella rete.
- MediaServer ControlPoint: che è il client (dispositivo master) che cerca i server nella rete e fruisce dei contenti messi a disposizione da questo.

- RUI Client/server: interfaccia di controllo remota (RUI) che invia e riceve i comandi (play, pausa, stop, etc.) fra il client e il server.
- MediaRenderer DCP: dispositivo slave che fornisce un servizio di renderizzazione dei contenuti.
- RenderingControl DCP: controlla le impostazioni del MediaRenderer.

Il protocollo nasce con due problemi che lo standard ad esso successivo, il Devices Profile for Web Services (DPWS) riesce ad eliminare:

- E' basato su HTTP over UDP, che ha l'inconveniente di non essere ancora stato standardizzato.
- Non incorpora un protocollo di autenticazione.

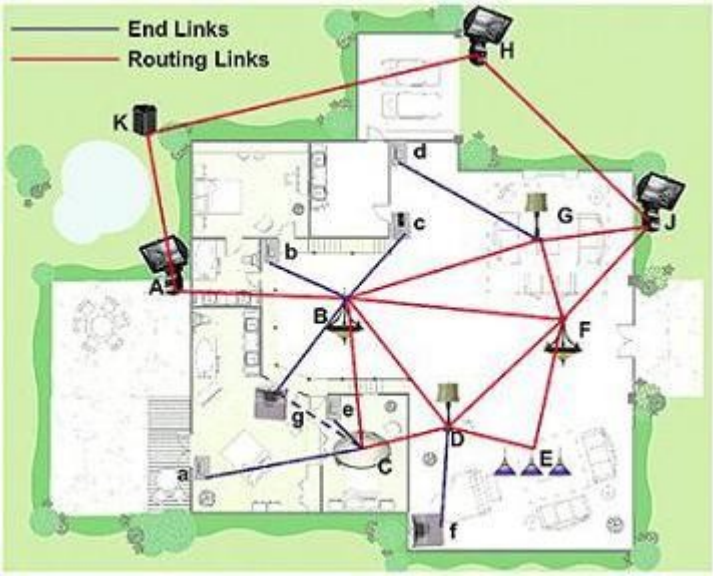
ZigBEE

Nasce nel 2004 come specifica WPAN per una suite di protocolli di alto livello che possano usare tecnologie radio che trasportino l'informazione come segnale digitale in contesti di basso consumo.
Le specifiche sono disponibili liberamente per scopi non commerciali direttamente sul sito web della ZigBee Alliance.
Opera nelle bande di frequenza radio industriale, scientifica e medica (868MHz in europa). La tecnologia è stata siluppata per essere meno costosa e più semplice rispetto ad altre soluzioni WPAN come il Bluetooth, come riferimento di questo fatto va riportato che il dispositivo (nodo) ZigBEE più complesso richiede solo circa il 10% di software rispetto ad analoghe soluzioni Bluetooth o WiFi.
I protocolli ZigBee sono progettati per l'uso in applicazioni embedded che richiedano un basso transfer rate e bassi consumi. L'obiettivo attuale di ZigBee è di definire una rete Mesh non mirata, economica e autogestita che possa essere utilizzata per scopi quali il controllo industriale, le reti di sensori, domotica, ecc. La rete risultante avrà un consumo energetico talmente basso da poter funzionare per uno o due anni sfruttando la batteria incorporata nei singoli nodi.
Esistono tre diversi tipi di dispositivi ZigBEE:

- Coordinator (ZC): servono come radice dell'albero ZigBEE e possono funzionare da bridge verso altre reti. Deve essere installato un solo coordinatore per ogni rete, questo può funzionare anche da storage per alcune informazioni sulla rete come le chiavi di sicurezza.
- Router (ZR): servono per far passare (routing) dati da altri dispositivi.
- End Device (ZED): continene abbastanza funzionalità solo per dialogare col proprio nodo genitore (ZC o ZR), non può ricevere dati da altri dispositivi.

I protocolli si basano su di una recente ricerca nel campo degli algoritmi (Ad-hoc On-demand Distance Vector) che puntano a costruire delle reti ad-hoc di nodi a bassa velocità. Nella reti più grandi la rete reale sarà formata da cluster di cluster, ma si potranno anche formare reti a maglia o cluster singoli. I profili correnti derivati dai protocolli ZigBee supportano sia reti con radiofaro (beacon enabled) che reti "non-beacon enabled".
Nelle reti non-beacon enabled, viene utilizzato un meccanismo di accesso al canale di tipo CSMA/CA (accesso multiplo tramite rilevamento della portante senza collisioni). In questo tipo di reti i ZigBee Router solitamente tengono i loro ricevitori sempre attivi, il che provoca un consistente consumo di energia. In pratica queste reti sono "miste": alcuni dispositivi sono costantemente pronti a ricevere, mentre altri si limitano a trasmettere in presenza di uno stimolo esterno. L'esempio tipico di una rete di questo tipo è dato dagli interruttori wireless: il nodo ZigBee nella lampada può essere costantemente in ricezione, avendo la possibilità della connessione diretta alla rete elettrica, mentre l'interruttore (al pari di un telecomando) alimentato a batteria può rimanere inattivo fino all'istante in cui vi è necessità di mandare un segnale. A quel punto si attiva, invia il comando, riceve un segnale di ACK e ritorna inattivo. In questo esempio la lampada sarà un ZR, se non un ZC, mentre l'interruttore sarà uno ZED.
Nelle reti beacon enabled, i nodi detti ZigBee Router trasmettono periodicamente dei beacon per confermare la loro presenza agli altri nodi. Tra un beacon e l'altro i nodi possono cambiare modalità per risparmiare energia, abbassando il duty cycle. Comunque operazioni a basso duty cycle con

lunghi intervalli di beacon richiedono meccanismi di timing preciso, più difficili e costosi da realizzare.
In generale, i protocolli ZigBee minimizzano il tempo di attività del radiotrasmettitore, così da ridurre il consumo di energia. Nelle reti beacon enabled i nodi consumano energia solo nel periodo in cui c'è il beacon, mentre in quelle non-beacon enabled alcuni nodi sono sempre attivi (il loro consumo di energia è quindi alto) mentre altri sono per la maggior parte del tempo spenti.
I dispositivi ZigBee devono rispettare le norme dello standard IEEE 802.15.4-2003 Low-Rate Wireless Personal Area Network (WPAN). Esso specifica il protocollo di livello fisico (PHY), e la parte del livello data link del Medium Access Control (MAC). Questo standard opera nella banda ISM non licenziata 2.4 GHz, 915 MHz e 868 MHz. I trasmettitori radio usano una codifica DSSS.
La modalità di base di accesso al canale specificato da IEEE 802.15.4-2003 è il Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA). Questo significa che i nodi, controllano se il canale è libero, quando devono trasmettere. Vi sono alcune eccezioni all'uso del CSMA: i segnali di beacon, inviati secondo uno schema prefissato, i messaggi di acknowledge e le trasmissioni di dispositivi in reti beacon-oriented che hanno necessità di bassa latenza ed usano Guaranteed Time Slots (GTS) che per definizione non fa uso di CSMA.
Il software è progettato per rendere facile lo sviluppo su microprocessori piccoli e a basso costo. Il progetto dei radiotrasmettitori è stato ottimizzato per avere un basso costo unitario con produzioni su larga scala. Ha poca circuiteria analogica e usa il digitale ovunque sia possibile.
Anche se i radiotrasmettitori sono economici, il ZigBee Qualification Process comporta una validazione completa delle richieste del livello fisico. Questa minuziosa analisi del livello fisico ha molti vantaggi, poiché tutti i trasmettitori derivanti da uno stesso set di semiconduttori avranno le stesse caratteristiche RF. D'altra parte un livello fisico non certificato che presenta malfunzionamenti potrebbe influenzare negativamente le capacità della batteria di altri dispositivi di una rete ZigBee. In questo caso infatti i vincoli ingegneristici sono necessariamente stretti, in termini di banda e di consumo di energia. La maggior parte dei produttori integra radiotrasmettitori e microcontrollori su un singolo chip.
Un classico esempio di utilizzo nella domotica è una casa con controllo di luci, sistema di sicurezza, antincendio e condizionamento dell'aria.



Nel disegno si possono individuare linee rosse (che indicano un collegamento da router a router) e linee blu che denotano un collegamento da ZED a ZR.
In questo esempio il dispositivo illuminante B (che può anche essere uno ZC) ha identificato e stabilito delle route, attraverso i router embedded nei nodi A, F, C, G e D.
Tutti i router sono sempre dispositivi alimentati a rete (lampade, allarmi antincendio e anti fumo, pompe di calore, etc.), mentre gli end node sono alimentati a batteria (termostati, sensori di movimento, interruttori).

LonWorks

Venne creata dalla Echelon Corporation come protocollo a bassa occupazione di banda adatta a mezzi fisici quali Doppino incrociato, Onde convogliate, Fibra ottica e Radio Frequenza. Il suo maggiore impiego è nel campo del controllo dell'illuminazione e della climatizzazione (HVAC).
Il protocollo di comunicazione vero e proprio, facente parte della piattaforma per il networking in esame, si chiama LonTalk, dal 1999 è diventato standard ANSI. Successivamente vennero approvate anche le altre tecnologie dello strato fisico presentate dalla Echelon Corporation come una unica piattaforma.
Dal 2005 la comunità europea ha riconosciuto LonWorks come facente parte delle specifiche per la building automation.
Molti degli standard nati attorno ai protocolli del LonWorks includono anche le specifiche per le due tecnologie fisiche più usate, il doppino incrociato e l'onda convogliata, in più la piattaforma nasce con uno standard di Ip tunneling adatto all'interfacciamento con sistemi di controllo remoti e con applicazioni e dispositvi basati su IP.
Una caratteristica peculiare del LonWorks è la standardizzazione dei valori che le variabili descriventi una grandezza fisica possono assumere. La lista di questi standard viene mantenuta dalla LonMark International, una organizzazione multinazionale creata per promuovere l'integrazione fra i sistemi di controllo multimarca. Ognuno di questi standard viene chiamato in gergo snivet, dall'acronimo di Standard Network Variable Types (SNVT), quindi, ad esempio, un termostato che segue lo SNVT per la temperatura, fornirà un valore da 0 a 65535, corrispondente al range di temperature da -274.0°C a 6279.5°C
Avendo avuto un grosso sviluppo e una buona base di installato (viene anche usato nel controllo e automazione interna dei treni), si possono trovare sul mercato molti circuiti integrati, chiamati Neuroni negli ambienti LonWorks, che incorporano già il protocollo nella logica che sviluppano.
Si stimano 60 milioni di dispositivi LonWork installati nel mondo.

X10

L'X10 è uno standard internazionale e aperto per la comunicazione fra dispositivi usato per l'automazione e la domotica. Usa principalmente onde convogliate per l'invio di segnali e controllo, l'informazione digitale viene rappresentata da brevi transizioni in radiofrequenza. Esiste anche una specifica per l'utilizzo di tecnologie radio.
E' stato sviluppato nel 1975 da Pico Electronics proprio con l'intenzione di creare uno standard per il controllo remoto di dispositivi e apparecchi. Fu la prima tecnologia domotica ed è tuttora la più utilizzata.
Il cablaggio elettrico della casa viene utilizzato per inviare dati digitali attraverso una codifica con portante a 120kHz che viene trasmessa come una transizione nel momento in cui la corrente alternata attraversa lo 0, un bit viene trasmesso ad ogni attraversamento dello 0.
Il controllore invia così un indirizzo e un comando al dispositivo controllato. Esistono controllori e dispositivi avanzati che possono scambiarsi informazioni di stato (on/off, livello delle luci, temperatura, etc.).
Essendo la portante del segnale a una frequenza maggiore rispetto alla frequenza di rete, i segnali inviati non possono passare attraverso trasformatori di potenza o attraverso le fasi di un sistema multifase. In più, a causa della sincronizzazione con lo 0 dell'onda AC, non riuscirebbero a essere correttamente temporizzati durante in accoppiamento di fase in un sistema a tre fasi.
Un altro punto delicato è la possibilità di confinare i segnali all'area locale evitando che i controlli in una casa interferiscano con i vicini, a questo scopo vengono utilizzati filtri induttivi come attenuatori.
Sia che venga utilizzata l'onda convogliata che la comunicazione radio, i pacchetti X10 inviati consistono sempre di 4 bit chiamati codice della casa (nel protocollo, per semplicità le possibili combinazioni dei 4 bit vengono anche etichettate come lettere da A a P), seguito da uno o più gruppi di 4 bit che individuano il codice di unità (etichettate come numeri da 1 a 16) e alla fine si

trova il comando di 4 bit, in realtà il frame minimo può non contenere il codice di unità, ma avere direttamente il comando (per esempio nel caso di un spegni tutto), la selezione fra i due modi avviene grazie all'ultimo bit (0 = codice di unità, 1 = comando).
All'installazione ogni dispositivo viene programmato per rispondere a uno solo dei 256 possibili indirizzi (16 codici di casa * 16 codici di unità) in modo da reagire solo ai comandi dedicati a lui.
Tutti i segnali vengono inviati due volte per ridurre i falsi segnali e fare in modo che il ricevente capisca il comando anche in mezzo al rumore della linea, contando la ritrasmissione, il controllo, etc. il data rate si attesta intorno ai 20bit/s, quindi così basso che la tecnologia è effettivamente confinata al mero on/off dei dispositivi o a operazioni davvero semplici.
Per permettere la sincronizzazione col pacchetto inviato, ogni frame inizia con uno start code 1110.
Ogni volta che un dato cambia da un indirizzo ad un altro, da un indirizzo a un comando o da un comando ad un altro, i frame devono essere suddivisi da almeno 6 zero che resettino i registri a scorrimento che decodificano il pacchetto ricevuto.
Per permettere il funzionamento di pulsantiere wireless, interruttori remoti, moduli di allarme, sensori e simili, viene usato il protocollo radio che opera a 433MHz, i dati scambiati da questi dispositivi sono molto simili al protocollo su onda convogliata, il ricevitore radio fornisce anche un bridge che traduce i pacchetti radio in pacchetti di controllo ordinari.
I controller X10 possono variare da molto semplici a molto sofisticati, i più semplici possono comandare solo 4 dispositivi a 4 indirizzi sequenziali. Il minimo set di comandi è dato da:

- Unità 1 on/off
- Unità 2 on/off
- Unità 3 on/off
- Unità 4 on/off
- Innalza e abbassa la luce (dell'ultima unità selezionata)
- Accendi o spegni tutto

Lo scheduling (programmazione) di eventi può essere ottenuto con i controllori più sofisticati che incorporano anche dei timer. Controllori ancora più sofisticati possono anceh dialogare direttamente con PC o incorporare programmi per eseguire scene o rispondere alle letture di sensori esterni con azioni complicate.
Il problema maggiore di X10 è l'eccessiva attenuazione del segnale quando deve passare da una fase all'altra di una linea trifase, che semplicamente potrebbe non trovare nemmeno un percorso elettrico per passarvi o subire troppo l'impedenza dei trasformatori, in più le TV o i dispositivi wireless possono generare falsi comandi di accensione o spegnimento, i filtri antirumore possono aiutare l'eliminazione di questi segnali spuri, ma se non vengono realizzati apposta per vivere in un ambiente X10 potrebbero anche filtrare i veri comandi X10.
In più, i moderni PC, TV e ricevitori satellitari possono, a causa delle capacità in ingresso, cortocircuitare il segnale X10 dalla linea direttamente a massa o al neutro, non faccendo più giungere il comando ai dispositivi vicini, per questo motivo esistono filtri da usare fra la presa di questi dispositivi e la presa di rete.
Alcuni controllori X10 possono non lavorare bene in presenza di dispositivi a basso consumo (50W) o che non presentano un carico resistivo.
Se due comandi X10 vengono inviati nello stesso momento, collideranno sulla linea e il ricevitore non potrà decodificare il messaggio.
Esistono bridge che possono tradurre il protocollo X10 a altri standard della domotica.

C-Bus

Procollo aperto per l'automazione principalmente usato in Australia anche se inizia ad essere utilizzato anche in USA, Asia, Russia, UK e Sud Africa.
E' stato creato dalla Clipsal per essere usato in congiunzione con i propri dispositivi per la domotica, nelle intenzioni dei sostenitori dovrebbe prendere il posto del più anziano ed utilizzato X10.
Il C-Bus nasce per controllare l'illuminazione, tutti i dispositivi elettrici e interfacciarsi con i

dispositivi di sicurezza e i prodotti AV. Ne esistono due versioni: cablata e wireless, l'interfacciamento fra le due versioni può essere effettuato attraverso un gateway.
La versione cablata usa un cavo di rete CAT5 standard che può essere lungo al massimo 1000, estendibile usando dei Bridge per le reti C-Bus, il massimo numero di unità installabile in una rete è 100, ma anche questo può essere esteso grazie ai Bridge.
Il massimo numero di reti in una installazione è 255, sempre che non venga usata una interfaccia ethernet per il C-Bus, a quel punto la limitazione viene fornita dagli IP utilizzabili. Attraverso l'uso di 6 network bridge si può raggiungere la massima quantità di reti collegate in serie che è 7.
La sincronia dei dati lungo il C-Bus viene garantita da almeno una unità di generazione di clock, che quindi è un componente che deve sempre essere presente.
Il problema maggiore per l'adozione del C-Bus cablato è che richiede una nuova posa di cavi per funzionare, non può utilizzare quella già esistente, quindi è adatto principalmente all'utilizzo nelle nuove construzioni.
Vista l'apertura delle specifiche è facile trovare interfacce verso altri protocolli come TCP/IP, Crestron, AMX, LonWorks, ModBUS.

CEBus

E' un set aperto di standard e protocolli per il controllo di illuminazione e dispositivi elettronici adatto sia a situazioni casalinghe che in uffici, le specifiche coprono lo scambio di informazioni via onde convogliate, doppini intrecciati, cavi coassiali, infrarossi, Radio Frequenza e Fibra ottica.
Venne presentato nel 1992 in risposta alle richieste del mercato di estendere le funzionalità e l'installabilità di X10.
Mirando in primo luogo alla sostituzione del protocollo X10, la principale tecnologia che lo distingue è il trasporto attraverso onde convogliate. L'informazione viene trasferita attraverso tecniche di modulazione a espansione di spettro in cui la modulazione inizia ad una certa frequenza che viene alterata durante il ciclo. Sia la presenza che l'assenza di incremento della frequenza in un determinato periodo portano alla definizione dei digit, l'incremento varia linearmente da 100 a 400 kHz in 100 microsecondi. L'incremento viene definito stato superiore, la sua assenza stato inferiore.
Se uno qualsiasi dei due stati permane per 100 microsecondi, viene interpretato come 1, lo 0 si ottiene se lo stato permane per 200 microsecondi. Da ciò si evince che la frequenza di trasmissione è variabile in dipendenza dal numenro di 1 e 0 che si trasmettono. Un incremento della durata di 400 microsecondi indica invece la fine del frame.
Anche la lunghezza dei pacchetti inviati è variabile, il minimo è 64bit.
L'indirizzamento dei dispositivi viene fatto dalla casa costruttrice che può scegliere in un range di 4 miliardi di possibilità.
Lo standard definisce anche un linguaggio OO che include primitive per comandi come variazione di volume, temperatura, etc.

CAN

Il Controller Area Network, noto anche come CAN-bus, è uno standard seriale per bus di campo (principalmente in ambiente automotive), di tipo multicast, introdotto negli anni 80 dalla Robert Bosch GmbH, per collegare unità elettroniche di controllo (ECU). Il CAN è stato espressamente progettato per funzionare senza problemi anche in ambienti fortemente disturbati dalla presenza di onde elettromagnetiche e può utilizzare come mezzo trasmissivo una linea a differenza di potenziale bilanciata come la RS-485. L'immunità ai distubi EMC può essere ulteriormente aumentata utilizzando cavi di tipo twisted pair (doppino intrecciato).
Sebbene inizialmente applicata in ambito automotive, come bus per autoveicoli, attualmente è usata in molte applicazioni industriali di tipo embedded, dove è richiesto un alto livello di immunità ai disturbi. Il bit rate può raggiungere 1 Mbit/s per reti lunghe meno di 40 m. Velocità inferiori consentono di raggiungere distanze maggiori (ad es. 125 kbit/s per 500 m). Il protocollo di comunicazione del CAN è standardizzato come ISO 11898-1 (2003). Questo standard descrive

principalmente lo strato (layer) di scambio dati (data link layer), composto dallo strato sottostante (sublayer) "logico" (Logical Link Control, LLC) e dallo strato sottostante del Media Access Control, (MAC) e da alcuni aspetti dello strato "fisico" (physical layer) descritto dal modello ISO/OSI (ISO/OSI Reference Model). I protocolli di tutti gli altri layer sono lasciati alla libera scelta del progettista della rete.

ModBUS

Il Modbus è un protocollo di comunicazione seriale creato da Modicon nel 1979 per mettere in comunicazione i propri controllori in logica programmabile (PLC). E' diventato uno standard de facto nella comunicazione di tipo industriale, ed è ora il protocollo di connessione più diffuso fra i dispositivi elettronici industriali. Le principali ragioni di un così elevato utilizzo del Modbus rispetto agli altri protocolli di comunicazione sono:

- E' un protocollo pubblicato apertamente e royalty-free
- Può essere implementato in pochi giorni, non in mesi
- Muove raw bits e words senza porre molte restrizioni ai venditori

Modbus consente la comunicazione fra diversi dispositivi connessi alla stessa rete, per esempio un sistema che misura la temperatura e l'umidità e comunica il risultato a un computer. Modbus è spesso usato per connettere un computer supervisore con un unità terminale remota (RTU) nel controllo di supervisione e sistemi di acquisizione dati (SCADA). Esistono due versioni del protocollo: una su porta seriale (RS485 di default, ma anche RS485) e Ethernet.
Esistono due varianti, con differenti rappresentazioni dei dati numerici e piccole differenze sul protocollo stesso. Modbus RTU è una rappresentazione dei dati compatta di tipo esadecimale. Modbus ASCII è facilmente leggibile e ridondante. Entrambe le varianti usano la comunicazione seriale. Il formato RTU fa seguire ai comandi/dati un campo checksum di tipo CRC (cyclic redundancy check) mentre il formato ASCII usa un checksum di tipo LRU (longitudinal redundancy check). I nodi configurati per la variante RTU non può comunicare con nodi configurati per l'ASCII e viceversa. Modbus/TCP è molto simile al Modbus RTU, ma trasmette i pacchetti del protocollo dentro pacchetti di dati TCP/IP.
A ogni periferica che necessita di comunicare per mezzo del Modbus viene assegnato un indirizzo unico. Ognuna di queste può inviare un comando Modbus, sebbene generalmente (nel seriale obbligatoriamente) solo una periferica agisce come master. Un comando Modbus contiene l'indirizzo Modbus della periferica con la quale si vuole comunicare. Solo quest'ultima agirà sul comando, sebbene anche le altre periferiche lo ricevano. Tutti i comandi Modbus contengono informazioni di controllo, che assicurano che il comando arrivato sia corretto. I comandi base possono chiedere ad un RTU di cambiare un valore in uno dei suoi registri, così come comandare alla periferica di restituire uno o più valori contenuti nei suoi registri.
Ci sono diversi modem che supportano Modbus. Alcuni di questi sono specificatamente progettati per questo protocollo. Alcune implementazioni usano fili, comunicazioni wireless o anche SMS o GPRS. Problemi tipici in cui può imbattersi il progettista sono l'alta latenza e problemi di temporizzazione.

KNX

KNX è il primo standard di home & building automation aperto, privo di royalty ed indipendente dalla piattaforma, approvato come standard europeo (EN 50090 - EN 13321-1) e mondiale (ISO/IEC 14543). Lo standard è stato sviluppato da KNX Association sulla base dell'esperienza dei suoi predecessori BatiBUS, EIB ed EHS e permette installazioni completamente distribuite.
Lo standard KNX prevede diversi mezzi trasmissivi che possono essere utilizzati in combinazione con uno o più modi di configurazione in funzione della particolare applicazione.

- TP-0 (Twisted Pair, tipo 0) Mezzo trasmissivo basato su cavo a conduttori intrecciati con bitrate di 4800 bits/s, proveniente da BatiBUS. I prodotti certificati KNX TP0 funzionano sulla stessa linea bus dei componenti certificati BatiBUS ma non scambiano informazioni

con essi.

- TP-1 (Twisted Pair, tipo 1) Mezzo trasmissivo basato su cavo a conduttori intrecciati con bitrate di 9600 bit/s, proveniente da EIB. I prodotti certificati EIB e KNX TP1 funzionano e comunicano fra di loro sulla stessa linea bus.
- PL-110 (Power Line, 110 kHz) Mezzo trasmissivo ad onda convogliata (power-line) con bitrate di 1200 bit/s, proveniente da EIB. I prodotti certificati EIB e KNX PL110 funzionano e comunicano fra di loro sulla stessa rete di distribuzione dell'alimentazione elettrica.
- PL-132 (Power Line, 132 kHz) Mezzo trasmissivo ad onda convogliata (power-line) con bitrate di 2400 bits/s, proveniente da EHS dove viene tuttora utilizzato. I componenti certificati KNX PL132 ed EHS 1.3a funzionano sulla stessa rete ma non comunicano fra loro senza un convertitore di protocollo dedicato.
- RF (Radio Frequency, 868 MHz) Mezzo trasmissivo in radiofrequenza con bitrate di 38.4 kbit/s, sviluppato direttamente all'interno della piattaforma standard KNX.
- Ethernet (KNXnet/IP) Mezzo trasmissivo diffuso che può essere utilizzato unitamente alle specifiche “KNXnet/IP” che permettono il tunnelling di frame KNX incorporati in frame IP (Internet Protocol).

Esistono tre classi di dispositivi KNX:

- A-mode o modo automatico: dispositivi che possono automaticamente configurarsi e sono prodotti mirati all'utente finale che può acquistarli e installarli senza interventi di tecnici.
- E-mode o modo semplice: sono dispositivi che necessitano di un minimo di studio per essere installati, il loro comportamento è pre-programmato, ma alcuni parametri di configurazione devono essere adattati alle richieste dell'utente.
- S-mode o modo sistema: installati e programmati da tecnici specializzati, questi dispositivi non presentano alcun comportamento di default.

AMX

AMX progetta e produce hardware e software per il controllo remoto di una grande varietà di equipaggiamenti.
Installazioni tipiche includono automazione di Auditorium e Sale conferenza, musei, home theater, dove gli utenti utilizzano touchscreen fissi o wireless per controllare dispositivi come proiettori, display, PC, lettori DVD e VCR, videocamere, sistemi di teleconferenza, switch A/V, schermi motorizzati, luci e un altra varietà di altri tipi di equipaggiamento. Altri usi comuni includono sistemi di intrattenimento, controlli industriali, sistemi di sicurezza, hotel, ristoranti, etc.
I sistemi AMX vengono configurati partendo da hardware modulare, permettendo una personalizzazione molto elevata per incontrare il fabbisogno del cliente, in più possono scalare facilmente fornendo una grande adattabilità futura.
Programmazioni personalizzate permettono di riconfigurare funzioni con un semplice pulsante, rendendo molto semplice lavorare su sistemi complessi. Per esempio, premendo un singolo bottone chiamato Video, possono abbassarsi le luci, chiudersi le persiane, scendere lo schermo motorizzato e accendersi il proiettore, selezionando automaticamente l'ingresso video e attivando sulla matrice A/V l'incrocio che manda al sistema audio 5.1 l'audio del DVD. Sui touchscreen possono essere riportate le sole funzionalità più utili per l'utente medio, nascondendo magari le impostazioni in sottomenu protetti da password.
I nuovi sistemi NetLinx possono essere controllati via IP da remoto.
La programmazione e configurazione avviene attraverso molti programmi che supportano add-in per caratteristiche avanzate e RAD. La suite completa dei software per la programmazione si chiama NetLinx Studio fornendo anche facilities di debug e test.
Naturalmente programmare un sistema AMX, essendo questo completamente centralizzato, è un progetto difficilmente organizzabile in team, il progettista/programmatore deve mettere in campo una serie i conoscenze che spaziano dalla programmazione, i sistemi di computer, progettazionie di interfacce utente, programmazione guidata dagli eventi, tecnologia AV,gestione dei clienti, visione di insieme e prohect management.

Un tipico sistema AMX si compone di:

- Controller: il processore centrale, il cuore dall'applicazione, i comandi gli sono inviati attraverso le interfacce utente e il controllore, attraverso le card installate nei suoi slot di espansione o interne, interagisce con i dispositivi richiesti.
- Dispositivi controllabili: sono l'insieme dei dispositivi che il controllore è stato programmato per controllare.

CRESNET

Il bus Cresnet è un bus proprietario che definisce la spina dorsale delle comunicazioni fra vari dispositivi della Crestron, quali Touchpanel, tastiere, moduli di espansione, etc. Fisicamente si presenta come un cavo di rete a 4 fili che fornisce comunicazione bidirezionale e alimentazione a 24V. Supporta cablaggi fino a 5Km e qualsiasi topologia di rete.
Le reti crestron sono il classico esempio di installazione centralizzata, uno o più processori contengono la logica di tutti i dispositivi e le interazioni fra essi, dando così la possibilità di comandare anche dispositivi non direttamente nati per la domotica. Tutta la linea di prodotti crestron è molto costosa, ma anche i processori base permettono il controllo diretto di molte perferiche diverse attraverso una dotazione minima di porte seriali, ethernet, relay, contatti digitali e IR direttamente installati nella macchina.
La programamzione della logica e della eventuale grafica per i touchscreen crestron è fatta attraverso programmi che rendono semplice esprimere le interazione logiche fra le azioni compiute dall'utente e ciò che avviene nell'ambiente.
Oltre al prezzo, il principale problema dei prodotti Crestron è la totale centralizzazione della logica, dovendo, per ogni cambiamento di funzionalità o sostituzione di dispositivi, riscrivere parte del programma caricato nel processore centrale.
Per contro sono degli ottimi controllori e supervisori anche per altri bus, esistono molte interfacce facilmente configurabili per dialogare con i principali bus esistenti.
Crestron e AMX sono competitori diretti nel mercato, il loro range di prodotti è simile così come l'architettura e le caratteristiche.