3. MODELOS

3.1. Introducción.

La red de control de un sistema de automatización de un edificio consta de los siguientes elementos [3]:

- Conjunto de sensores, controladores y actuadores, que permiten interactuar con el medio y automatizar el edificio.
- Uno o varios equipos con capacidad de procesamiento y capaces de controlar el conjunto de sensores y actuadores. Por otra parte, este equipo permitirá que el usuario interactúe con toda la instalación.
- Interfaz con el usuario. Le permite conocer al usuario el estado de la instalación y puede llegar a ser una verdadera subred dentro de la red de control.
- Medio de transmisión. A través del cual se intercambia la información. Pueden ser varios.

En lo referente a la conexión de los distintos dispositivos, existe en el mercado gran cantidad de protocolos de control diseñados específicamente para esta tarea. Estos sistemas suelen incluir los tres primeros niveles y el nivel de aplicación del modelo OSI. Están diseñados para ser incluidos al mínimo coste posible en pequeños dispositivos, que se caracterizan por su escasa capacidad de procesado, sus limitados recursos de memoria y una reducida tasa de transferencia de datos.
En la actualidad gracias a la reducción en tamaño y coste del hardware, la red domótica incluye otros elementos electrónicos más complejos y que requieren de mayor capacidad. Además, se ha extendido la implantación de distintos tipos de redes locales que son capaces de proporcionar un elevado ancho de banda para ser compartido por diversos dispositivos.
Por estos motivos, la tendencia actual es la incorporación de TCP/IP como parte de estos protocolos. Así la única capa que se especificará será la de aplicación, que incluirá el conjunto de propiedades y operaciones de los dispositivos. Las técnicas de configuración automática (Plug&Play) también acabarán por imponerse.

Como se ha dicho, el sistema central va a proporcionarle al usuario la posibilidad de monitorizar y actuar sobre la instalación. Esta interacción puede llevarse a cabo por distintos medios: PC, teléfono fijo o móvil, PDA, etc. Estos sistemas pueden combinarse para proporcionar más de un acceso, constituyendo una verdadera red de datos. Además, si se requiere se puede incluir un acceso vía web.

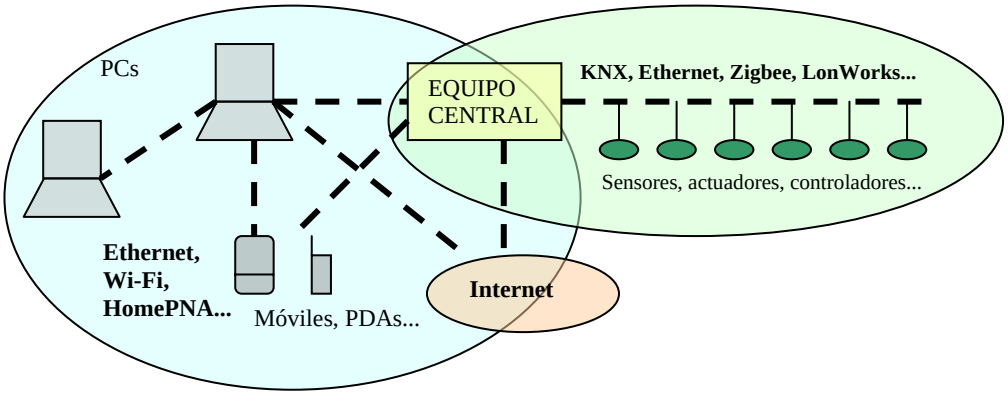

Ilustración 3.1-1 Red de control.

Existe la posibilidad de integrar distintas soluciones dentro de una instalación, ya que los requerimientos de los dispositivos van a ser distintos. Así, por ejemplo, se podría establecer una comunicación inalámbrica Wi-Fi con el conjunto de cámaras de seguridad que necesitan una capacidad alta para transmitir, mientras que, para el conjunto de detectores de presencia, que transmiten poca cantidad de información, se podría optar por una solución más económica, como puede ser Zigbee. Igual ocurre con la comunicación con el usuario.

3.2. Modelos específicos.

Estos modelos surgen a principios de los años ochenta para dar solución a la automatización de edificios. En sus comienzos son sistemas sencillos destinados a controlar un conjunto reducido de sensores y actuadores. A medida que ha ido evolucionando el sector han ido apareciendo nuevos modelos y se han ido mejorando los que ya existían.
Existe gran variedad de sistemas en el mercado tanto en prestaciones como en precio y esto permite elegir el sistema que mejor se adapte a las necesidades del usuario. Sin embargo, esta diversidad de opciones ha obstaculizado la integración y la unión de diferentes dispositivos y marcas dentro de una misma instalación. En la actualidad, las asociaciones y fabricantes relacionados con el sector domótico aúnan esfuerzos para lograr una completa integración. Ejemplos de este trabajo son soluciones como KNX, HES o SCP.

En su mayoría, estos protocolos son abiertos, sin embargo, existen otros muchos de carácter propietario. A estos últimos se recurre cuando se necesitan sistemas robustos y con alto grado de sofisticación, por lo que principalmente se utilizan en grandes instalaciones.

Se pueden encontrar en el mundo multitud de edificios que poseen una instalación domótica, en su mayoría grandes bancos y multinacionales, pero también hospitales o centros gubernamentales. En Europa se pueden destacar las instalaciones EIB en el Banco Central de Zurich, el hotel I'An en Rochehaut (Bélgica) o el hospital de la Cruz Roja en Barnbach (Alemania). También existen soluciones conjuntas, así el complejo de oficinas Einstein en Munich y la factoría Stihl en Waiblingen (Alemania) poseen sistemas EIB y Bacnet.
La Diputación de Barcelona, el edificio del BBVA en Madrid o el edificio madrileño de Telefónica cuentan en España con los últimos avances en inmótica.

A continuación se detallan los modelos más destacados en el sector de la automatización de edificios.

3.2.1. KNX.

Con el objetivo de unificar los protocolos domóticos en Europa nace KNX, partiendo de los estándares existentes EIB, EHS y BatiBUS. Se pretende con este estándar común y abierto competir en precios y calidad con los sistemas norteamericanos de automatización de viviendas y oficinas [22].

Fue desarrollado por la Konnex Association, una agrupación creada en 1999 por la EIBA, EHSA y BATIBUS y está formada por empresas relacionadas con el sector domótico. Actualmente se encarga de promover y mejorar KNX. En Junio del año 2003, KNX se convierte en el estándar europeo EN-50090 de CELENEC.

KNX se basa en la tecnología EIB a la que le añade nuevos medios físicos y los modos de configuración de BatiBUS y EHS.

3.2.1.1 EIB, EHS y BatiBUS.

a) EIB:

Protocolo de control domótico promovido por la EIBA (European Installation Bus Associtation). La EIBA es una asociación europea de empresas, líderes en el sector electrónico, que se unieron en 1990 para crear un protocolo inmótico europeo. Tiene su sede en Bruselas y en la actualidad cuenta con más de 110 miembros [24].

Las características más destacadas de este sistema son:

- Basado en el modelo OSI, definiendo los niveles 1, 2, 3, 4 y 7.
- Organización en bus descentralizada con transmisión en serie.
- Gran cantidad y diversidad de dispositivos. Además, las empresas participantes en EIBA garantizan la compatibilidad entre sus productos, por lo que es posible emplear dispositivos de distintos fabricantes dentro de una instalación EIB.
- El medio físico más utilizado es el par trenzado a 9,6 Kbps (EIB.TP). Funciona sobre otros medios físicos: corriente portadora, ethernet a 10 Mbps, RF e IR, pero son medios poco extendidos.
- Acceso al medio mediante CSMA-CA con resolución positiva. Así, si se detecta colisión, el que tiene mayor prioridad es el que continua transmisión.
- Adaptable y modular.
- Los productos EIB ya instalados son compatibles con los nuevos productos KNX.

Además, se dispone de una herramienta software, ETS, que permite minimizar el esfuerzo y el tiempo de diseño del proyecto.

b) EHS:

EHS (European Home System) es un protocolo abierto, desarrollado en 1992 y claramente enfocado al mercado residencial. Tiene el respaldo de la EHSA (EHS Association), que promueve el uso de EHS y es la encargada de sus mejoras tecnológicas [22].

Sus características más importantes son:

- Sistema descentralizado.
- Medios físicos:
  - PL2400 a 2.4 Kbps.
  - PT0 a 4.8 Kbps.
  - PT1 a 9.6 Kbps.
  - PT2 a 64 Kbps.
  - IR-1200 a 1.2 Kbps.
  - RF-1100 a 1.1 Kbps.
- Técnica de acceso al medio CSMA-CA.
- Filosofía plug&play, que permite a los dispositivos configurarse automáticamente y que la ampliación de la instalación resulte más sencilla.

c) BatiBUS:

BatiBUS [17] es un protocolo desarrollado por la empresa francesa Merlin Gerin Schneider Electric. En 1989, dicha empresa crea junto a otras el BCI (BatiBUS Club International), cuyo propósito era promover el uso del estándar. Posteriormente obtuvo la certificación como estándar europeo CELENEC (NFC 46620) y como estándar internacional ISO (ISO/IEC JTC 1 SC25).

En la actualidad está prácticamente en desuso pero fue muy utilizado en los antiguos sistemas industriales franceses.

Las principales características de BatiBUS son:

- Basado en el modelo OSI, definiendo las capas 1, 2 y 7.
- Sencillo de instalar.
- Bajo coste.
- Arquitectura flexible que permite que el sistema sea fácil de extender.
- Comunicaciones: bidireccional, half duplex y distribuida.
- Medio de transmisión: único bus de par trenzado a 4.8 Kbps (TP0).
- Para el acceso al medio emplea la técnica CSMA-CA con resolución positiva. Así, si se detecta colisión, el que tiene mayor prioridad es el que continua transmisión.

3.2.1.2 Topología.

El sistema KNX hereda la topología basada en distintos niveles de EIB. En primer lugar, los dispositivos (sensores, actuadores, etc.) se conectan a una línea, hasta un máximo de 256 aparatos. Mediante una línea principal y un acoplador de línea (AL), las líneas (máximo 15) se agrupan en áreas o zonas y estas últimas pueden unirse por medio de una línea dorsal a través de un acoplador de zona (AA). El número máximo de zonas que se pueden agruparse son 15 [12].

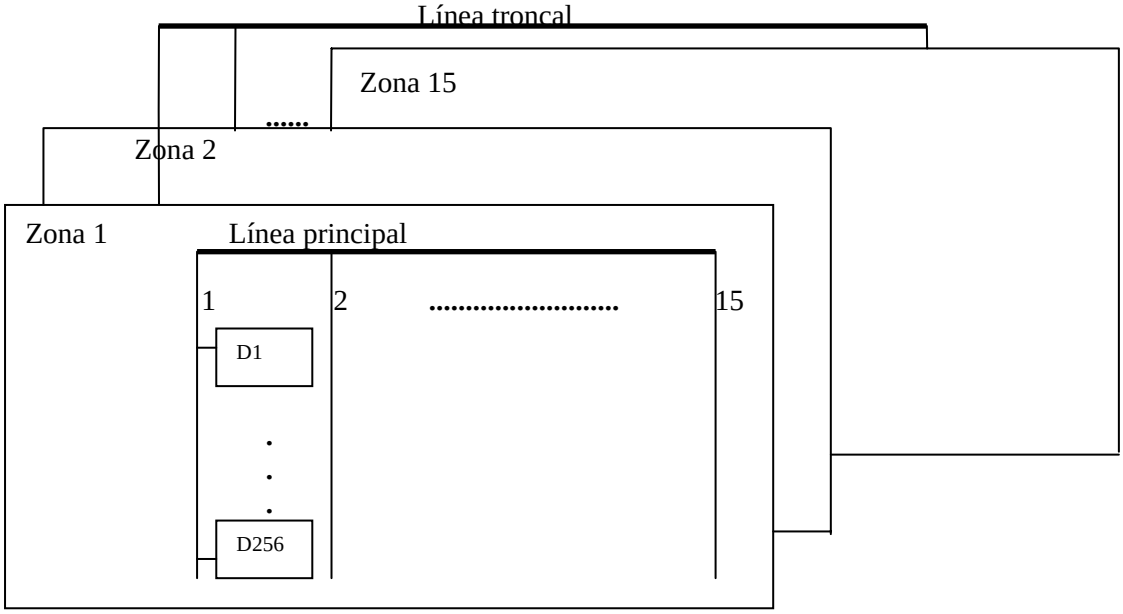

Ilustración 3.2.1-1. Topología.

Cada línea va a contar con su propia fuente de alimentación, y estará galvánicamente aislada del resto de las líneas. Esto implica que si una línea falla, el resto puede seguir funcionando sin ningún problema.
Gracias a la división jerárquica en zonas y líneas, el tráfico de datos locales no afecta al resto de líneas o zonas y se consigue una red menos congestionada. El acoplador de línea no permitirá el paso hacia otras líneas de información si los destinos pertenecen a la misma línea que el elemento que generó el envío. Por otra parte, tampoco dejará pasar los datagramas de otras líneas o zonas que no conciernan a elementos de su línea.
Además, esta organización permite que el mantenimiento y la ampliación del sistema resulten muy sencillos.

3.2.1.3 Modelo.

KNX está basado en la pila de protocolos de EIB, que especifica los niveles 1, 2, 3, 4 y 7 del modelo OSI [12].

Nivel físico:

- Comunicación bidireccional semiduplex.
- Transferencia asíncrona.
- Medios de transmisión:
    - Par trenzado:
        - ➔ TP0 a 2.4 Kbps.
        - ➔ TP1 a 9.6 Kbps.
    - Línea eléctrica:
        - ➔ PL110 a 1.2 Kbps.
        - ➔ PL132 a 2.4 Kbps.
    - Radiofrecuecia en la banda de 868 Mhz.
    - Ethernet a 10 Mbps, aprovechando las normas EHS y EIB existentes.

Nivel de enlace:

- Emplea CSMA/CA para acceder al medio.
- Cada dispositivo o grupo posee una dirección de 16 bits para identificarlos.
- Formato de trama:

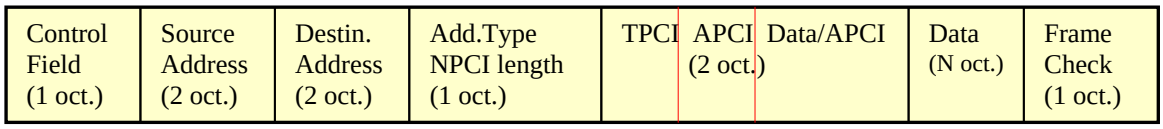

Ilustración 3.2.1-2. Formato de trama.

Nivel de red:

- Implementado en nodos con funciones de encaminamiento.
- Control de flujo.
- Garantiza al nivel transporte la independencia de la ruta y de la topología del segmento de red.

Nivel de transporte:

- 4 tipos de comunicaciones:
    - Multicast.
    - Broadcast.
    - Punto a punto no orientada a conexión.
    - Punto a punto orientada a conexión.

Nivel de aplicación:

El servicio de aplicación es distinto dependiendo del tipo de comunicación. El tipo broadcast y el punto a punto están relacionados con la red de gestión y el tipo multicast está destinado a operaciones runtime.

3.2.1.4 Modos de configuración.

El estándar KNX contempla 3 modos de configuración [12]:

- Modo-S (system): Los nodos del sistema son configurados mediante una aplicación sobre PC. Sólo los instaladores profesionales tendrán acceso a este tipo de material y a las herramientas de desarrollo.
- Modo-E (easy): Durante la instalación se configuran pequeños detalles sin necesidad de PC, ya que los dispositivos son programados en fábrica para una función determinada. Tendrán una funcionalidad más limitada que el modo-S ya que viene establecida de fábrica.
- Modo-A (automatic): No se necesita configurar nada porque los dispositivos presentan capacidad plug&play.

3.2.1.5 KNX ANubis.

La especificación KNX ha ido extendiéndose con lo que se denomina ANubis. ANubis (Advance Network for Unified Building Integration and Services) es una mezcla de protocolos, interfaces, modelos y herramientas para integrar una instalación KNX en un entorno LAN o WAN. Como ejemplo de las nuevas funcionalidades la posibilidad de transportar tramas KNX sobre IP [12].

3.2.1.6 Herramientas software.

KNX presenta una serie de herramientas software sobre PC, que facilita el diseño y la configuración de instalaciones KNX. Estas herramientas, denominadas ETS (EIB Tool Software), se heredan de EIB y tienen dos tareas [3]:

- Diseño y configuración de dispositivos del modo S. El ETS accede a un conjunto de datos del dispositivo, proporcionado por el fabricante, y que contiene detalles de ese dispositivo para posteriormente configurarlo dentro de la red.
- Integración de redes con dispositivos KNX de distintos modos. El ETS es capaz de explorar la red par descubrir los dispositivos presente en la instalación y ajustar parámetros.

El ETS consta de los siguientes módulos, usados para realizar las diferentes tareas necesarias en la fase de diseño de proyecto y puesta en marcha:

- Configuración: por medio de este módulo se definen la configuración general del ETS, opciones generales, impresión, contraseñas, idiomas, formato de las direcciones de grupo y filtro del fabricante.
- Diseño de proyecto: a través de este módulo pueden definirse las estructuras del proyecto, así como insertar y conectare los componentes necesarios para implementar las funciones del sistema.
- Puesta en marcha/test: este módulo facilita la puesta en funcionamiento y consiguiente comprobación de los sistemas.
- Administración de productos: este módulo permite gestionar los productos de los distintos fabricantes. Por ejemplo, se pueden importar los datos de los productos de un fabricante en concreto desde un disquete o CD-ROM.
- Herramientas de conversión: permiten al usuario recuperar y editar proyectos creados con versiones anteriores de ETS.

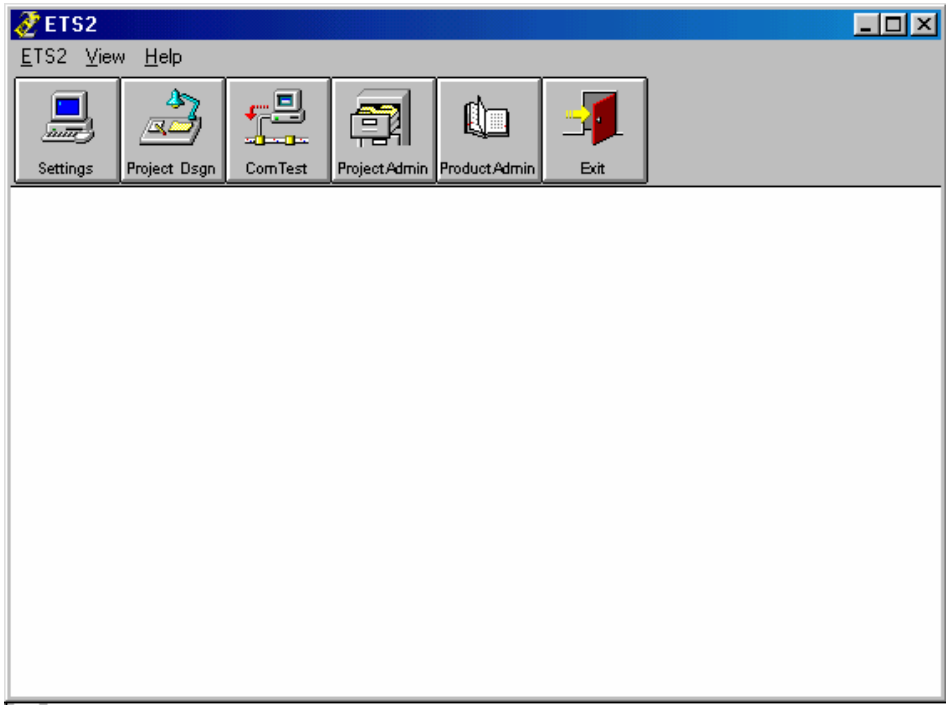

Ilustración 3.2.1-3. Herramienta ETS [3].

3.2.1.7 Norma EN-50090.

La norma EN 50090 se divide en nueve partes [12]:

- EN 50090-1: Estructura de la normalización.
- EN 50090-2: Generalidades del sistema:
  - EN 50090-2-1. Arquitectura.
  - EN 50090-2-2. Requisitos técnicos generales.
  - EN 50090-2-3. Seguridad funcional “Normal”.
  - EN 50090-2-4. Seguridad funcional “Seguridad Relacionada”.
- EN 50090-3: Aspectos de la aplicación:
  - EN 50090-3-1. Introducción.
  - EN 50090-3-2. Proceso Usuario.
  - EN 50090-3-3. Interconexión.
- EN 50090-4: Medio independiente:
  - EN 50090-4-1. Capa de Aplicación.
  - EN 50090-4-2. Capa de Transporte, Red y partes generales de la capa de unión de datos para HBES Clase 1.
- EN 50090-5: Soporte y capas dependientes del soporte:
  - EN 50090-5-1. Corrientes portadoras.
  - EN 50090-5-2. Par trenzado Clase 1.
  - EN 50090-5-3. Cable coaxial.
  - EN 50090-5-4. Infrarrojos.
  - EN 50090-5-5. Radio Frecuencia.
- EN 50090-6: Interfaces:
  - EN 50090-6-1. Interface Universal.
  - EN 50090-6-2. Proceso de Interface.
  - EN 50090-6-3. Interface del Medio.

    - EN 50090-6-4. Pasarelas residenciales.
- EN 50090-7: Gestión del sistema:
    - EN 50090-7-1. Procedimientos de gestión.
- EN 50090-8: Conformidad de productos.
    - EN 50090-8-1.Conformidad.
    - EN 50090-8-2. Perfiles de dispositivos.
- EN 50090-9: Requerimientos de instalación:
    - EN 50090-9-1. Par trenzado Clase 1 Cableado.
    - EN 50090-9-2. Inspección.

3.2.2. BACnet.

BACnet (Building Automation and Control NETwork) es un protocolo abierto, diseñado específicamente para el control de edificios. Fue desarrollado bajo el patrocinio de ASHARE, asociación norteamericana de fabricantes e instaladores de equipos de calefacción y aire acondicionado. En la actualidad, ASHARE se encarga del mantenimiento, mientras que la promoción y el fomento de BACnet lo lleva a cabo BMA (BACnet Manufacture Association), que es un organismo constituido por empresas relacionadas con equipos que utilizan BACnet para su comunicación [17].

Adoptado por ANSI como estándar americano en 1995 (ANSI/ASHARE 135-1995). En el año 2003 se convirtió en estándar internacional ISO (ISO 16484-5) y en norma europea CEN (CEN TC 247).

Presenta una arquitectura flexible y puede ser fácilmente aumentado y mejorado. Además, puede ser implementado en aparatos de diverso tamaño y es un protocolo que no depende de la tecnología subyacente. Este conjunto de propiedades le proporcionan gran versatilidad.

3.2.2.1 Modelo.

BACnet no define un nivel físico, enlace y red concretos. Soporta cinco tipos de tecnologías de red [17]:

- Ethernet. Las principales ventajas son que está preinstalado en muchos tipos de edificios y es muy rápido (1Gbps). Por el contrario, presenta alto coste por dispositivo y limitaciones de distancias.
- ARCNET. Se trata de un estándar ANSI, que soporta varios medios de transmisión y que alcanza velocidades de hasta 7.5 Mbps. Como inconvenientes aparecen el elevado coste de los dispositivos y las limitaciones de distancias.
- Punto a punto. Se usa sobre líneas telefónicas punto a punto de baja velocidad (56Kbps). Su principal ventaja es el bajo coste de los dispositivos.
- Master-Slave/Token Passing (MS/TP). Es un estándar ANSI que sólo soporta como medio de transmisión el par trenzado. Su velocidad de transmisión es baja, 76 Kbps pero su coste también es bajo.
- LonTalk. Usado en las redes domóticas LonWorks, soporta varios medios de transmisión y alcanza una velocidad de 1.25 Mbps. Sin embargo, muestra restricciones en el tamaño de las aplicaciones y en los rangos de distancia.
- Bacnet/IP. Los recursos BACnet son a la vez nodos IP, con su propia dirección IP y su pila de protocolos (TCP/IP).

La información en un sistema BACnet es representada mediante unas estructuras de datos denominadas objetos. Los objetos no son más que una colección de información relativa a una

función determinada, a una entrada o a una salida física. Cada objeto es caracterizado por un conjunto de propiedades que describen su modo de operación.

BACnet define un conjunto de veintitrés objetos estándar, que representan las funcionalidades típicas en un sistema de control de un edificio actual. Este conjunto de objetos puede extenderse fácilmente mediante la creación de otros objetos. A la colección de objetos que representan las funciones que realiza un recurso real se denomina recurso BACnet.

3.2.3. CEBus.

La tecnología CEBus (Consumer Electronics Bus) fue desarrollada por EIA (Electronics Industry Association), desde 1984 hasta su aprobación en Octubre de 1992 [10].

Se trata de un estándar americano, definido en EIA-600 y diseñado específicamente para el hogar. Sin embargo, el nivel físico no cumple la norma europea relativa a la transmisión por líneas eléctricas de baja tensión CELENEC EN-50065, por lo que no es conveniente su instalación en los hogares europeos.

En 1994 se crea CIC (CEBus Industry Council), asociación, sin ánimo de lucro, de fabricantes y empresas electrónicas que se encarga de los nuevos desarrollos de CEBus y la certificación de nuevos productos. Entre las empresas asociadas se pueden destacar Microsoft, IBM Honeywell o Sony.
El CIC dispone de laboratorios donde se verifica la conformidad de un producto CEBus y su rendimiento dentro de un entorno domótico. El logo CEBus en un producto certifica que el mismo a pasado las pruebas del CIC.

Al estar diseñado para el hogar, resulta simple su instalación y su uso y además permite que sea fácil su extensión. Como desventaja, existen pocos productos que lo implementan y son caros.

3.2.3.1 Modelo.

La especificación se basa en el modelo OSI, definiendo los niveles 1, 2, 3 y 7. Cada dispositivo posee una dirección que viene establecida de fábrica y se utiliza para la identificación unívoca del mismo dentro del bus [10].

Nivel físico:

- Medios de transmisión:
  - Línea eléctrica:
    - ➔ Tasa media: 7,5 Kbps.
    - ➔ Modulación en frecuencia con espectro ensanchado.
  - Par trenzado:
    - ➔ Régimen binario: 10 Kbps.
    - ➔ Modulación FSK.
    - ➔ Distancia máxima: 500 pies.
  - Radiofrecuencia:
    - ➔ Régimen binario: 10Kbpa.
    - ➔ Modulación binaria en fase.
    - ➔ Frecuencia central: 915 Mhz.
  - Coaxial:
    - ➔ Distancia máxima: 150 pies.
  - Infrarrojos.
  - Fibra óptica.

Nivel de enlace:

- Servicio no orientado a conexión con o sin asentimiento.
- Admite difusión.
- Admite direccionamiento de grupos de dispositivos.
- Formato de la trama de datos:

Preámbulo (8 bits)	Control (8)	Direcc. Dest. (16)	DHC (16)	Direcc. Orig. (16)	SHC (16)	Datos (máx. 256)	FCS (8)

Ilustración 3.2.3-1. Formato de trama.

DHC: Destination House Code. Identifica la dirección destino fuera del grupo de sistemas que comparten el mismo medio de comunicación. Junto con la dirección destino identifica unívocamente a un nodo o a un conjunto de nodos.
SHC: Source House Code. Identifica, junto con la dirección origen, el nodo fuente de la información. Si el campo SHC es null se considera que es igual al DHC.

Nivel de red:

No presenta una topología de red concreta. Por lo tanto, se puede implementar cualquiera, aunque lógicamente se trata como si fuera un bus.
Implementado en dispositivos con funcionalidad de router, que permiten comunicar distintos segmentos de red. Esta función puede estar integrada dentro de otro dispositivo con más tareas.

Nivel de aplicación:

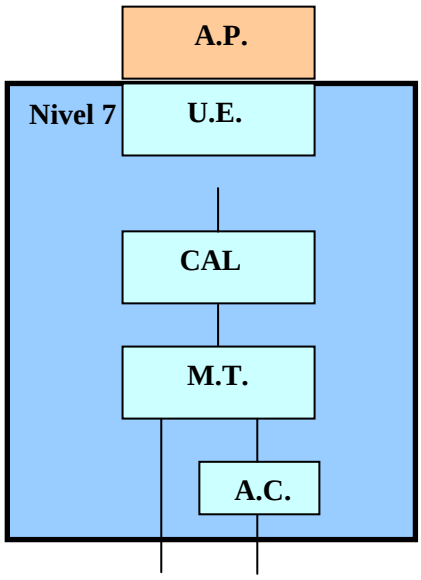

Ilustración 3.2.3-2. Nivel de aplicación.

- A.P.: Application Process. Lleva a cabo el procesamiento de la información. Conecta con la capa de aplicación mediante el U.E.
- U.E.: User Element. Llama los servicios de CAL Element para ejecutar los deseos del Application Process.

- CAL: Common Application Language. Lenguaje mediante el cual los recursos CEBus se comunican. Es un lenguaje orientado a comandos que permite controlar dispositivos CEBus y asignar recursos. Las funciones de asignación de recursos permiten pedir, usar y liberar recursos CEBus. Las funciones de control proporcionan la capacidad de enviar comando CAL a dispositivos remotos, y responder a comandos CAL.
- M.T.: Message Transfer. Elemento de comunicación dentro de la capa de aplicación. Se encarga de los servicios de autenticación y encriptación.
- A.C.: Association Control. Permite la asociación de dos procesos de aplicación.

3.2.3.2 Home Plug and Play.

Iniciativa del CIC para crear dispositivos con capacidad Plug&Play empleando la tecnología CEBus. Es un protocolo del nivel de aplicación que usa como base el CAL (Common Application Language) [10].

Permite que los distintos subsistemas que integran el sistema global se comuniquen entre sí, sin considerar las capas bajas. Para ello, define el contenido de los mensajes de control que se intercambian los distintos nodos y controladores, proporcionando todos los detalles necesarios para construir estos mensajes, los cuales provocan una determinada acción en un recurso.

Cuando un nuevo nodo se instala en el sistema debe ser inicializado y configurado. Con la filosofía plug&play es el propio sistema el que realiza el reconocimiento y la configuración del nuevo nodo sin apenas intervención ni del instalador ni del usuario final.

3.2.3.3 Norma EIA-600.

EIA-600 se divide en las siguientes partes [10]:

- EIA-600.10: Introducción al estándar CEBus.
- EIA-600.20: Descripción general.
- De EIA-600.31 a EIA-600.39: Medios físicos y nivel físico OSI.
- De EIA-600.41 a EIA-600.46: Niveles de enlace, red y aplicación de CEBus.
- De EIA-600.51 a EIA-600.54: Descripción de las capas OSI necesarias para implementar una función de rutado entre medios físicos EIA-600.
- De EIA-600.61 a EIA-600.64: Descripción de las capas OSI necesarias para implementar una función de brouter entre medios físicos y medios no físicos EIA-600 (radiofrecuencia e infrarrojos).
- De EIA-600.81 a EIA-600.82: Descripción de CAL (Common Application Language).

3.2.4. Zigbee.

Zigbee [33] es un estándar de comunicaciones sin cables, desarrollado por Zigbee Alliance. Dicha asociación fue creada por Invensys, Mitsubishi Electric, Motorola y Philips, con el objetivo de desarrollar un estándar de bajo coste, de bajo consumo y que proporcionara soluciones de comunicación sin cables a dispositivos que no requieren elevado ancho de banda pero sí un mínimo consumo de energía como es el caso de sensores y controladores.
En la actualidad, Zigbee Alliance está constituida por cerca de cien miembros, entre proveedores de servicios de Internet, operadores de red, fabricantes de equipos, etc., comprometidos a promover el uso de este nuevo estándar, llamado a ser uno de los importantes dentro del sector inalámbrico.

Zigbee se apoya en el estándar de nivel inferior IEEE 802.15.4, desarrollado por IEEE. IEEE 802.15.4 es un protocolo de paquetes de datos para redes sin cables, que especifica la capa física y la subcapa MAC. La subcapa LLC está estandarizada en la norma 802.2 y es común a los estándares 802, tales como 802.3, 802.11 y 802.15.1.
Zigbee toma todas las ventajas del estándar 802.15.4 y le añade la capa de red, seguridad y la aplicación software.

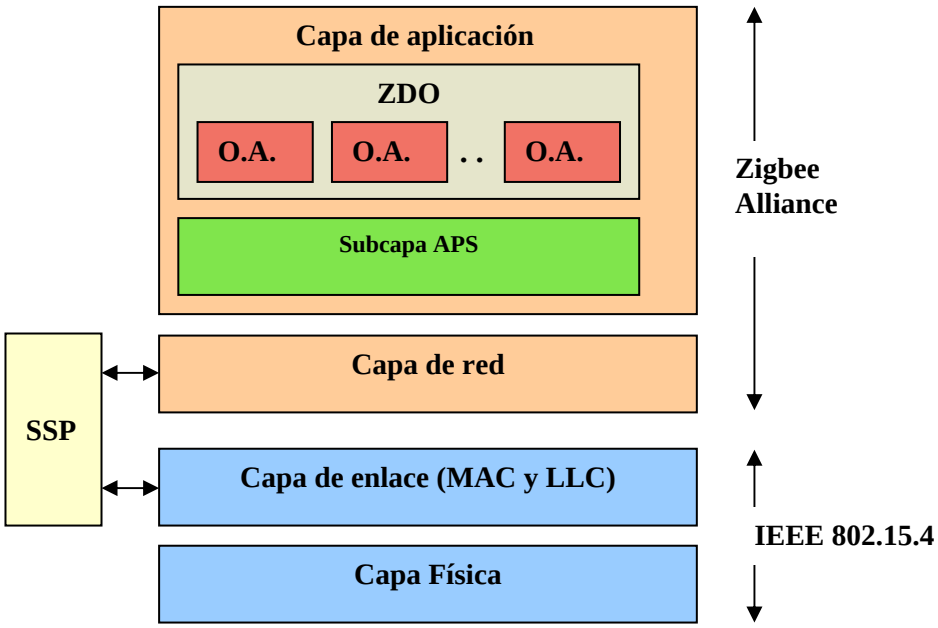

Ilustración 3.2.4-3.2.4-1. Capas Zigbee.

Aparte de la automatización y monitorización de edificios y hogares, Zigbee se puede aplicar también en sistemas de diagnóstico médico, periféricos para PC, juguetes, etc., gracias a su simplicidad y su bajo coste. Además cabe destacar que permite la comunicación entre recursos de distintos fabricantes y su bajo consumo de energía.

3.2.4.1 IEEE 802.15.4.

IEEE es el responsable del estándar 802.15.4, que define el nivel físico y la capa de acceso al medio. Es un protocolo simple, bidireccional y que presenta buenas cualidades técnicas en ambientes de baja SNR [13].
El alcance máximo está entorno a los 75-100 metros.
Utiliza DSSS (Direct Sequence Spread Spectrum) para mejorar la sensibilidad del receptor y obtener mayor robustez ante el multitrayecto y las interferencias.

Emplea tres bandas de radio:

- 2.4 GHz: de ámbito mundial, usada también por Wi-Fi y Bluetooth. Define dieciséis canales en la banda, con una tasa de datos de 250 Kbps. La modulación empleada es O-QPSK.
- 915 MHz: es la banda para Estados Unidos y parte de Asia. La tasa de datos es de 40 Kbps para cada uno de los diez canales definidos. Utiliza la modulación BPSK.
- 868 MHz: único canal para Europa a 20 Kbps. La modulación que usa es BPSK.

Se definen cuatro tipos de tramas en la capa MAC:

- Trama de datos. Emplea direcciones IEEE de 64 bits y direcciones cortas de 16 bits. Es posible comprobar si existen errores en los datos mediante el FCS.

FrameControl (2 oct.)	Data Sequence Number (1oct.)	Address Info. (4-20 oct.)	Data (N< 104 oct.)	FCS (2 oct.)

Ilustración 3.2.4-2. Trama de datos.

- Trama de asentimiento.
- Trama de comandos. Esta trama la utiliza el controlador de red para controlar y configurar los distintos nodos del sistema.

Frame Control	Data Sequence Number	Address Information	Comand type (1 oct.)	Data	FCS

Ilustración 3.2.4-3. Trama de comandos.

- Trama beacon. Es opcional y se utiliza para la sincronización de los nodos. Importante en redes extensas. Las envía el coordinador de red periódicamente para anunciar la estructura de supertrama a los dispositivos de la red.

El protocolo de capa MAC puede operar en dos modos, con o sin tramas beacon. Cuando no se emplean las tramas beacon el método que se emplea para acceder al medio es CSMA/CA, mientras que si se utilizan estas tramas se emplea una estructura de supertrama. Este modo se emplea cuando existen aplicaciones que requieren un ancho de banda dedicado.
Las supertramas está delimitadas por tramas beacon y se dividen en dos partes: parte activa y parte inactiva. Los dispositivos enviarán información solo durante el período activo y durante el período inactivo entrarán en el modo de baja potencia para el ahorro de energía.
La parte activa de cada supertrama se divide en 16 intervalos iguales de tiempo, agrupados en dos secciones:

- CAP (período de acceso con contienda). Durante este período los nodos de la red acceden a la misma mediante el método CSMA/CA.
- CFP (período libre de contienda). El coordinador de la red asigna en este período intervalos de tiempo para las aplicaciones que necesitan un ancho de banda dedicado. Estos slots se denominan GTS (Guaranteed Time Slots). Cuando un dispositivo tiene que enviar su información, esperará a que llegue su GTS asignado.

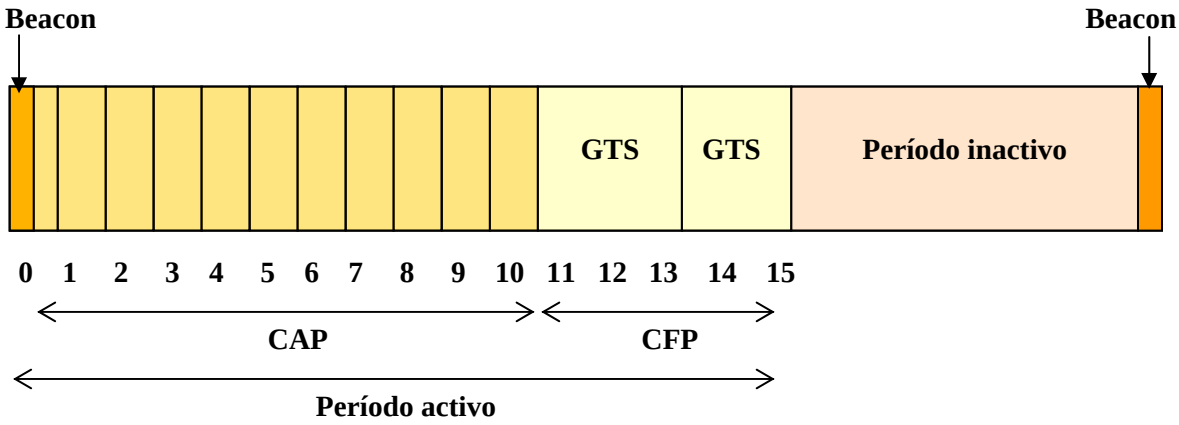

Ilustración 3.2.4-4. Formato supertrama.

3.2.4.2 Capa de red.

Entre sus responsabilidades destacan [21]:

- Gestión de unión/abandono de dispositivos.
- Direccionamiento.
- Sincronización dentro de la red.
- Encaminamiento de paquetes.
- Seguridad.

En una red Zigbee existen dos tipos de recursos: FFD (Full Function Device), encargados de tareas como el control de la red y el encaminamiento de paquetes y RFD (Reduce Funtion Device), que podrían verse como los nodos esclavos.

Existen tres topologías de red posibles:

- Estrella: un coordinador conectado a una serie de esclavos. Esta disposición es típica en el hogar, debido a su simplicidad y su bajo coste.

Ilustración 3.2.4-5. Estrella.

- Árbol: se usa para extender el rango de una red en estrella o para unir dos redes. Posee más de un FFD.

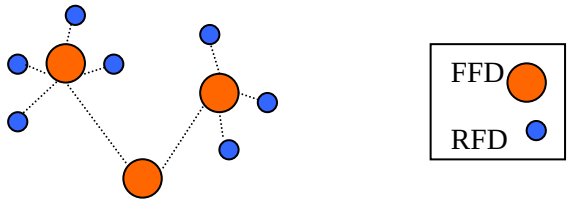

Ilustración 3.2.4-6. Árbol.

- Malla: topología adecuada para cubrir áreas extensas que contienen gran número de nodos.

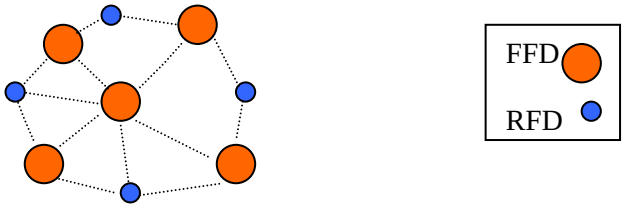

Ilustración 3.2.4-7. Malla.

3.2.4.3 Capa de aplicación.

La capa de aplicación está constituida por la subcapa APS (Application Support), el ZDO (Zigbee Device Object) y los objetos de aplicación. Esta subcapa proporciona servicios de descubrimiento y binding a los objetos, mientras que el ZDO contiene los objetos de aplicación (A.O.) y se encarga de definir el papel del dispositivo dentro de la red y de establecer una relación segura entre los dispositivos de la red, seleccionando uno de los mecanismos de seguridad que Zigbee implementa, como el de clave pública, clave simétrica, etc.

3.2.4.4 Seguridad.

El estándar Zigbee especifica tres niveles de seguridad [21]:

- Sin seguridad.
- Listas de control de acceso (ACL). Previene accesos no autorizados pero no proporciona cifrado de la información.
- Encriptación y autenticación AES (Advanced Encryption Standard) de 32 a 128 bits.

El proceso de seguridad puede llevarse a cabo en la capa MAC o en la capa de red, aunque la capa superior controla dicho proceso. Cuando se transmite (recibe) una trama segura se invoca al SSP (Security Services Provider) que es el que procesa la trama. El SSP mira el destino (origen) de la trama, recupera la clave asociada a ese destino (origen) y aplica el proceso de seguridad adecuado.
La implementación de la seguridad es transparente al usuario final, lo que resulta una ventaja importante en aplicaciones comerciales.

3.2.5. X-10.

X-10 es la tecnología por corrientes portadoras más antigua y más utilizada en sistemas de control doméstico. Fue desarrollada entre 1976 y 1978 por la empresa escocesa Pico Electronics. X-10, en sí, no es propietario pero los dispositivos X-10 deben incluir los circuitos diseñados por dicha empresa aunque el royalty no es muy elevado [1].

Es un protocolo que está muy extendido en el mercado residencial y de pequeñas empresas debido a su sencillez, flexibilidad y fácil manejo. Otra gran ventaja es su cómoda instalación ya que al emplear la red eléctrica no es necesario tender nuevos cables. Todas estas cualidades originan que sea la mejor solución para instalaciones domóticas pequeñas y no muy complejas.

El protocolo X-10 exige unas normas, que deben seguir los fabricantes de productos X-10 para lograr una correcta estandarización, de este modo productos de distintos fabricantes son compatibles e intercambiables. Entre los fabricantes más conocidos se encuentran: Leviton Manufacturing Co., General Electric, C&K Systems, Honeywell, Ademco, DSC, IBM, etc.

3.2.5.1 Modelo.

X-10 utiliza la red eléctrica de baja tensión para la transmisión de datos a muy baja velocidad (50 bps en Europa y 60 bps en Estados Unidos), empleando modulación de impulsos de 120 Khz [1].

El “1” binario se representa por un pulso de 120 Khz durante un milisegundo y de potencia 0,5 W, mientras que el “0” binario se representa por la ausencia de este pulso. Para insertar el impulso es necesario que la señal de corriente alterna presente un nulo de potencia. Al tratarse de un sistema trifásico el pulso de 1 ms se transmite tres veces para que coincida con el paso por cero en las tres fases (desfasadas 120º). Por tanto, el tiempo de bit coincide el periodo de la señal eléctrica.

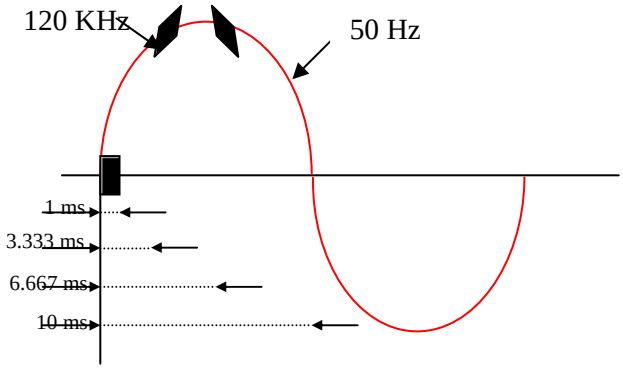

Ilustración 3.2.5-1. Señal X-10 [3].

El protocolo X-10 posee únicamente seis comandos, representados por un código de función. Las órdenes posibles son: encender, apagar, reducir, aumentar, todo encendido y todo apagado.
Es capaz de direccionar hasta 256 dispositivos, contemplando 16 grupos de direcciones llamados códigos de casa (letras A-P) y 16 direcciones individuales que se denominan códigos numéricos o de unidad (números 1.16).

Una trama X-10 está constituida por 11 bits correspondientes a un código de inicio de 2 bits, un código de casa de 4 bits y los últimos 5 bits representan o bien un código numérico o el código de función. Se tratará del código numérico cuando se transmite una trama de dirección y será el código de función cuando la trama que se envía indica una orden concreta al dispositivo con el que se comunicó previamente. Esta trama se transmite siempre dos veces por motivos de seguridad.

Código Inicio (2 bits)	Código de casa (4 bits)	Código Numérico o de Función (5 bits)

Ilustración 3.2.5-2. Formato trama.

El cambio de direccionamiento de un elemento es sencillo ya que se le puede cambiar su dirección física de manera manual. Cada dispositivo consta de una o dos ruedas con las que determinar el código de casa y el código de unidad.

3.2.5.2 Herramientas software.

Aunque el sistema no necesita ningún software especial para su manejo, existen en el mercado programas que permiten manejar, controlar y programar los dispositivos desde un PC. De esta forma y mediante un navegador web o una aplicación telnet se podría gobernar el sistema desde cualquier lugar del mundo [3].
Ejemplos de estos programas son:

- Active Home. Aplicación en modo local.
- HomeSeer. Software que permite el control a través de la web.
- HALL 2000. Controla dispositivos X-10 mediante la voz.

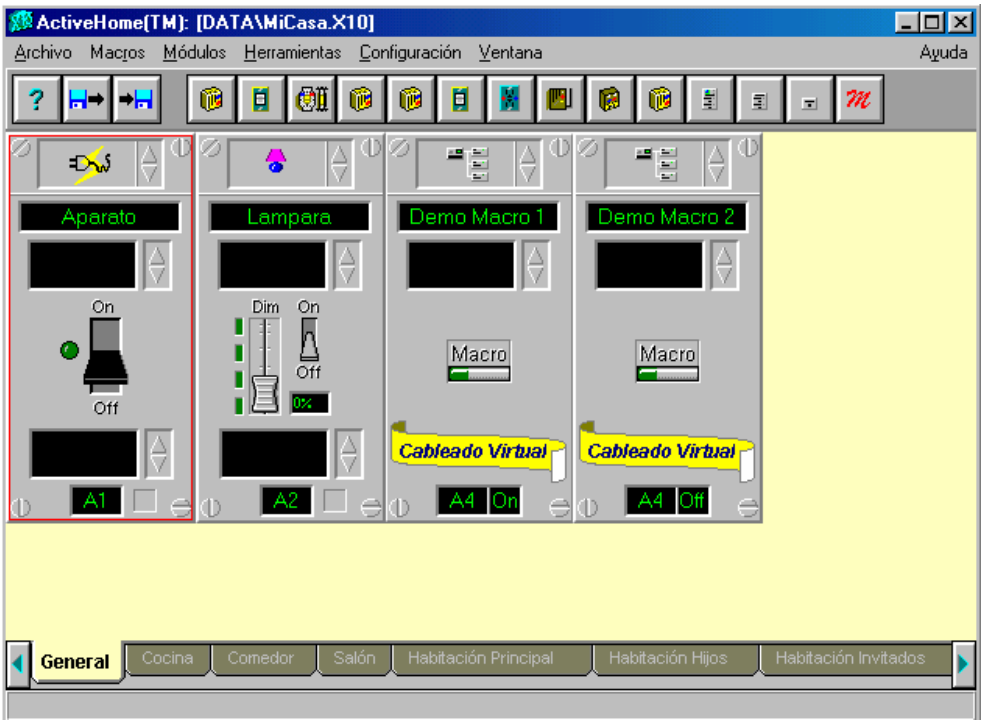

Figura 3.2.5-3. Programa ActiveHome [3].

3.2.6. LonWorks.

La tecnología propietaria LonWorks [23] fue desarrollada por la compañía Echelon en 1992. Una red LonWorks es una completa y robusta solución al problema del control de sistemas en edificios e industrias. Está especialmente indicada para la automatización a gran escala ya que para el hogar existen soluciones más económicas y de buenas prestaciones.
Los objetivos que persigue son flexibilidad y estandarización, interoperabilidad entre empresas fabricantes y compatibilidad total entre sistemas.
La tecnología LonWorks es abierta en el sentido de que no es necesario utilizar ningún software propietario para controlar, mantener o monitorizar la red.
Su principal inconveniente es la poca oferta de productos que hay en España, aunque en Estados Unidos se han desarrollado miles de proyectos con esta tecnología.

En Mayo de 1994, Echelon y diversas compañías fundaron LonMark Interoperability Association, cuya misión es trabajar para la fácil integración de sistemas basados en la tecnología LonWorks de distintos fabricantes. Actualmente existen cerca de 3.500 compañías que usan las redes de control LonWorks, la asociación les proporciona un foro abierto para que puedan trabajar conjuntamente y promover la compatibilidad de los recursos.
Los productos que se ajustan a las pautas de compatibilidad, establecidas por la asociación, llevan el logotipo LonMark. Este signo es un indicador de que el producto ha superado las pruebas de conformidad y ha sido diseñado para operar conjuntamente a través de una red LonWorks.

3.2.6.1 Neuron Chip.

Los dispositivos LonWorks deben incluir un microcontrolador específico, denominado Neuron Chip. Este circuito integrado fue diseñado por Echelon en 1990 y su producción sigue estando controlada por esta empresa, que sólo ha concedido licencia a tres fabricantes (Cypress Semiconductor, Motorola y Toshiba). Esto ha provocado que los precios no se hayan reducido en exceso [23].

Este chip está constituido internamente por tres microprocesadores. Dos de ellos están optimizados para ejecutar el protocolo de comunicaciones, mientras que el restante se dedica a ejecutar el programa de control. Disponer de dos procesadores destinados a tareas de comunicación y otro dedicado a la aplicación asegura que la complejidad del programa no afecta negativamente a la respuesta de la red. Además, encapsular ambas funciones en un solo chip ahorra tiempos de diseño y producción.
Además, consta de memoria EEPROM, RAM y ROM y subsistemas de comunicación y entrada/salida. La memoria de sólo lectura contiene un sistema operativo, el protocolo LonTalk y una librería de entrada/salida.

Las aplicaciones para el Neuron Chip se escriben en un lenguaje variante del C conocido como Neuron C, lo que simplifica la configuración de nodos y la red. Los elementos que caracterizan este lenguaje son las variables de red, la sentencia “when” que provoca la activación por eventos de diversas acciones que son ejecutadas de forma cooperativa, y los objetos de entrada/salida.

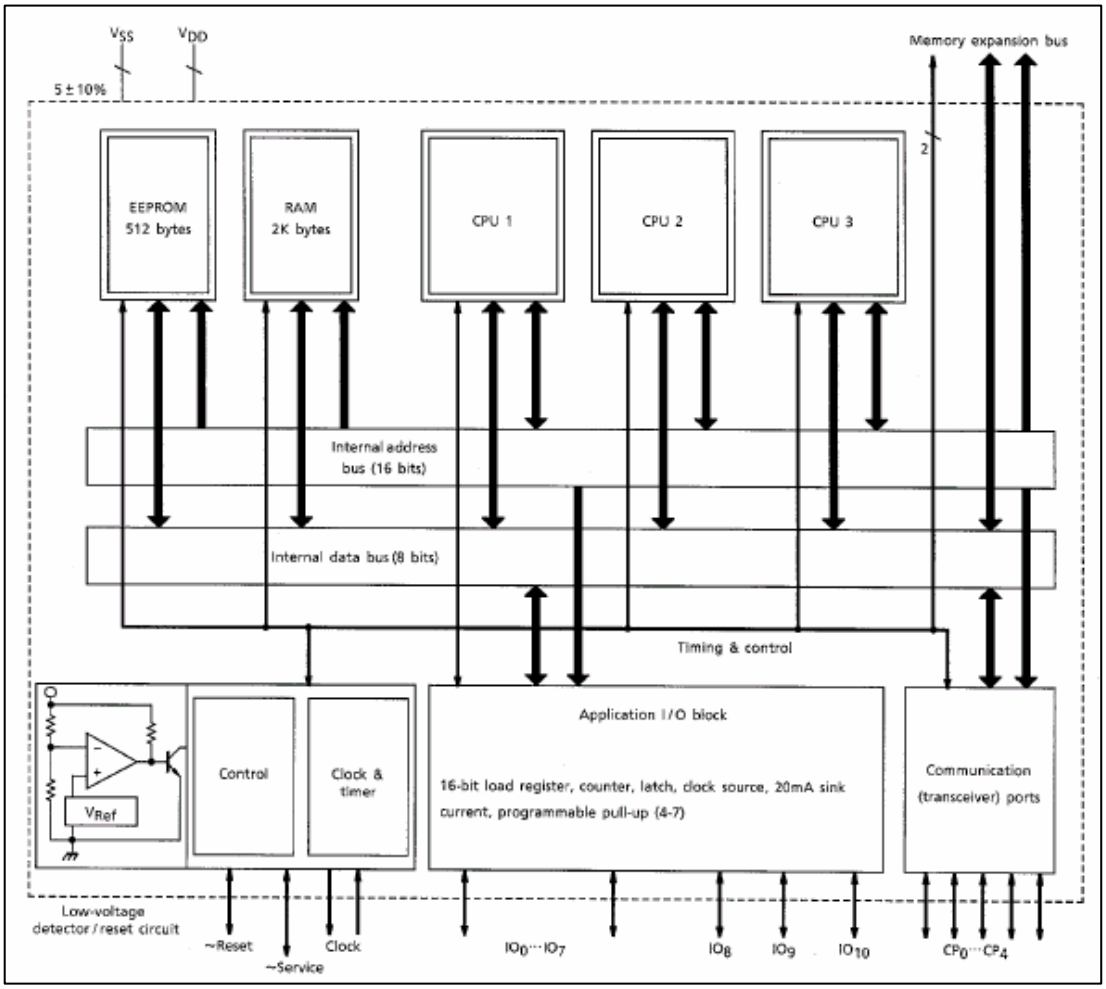

Ilustración 3.2.6-1. Diagrama de bloques de un Neuron Chip de Toshiba.

3.2.6.2 Modelo.

La tecnología LonWorks se basa en el modelo de capas OSI, implementando los siete niveles que especifica dicho modelo. Esto le proporciona una gran ventaja frente a otras tecnologías de control ya que proporciona servicios completamente implementados en la solución. En cambio, dichos servicios deben implementarse en la capa de aplicación en dispositivos basados en otros protocolos, provocando posibles incompatibilidades entre diferentes implementaciones de distintos fabricantes.

Soporta gran variedad de medios de transmisión: par trenzado, línea eléctrica, radiofrecuencia, infrarrojos, coaxial y fibra óptica. El Neuron Chip proporciona un puerto que puede configurarse para actuar como interfaz de diversos transceptores de línea. El transceptor proporciona una interfaz de comunicación física entre el dispositivo y el medio físico. Este transceptor se encarga de adaptar las señales del circuito integrado a los niveles necesarios de cada medio. Dependiendo del transceptor usado se tendrá distinta velocidad binaria, topología de red, distancia de alcance y dispositivos que soporta. Dispositivos con distintos tipos de transceptores pueden operar juntos pero requieren el uso de un router [23].

Tipo de canal	Medio	Régimen binario	Transceptores compatibles	Dispositivos soportados	Distancia máxima
TP/FT-10	Par trenzado	78 Kbps	FTT-10, FTT-	64-128	500 m(topología libre)

	(topología libre o en bus)		10A, LPT-10		2200 m (topología en bus)
TP/XF-1250	Par trenzado (topología en bus)	1.25 Mbps	TPT/XF-1250	64	125 m
PL-20	Línea eléctrica	5.4 Kbps	PLT-20, PLT-21, PLT-22	Depende del entorno	Depende del entorno
IP-10	LonWorks sobre IP	Determinado por la red IP	Determinados por la red IP	Determinados por la red IP	Determinados por la red IP

Tabla 3.2.6-1: Canales LonWorks.

Se emplea como mecanismo de acceso al medio el conocido como predictive p persistent CSMA, cuyo objetivo es la reducción de colisiones incluso en situaciones de sobrecarga de la red.

El protocolo LonWorks soporta varios tipos de direcciones:

- Dirección física. Se trata de la dirección asignada durante el proceso de fabricación del dispositivo. Se graba en la EEPROM del Neuron Chip y no se modifica durante el tiempo de vida del dispositivo. Consta de 48 bits y se denomina Neuron ID.
- Dirección de dispositivo. Por motivos de eficiencia en el encaminamiento la dirección física no se emplea y es durante la instalación del nodo en una red determinada cuando se fija la dirección de dispositivo. Esta dirección consta de tres campos: identificador de dominio, identificador de subred e identificador de nodo. Los nodos necesitan pertenecer al mismo dominio para intercambiarse mensajes. Dentro de un dominio pueden existir hasta 256 subredes y 32.385 nodos y una red puede llegar a tener 2^{48} dominios.
- Dirección de grupo. Se define un grupo como una asociación lógica de dispositivos dentro de un dominio. A diferencia de una subred, los dispositivos pueden agruparse sin considerar la localización física dentro del dominio. Los grupos proporcionan un método eficiente para optimizar el ancho de banda de la red cuando se necesitan enviar un paquete a múltiples dispositivos.
- Dirección de difusión. Una dirección de difusión identifica a todos los dispositivos dentro de una subred o de un dominio. Esta dirección permite el envío de un paquete a todos los dispositivos.

Los nodos LonWorks se comunican mediante el protocolo LonTalk [11]. Este protocolo fue desarrollado por Echelon en 1990 y permite que los programas de aplicación de distintos dispositivos se envíen mensajes sin necesidad de conocer la topología de la red. Este protocolo está definido por el estándar ANSI/EIA 709.1.
El protocolo se asegura la fiabilidad de las transmisiones mediante la confirmación de un envío correcto entre emisor y receptor.
La integridad de los datos se garantiza mediante un control de errores basado en códigos de polinomios de 16 bits. Para que la red sea más segura, cada transmisión de paquete se realiza usando un sistema de autenticación de remitente
Además, proporciona comunicaciones peer-to-peer y transmisiones prioritarias.
Todas las comunicaciones entre dispositivos constan de uno o varios paquetes. Cada paquete está compuesto por uno o más bytes de longitud y contiene la información requerida por cada una de las capas.

El protocolo implementa el concepto de variable de red. Estas variables simplifican en gran medida las tareas de diseño de los programas de aplicación para la compatibilidad entre productos de distintos fabricantes.
Una variable de red es un conjunto de datos que un programa de aplicación espera obtener de otro dispositivo de la red (variable de red de entrada) o que proporcionará a otro dispositivo de

la red (variable de red de salida). Cuando un programa de aplicación tiene un cambio en el valor de alguna de sus variables de salida, pasa el nuevo valor al firmware del dispositivo, que se encargará de transmitir el dato al dispositivo correspondiente. Del mismo modo, cuando el firmware recibe un valor actualizado de una variable de red de entrada lo hace llegar al programa de aplicación.
Se puede decir que se crea una conexión lógica entre una variable de red de entrada de un dispositivo y una variable de red de salida de otro dispositivo. Esta conexión tiene el mismo efecto que una conexión física entre ambos dispositivos.
Todas las variables de red tienen un tipo que define las unidades, escalado y estructura de los datos contenidos dentro de la variable. Las variables deben tener el mismo tipo para poder conectarse.

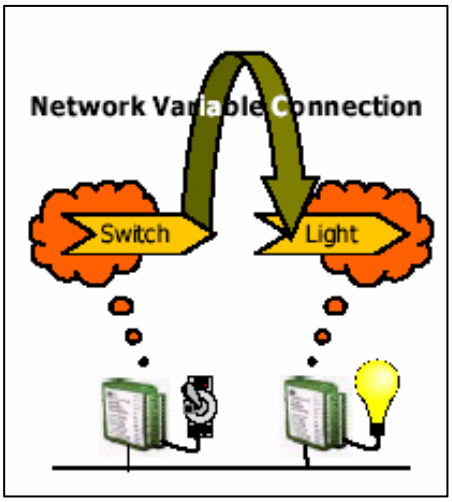

Ilustración 3.2.6-2. Variables de red.

3.2.6.3 Herramientas software.

Echelon tiene desarrollado una amplia variedad de software para el sistema LonWorks. También, diversas empresas comercializan su propio software. Entre estas aplicaciones software se pueden destacar [3]:

- NodeBuilder. Paquete software de desarrollo de dispositivos, desarrollado por Echelon para Microsoft Windows. Incluye un compilador y un depurador del lenguaje Neuron C.
- LonMaker de Echelon. Herramienta de integración para el diseño, instalación y mantenimiento de redes. Integra una herramienta de ingeniería de interfaz gráfica, una herramienta de servicio e instalación gráfica, y una herramienta de operaciones de red IHM (Interfaz Hombre Máquina).

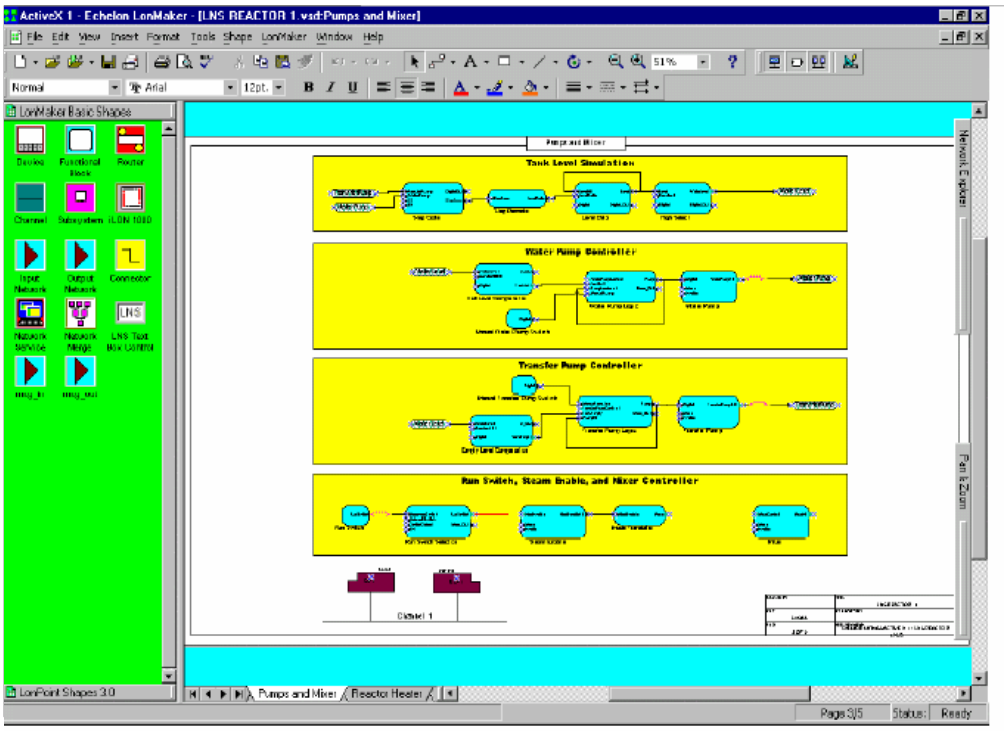

Ilustración 3.2.6-3. Herramienta LonMaker [3].

- LonManager. Analizador de Echelon para el protocolo LonWorks. Permite observar, analizar y diagnosticar problemas en la red.
- Gadget. Software para LonWorks de Adept System y analizador de redes.
- PathFinder. Herramienta para el diseño y el mantenimiento de redes LonWorks desarrollado por la empresa TLON.

3.2.7. HES.

El HES (Home Electronic System) es un estándar internacional bajo desarrollado dentro de la ISO y el IEC (ISO/IEC 10192-3). Está destinado para el control y la comunicación de pequeños edificios comerciales y para construcciones de viviendas con oficinas [18].

HES especifica el hardware y el software que permitirá a los distintos fabricantes ofrecer un conjunto de productos que pueden conectarse a diversas redes domóticas.

Existen tres tipos de clases de HES: para telecontrol (clase 1), para ancho de banda medio (clase 2) y para ancho de banda alto (clase 3).

Se distinguen los siguientes componentes de HES:

- Interfaz universal. La aplicación incorpora una interfaz para la comunicación entre distintas redes del hogar.
- Pasarela residencial. Se encarga de unir la red de control domótico del hogar con las redes externas, mediante la traducción del protocolo de comunicación de una WAN al de una LAN y viceversa.
- Métodos y modelos de interoperabilidad. Permiten que aplicaciones creadas por distintos fabricantes puedan comunicarse entre sí. Necesario para la integración de los recursos del sistema.

3.2.8. SCP.

Ante el gran número de protocolos de control existentes en Estados Unidos, Microsoft y General Electric se unen con el objetivo de lograr la convergencia de la amplia variedad de soluciones.
Con esta finalidad desarrollan SCP (Simple Control Protocol) siendo un protocolo abierto y libre de royalties que permite una comunicación robusta y segura entre dispositivos domóticos.

3.2.8.1 Características.

SCP [1] es un protocolo peer-to-peer, optimizado para redes de baja velocidad y con mucho ruido. Para la transmisión de datos emplea la red eléctrica, adoptando el nivel físico de CEBus. En la actualidad, están en vía de desarrollo otros medios físicos como el par trenzado y la radiofrecuencia.

Una de las ventajas que SCP posee, es la facilidad para la ampliación de la red y ante cambios de la misma, ya que permite el descubrimiento automático de dispositivos.

Una red física SCP es capaz de soportar aproximadamente 1.000 subredes lógicas, y en cada una de estas subredes pueden existir en torno a 2.00 dispositivos. Estos dispositivos pueden comunicarse mediante punto a punto o a través de mensajes de difusión. Estos mensajes pueden ir cifrados ya que SCP tiene varios modelos de seguridad [3].

3.2.9. HBS.

El HBS (Home Bus System) [3] es un estándar creado por un consorcio de empresas japonesas y el gobierno del país, cuyo objetivo es especificar un estándar de comunicación de dispositivos domóticos. Como medio de comunicación puede emplear cualquiera, aunque generalmente utiliza par trenzado y coaxial.

3.3. Arquitecturas software.

En la actualidad, la tendencia en el sector de la automatización del hogar o la oficina va encaminada al desarrollo de arquitecturas distribuidas que sean independientes del medio físico o el sistema operativo empleado. Así surgen Havi (Home Audio Video Interoperability), Obix, UPnP o Jini. Sus objetivos son similares, conseguir la compatibilidad entre dispositivos de distintos fabricantes y facilitar el uso al cliente. Tienen gran aceptación entre los periféricos (impresoras, escáner, etc.) y en el entorno multimedia (cámaras de vídeo o de fotos digitales, televisores, MP3s, móviles, etc.) ya que cumplen con los requisitos de capacidad y retraso exigidos en este tipo de aplicaciones. A continuación se describen UPnP y Jini, que son las dos arquitecturas más completas en estos momentos y se comenta la emergente iniciativa Obix.

Por otra parte, se describe el protocolo Modbus, muy empleado en el sector industrial y que permite una comunicación simple entre dispositivos de pocos recursos [22].

3.3.1. Modbus.

Protocolo de la capa de aplicación que proporciona comunicaciones cliente-servidor entre recursos inteligentes. Fue desarrollado por Modicon (actualmente Schneider Automation) en 1979 [29].

Es una especificación abierta muy extendida en el mundo industrial debido a su simplicidad. Usado en dispositivos como PLC, HMI, drivers, sensores o actuadores remotos.
Define una estructura de mensajes que puede ser reconocida por los diferentes dispositivos independientemente del tipo de red de comunicaciones utilizada. El protocolo describe el proceso para acceder a la información de un dispositivo, cómo debe responder éste y cómo se notifican las situaciones de error.

Es soportado por redes industriales Modbus y por redes estándar. Actualmente se implementa usando:

- TCP/IP sobre Ethernet.
- Transmisión serie asíncrona sobre una variedad de medios (cable, fibra, radio, etc.).
- Modbus plus: red de alta velocidad de paso de testigo.

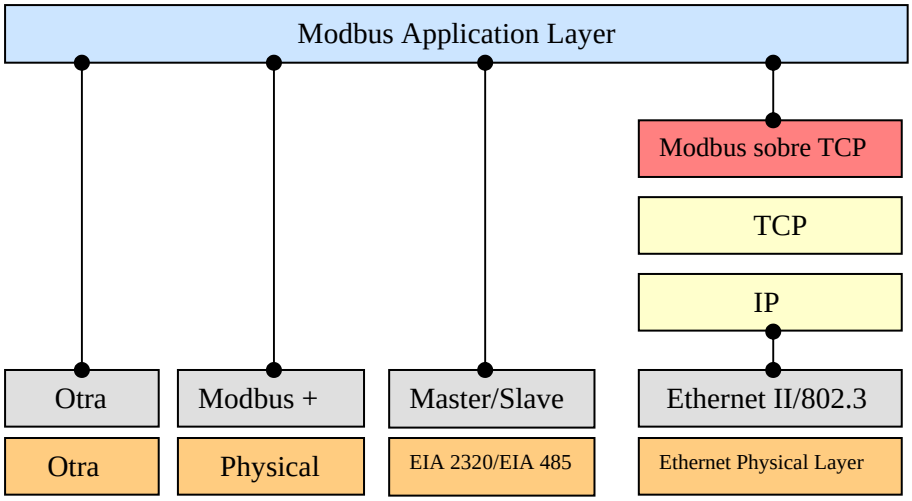

Ilustración 3.3.1-1. Arquitectura Modbus.

3.3.1.1 Formato de trama.

Existen dos variantes en el formato de la trama [29]:

- ASCII: Cada byte se envía como dos caracteres ASCII. El inicio de la trama se identifica al recibir el carácter ":" (ASCII 3A hex). Para la detección de errores, se aplica un LRC (Comprobación Longitudinal Redundante) al mensaje, excluyendo los campos comienzo y fin de trama. El mensaje finaliza con los caracteres retorno de carro y avance de línea (ASCII 0D0A hex).

Comienzo (1 carácter)	Dirección (2 caract.)	Función (2 caract.)	Datos (N caract.)	LRC (2 caract.)	Fin Trama (2 caract.)

Ilustración 3.3.1-2. Trama ASCII.

- RTU (Remote Terminal Unit): Cada byte contiene 2 dígitos hexadecimales de 4 bits. Los mensajes comienzan con un período silencioso de al menos 3,5 tiempos de carácter. La detección de errores se lleva a cabo mediante un CRC (Código de redundancia cíclico) aplicado a la trama. Este es el último campo que se transmite, siendo necesario un período de silencio de 3,5 tiempos de carácter para identificar el final de la trama.

Arranque (3,5 silencios)	Dirección (1 byte)	Función (1 byte)	Datos (N bytes)	CRC (2 bytes)	Final (3,5 silencios)

Ilustración 3.3.1-3. Trama RTU.

El maestro puede direccionar esclavos individualmente o puede generar un mensaje en modo difusión a todos los esclavos. Las direcciones individuales permitidas se encuentran en el rango 1-247 y se reserva la dirección 0 para los mensajes de difusión.
Los dispositivos monitorizan la red continuamente para detectar el comienzo de una trama. Cuando se comienza a recibir una trama, el recurso descodifica el campo dirección para conocer si el destinatario del mensaje es él. Los esclavos devuelven un mensaje (llamado 'respuesta') a las peticiones que les son direccionadas individualmente y no devuelven respuestas a peticiones en modo difusión enviadas desde el maestro.

En una trama petición, el campo dirección permite identificar el dispositivo al que va dirigido el mensaje. Cuando se trata de una respuesta, el esclavo incluye en este campo su propia dirección para que el maestro reconozca el dispositivo que le está enviando la respuesta.
Si la trama es enviada por el maestro, el campo función contiene un código que representa la acción que debe ejecutar el esclavo. El dispositivo esclavo usa este campo para indicar si la respuesta es normal (libre de errores) o bien si es una respuesta de excepción. En el primer caso incluye el código de la función original y en el segundo, ese mismo código pero con su bit más significativo puesto a uno.
El campo datos puede no existir en algunos mensajes. En dicho campo, el maestro introduce información necesaria para que el receptor ejecute la acción determinada por el código de función. Cuando la trama es una respuesta, contendrá los datos solicitados o un código de excepción que la aplicación del maestro podrá usar para determinar la próxima acción a realizar.

Sobre redes distintas a redes Modbus, los mensajes del protocolo Modbus están integrados en la trama o estructura de paquetes utilizadas sobre la red. Con software de aplicación asociado (drivers y librerías) se proporciona la conversión entre el mensaje de protocolo Modbus y las tramas específicas de los protocolos que esas redes utilizan para comunicar entre sus dispositivos nodo.
Esta conversión también alcanza a la resolución de direcciones de nodos, caminos de enrutamiento y métodos de comprobación de error específicos para cada tipo de red. Las direcciones de dispositivo contenidas en el protocolo Modbus serán convertidas en direcciones de nodo, previamente a la transmisión de los mensajes. Los campos de comprobación de error también serán aplicados a los paquetes del mensaje, de manera consistente con el protocolo de cada red.

3.3.1.2 Modbus TCP/IP.

La especificación Modbus TCP/IP fue desarrollada en 1999 y proporciona simplicidad, bajo coste y facilidad de desarrollo bajo cualquier sistema operativo.
Cuando el protocolo Modbus se implementa sobre redes TCP/IP el formato de la unidad de datos de aplicación es el siguiente:

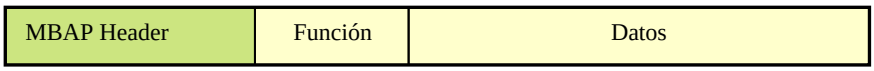

Ilustración 3.3.1-4. Trama TCP/IP.

TCP/IP emplea la cabecera MBAP (ModBus Application Protocol). Esta cabecera consta de 7 bytes y permite identificar la unidad de datos de aplicación Modbus.

3.3.2. UPnP.

Universal Plug and Play (UPnP) [31]es una arquitectura software, abierta y distribuida, que permite a los dispositivos, instalados dentro del hogar o la oficina, comunicarse y compartir recursos de forma automática, sencilla y transparente al usuario.

UPnP surge del trabajo del UPnP Forum, asociación constituida en junio del año 1999 y formada por compañías de diversos sectores (informática, electrónica de consumo, automatización del hogar, etc.). En la actualidad, esta alianza consta de alrededor de 600 miembros, entre los que destacan IBM, Microsoft, LG o Siemens, y se encarga de promover el uso y el desarrollo de dispositivos UPnP. UPnP es la tecnología que Microsoft propone en el campo de la domótica/inmótica y hacer frente a Jini.

UPnP garantiza la compatibilidad entre productos de diversos fabricantes y además, es independiente del sistema operativo y del lenguaje de programación.
Se apoya en la pila de protocolo de Internet, se construye sobre TCP, IP, UDP, HTTP y XML, entre otros. Está basado en SOAP (Simple Object Access Protocol) y para su utilización con dispositivos no IP se recurre al protocolo SCP (Simple Control Protocol).
Al ser independiente del medio físico, es capaz de trabajar sobre línea eléctrica, línea telefónica, Ethernet, radiofrecuencia, wireless o IEEE 1394.

Facilita la instalación de dispositivos ya que es capaz de descubrir de forma automática, nuevos recursos que se conectan a la red. Cuando se produce una nueva incorporación, se le asigna una dirección IP y un nombre lógico, se le informa de las funciones y prestaciones de los demás equipos conectados y se informa al resto de la capacidad y funciones del nuevo elemento. Todo esto de manera transparente al usuario, por lo que resulta sencilla la ampliación o los cambios en la red.

3.3.2.1 Funcionamiento.

Cuando un dispositivo se conecta y trabaja dentro de una red sigue, de forma transparente al usuario, la serie de pasos que se detallan a continuación. La pila de protocolos que utiliza se muestra en la figura 3.3.2-1 [31].

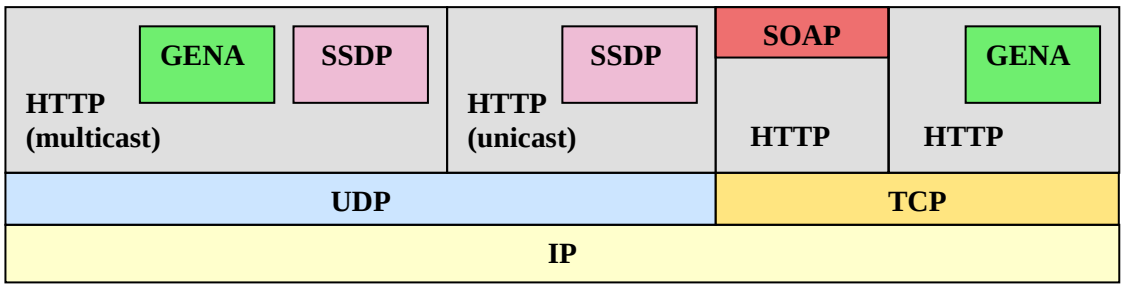

Figura 3.3.2-1. Pila de protocolos.

Paso 0: Obtención de dirección IP.

El dispositivo debe disponer de un cliente DHCP que buscará al servidor DHCP cuando se conecte por primera vez a la red. Si el servidor está disponible, el dispositivo deberá emplear la dirección IP asignada por el mismo. Si el servidor no está disponible tendrá que obtener una dirección de forma automática (Auto-IP).

Paso 1: Descubrimiento.

Cuando el dispositivo se añade a una red, el protocolo de descubrimiento de UPnP permite que éste anuncie sus servicios a los puntos de control de la red. De manera similar, cuando un punto de control se une a la red, el protocolo le permite buscar los dispositivos dentro de la red. En ambos casos, lo que se produce es un intercambio de mensajes que contienen especificaciones esenciales sobre el dispositivo o sobre alguno de sus servicios.
Este protocolo juega un papel importante en la compatibilidad de dispositivos y puntos de control que usan distintas versiones de UPnP dentro de una misma red. Los mensajes intercambiados durante el descubrimiento contienen información sobre las versiones que el dispositivo es capaz de soportar.

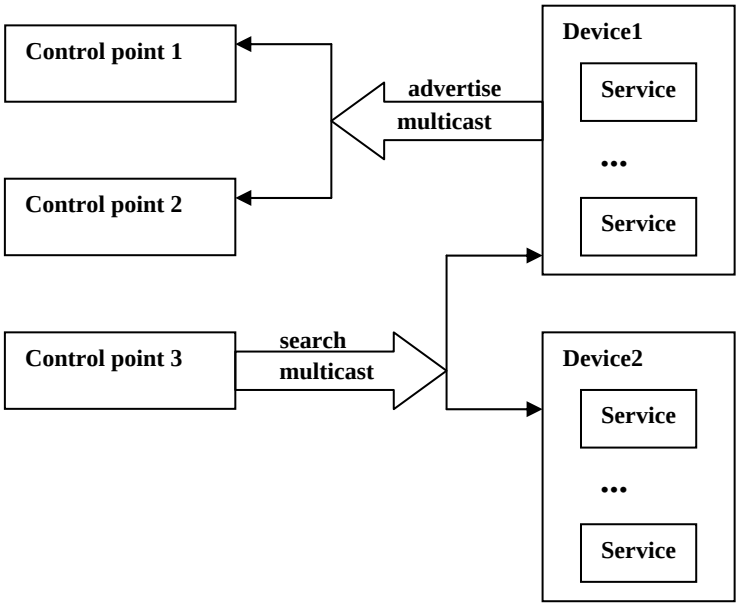

Figura 3.3.2-2. Descubrimiento.

Paso 2: Descripción.

Cuando un punto de control descubre un dispositivo, apenas conoce nada del mismo y obtiene una descripción detallada del dispositivo y sus capacidades mediante la URL proporcionada por el dispositivo en el mensaje de descubrimiento.
Esta descripción está escrita en sintaxis XML y se divide en dos partes:

- Descripción del dispositivo. Detalla información del fabricante como modelo, número de serie, etc.
- Descripciones de servicio. Especifica las capacidades del dispositivo (nombre, tipo, etc.). Además, incluye una lista de comandos, parámetros y variables que modelan el estado del servicio en tiempo de ejecución.

Paso 3: Control.

Conocido un dispositivo y sus servicios, un punto de control puede interrogar a esos servicios para invocar acciones o puede sondearlos para obtener valores de sus variables de estado. La invocación de acciones es una especie de llamada a procedimiento remoto; el punto de control manda la acción al servicio del dispositivo, y cuando la acción finaliza, el servicio le devuelve los resultados o los errores.
La acción, los resultados y los errores son encapsulados en SOAP y tanto las peticiones como las respuestas se realizan vía http.

Paso 4: Control de sucesos.

A través de este paso, los controladores conocen los cambios que se producen en las variables de un servicio determinado.
La notificación de estos cambios se realiza mediante el envío de mensajes de eventos. Estos mensajes contienen los nombres de las variables que han cambiado y el valor actual de esas variables. Para recibir estos mensajes, el punto de control debe enviar previamente un mensaje al servicio encargado de notificar los eventos, indicándole que desee recibir mesajes cuando se produzcan cambios.

Paso 5: Presentación.

Una vez que el punto de control ha descubierto un dispositivo y ha obtenido una descripción del mismo, está preparado para comenzar la presentación.
La presentación expone una interfaz de usuario basada en HTML para el control y/o la visualización del estado del dispositivo. Si el dispositivo tiene una URL para la presentación, el punto de control puede recuperar una página desde esa URL, cargar la página dentro de un browser, y dependiendo de las propiedades de esta página, permitir al usuario controlar el dispositivo y/o monitorizar su estado. Para obtener la página de presentación, el punto de control realiza una petición http a la URL de presentación, y el dispositivo devuelve esa página.

3.3.3. Obix.

Obix (Open Building Information eXchage) ha sido desarrollado por el comité XML/Web Service Guideline, dentro de la asociación CABA (Continental Automated Buildings Association). Es en Abril del año 2003 cuando dicho comité se crea para llevar a cabo este proyecto [21].

Obix es una iniciativa industrial para definir mecanismos XML y servicios web para sistemas de control de edificios. Facilita el intercambio de información entre edificios inteligentes y comunica sistemas mecánicos y electrónicos dentro del edificio. La especificación define un conjunto de formatos XML que permite el tránsito de la información.

3.3.4. Jini.

Jini [28] (Java Intelligent Network Infrastructure) es una API desarrollada por Sun Microsystems, construida sobre la plataforma J2EE. Se trata de un conjunto de interfaces y protocolos que proporcionan mecanismos simples para que los dispositivos conectados a una red, sean capaces de aprovechar los servicios facilitados por el resto de elementos de la red. Y esto lo realiza sin apenas necesidad de intervención por parte del usuario y sin el empleo de "drivers", ya que se basa en la tecnología "plug&play".

Jini es una herramienta que permite desarrollar sistemas distribuidos con un alto grado de dinamismo, donde los elementos del sistema aparecen y desaparecen frecuentemente de manera transparente al usuario. Sun Microsystems habla de comunidad espontánea con la idea de la posibilidad de crear una red Jini en cualquier lugar, en cualquier instante y entre dispositivos que nunca antes han trabajado juntos.

Los componentes Jini pueden funcionar en distintas plataformas hardware (ordenadores personales, teléfonos móviles, PDAs, etc.), siendo necesario que la plataforma en cuestión soporte Java.

Jini va a suponer que el medio de transmisión que lo soporta, posee el ancho de banda y la fiabilidad necesaria y que los dispositivos tienen la capacidad de procesamiento y memoria suficientes. Esto supone un problema a la hora de implementar Jini en dispositivos pequeños.

Jini ha contado desde el principio con el interés de múltiples empresas y existe una constante colaboración entre Sun Microsystems y estas compañías para sacar adelante esta tecnología. Por destacar algunas de ellas, se pueden nombrar: 3Com, Cisco, Xerox, HP, Nokia, Ericsson, Phillips, Sony, etc.
Además, cuenta con diversos grupos trabajando para mejorar e introducir Jini en el mundo real: Jini Printer Working Group o Jini Storage Working Group. Estos grupos están formados por miembros de la "comunidad Jini". Esta comunidad se estableció en Enero de 1999 y no era más que un sitio web hasta su conversión en comunidad formal en Noviembre de 1999. Desde ella, cualquiera puede colaborar o seguir el desarrollo de Jini y constituye el punto de referencia más importante que existe relacionado con el tema.

3.3.4.1 Arquitectura.

El sistema Jini se sustenta sobre la tecnología Java y le añade una serie de elementos propios: el servicio Lookup, los protocolos Discovery/Join y la seguridad distribuida [28].

Se basa en la creación de federaciones de máquinas virtuales Java (JVM) y emplea RMI (Remote Method Invocation) para que los objetos Java puedan ser invocados desde otro objeto o clase remota a través de la red. RMI constituye una parte fundamental de la tecnología Jini ya que facilita la comunicación entre los distintos servicios que se pueden encontrar en el sistema.

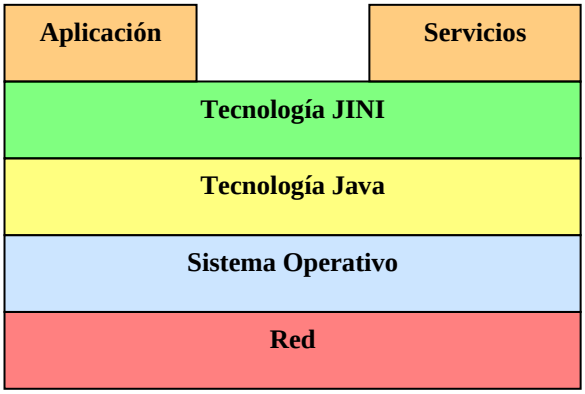

Figura 3.3.4-1. Arquitectura Jini.

En lo más alto de la arquitectura Jini se encuentran los servicios, que aprovechan las capas inferiores para ofrecer los recursos a los usuarios de la red. Los servicios son las entidades que representan todo aquello que pueda ser útil para un usuario o para otros servicios: dispositivos, datos, cálculos, etc. Cada servicio posee un interfaz donde se describe el propio servicio y aquello que ofrece a la red, es decir, define el conjunto de métodos que los usuarios pueden invocar para acceder al mismo.
Este conjunto de servicios se pueden activar y desactivar de forma dinámica dentro del sistema, y para ello, Jini proporciona mecanismos para crear, buscar, comunicar y utilizar dichos servicios dentro la red. Los servicios se comunican entre sí mediante un protocolo de servicios, que está formado por un conjunto de interfaces implementados en Java.
Dentro de estos servicios, Jini cuenta con un servicio fundamental, denominado Lookup Service destinado a registrar las activaciones y las desactivaciones de dispositivos y de otros servicios. Juega un papel intermedio entre los distintos servicios presentes en la red, ya que cualquier servicio que desee anunciar su presencia o su ausencia dentro de la red deberá acudir al servicio de lookup.

Por otra parte, realiza una monitorización de la red, debido a que conoce en todo momento el estado de la red y por tanto, cuando un usuario desee utilizar cualquier servicio tendrá que interrogar primero al lookup. Cuando se quiere utilizar un servicio, el cliente accede a la tabla de servicios del lookup service para saber si el servicio está registrado. En caso de encontrarlo el cliente se descarga el código de control del servicio buscado.
La interacción de dispositivos y servicios remotos se llevan a cabo mediante el método de invocación remota de Java (RMI).
De cierta forma, el servicio de lookup actúa como servidor de servicios pero puede existir más de uno, dependiendo de la organización federativa Jini.

Cuando un dispositivo cualquiera se conecta a la red, utiliza el protocolo de Jini discovery para dar a conocer las funciones que es capaz de llevar a cabo. La ejecución del protocolo discovery implica una comunicación entre el nuevo servicio y el servicio de Lookup. Para ello, el dispositivo lanza una señal multicast para localizar alguno de estos servicios, y una vez que el nuevo servicio ha contactado con uno o más servicios de lookup, pasará a una segunda fase del protocolo denominada join, en la que decidirá cómo registrarse y con qué servicio(s) de lookup hacerlo, entrando a formar parte de la federación de servicios Jini. Por su parte, el servicio de lookup cargará un objeto del dispositivo que contendrá el interfaz con los métodos y los atributos con los que los usuarios podrán acceder al servicio proporcionado por el nuevo dispositivo.
Para encontrar el servicio deseado los clientes deben seguir una plantilla de búsqueda donde se introducen palabras claves, que pueden coincidir con los atributos definidos por el servicio, y que permitan reconocerlo.

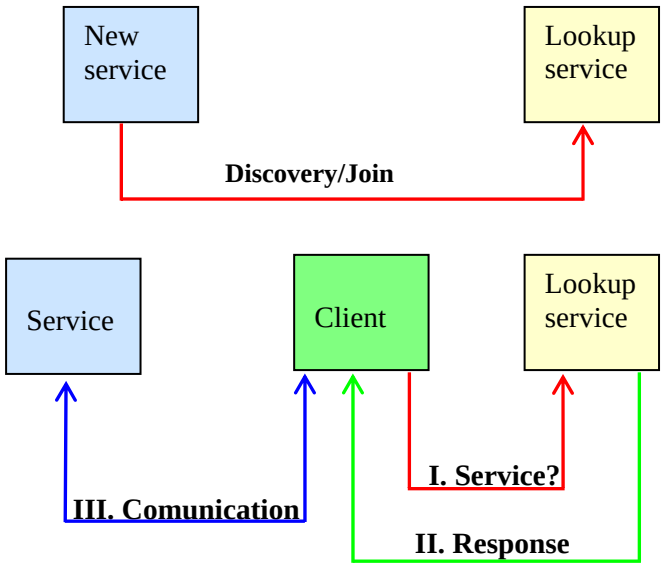

Ilustración 3.3.4-2. Descubrimiento y acceso a un servicio.

Con respecto a la seguridad, el sistema se basa en una lista de control de acceso. Los objetos de la red que están ofreciendo servicios están asociados a la lista de acceso y a través de ella se da permiso a los usuarios de esos servicios. Los permisos pueden ser o no de carácter exclusivo, dependiendo de si sólo puede ser usado por único usuario o compartido por varios.

Por último, cabe destacar que un sistema como Jini necesita cierta organización en cuanto al uso de recursos de los que se disponen. Aparece entones el concepto de leasing, que asigna a cada usuario un tiempo de utilización de un determinado servicio. Este tiempo se establece durante un período de negociación entre el usuario y el proveedor del servicio, y una vez finalizado el tiempo de uso se termina el derecho a utilización del servicio aunque puede ocurrir que el usuario consiga renovar dicho tiempo.

3.4. Redes de datos.

Existen en el mercado diversas posibilidades a la hora de establecer una red de datos. Las tecnologías existentes se pueden clasificar en dos grandes grupos: cableadas e inalámbricas, cada una con sus ventajas e inconvenientes.
Las redes cableadas son más seguras pero su instalación en una vivienda u oficina resulta más costosa que las redes sin cables. Esto último no resultaría un problema debido a que se pueden aprovechar las infraestructuras ya existentes como la línea eléctrica (HomePlug) o la telefónica (HomePNA), sin embargo, el coste del equipamiento resulta elevado. Por el contrario, tecnologías que necesitan nuevos cables como Ethernet, USB o FireWire están más extendidas porque la inversión en equipamiento y accesorios es menor.
Hoy en día las tecnologías inalámbricas están en auge. Aunque son redes menos seguras, presenta alta ubicuidad y no son necesarias ni obras ni reformas para su instalación. Esto último resulta muy interesante a la hora de dotar con los avances tecnológicos a un edificio histórico, donde las obras resultan complicadas.

A continuación se presentan las tecnologías más extendidas en la actualidad. Cada una presenta una serie de propiedades que le proporciona una utilidad o un ámbito de aplicación específico y que se ajustara en menor o mayor medida a las necesidades y requerimientos del usuario.

3.4.1. IEEE 802.11

En Junio de 1997, el IEEE publica la norma IEEE 802.11, que permite las comunicaciones vía radio en redes locales. La publicación de este estándar, junto con el desarrollo de equipos portátiles y móviles, ha provocado una verdadera expansión de las comunicaciones y sistemas inalámbricos en un corto período de tiempo.
El trabajo del IEEE ha dado lugar a la aparición en el mercado de tres protocolos dentro del grupo IEEE 802.11: 802.11b, 802.11a y 802.11g. En la siguiente tabla se muestran algunas características de estos estándares [14]:

Estándar	802.11b	802.11a	802.11g
Año aprobación	**1999**	**2002**	**2003**
Velocidad máxima	**11 Mbps**	**54 Mbps**	**54 Mbps**
Frecuencia	**2.4 GHz**	**5 GHz**	**2.4 GHz**
Cobertura	**Buena**	**Baja**	**Buena**

Tabla 3.4.1-1. Estándares IEEE 802.11.

La expresión Wi-Fi (abreviatura de "*Wireless Fidelity*") [33] se emplea comúnmente para hacer referencia al estándar 802.11b. Realmente, sirve para certificar la compatibilidad de productos de distintos fabricantes y que incorporan cualquier variante de la tecnología inalámbrica 802.11. En un principio, la expresión Wi-Fi era utilizada únicamente para los aparatos con tecnología 802.11b, ya que se convirtió en el estándar dominante en el desarrollo de las redes inalámbricas. Posteriormente, se ha extendido a aparatos provistos con las tecnologías 802.11a y 802.11g.

Entre las ventajas de Wi-Fi, cabe destacar que hace posible la conexión inalámbrica de banda ancha de forma sencilla y económica, ya que su instalación no requiere de obras o reformas. Además, es una tecnología que posee múltiples aplicaciones y existe una amplia gama de productos y sistemas que la incorporan.

Sin embargo, una red Wi-Fi es más vulnerable que cualquier red cableada, debido a que generalmente es accesible más allá del recinto físico donde se ha instalado. Por este motivo, se le da gran importancia a los mecanismos de seguridad y control de acceso.

Se trata de un protocolo de comunicaciones de carácter radioeléctrico, por lo que está obligado al cumplimiento de cierta normativa. En el caso de España, debe acatar las normas relativas a restricciones de emisiones radioeléctricas (Real Decreto 1066/2001), medidas de protección sanitaria frente a dichas emisiones (Orden CTE/23/2002) y despliegue de redes sin cables (UN-85 y UN-128 del CNAF).

En 1999 se crea Wi-Fi Alliance, una organización internacional, sin ánimo de lucro, formada para la certificar la compatibilidad de productos inalámbricos de redes de área local basados en la especificación del IEEE 802.11. En la actualidad, esta asociación consta de 200 miembros, que representan a un grupo de empresas relevantes del sector.

3.4.1.1 Aspectos tecnológicos.

El estándar sólo define las capas físicas y MAC. La capa MAC se encarga de la entrega segura de los datos, de la privacidad de los mismos y del control de acceso al medio. Para esto último, se implementan dos técnicas basadas en CSMA [14]:

- DCF: Acceso al medio mediante proceso de contención. Se utiliza un período de contención aleatorio para acceder al medio.
- PCF: Acceso al medio mediante un proceso centralizado en un controlador central. Su funcionamiento se apoya en el DCF.

El formato de tramas MAC es común para control y datos. Los campos son:

- FC: información de control.
- D/I: tiempo que se usará el canal, en microsegundos.
- Dirección: direcciones origen y destino.
- SC: control de secuencia.
- Datos: carga útil, de cero a 2312 bytes.
- CRC: código cíclico redundante.

FC (2)	D/I (2)	Dirección (6)	Dirección (6)	Dirección (6)	SC (2)	Dirección (6)	Datos	CRC (4)

Ilustración 3.4.1-1. Formato trama MAC (Tamaño en bytes).

IEEE 802.11b

Funciona sobre la banda libre ICM (Industrial, Científica y Médica), entorno a 2,4 GHz. Consigue alcanzar hasta 11 Mbps usando la modulación DSSS con el sistema de codificación CCK (Complementary Code Keying).

Posee la característica denominada DRS (Dynamic Rate Shifting), que permite reducir la velocidad para compensar los posibles problemas de recepción debido a las distancias o los materiales atravesados. Así, la velocidad de transmisión podrá tomar los valores 1, 2, 5.5 u 11 Mbps.

La cobertura alcanzada va a depender de diversos factores, como el tipo de antena, la velocidad o los amplificadores usados. Aproximadamente se pueden alcanzar entorno a los 350 m en espacios abiertos, reduciéndose considerablemente si se habla de recintos cerrados. A menor velocidad más distancia se cubre.

IEEE 802.11a

Su funcionamiento se da sobre la banda de frecuencia de 5 GHz (de 5.150 MHz a 5.350 MHz y de 5.470 MHz a 5.725 MHz), utilizando la técnica de modulación de radio OFDM (Ortogonal Frequency Division Multiplexing). Con esta técnica se consigue aumentar considerablemente la velocidad de transmisión, llegando hasta 54 Mbps.

Frente a este aumento en la velocidad manifiesta varios inconvenientes: el nivel de consumo es mayor que el de 802.11b y las distancias de coberturas se reducen significativamente (aproximadamente 150 m).

IEEE 802.11g

Trabaja sobre la frecuencia de los 2,4 GHz y es capaz de utilizar los métodos de modulación de las dos normas anteriores: DSSS y OFDM.
Al soportar ambas codificaciones, este nuevo estándar será capaz de incrementar notablemente la velocidad de transmisión, pudiendo llegar hasta los 54 Mbps que oferta la norma 802.11a, aunque manteniendo las características propias del 802.11b en cuanto a distancia, niveles de consumo y frecuencia utilizada.

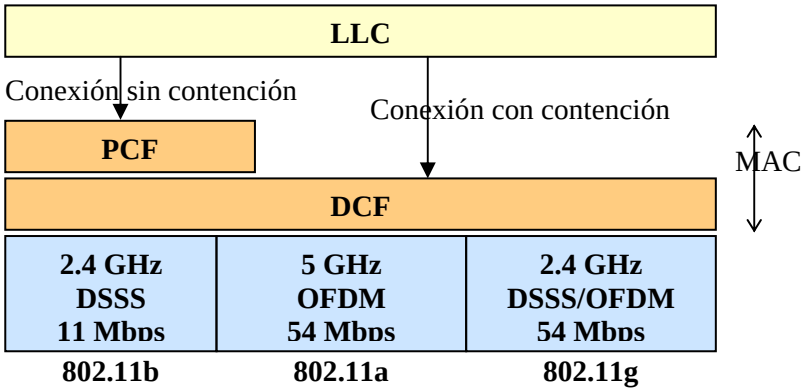

Ilustración 3.4.1-2. Arquitectura Wi-Fi.

3.4.1.2 Seguridad.

Desde el nacimiento de las tecnologías inalámbricas, la seguridad es un aspecto que ha tenido gran importancia, sin embargo presenta notables carencias. Esta falta de seguridad ocasiona que terceros puedan acceder a la red y sean capaces de acceder a la información y manipularla.

Actualmente existen herramientas, funciones y protocolos de seguridad que ofrecen cierta protección para redes WLAN. El nivel de seguridad va a depender del tipo y funcionalidad de la red, así como de las necesidades del usuario.
Generalmente las medidas utilizadas son [14]:

- ACL (Access Control List): Permite el acceso a la red a aquellas direcciones MAC que se encuentran registradas en la lista de control de acceso.
- CNAC (Closed Network Access Control): Los dispositivos que desean unirse a la red deben conocer el SSID (Service Set IDentifier) de la misma. El SSID es una cadena de caracteres que identifica a cada red.
- WEP (Wired Equivalent Privacy): Sistema que emplea una clave para la autenticación del acceso y el cifrado de la información que se transmite entre los extremos de la comunicación.
- DSL (Dynamic Security Link): Mecanismo de autenticación a través de la asignación dinámica de claves.
- RADIUS (Remote Authenticated Dial-In User Service): Sistema de gestión centralizada que da una solución de autenticación para entornos con un elevado número de usuarios, desarrollada por el grupo 802.1x del IEEE.
- WPA (Wi-Fi Protected Access): Protocolo que está sustituyendo a WEP. Proporciona autenticación de usuarios utilizando TKIP (Temporal Key Integrity Protocol) y mejora la forma de codificar los datos respecto a WEP.

3.4.2. Bluetooth.

La tecnología sin cables Bluetooth ha revolucionado el mercado de las redes de área personal inalámbricas (WPAN) [20].
Las WPAN constituyen un diseño de red de corto alcance, que permite conectar entre sí dispositivos como ordenadores, PDAs, impresoras, ratones, micrófonos, auriculares, lectores de código de barras, sensores, displays, localizadores, teléfonos móviles y otros equipos de electrónica de consumo.
Bluetooth proporciona conexión sin cables de bajo coste entre dispositivos que se encuentren en un rango de 10 metros, aunque se puede ampliar a 100 metros si se emplean repetidores. Se trata de una tecnología apta para la transmisión de voz, la transferencia de ficheros, la conexión a Internet o las redes ad hoc.
El desarrollo de Bluetooth y su difusión en el mercado es llevada a cabo por Bluetooth SIG (Special Interest Group), organización formada por empresas líderes en el sector de las telecomunicaciones como 3Com, Ericsson, IBM, Lucent o Nokia, entre otras.

3.4.2.1 Aspectos tecnológicos.

Bluetooth [20] trabaja en la banda sin licencia para aplicaciones ICM, en el rango 2,402 GHz a 2,480 GHz, con modulación GSFK y método de acceso al medio CDMA/FH (Code Division Multiple Access/ Frecuency Hop).
Para la transmisión de voz dispone de tres canales a 64 Kbps, mientras que la transferencia de datos se puede llevar a cabo a 721 Kbps si es de forma asimétrica y a 432 Kbps si se realiza simétricamente.
Define un alcance corto de alrededor de 10 metros para el que se necesita una potencia de 0 dBm. Opcionalmente puede alcanzar 100 metros de alcance para los que se requieren 20 dBm de potencia.

Los dispositivos Bluetooth se agrupan en lo que se denomina piconet. Una piconet es una asociación de un máximo de 8 dispositivos que se conectan sobre la marcha. Cada piconet se

caracteriza por una secuencia de salto en frecuencia diferente y pueden existir hasta 10 piconets en la misma área de cobertura.

Especifica dos tipos de enlaces físicos:

- SCO. Conexión punto a punto con ancho de banda fijo, usado para comunicaciones de voz. No se asegura la entrega.
- ACL. Enlace punto a multipunto sin reserva de ancho de banda. Necesita asegurar la entrega y se emplea para la transferencia de datos sin requerimientos temporales pero sí de fiabilidad.

Arquitectura de protocolos de Bluetooth:

- Radio. Especifica el interfaz radio.
- Banda base. Se encarga de establecer las conexiones entre dispositivos, controlando la sincronización entre los mismos y el acceso al medio. Además, se hace cargo del control de potencia y de la temporización.
- LM/LMP. Permite la creación y la eliminación de un enlace entre dispositivos, configura el enlace y determina el estado de una conexión.
- L2CAP. Sólo se usa en ACL. Implementa el protocolo de enlace de datos en medio compartido (servicio con o sin conexión).

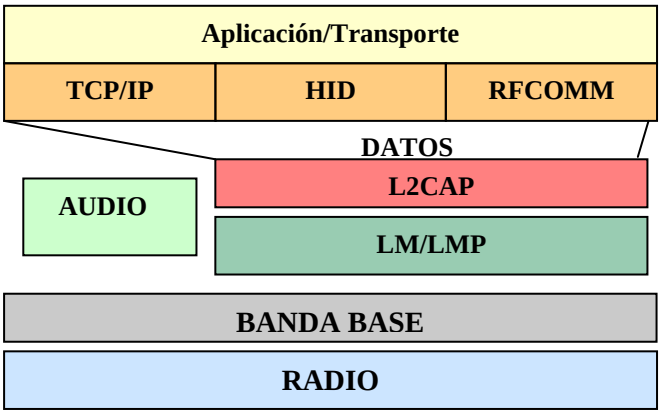

Ilustración 3.4.2-1. Arquitectura Bluetooth.

3.4.3. IrDA.

Se conoce como IrDA (Infrared Data Association) [2] a la tecnología de corto alcance que trabaja dentro de la banda de los infrarrojos (850 nm). Esto supone una ventaja frente a otros sistemas sin cables, ya que no van a existir interferencias al trabajar a una frecuencia distinta al resto.

Presenta sólo comunicaciones punto a punto con visión directa. Los dispositivos que desean comunicarse mediante infrarrojos deben estar muy cerca debido a que la distancia de alcance es pequeña y, además, deben permanecer fijos cuando se realiza la sincronización.
Debido a su escaso rango de cobertura IrDA suele emplearse en redes de área personal, aunque ocasionalmente se puede usar en aplicaciones específicas de WLAN. Está muy extendido su uso en sistemas para el control remoto de dispositivos o para la conexión de periféricos a un PC.

3.4.3.1 Aspectos tecnológicos.

El estándar IrDa-1.1 alcanza una velocidad de transmisión máxima de 4 Mbps y su radio de cobertura no es superior a los 2 metros [2].

Arquitectura de protocolos IrDA:

- Capa física. Define canales half-duplex con bajas interferencias. Se encarga de modular los datos para la transmisión, delimitar las tramas para la sincronización e introducir CRC para la detección de errores.
- IrLAP. Implementa un protocolo de enlace de datos basado en HDLC. Los servicios que ofrecen son: detección de dispositivos, conexión y desconexión de los mismos y envío de datos de forma segura.
- IrLMP. Proporciona multiplexación de datos de distintas aplicaciones en una única conexión IrLAP.
- IAS. Se encarga de adquirir información sobre los servicios de los dispositivos.
- Tiny TP. Protocolo opcional que proporciona control de flujo basado en créditos, segmentación y ensamblado.
- IrOBEX. Protocolo opcional que realiza funciones de transferencia de ficheros.
- IrCOMM. Emula puertos serie y paralelo. Es opcional.
- IrLAN. Es un protocolo opcional y permite el acceso a LAN.

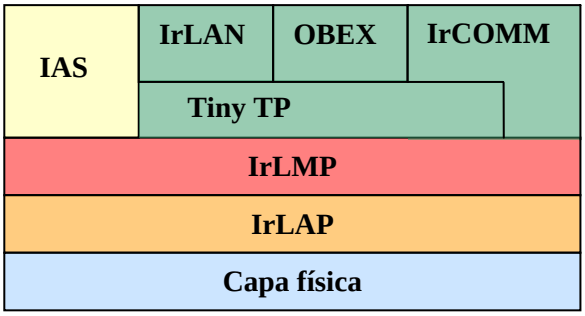

Ilustración 3.4.3-1. Protocolos IrDA.

3.4.4. Home RF.

Home RF es una tecnología que proporciona transmisión digital inalámbrica. Ha sido desarrollada por el Home RF Working Group, organización creada en Marzo de 1998 y que en la actualidad cuenta con más de noventa miembros, entre los que se encuentran compañías líderes en el sector de las telecomunicaciones y de la electrónica de consumo [27].

Es una especificación que soporta comunicaciones de voz y datos en tiempo real, gracias al empleo del protocolo SWAP (Shared Wireless Access Protocol). Una de las ventajas de Home RF es que permite la distribución de vídeo y audio en dispositivos con escasos recursos hardware.

3.4.4.1 Aspectos tecnológicos.

Al igual que Bluetooth y Wi-Fi, Home RF trabaja en la banda de frecuencias de uso común ICM en el rango de los 2,4 GHz, empleando espectro ensanchado por salto en frecuencia (FHSS).
SWAP 1.0 admite una velocidad cercana a los 2 Mbps pero la nueva versión (SWAP 2.0) es capaz de llegar hasta los 10 Mbps, reduciéndose a la mitad si se desea mayor distancia de cobertura. Soporta un máximo de 127 dispositivos en un radio de 50 metros.

La especificación SWAP define una interfaz común que soporta hasta 6 conexiones de voz simultáneas y datos a través de la red sin cables del hogar o la oficina. Para optimizar estas transferencias, el nivel MAC emplea un esquema TDMA para las comunicaciones vocales mientras que utiliza CSMA/CA para la transmisión de datos asíncronos [27].

Al tratarse de una tecnología inalámbrica la seguridad es un aspecto crítico. Home RF proporciona cifrado de datos mediante una clave de 56 bits. Por otra parte, utiliza dirección IP 24 bits que evita el acceso a la red de usuarios externos.

3.4.5. Ethernet.

La norma IEEE 802.3, conocida comúnmente como Ethernet, especifica la red local que presenta una topología lógica y física en forma de bus [15].
Este tipo de redes surge a finales de los años setenta y fue desarrollada inicialmente por DEC, Intel y Xeron. En 1983 se convierte en la norma IEEE 802.3 y se adopta como estándar ISO (ISO 8802.3).
En sus inicios presentó gran competencia con las redes Token Ring, pero en la actualidad éstas apenas se instalan y las redes Ethernet cubren la gran parte de las redes empresariales.

A lo largo de estas dos décadas las redes Ethernet han ido evolucionado para satisfacer la demanda de los usuarios. Esta evolución se traduce en dos nuevos estándares que proporcionan mayor velocidad que la norma original: Fast Ethernet y Gigabit Ethernet. Estas nuevas versiones son compatibles con la inicial, lo que supone una gran ventaja ya que todo el equipamiento anterior sigue siendo válido.

3.4.5.1 Aspectos tecnológicos.

La velocidad original de Ethernet es de 10 Mbps. Para esta velocidad, el estándar ofrece cuatro posibilidades de cableado [15]:

- 10Base-5 (Thick Ethernet): sobre coaxial grueso, en la actualidad apenas se usa. Acepta 100 puestos de trabajo en una longitud máxima de 500 metros.
- 10Base-2 (Thin Ethernet): sobre coaxial fino es capaz de mantener sobre una distancia de 185 metros 100 puestos de trabajos, espaciados como mínimo medio metro.
- 10Base-T: se emplea cable de pares trenzados sin apantallar (UTP), ya que es más económico y fácil de manipular. Presenta topología física en estrella y cada estación de trabajo puede situarse a una distancia de hasta 100 metros.
- 10Base-F: utiliza fibra óptica multimodo y permite un total de 1024 nodos en un rango de 2000 metros.

Al tratarse de una topología donde diversos equipos comparten un único medio es necesario un mecanismo que arbitre el acceso al mismo. Ethernet emplea la técnica CSMA/CD (Carrier Sense, Multiple Access with Collision Detect). En este método la estación antes de transmitir la información comprueba que el medio está vacío y durante la transferencia comprobará el canal para verificar que no existe colisión en ningún momento.

3.4.5.2 Fast Ethernet y Gigabit Ethernet.

Fast Ethernet es una evolución de Ethernet que consigue alcanzar una velocidad de transmisión de 100 Mbps. La subcapa MAC, el formato de tramas y el cableado son los mismos que los de 10Base-T. Presenta mayor resistencia ante los errores que la versión original [15].

Gigabit Ethernet supone el siguiente paso en la evolución de las redes Ethernet de gran velocidad. Este nuevo estándar alcanza una velocidad de 1 Gbps y especifica dos medios de transmisión posibles, la fibra óptica y el cable coaxial de 150Ω [15].

3.4.6. HomePlug.

La especificación HomePlug (Junio 2001) es una tecnología que utiliza la instalación eléctrica de baja tensión de la vivienda o la oficina para crear una red de datos. La gran ventaja que presenta es que no es necesario equipar al edificio con nuevos cables [25].
Aunque existen en el mercado otras tecnologías que presentan similares características, la industria ha elegido a HomePlug como estándar de facto para la transmisión de datos por la red eléctrica.

La organización encargada de la creación de estándares HomePlug es la HomePlug Alliance, fundada en el 2000 y constituida actualmente por más de 100 empresas relacionadas con las tecnologías de la información y la electrónica de consumo.
Esta asociación se encarga también de promover y difundir en el mercado los productos y servicios HomePlug.

Esta tecnología es compatible con otros sistemas que también emplean la red eléctrica como X-10, pero presenta interferencias con CEBus o LonWorks por lo que su uso simultáneo presenta ciertas limitaciones.

3.4.6.1 Tecnología.

La especificación define una robusta capa física y una eficiente capa MAC. El protocolo MAC controla la división del medio entre múltiples usuarios, mientras que la capa física se encarga de la modulación, codificación y formato básico de los datos [25].

Ocupa la banda que va desde los 4,5 a los 21 MHz y emplea modulación OFDM (Orthogonal Frequency Division Multiplexing) para conseguir mayor ancho de banda y alta eficiencia espectral. La velocidad que puede alcanzar está entorno a 14 Mbps pero dependerá de las condiciones del medio (topología y fuentes de ruido).

El protocolo de acceso al medio de la tecnología HomePlug es una variante de la conocida técnica CSMA/CA, a la que se le añaden una serie de características para soportar prioridad de clases.

Al usar la línea de baja tensión cualquier individuo, que se conectará a ella, podría interceptar los datos que se están enviando. Por este motivo, se cifran los datos mediante el mecanismo DES-56 que emplea una clave de cifrado de 56 bits.

El principal problema que presenta esta tecnología es que la red eléctrica es un medio hostil para la transferencia de datos. Por un lado, esta transmisión se ve influenciada por las interferencias y perturbaciones que provocan los dispositivos conectado a la red. Por otro, el cableado ocasiona filtrado a determinadas frecuencias, resonancias o cambios en el valor de las impedancias.
Para contrarrestar todo esto se emplea la modulación OFDM. Esta técnica permite que la transmisión de datos se adapte dinámicamente a las condiciones de ruido de la red, potenciando

el uso de frecuencias donde el ruido y la atenuación son menores. Además, se implementa el método de detección y corrección de errores hacia delante (FEC).

3.4.7. HomePNA.

En Junio de 1998, un grupo de compañías relacionadas con el sector de las telecomunicaciones funda la Home Phoneline Networking Alliance (HomePNA). El objetivo de esta organización es el de desarrollar estándares comunes para aprovechar la red telefónica del hogar y proporcionar transmisión de datos por el cableado telefónico [26].

3.4.7.1 Tecnología.

En la actualidad existen tres especificaciones aprobadas por HomePNA [26]. La primera de las tecnologías, HPNA 1.0, alcanza una velocidad de 1 Mbps y emplea modulación PPM (Pulse Position Modulation). Esta tasa resulta insuficiente para competir con el resto de redes locales que existen en el mercado y la alianza decide entonces, diseñar una nueva versión que llega a alcanzar los 32 Mbps.
En Junio del año 2003 se aprueba HPNA 3.0 que mejora la velocidad de la anterior hasta los 128 Mbps. Es capaz de soportar distancias de 300 metros y hasta 50 dispositivos conectados en la red.

HPNA ocupa la banda libre de los cables telefónicos comprendida entre los 4 y los 10 MHz. Emplea una modulación FDQAM (Frequency Diverse QAM) que permite, junto con una serie de filtros, la utilización simultánea del teléfono, del acceso a xDSL y de la red de área local HomePNA.

Como técnica de acceso al medio emplea CSMA/CD. Para permitir las transferencias en tiempo real introduce niveles de prioridad y emplea un algoritmo de resolución de colisiones denominado DFPQ (Distributed Fair Priority Queuing).

3.4.8. IEEE 1394.

En 1986 la empresa Apple desarrolla un bus serie de alta velocidad, conocido con el nombre de Firewire. Es en 1995 cuando se convierte en el estándar IEEE 1394 y está definido como draft estándar de ANSI (P1394).
Se trata de una tecnología de alta velocidad adecuada para aplicaciones multimedia y para la conexión de dispositivos digitales que necesiten elevada tasa binaria.

Es un estándar que está ampliamente implantado en dispositivos digitales de fabricantes como Sony, Canon o JVC. Además, cuenta con el respaldo de la 1394 Trade Association, consorcio internacional constituido por más de 170 empresas y dedicado a promover y desarrollar los estándares IEEE 1394 [16].

3.4.8.1 Características.

IEEE 1394 proporciona una velocidad de 400 Mbps en su primera versión y llega a los 800 Mbps en la segunda especificación (IEEE 1394b). Es capaz de mantener 63 dispositivos conectados al mismo bus en un rango que va desde 50 a 100 metros, dependiendo de la versión y del medio empleado (par trenzado, fibra óptica de vidrio o fibra plástica) [16].

Soporta la transferencia de datos isócronos, es decir, aquellos que necesitan un ancho de banda garantizado para transmitir. Esto es fundamental para dispositivos que transmiten en tiempo real tales como los de vídeo o audio.

Presenta una arquitectura flexible, con topología peer-to-peer y capacidad plug&play que permite de forma automática la identificación de nuevos dispositivos y la reconfiguración del bus. El inconveniente principal es su precio.

3.5. Comparativa.

3.5.1. Específicos.

	KNX	Bacnet	CEBus	X-10	LonWorks
Propietario	No	No	No	Sí	Sí
Medio físico más empleado	Par trenzado	Par trenzado/ Coaxial/ Línea telefónica/ Fibra óptica	Línea eléctrica	Línea eléctrica	Coaxial/ Par trenzado/ Línea eléctrica/ Fibra óptica
Velocidad	2,4 Kbps/ 9,6 Kbps *	De 56 Kbps a 1 Gbps *	7,5 Kbps	50 bps/ 60 bps	De 78 Kbps a 1,25 Mbps
Área de aplicación	Viviendas y oficinas	Viviendas y oficinas	Viviendas	Viviendas	Oficinas e industrias
Ámbito	Europa	Internacional	América	Europa/ América	Internacional
Principal ventaja	Unifica protocolos domóticos en Europa	Versátil	Fácil de instalar, usar y extender	Madurez y sencillez	Compatibilidad entre dispositivos de distintos fabricantes
Principal desventaja	Muy reciente	Caro	Pocos productos a precios altos	Muy baja capacidad	Caro

* Depende del tipo de cable.

3.5.2. Cableadas.

	Ethernet	HomePlug	HomePNA	IEEE 1394	USB
Medio	Coaxial/ Par trenzado/ Fibra óptica	Línea eléctrica De baja tensión	Cable telefónico	Par trenzado/ Fibra óptica	Cable de pares
Velocidad (Mbps)	10	14	128	400/ 800	480
Alcance (m)	De 100 a 2000 *	**	300	De 50 a 100 *	-
Dispositivos soportados	De 100 a 1024 *	**	50	63	127
Coste instalación	Alto	Bajo	Bajo	Alto	Alto
Principal ventaja	Flexible ante cambios	Gran número de accesos	No necesita reformas para su instalación	Gran velocidad	Plug&Play

* Depende del cable empleado.
**Depende de la topología y de las fuentes de ruido.

3.5.3. Inalambricas.

	Wi-Fi	Zigbee	Bluetooth	Home RF	IrDA
Frecuencia	2.4 GHz	2.4 GHz/915 MHz/ 868 MHz	2.4 GHz	2.4 GHz	850 nm
Velocidad (Kbps)	11000	250 (2.4)/40 (915)/ 20 (868)	1000	10000	4000
Alcance (m)	100-400	75-100	10-100	50-100	1
Dispositivos soportados	128	255	8	128	2
Acceso al medio	DCF-PCF	CSMA/CA	FH/TDD/TDMA	TDMA-CSMA/CA	-
Coste	Medio/Alto	Bajo	Bajo	Medio	Bajo
Consumo de potencia	Bajo	Bajo	Bajo	Medio	Medio
Aplicación principal	WLAN en viviendas y en oficinas	Red de sensores inalámbrica	WPAN	WLAN en viviendas	Control remoto WPAN

3.6. Autómatas programables o PLC.

Esta solución, aunque no se considera como un estándar de control domótico o inmótico, desempeña un papel importante en muchas aplicaciones debido a que son sistemas bien conocidos en entornos industriales, donde se utilizan mucho.
Los autómatas programables o PLC (Programmable Logic Controller) son dispositivos que contienen un programa que se ejecuta secuencialmente y de forma iterativa.
La forma de programarlos no es accesible para el público en general, aunque algunas marcas han lanzado productos sofware para facilitar la programación de dichos dispositivos. Existe en el mercado variedad de herramientas para programar los PLCs y simuladores para PC que permiten llevar a cabo tareasa de depuración y mantenimiento, sin embargo, no se encuentran muchas aplicaciones específicas para el diseño de aplicaciones domóticas e inmóticas con autómatas [3].

3.7. Sistemas propietarios.

Diversos fabricantes del sector se apoyan en los estándares anteriormente mencionados, para desarrollar sistemas propietarios completos. Estos sistemas son distribuidos por un único fabricante y aunque son más costosos, se adaptan perfectamente a las necesidades que el usuario demanda.
Dentro de los múltiples sistemas que existen en el mercado alguno de ellos son [3]:

- *Simon VIS.* Se trata de un producto danés que la empresa española Simón lo ha adaptado para su inclusión en el mercado español, dentro del ámbito de pequeñas y medianas instalaciones. El sistema se fundamenta en la centralización de los diversos módulos que componen el mismo. Utiliza cableado dedicado y protocolo propietario de comunicación. Basado en un autómata programable o PLC, el sistema es modular, de forma que la configuración puede crecer y ser fácilmente reprogramada para atender las últimas necesidades del usuario.
  La programación del sistema se lleva a cabo desde un ordenador personal mediante un software desarrollado por la empresa denominado TermVIS.

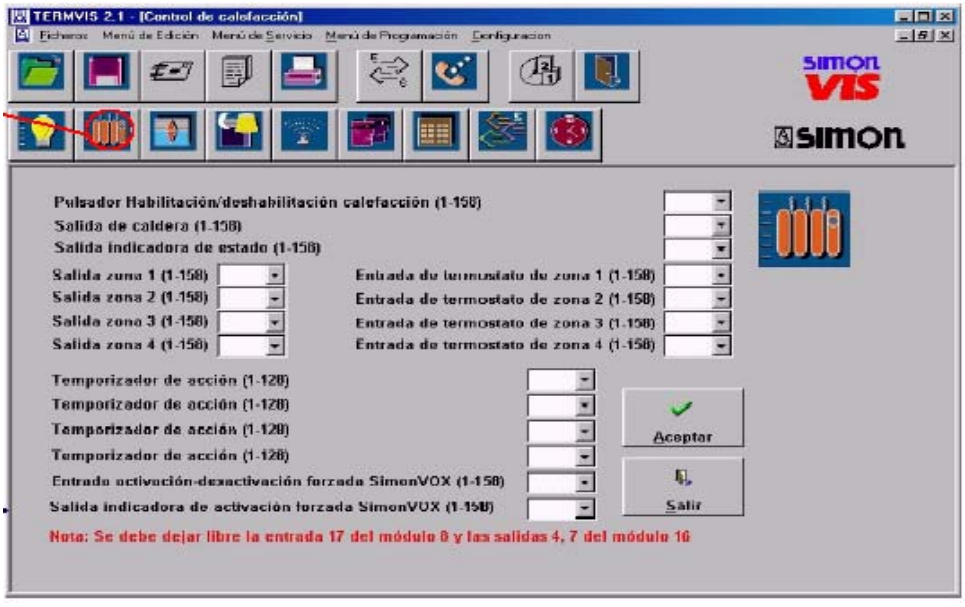

Figura 3.7-1. Simon VIS [3].

- *Dialogo.* Sistema descentralizado, cuyos módulos se comunican mediante un bus de control LonWorks. Se trata de un producto de la empresa BJC. Gracias a su arquitectura, resulta fácil de instalar y permite disponer de hasta 1200 dispositivos. La instalación se diseña mediante un software específico BJC Dialogo.
- *Domaike.* De la empresa española Aike Tecnologies de l`habitat, se trata de un sistema que integra todas las funciones en una unidad central. Incorpora varias tecnologías de transmisión de datos.
- *Hometronic.* Sistema centralizado de Honeywell, que emplea la tecnología de radiofrecuencia, operando en la banda ISM entre 433,05 y 434,79 MHz. Es modular y resulta fácilmente ampliable.
- *Vantage.* Sistema americano que posee inteligencia centralizada en una o varias unidades. La comunicación maestros-esclavos se realiza mediante un protocolo propietario.
- *Biodom.* De la empresa española Bioingeniería Aragonesa S.L., miembro de la EHSA. Se apoya en el estándar EHS y el sistema sigue la filosofía Plug&Play.
- *Concelac.* Sistema de la empresa Logical Design, que se caracteriza por su capacidad de integración en redes de área local.
- *Dialoc.* Desarrollado por la empresa alemana Weidmüller. Emplea el protocolo LonWorks para comunicarse.
- *Amigo.* Se trata de un sistema descentralizado con comunicación por bus de control, que emplea el protocolo Batibus. Desarrollado por la empresa Eunea Merlin Gerin (Sheneider Electric España, S.A.).