ESCUELA SUPERIOR DE INGENIEROS

INGENIERÍA DE TELECOMUNICACIÓN

Proyecto Fin de Carrera

PANORÁMICA DE LOS SISTEMAS DOMÓTICOS E INMÓTICOS

Departamento de Ingeniería de Sistemas y Automática.
Área de Ingeniería Telemática.

Septiembre 2005.

Autor: ***Mª Josefa Bouzas Millares.***
Tutor: ***D. Antonio J. Estepa Alonso.***

ÍNDICE

0. OBJETIVOS DEL PROYECTO

Con la realización del proyecto fin de carrera con título ***"Panorámica de los sistemas domóticos e*** *inmóticos" se persiguen los siguientes objetivos*:

- *Obtener una visión del estado del sector domótico e inmótico en la actualidad, debido a que se trata de una tecnología emergente y con grandes perspectivas de futuro que involucra a la mayoría de los sectores de la sociedad.*

- *Conocer el tipo de aplicaciones y mejoras que se pueden introducir en un edificio para dotarlo de "inteligencia" y los beneficios que los usuarios de los mismos pueden obtener gracias a esta automatización.*

- *Presentar las normas, estándares y protocolos de comunicación que actualmente se emplean para lograr la interconexión de los diversos dispositivos que constituyen la red domótica. Además, dar a conocer las asociaciones y organismos que respaldan cada uno de estos estándares.*

- *Resumir los distintos componentes que son necesarios para automatizar un edificio, así como sus principales características y las diversas posibilidades del mercado.*

1. INTRODUCCIÓN

1.1. Conceptos de domótica e inmótica.

El sector de la construcción no es ajeno al espectacular crecimiento experimentado por la informática, la electrónica y las telecomunicaciones en los últimos tiempos, y es por ello que cada vez más incorpora elementos tecnológicos en las edificaciones. Esta incorporación ha llevado a empresas relacionadas con la informática y las telecomunicaciones a desarrollar una industria relacionada con las aplicaciones y los elementos que se pueden agregar en un edificio, dotándolo, se podría decir, de inteligencia.

A la hora de definir este nuevo sector se pueden distinguir dos nuevos conceptos: domótica e inmótica, el primero destinado a la automatización de las viviendas y el segundo adecuado para el resto de edificaciones. Esta división no está adoptada de manera generalizada y el término domótica es el más popular y el más extendido, empleándose el concepto de sistemas domóticos referidos también al sector terciario o incluso el término de domótica de grandes edificios.
En inglés los conceptos que se emplean son *home systems*, *smart house* o *intelligent building technologies* [3].

De forma más rigurosa se puede definir la domótica como ciencia y los elementos y servicios desarrollados por ella que proporcionan algún nivel de automatización o automatismo de forma integrada dentro de la casa y capaz de satisfacer las necesidades básicas de seguridad, comunicación, gestión energética y confort, del hombre y de su entorno más cercano. Etimológicamente, la palabra domótica fue acuñada en Francia y procede de la unión de *domus* (casa en latín) y *robotique* (robótica) [1].
Existen múltiples definiciones de domótica, elaboradas por los distintos expertos del tema pero en la gran mayoría se destaca la idea de mejorar la calidad de vida de los usuarios de estos sistemas.

Por inmótica se entiende la incorporación de sistemas que proporcionan algún nivel de automatización dentro del equipamiento de las edificaciones del sector terciario, como son hospitales, edificios de oficinas, grandes superficies, parques tecnológicos, etc.
De forma óptima e integrada proporciona a los distintos controles y automatismos que se incluyen en el edificio, comunicación, control, monitorización, gestión y mantenimiento de los mismos.
También surge el concepto de BMS (Building Management System) para hacer referencia al nuevo tipo de instalaciones integradas en las grandes edificaciones [1].

Aparte de estos conceptos, existen diversas nociones como edificio sostenible, biocontrucción, ambiente inteligente, gestión técnica de edificios, urbótica, etc., que no quedan bien definidas y la frontera entre unas y otras no es del todo clara.

1.2. Características y beneficios del edificio inteligente.

Las características que debe cumplir un buen sistema inmótico son [1]:

- Integración. Es la propiedad fundamental de un edificio inteligente. Es lo que diferencia un edificio inteligente de un edificio automatizado. En una instalación automatizada, los diversos autómatas actúan de forma aislada. Al integrar el

conjunto de sensores, controles, actuadores... el edificio es capaz de detectar lo que ocurre en su interior y en su alrededor y actuar en consecuencia.
- Flexibilidad. El sistema debe ser capaz de adaptarse con facilidad a la incorporación de nuevos subsistemas en su arquitectura. Resulta fundamental que tras una inversión inicial que puede resultar importante, se pueda actualizar de forma rápida y cómoda el sistema con tecnologías futuras.
- Fiabilidad. El número de funciones que controla el sistema será elevado por lo que es necesario reducir los errores al mínimo para que las consecuencias ocasionadas sean irrelevantes.
- Manejo sencillo. El sistema será controlado por más de un empleado y, generalmente, será personal no cualificado. Por ello, es necesario que el funcionamiento que permite controlar el sistema sea de fácil uso y rápida compresión a la hora de aprender a usarlo.

Los costes asociados a la implantación de un sistema inmótico en un edificio pueden parecer, a priori, elevados. Sin embargo, los beneficios que aporta esta implantación, suponen una buena inversión. Además, el desarrollo de las tecnologías y las telecomunicaciones provocan que estos sistemas sean cada día más económicos.

Los beneficios que se obtienen son:

- Reduce el consumo de energía. El edificio inteligente controla de forma óptima el uso de la energía, provocando un ahorro económico considerable. Además, contribuye a proteger el medio ambiente.
- Aumenta el confort. Un edificio inteligente proporciona a los ocupantes del mismo un ambiente más confortable, lo que provoca mejores condiciones de trabajo y favorece la producción de los empleados.
- Aumenta la seguridad. Una de las áreas a la que más importancia da un sistema inmótico es la seguridad. Generalmente el edificio contará con un equipamiento caro y con información que deberán ser protegidos ante intrusiones y alarmas técnicas (inundaciones, incendios, etc.). El edificio incluirá un sistema que protejan los recursos de forma óptima.
- Gestión remota. Disponiendo de un acceso a Internet, desde cualquier rincón del mundo se puede controlar y variar cualquier parámetro del sistema.
- Buena impresión. La introducción de tecnología en edificios de oficinas provoca buena imagen ante los clientes.

Aparte de estos beneficios, propios de la instalación de un sistema inteligente en un edificio y que afectan principalmente al usuario final, se puede considerar que esta nueva industria permite a distintos sectores obtener nuevas oportunidades de negocio y aumentar sus beneficios. Estos sectores son:

- Relacionados con el mundo de la construcción. Para promotores, arquitectos y constructores, la inmótica supone un valor añadido a la hora de participar en el competitivo mundo inmobiliario. Por otro lado, los instaladores encuentran una nueva oportunidad de mercado, no sólo en la instalación sino también en el mantenimiento del sistema.
- Relacionados con el mundo de la electrónica. Los fabricantes de productos aumentan su área de mercado al diseñar y desarrollar los dispositivos que se van a utilizar en el hogar y la oficina, destacando los fabricantes de electrónica de consumo (música, televisores, etc.) y los de electrodomésticos (lavadoras, frigoríficos, etc.). Además pueden aparecer fabricantes dedicados en exclusiva a los sistemas domóticos (pasarelas, sensores, etc.).
- Relacionados con el mundo de las telecomunicaciones. Con la introducción de la domótica/inmótica, los proveedores de servicios ven aumentadas las posibilidades

de aplicaciones y servicios que pueden ofrecer. Además, esta incorporación se traduce en un aumento en las ventas de accesos de banda ancha y así los operadores de telecomunicaciones aprovechan en mayor medida la costosa infraestructura que poseen desplegada.

Por último, destacar que toda esta actividad económica generada alrededor de los edificios inteligentes supone también un beneficio para el estado y la administración pública. Además, se produce un ahorro energético de forma global y la posibilidad de abrir nuevas vías de investigación y desarrollo.

1.3. Sectores relacionados.

Tal y como se comenta en el apartado anterior existen distintos sectores de la sociedad que se ven afectados de forma más o menos directa con la introducción de la inmótica en la vida diaria. Aunque el principal protagonista es el usuario, ya que es el que va a determinar la evolución del sector, los agentes que también intervienen son [6]:

- *Promotor.* Es un actor primordial ya que dispone el suelo sobre el que va a construirse, y delimita las características básicas del nuevo edificio. El promotor deberá conocer las nuevas demandas del comprador par ir incorporándolas a las nuevas construcciones.
- *Arquitecto.* Se encarga del diseño del edificio y deberá determinar las instalaciones de servicios avanzados.
- *Constructor.* Pone en práctica el proyecto del arquitecto, coordinando al colectivo de especialistas que deben instalar las infraestructuras tecnológicas del nuevo edificio.
- *Inmobiliaria.* Posee contacto directo con el usuario. Tendrá que transmitirle al comprador el valor de los nuevos servicios que incorpora el inmueble.
- *Instalador.* Es el encargado de montar los dispositivos al usuario. Es primordial que conozca las nuevas tendencias y sea cada vez más especializado.
- *Fabricante de material electrónico.* Su contribución es esencial para que la incorporación de los nuevos servicios a la vida cotidiana sea una realidad.
- *Proveedor de servicios.* Ofrecen a los usuarios los servicios y las aplicaciones.

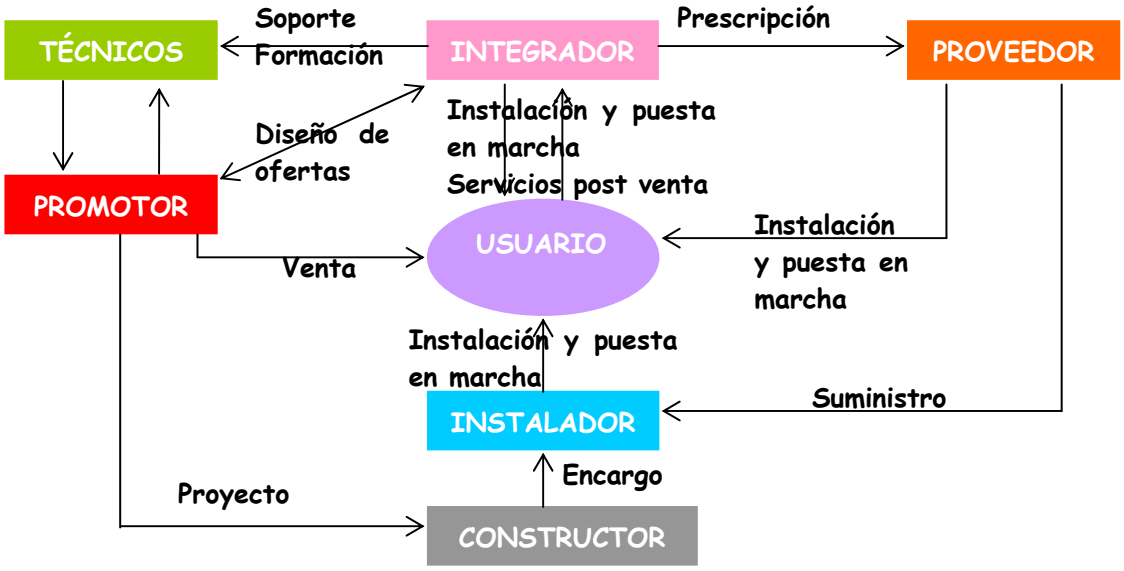


Figura 1.3-1. Protagonistas [6].

Además, la industria emergente provoca la aparición de nuevos elementos en la actividad empresarial como pueden ser las consultoras de sistemas inteligentes o los integradores de soluciones domóticas.

1.4. Pasado, presente y futuro de los edificios inteligentes.

El concepto de edificio inteligente surge en Estados Unidos a finales de la década de los setenta y principio de los ochenta, cuando al desarrollo de las telecomunicaciones se le añade una época donde se produce una elevada actividad en la construcción de edificios de oficinas. Al desarrollo de esta nueva rama de las telecomunicaciones contribuyeron [9]:

- Introducción del primer sistema para la gestión de edificios al comienzo de los setenta, que proporcionaba la integración y la monitorización de los sistemas de ventilación, calefacción y aire acondicionado.
- Necesidad de redes de datos para aunar el volumen de cableado que invadían las oficinas, debido a la incorporación de los ordenadores y los equipos de comunicaciones.
- Crisis energética a mediados de los setenta, que obligó a buscar soluciones para ahorrar energía.

En España la domótica y la inmótica comienzan a desarrollarse a partir de 1990, influidas por el auge que alcanza todo lo referente a la automatización de la vivienda en Francia y en Japón y de los edificios de oficinas en Estados Unidos. Son las grandes empresas y entidades bancarias las que comienzan a instalar en su edificio sistemas domóticos. Así, según el Colegio Oficial de Arquitectos de Madrid, en el año 1995, los edificios censados como inteligentes se distribuyen de la manera que indica la siguiente figura [3].

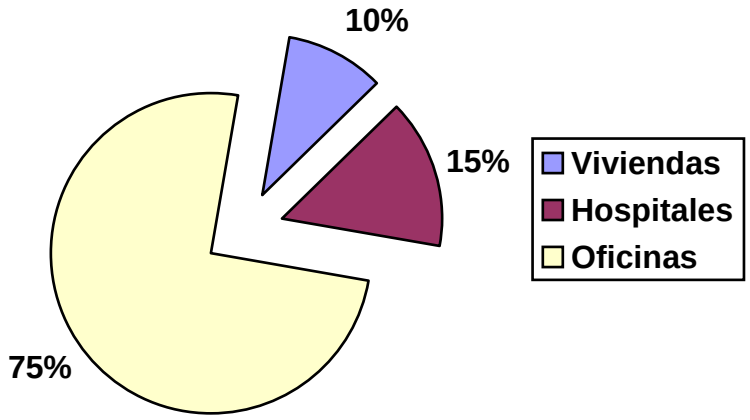


Figura 1.4-1. Distribución de edificios inteligentes en 1995 [3].

No sería hasta los años 2002-2003 cuando el concepto de domótica pasa a ser conocido por la sociedad. En la actualidad el número de viviendas domotizadas todavía es bajo respecto al total de viviendas, principalmente porque son pocas las personas dispuestas a realizar un desembolso adicional para construir una casa inteligente. Por el contrario, gran parte de edificios de oficinas, hoteles, etc., de nueva construcción incluyen algún tipo de sistema automatizado.

El desarrollo de esta tecnología está siendo impulsado por la creación de nuevas empresas y la aparición de asociaciones dedicadas a su promoción. Dentro de estas asociaciones destacan [3]:

- AIDA: Asociación de Inmótica y Domótica Avanzada.
- ANAVIF: Asociación Nacional para la Vivienda del Futuro.
- CEDOM: Comité Español para la gestión técnica de edificación y viviendas.
- G2V: Grupo de empresas de construcción e instalaciones domóticas e inmóticas.

Además, en los últimos años se han organizado ferias, congresos y jornadas específicas o muy relacionadas con el sector: INTERDOMO, FIDMA, MATELEC, Jornadas Nacionales de Domótica, etc.

Un papel fundamental en el desarrollo e implantación de servicios domóticos e inmóticos, lo juega el acceso de banda ancha, sus posibilidades e implicaciones en la sociedad actual, ya que posibilita el desarrollo de nuevos servicios. Es por tanto, que su implantación en la vida de los usuarios debe ser total para que la oferta de servicios a través de ella sea una realidad.

Por otra parte, la oferta de dispositivos domóticos cada vez es más amplia, provocando una reducción del tamaño, coste y complejidad de los mismos y esto se traduce en una aproximación al público en general. Los estudios demuestran unas expectativas de futuro inmejorables, así, según el Ministerio de Industria, en el año 2003 el porcentaje de viviendas domotizadas apenas llegaba al 3%, en el 2004 está cerca del 4,5% y para el año 2007 se prevé un aumento de hasta el 8,5%.
Ante esta perspectiva el número de empresas interesadas en introducirse en este sector es elevado. Empresas como Telefónica, Vodafone, Iberdrola, Gas Natural, Siemens, Samsung, Seguritas Direct, etc., están implicadas en la industria domótica/inmótica.

1.5. Normativa.

Hasta hace pocos años no existía en España una legislación específica para la gestión técnica de edificios. El desarrollo de las tecnologías, la necesidad de aplicar las directivas europeas relacionadas con el sector y la liberalización de las telecomunicaciones han promovido la aparición de la normativa vigente.
A continuación se muestra las normas más relevantes en este campo pero habría que tener en cuenta también la legislación en el ámbito autonómico y municipal [7].

1.5.1. Ámbito europeo.

- *Reglamento Nº 2887/2000.* Reglamento sobre acceso desagregado al bucle local.
- *Paquete TELECOM (Marzo 2000):*
  1. Directiva 2002/21: “Directiva marco”.
  2. Directiva 2002/19: “Directiva acceso e interconexión”.
  3. Directiva 2002/20: “Directiva de autorizaciones”.
  4. Directiva 2002/22: “Directiva Servicio Universal”.
  5. Decisión 676/2002: “Decisión espectro radioeléctrico”.

1.5.2. Ámbito nacional.

1.5.2.1 De carácter general.

- *Ley 32/2003.*Ley General de Telecomunicaciones.

- *Ley 38/1999*. Ley Ordenación de la edificación.
- *Ley 8/1999*. Reforma la Ley 49/1960 sobre propiedad horizontal.
- *Real Decreto 8421/2002*. Reglamento Electrotécnico para Baja Tensión.

1.5.2.2 Telecomunicaciones en edificios.

- *Real Decreto-Ley 1/1998*. Sobre infraestructuras comunes para el acceso a servicios de telecomunicaciones en edificios.
- *Real Decreto 401/2003*. Aprueba el Reglamento regulador de las infraestructuras comunes de telecomunicaciones para el acceso a los servicios de telecomunicación en el interior de los edificios y de la actividad de instalación de equipos y sistemas de telecomunicaciones.
- *Orden CTE/1296/2003*. Desarrolla el Real Decreto 401/2003.

1.5.2.3 Seguridad y gestión de la energía.

- *ITC-BT-51: Instrucción Técnica Complementaria para Baja Tensión.* Establece los requisitos específicos de la instalación de los sistemas de automatización, gestión técnica de la energía y seguridad para viviendas y edificios.
- *Real Decreto 1942/1993.* Reglamento de instalaciones de protección contra incendios.
- *Real Decreto 1853/1993.* Reglamento de instalaciones de gas en locales destinados a usos domésticos, colectivos o comerciales.
- *Real Decreto 1751/1998.* Reglamento de instalaciones técnicas de edificios.

1.5.3. Organismos de normalización y normas técnicas.

Los organismos dedicados a la normalización de servicios, dispositivos o infraestructuras del sector son: ISO e ITU a nivel internacional, CELENEC y ETSI a nivel europeo y AENOR en el ámbito nacional [7].

1.5.3.1 ISO.

La principal iniciativa de ISO en el sector domótico es el desarrollo de un estándar a nivel mundial: HES (ISO/IEC 10192). Se trata de un trabajo elaborado por el grupo ISO/IEC JTC1/SC25/WG1 en el que han colaborado expertos de Asia, Europa y Norte América.
Por otra parte, trabaja para la aceptación como normas ISO de distintos protocolos domóticos. Ejemplo de este trabajo es ISO 16484 donde se aprueba BACnet como norma ISO.

1.5.3.2 ITU.

Entre los trabajos relacionados con la domótica, desarrollados por la ITU destaca la elaboración de unos estándares internacionales para redes telefónicas recogidos en las normas G.989.1, G.989.2 y G.989.3, basados en la segunda versión de HomePNA.

1.5.3.3 CELENEC.

EN 50090 (Home & Building Electronic Systems) se trata de una norma europea desarrollada por el comité CLC/TC205 “Sistemas electrónicos para viviendas y edificios” de CENELEC

(Comité Europeo de Normalización Electrotécnica). Está constituida por diversas partes y se incluye el estándar KNX como parte integrante de las mismas.
La aprobación de las distintas partes no supone obligado cumplimiento mientras que un documento legislativo nacional no haga referencia a la misma. Sin embargo, las empresas fabricantes de productos que deseen adoptar el sistema KNX deberán cumplir: ISO 9000-1, EN 50090-2-2 y Certificación Konnex.

1.5.3.4 ETSI.

El Instituto Europeo de Normas de Telecomunicaciones (ETSI) es un organismo dedicado a la elaboración de las normas de telecomunicación que faciliten la estandarización del sector. En el ETSI participan como miembros no sólo las Administraciones, sino también los operadores de red, la industria, los centros de investigación y los usuarios de los servicios de telecomunicación.

En lo referente a edificios y viviendas inteligentes, el ETSI ha creado, junto con CELENEC y CEN, la iniciativa ICTSB (Information and Communications Technologies Standard Board) que se encarga, entre otras tareas, de los trabajos de normalización en este terreno. Dentro de ICTSB el grupo de trabajo destinado al sector es el SHSSG (Smart House Standards Steering Group).

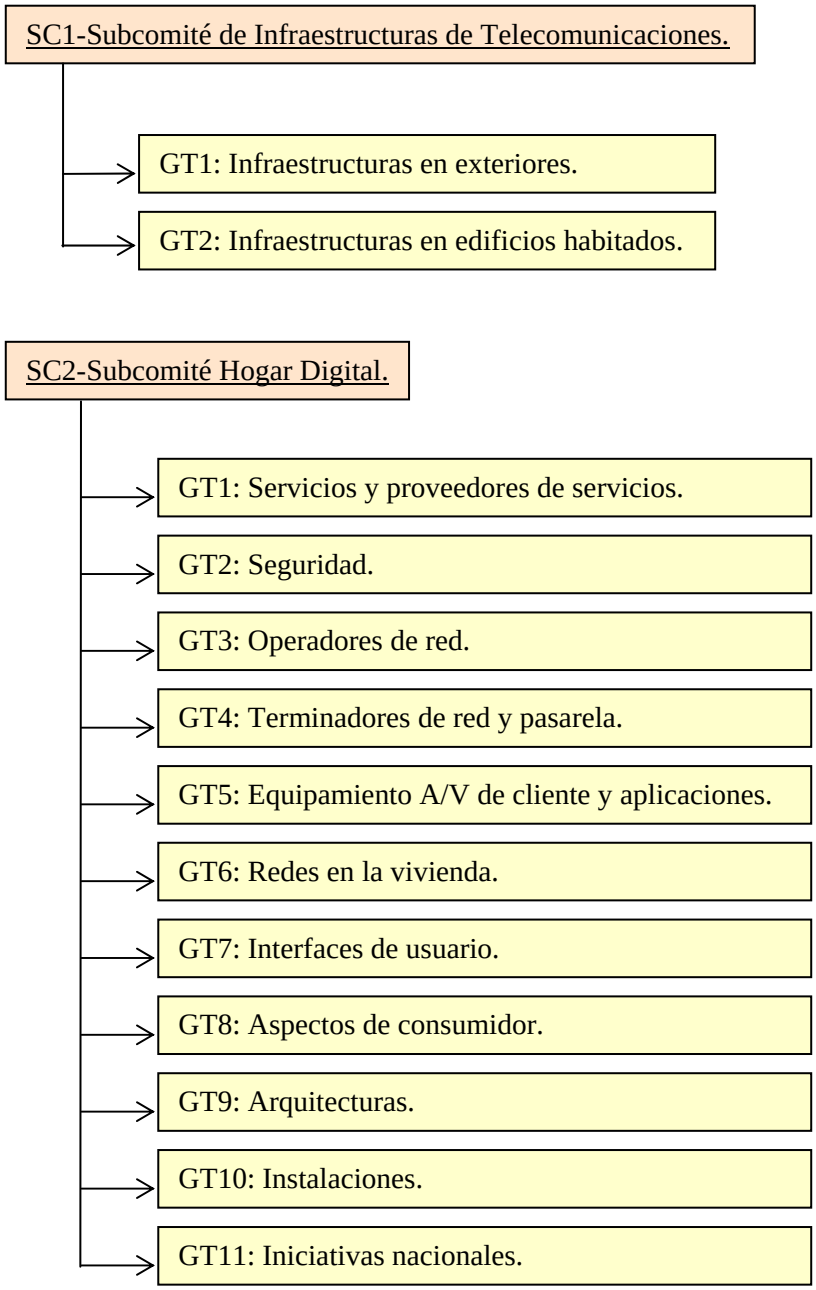
Por otra parte, los comités técnicos de la ETSI, ETSI/AT y ETSI/HF, están desarrollando trabajos en este campo.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, junto con la Asociación Española de Normalización y Certificación (AENOR), participa en la elaboración y transposición de las normas técnicas e informes procedentes del ETSI, convirtiéndolos en normas nacionales.

1.5.3.5 AENOR.

El Comité Técnico de Normalización 133 “Telecomunicaciones” se encarga de la normalización de las tecnologías, los equipos, los productos, las infraestructuras, las redes, los medios, los servicios y otros aspectos en el ámbito de las telecomunicaciones. Además, realiza un seguimiento de cualquier tema desarrollado por el Instituto Europeo de Normas de Telecomunicación (ETSI).

Este comité se organiza de la siguiente manera:



En el seno de AENOR también trabaja en esta normalización, el subcomité AEN/CTN 202/205 “Sistemas Electrónicos Domésticos y en Edificios”.

2. APLICACIONES EN EDIFICIOS INTELIGENTES

2.1. Introducción.

Las instalaciones inmóticas que se implantan en un edificio van encaminadas a lograr, principalmente, un ahorro energético y un aumento de la seguridad y el confort. Sin embargo, un sistema inmótico no tiene por qué ser completo, en su diseño se pueden considerar las necesidades que el cliente verdaderamente demande, contemplando las posibles futuras ampliaciones [1].

Los sistemas que se pueden instalar en un edificio dependerán de diversos factores como las necesidades de la empresa, las características del edificio o la inversión que se esté dispuesto a realizar.

En este apartado se abordan las aplicaciones que se pueden desarrollar en un edificio, centrándose en construcciones destinadas al sector terciario.

2.2. Confort y ahorro energético.

Los sistemas inteligentes de climatización y de iluminación, entre otros, producen dos beneficios a la vez: aumento del confort en el edificio y disminución del consumo energético.

En domótica la búsqueda del confort dentro de la casa es una de las tareas principales, ya que el usuario desea encontrar en su hogar las mejores condiciones para disfrutar de su tiempo de descanso y ocio.
A simple vista, puede parecer que el confort en la automatización de edificios del sector terciario es un valor secundario, dándoles mayor prioridad a la seguridad y al ahorro de energía. Sin embargo, el bienestar de los usuarios del edificio puede llevar asociado unos beneficios a tener en cuenta. Por ejemplo, en clínicas u hoteles, las propiedades de confort que puede presentar un edificio inteligente suponen un valor añadido cuando el cliente deba escoger entre varias opciones.
Además, en edificios de oficinas un ambiente adecuado provoca mayor productividad de la empresa. Por un lado, el rendimiento de un trabajador que desempeña su tarea en un lugar con condiciones de trabajo atractivas será mayor y, por otro, los clientes encontraran una empresa que busca el bienestar de los mismos y equipada con los últimos avances tecnológicos.

Dentro de la búsqueda del confort de los empleados, una de las aplicaciones que puede resultar útil es el conocimiento de tráfico en un momento dado. El sistema instalado en el edificio podría proporcionar automáticamente a los empleados el reporte del tránsito con destino a su casa minutos antes de la hora de salida del trabajo.

Uno de los mayores gastos a los que tiene que hacer frente una empresa es el asociado a la gran cantidad de energía consumida en el edificio. Aunque se buscan alternativas para obtener diversas fuentes de energía, como la instalación de paneles solares o más recientemente ventanales de vidrio capaces de generar energía eléctrica, un ahorro sustancial puede lograrse gestionando de forma óptima los distintos sistemas eléctricos.

2.2.1. Climatización.

En los sistemas CVC (climatización, ventilación y calefacción) es donde mayores inversiones se están realizando pues además de abarcar gran parte del consumo energético, están presentes en casi todas las instalaciones y son la primera contribución al bienestar.

El sistema será capaz de ajustar automáticamente los niveles de humedad y temperatura en el interior del edificio en función de la temperatura exterior. Este ajuste tendrá en cuenta la zona y el horario de ocupación.
La zonificación del efecto de climatización permite dividir el edificio en zonas independientes de regulación y programación según sus requisitos de uso o condiciones térmicas, aumentando la eficiencia global de la instalación.
Dependiendo del sistema que se instale, la gestión de los horarios de funcionamiento de la instalación será diversa. Los sistemas más avanzados serán capaces de detectar si la zona se encuentra ocupada o desocupada y actuar en consecuencia. Otros sistemas se programarán inicialmente según los diferentes horarios de ocupación, por ejemplo, los edificios de oficinas en días festivos o por la noche poseen unas necesidades de climatización menores [4].

Zonas que merecen una especial atención son las salas de máquinas. Estas estancias deberán contar con elementos que controlen de forma precisa la temperatura y la humedad del recinto, ya que una pérdida de control de estos factores puede provocar un deterioro o falta del servicio o pérdida de datos.

2.2.2. Iluminación.

El sistema de iluminación mantendrá el nivel de iluminación deseado mediante el control y ajuste de los siguientes parámetros de cada lámpara [9]:

- On/off.
- Nivel de luz.
- Color de la luz.
- Enfoque.
- Apertura.
- Orientación.
- Posición en el espacio.

El nivel de luz se regula según la época del año y la hora del día. Se busca aprovechar de forma óptima la luz solar y para ello se considerará la posibilidad de modificar el tintado de los cristales y se tendrá en cuenta la presencia o no de persianas o toldos, los cuales se podrán regular automáticamente.

El encendido y apagado de las luces se lleva a cabo mediante la programación de horarios o con sensores de presencia. Estos sensores permiten un considerable ahorro de energía ya que logran que las zonas menos frecuentadas como escaleras, aseos, pasillos o aparcamientos permanezcan sin luz si no se detectan personas.
Los tradicionales interruptores de encendido y apagado seguirán apareciendo pero se les puede añadir mayor funcionalidad como el control de la intensidad luminosa o tareas de control de acceso, permitiendo el encendido o apagado de una zona a unos determinados usuarios.

La instalación puede ser programada para situaciones especiales, como una proyección en una sala de proyecciones dentro de un edificio de oficinas. Al activar esta opción, por ejemplo, se cerrarán las cortinas mientras que las luces centrales se apagan lentamente y la intensidad de las

laterales disminuye un tanto por ciento. Cuando se inicie la proyección y tras un pequeño lapso de tiempo, se apagarán completamente dejando encendida tenuemente la luz de la entrada.

Otro ejemplo en el que puede resultar útil la regulación de la luminosidad, se produce en situaciones de evacuación ante incendios. Así, se pueden iluminar con mayor intensidad las vías de salida y oscurecer de forma ostensible los accesos que no conducen a la salida o llevan a la zona conflictiva.

2.2.3. Gestión de los ascensores.

Con la gestión de ascensores se busca mejorar el servicio al usuario en cuanto a velocidad y seguridad, garantizándole, por otra parte, una sensación de confort. Además, una gestión eficiente del conjunto de ascensores permitirá ahorrar energía ya que se evitan los viajes innecesarios, y tener mayor seguridad al monitorizar y controlar los accesos a las plantas del edificio.

Es necesario establecer una red de comunicación interna entre el grupo de ascensores, para que sea posible el intercambio de datos sobre las llamadas realizadas y el número de personas, tanto dentro de la cabina como fuera. Esta comunicación permitirá conocer para cada cabina los datos de funcionamiento, su ubicación o su dirección, y así determinar qué cabina es la más adecuada para atender la llamada desde el exterior.
El sistema inmótico va a ser capaz de limitar el recorrido del elevador restringiendo el acceso a determinadas plantas con motivos de seguridad o mantenimiento. También se puede programar para que un determinado ascensor atienda exclusivamente las llamadas hacia o desde una determinada planta, útil cuando se espera un tráfico excepcional con motivo de una conferencia, reunión, exposición, etc.
Se podría tener en cuenta el horario de entrada y salida de trabajadores. Así, para facilitar la entrada de personal, los elevadores se posicionan en la planta baja automáticamente y sólo atenderían las llamadas exteriores en dirección de subida. Igual ocurriría a la hora de salida, las cabinas estarían en las plantas superiores, atendiendo únicamente las llamadas exteriores en dirección de bajada.
Evidentemente, se podrán programar las cabinas para que actúen de forma especial en caso de incendio, avería o corte en el suministro eléctrico.
Por otra parte, se consigue un ahorro energético desconectando un número de elevadores en horas de poco tráfico [8].

2.2.4. Otros.

Dependiendo de las infraestructuras que posee el edificio se pueden incluir distintos sistemas domóticos que contribuyen a mejorar el equipamiento del edificio.
Por ejemplo, si la edificación tiene zonas ajardinadas se puede incluir un sistema de riego automático que se active únicamente cuando sea necesario. Si el edificio posee parking subterráneo se podría añadir un sistema purificador de aire que entre en funcionamiento cuando se supere un nivel prefijado de dióxido de carbono.
Se puede dotar al edificio de una instalación de hilo musical, que permita su uso como sistema de megafonía para localizar a alguien o informar a parte o a todo el recinto de una situación excepcional.

Por último, mencionar que, si se trata de una vivienda, la gestión automática de cualquier dispositivo o electrodoméstico, el establecimiento de la denominada red multimedia (conexión entre televisores, DVDs, equipos de música, cámaras, PCs...) y los mecanismos de tele asistencia favorecen la calidad de vida dentro del hogar.

2.3. Seguridad.

La protección de los edificios es una cuestión que desde siempre ha presentado interés y en este terreno se invierten grandes cantidades de dinero. La gestión de la seguridad debe contemplar tanto la seguridad personal como la seguridad del patrimonio, considerando parte del patrimonio la información que, en la mayoría de los casos confidencial, se maneja.

Los sistemas automatizados de seguridad abarcan tanto la detección de intrusos o robo como lo que se denominan alarmas técnicas que incluyen las detecciones de fugas, inundaciones o incendios.

2.3.1. Gestión de la seguridad básica.

Se pueden distinguir dos zonas bien diferenciadas: el interior, donde el grado de seguridad debe ser máximo, y el exterior, en donde se permite un grado de seguridad menor.

La seguridad en la zona exterior del edificio suele contar con elementos de protección pasivos como son rejas o muros a los que se le añaden sistemas más sofisticados como cámaras de vigilancia o barreras de infrarrojos.
La inclusión de detectores de vibración y de rotura de cristales permitirá una detección prematura antes de entrar en el edificio.

Los sistemas de vigilancia que permiten la detección de una posible intrusión en el interior del edificio se basan en la distribución de sensores de presencia o movimiento situados en zonas estratégicas del edificio. Generalmente, se suelen añadir una serie de cámaras que permiten recibir en tiempo real lo que ocurre en las distintas zonas del edificio. En este punto, se pueden encontrar distintas posibilidades: el tradicional sistema de circuito cerrado de televisión o las actuales cámaras IP, que permiten la visualización de imágenes desde cualquier lugar y que pueden llevar incorporada detectores de presencia.
Una vez detectada la intrusión el sistema será capaz de generar una alarma sonora y realizar una serie de llamadas telefónicas de aviso al centro de seguridad o a la policía.

Para dar impresión desde fuera de que hay gente dentro del edificio se emplea la simulación de presencia. Este sistema consiste en la programación de forma aleatoria y temporizada del encendido y apagado de luces o aparatos, subida y bajada de persianas o de cualquier otro parámetro que dé indicios de la presencia de personas en el interior [1].

2.3.2. Control de acceso.

A la hora de proteger el edificio ante posibles robos es conveniente conocer las personas que entran y salen del edificio así como las zonas del interior por las que se mueven. Dependiendo del sistema que se instale el grado de protección será mayor o menor.
Mediante todo tipo de tarjetas se permite validar / invalidar el acceso en zonas restringidas o en horarios prefijados, además de controlar la presencia y la situación de los empleados. También se pueden incorporar sistemas de lectura de datos del DNI, que leen los datos del visitante y los incorpora a una base de datos.
Ejemplos de estos dispositivos de control son las tarjetas magnéticas, los lectores de huella digital o el escáner de voz [1].

2.3.3. Gestión de alarmas técnicas.

La colocación por el edificio de diversos tipos de detectores permite advertir de incendios, fugas de gas, inundaciones, fallos en el suministro eléctrico, etc. Estos sistemas, aparte de avisar al personal encargado, pueden realizar automáticamente llamadas de socorro a los servicios de emergencia y reproducir una grabación donde se explica a los usuarios que deben hacer en esa situación [1].
Una ventaja importante en este tipo de instalaciones es la posibilidad de generar acciones que permitan reducir la gravedad del accidente. Desde el simple corte de una llave de paso para detener una fuga de agua hasta un verdadero dispositivo de seguridad, que en caso de incendio incluya el cierre de puertas cortafuegos, evacuación de humos, corte de la electricidad, inhabilitación de ascensores, etc.

Especial importancia suele tener la detección de incendios, ya que puede estar en juego la vida de las personas que se encuentran en el interior del edificio. Además, el sistema de detección anti-incendios debe seguir una legislación específica.

La elección del sistema de detección viene condicionada por diversos factores:

- Las pérdidas humanas o materiales en juego.
- La posibilidad de vigilancia constante y total por personas.
- La rapidez requerida.
- La fiabilidad requerida.
- La zona a vigilar.
- Su coherencia con el resto del plan de emergencia.
- Su coste económico.

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.

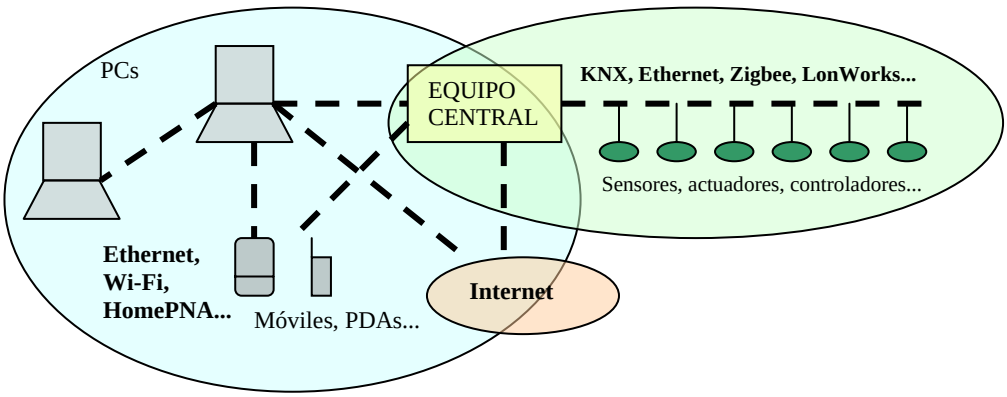


Ilustración 3.1-1 Red de control.

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].

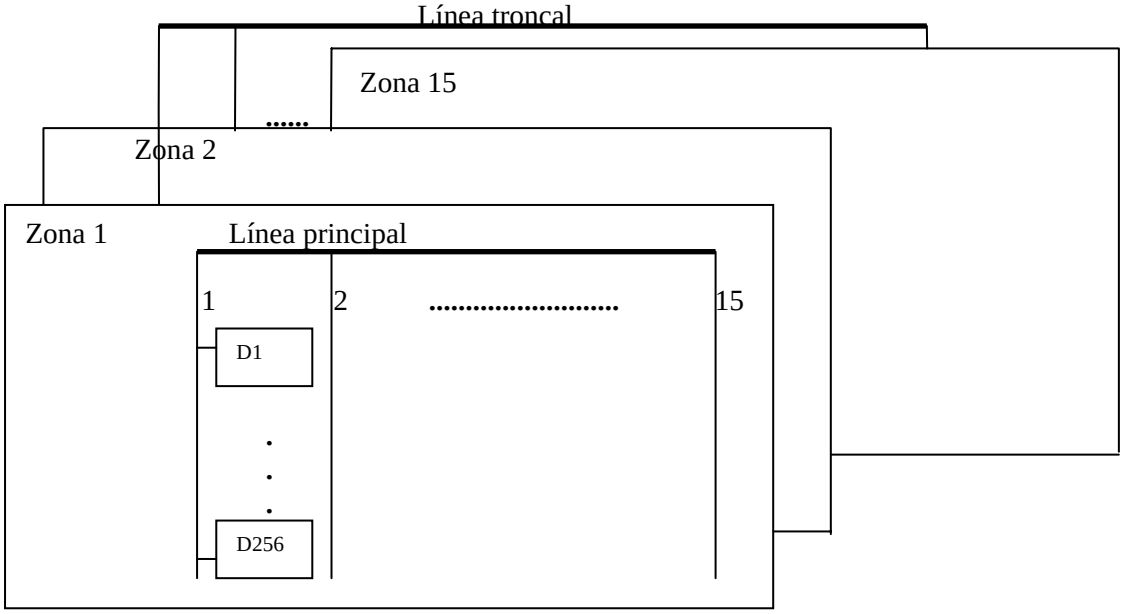


Ilustración 3.2.1-1. Topología.

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:

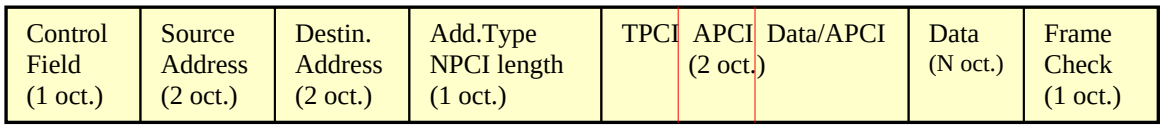


Ilustración 3.2.1-2. Formato de trama.

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.

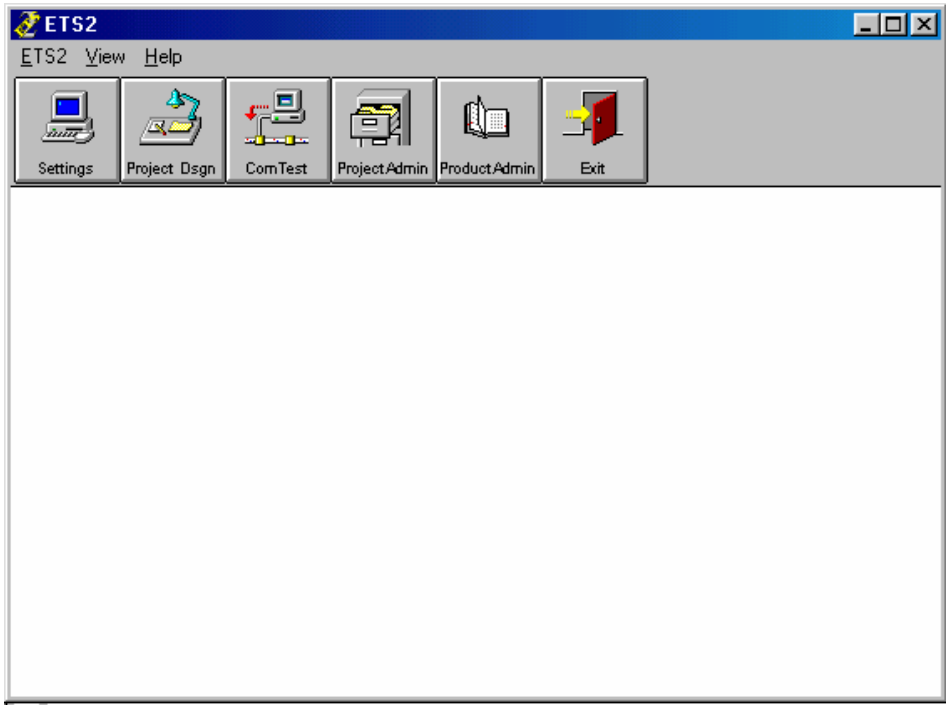


Ilustración 3.2.1-3. Herramienta ETS [3].

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:

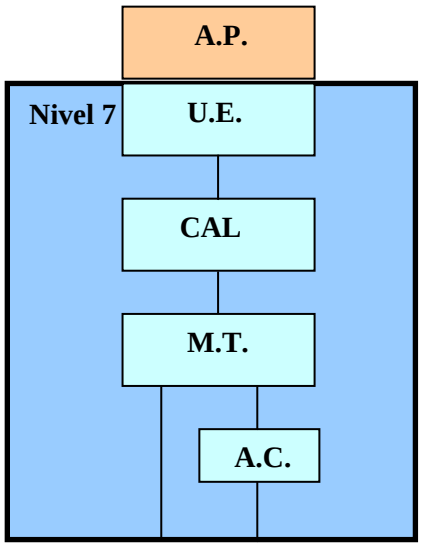


Ilustración 3.2.3-2. Nivel de aplicación.

- 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.

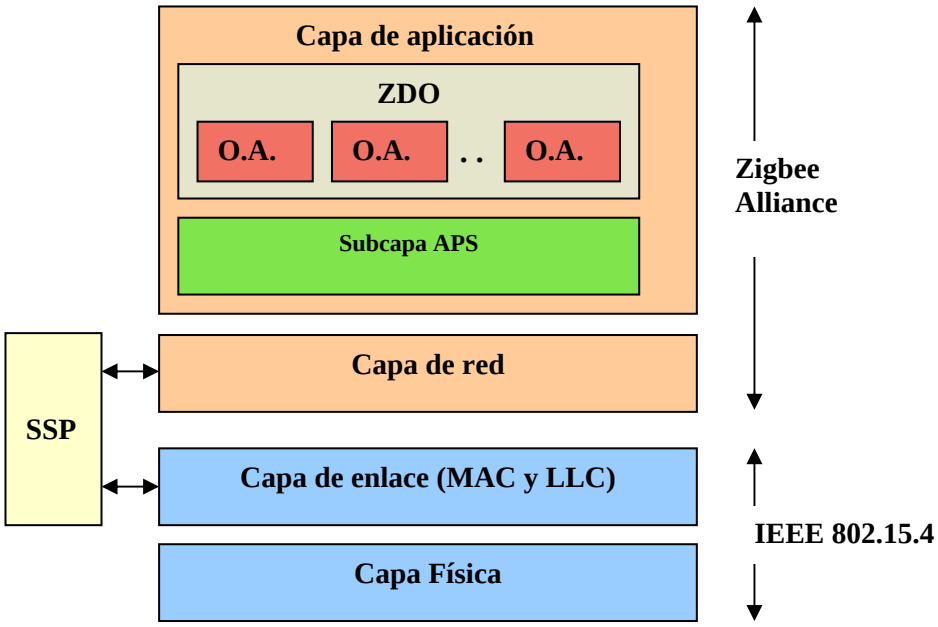


Ilustración 3.2.4-3.2.4-1. Capas Zigbee.

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.

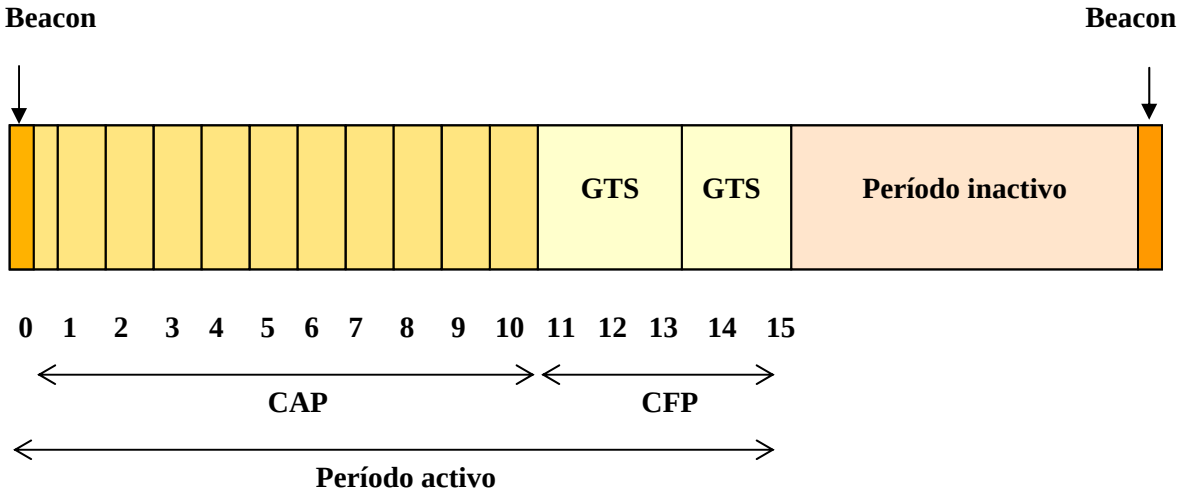


Ilustración 3.2.4-4. Formato supertrama.

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.

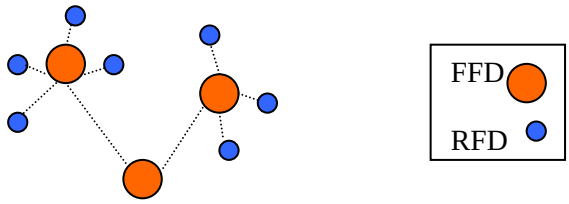


Ilustración 3.2.4-6. Árbol.

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

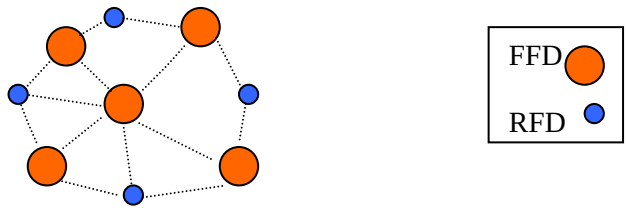


Ilustración 3.2.4-7. Malla.

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.

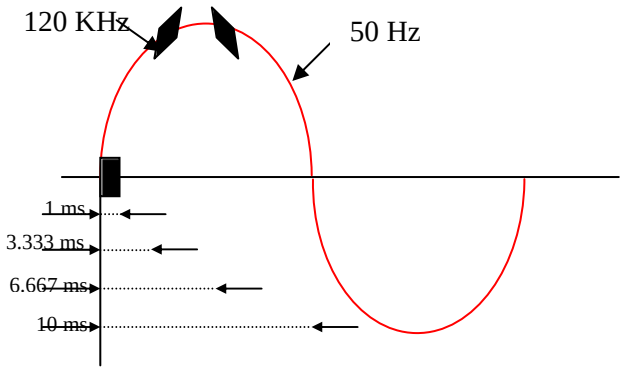


Ilustración 3.2.5-1. Señal X-10 [3].

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.

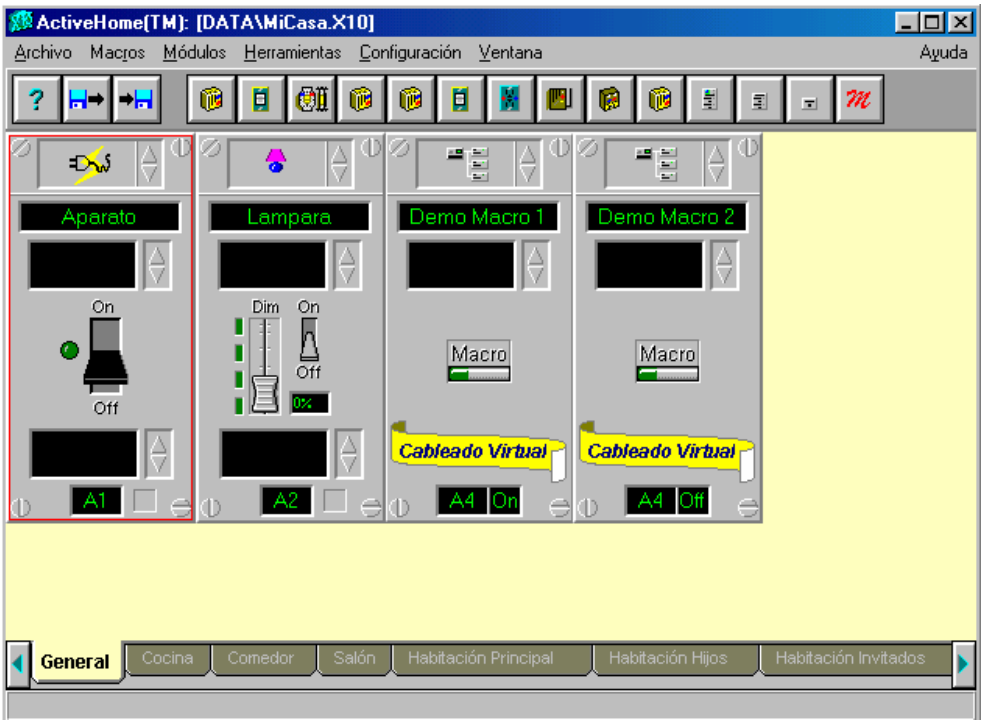


Figura 3.2.5-3. Programa ActiveHome [3].

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.

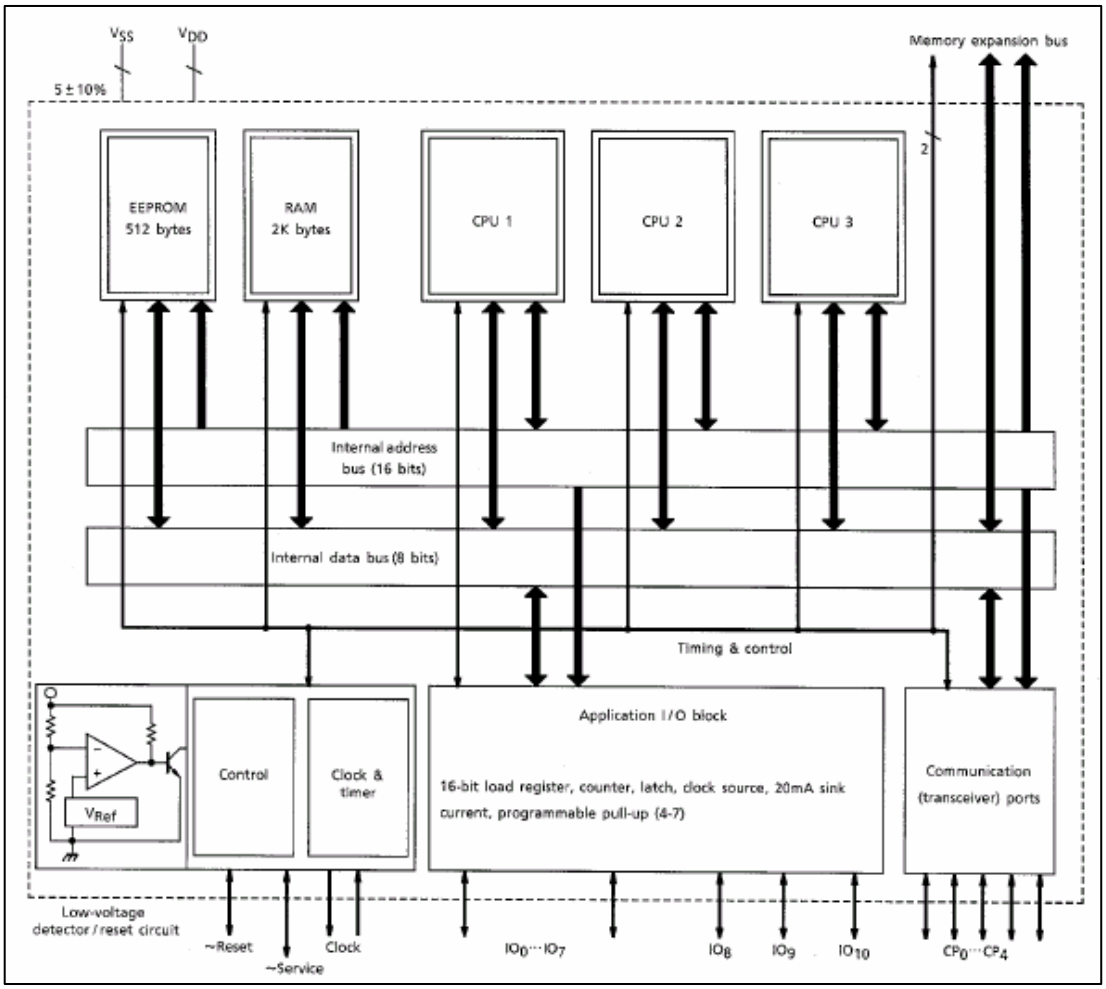


Ilustración 3.2.6-1. Diagrama de bloques de un Neuron Chip de Toshiba.

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 (topología libre o en bus)	78 Kbps	FTT-10, FTT-10A, LPT-10	64-128	500 m(topología libre) 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.

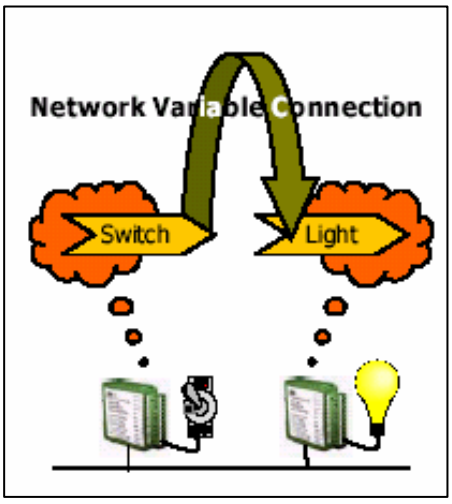


Ilustración 3.2.6-2. Variables de red.

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).

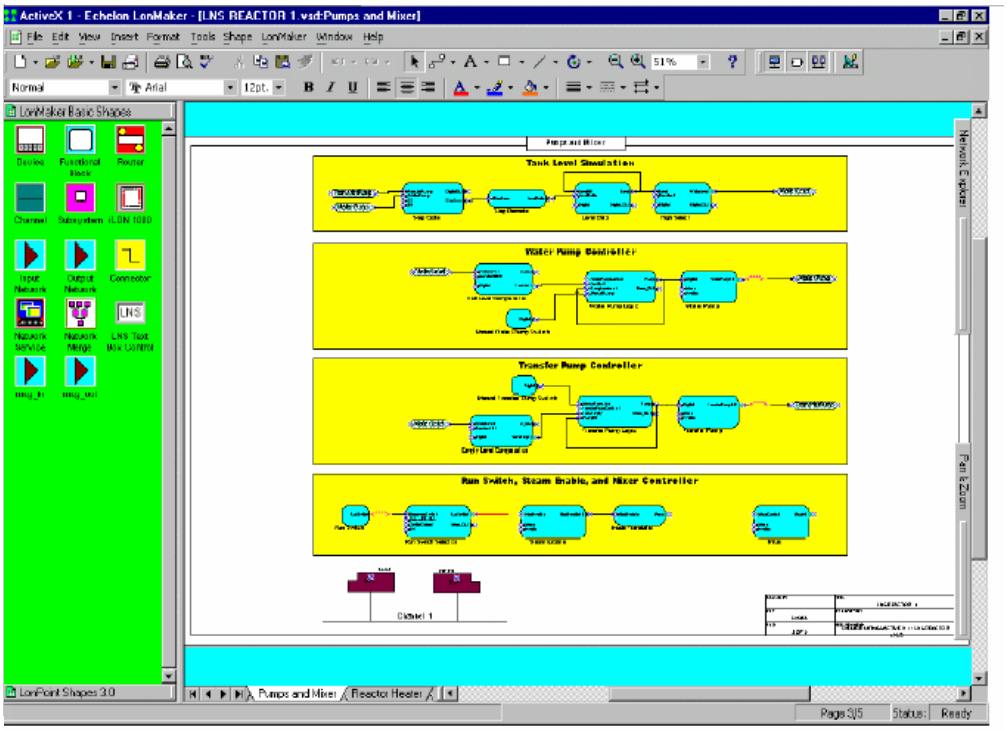


Ilustración 3.2.6-3. Herramienta LonMaker [3].

- 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.

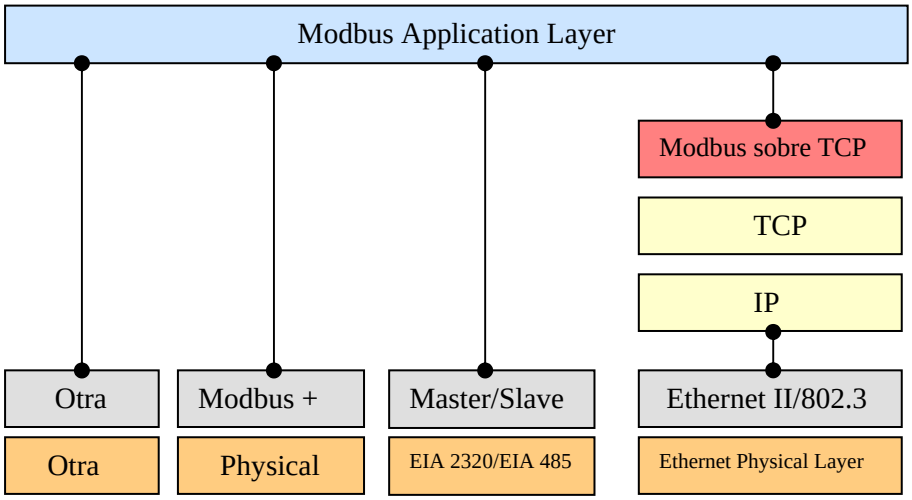


Ilustración 3.3.1-1. Arquitectura Modbus.

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:

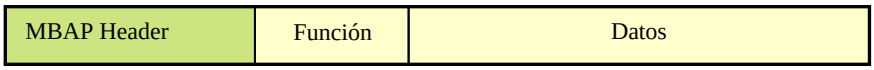


Ilustración 3.3.1-4. Trama TCP/IP.

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].

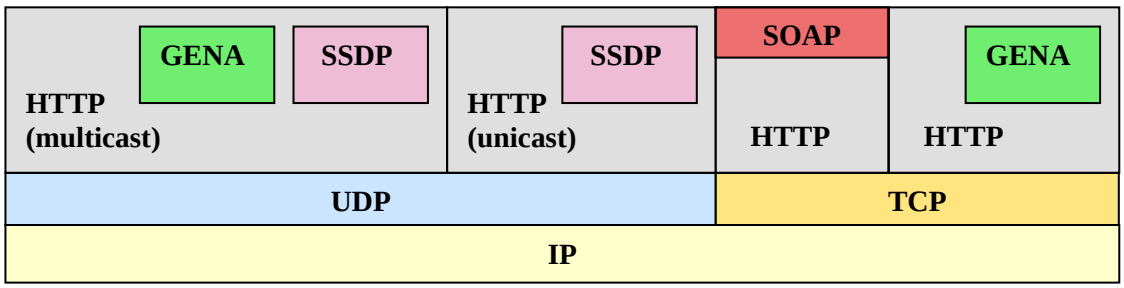


Figura 3.3.2-1. Pila de protocolos.

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.

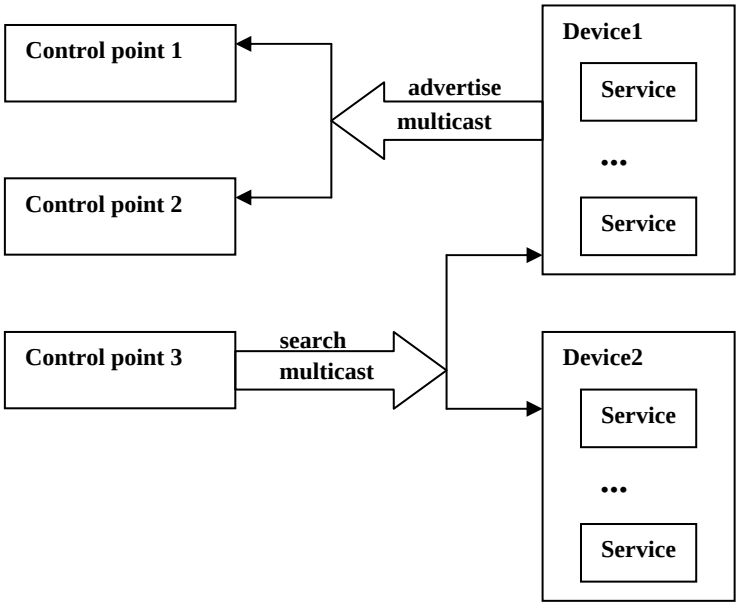


Figura 3.3.2-2. Descubrimiento.

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.

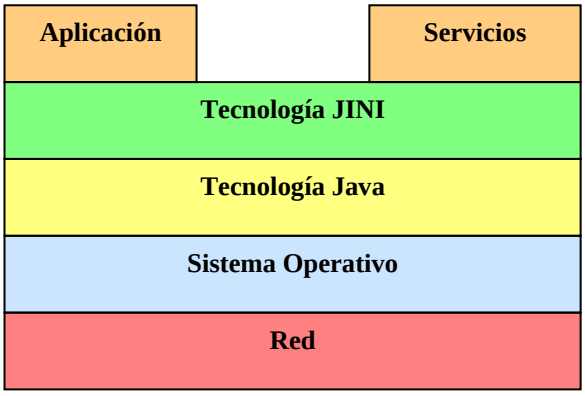


Figura 3.3.4-1. Arquitectura Jini.

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.

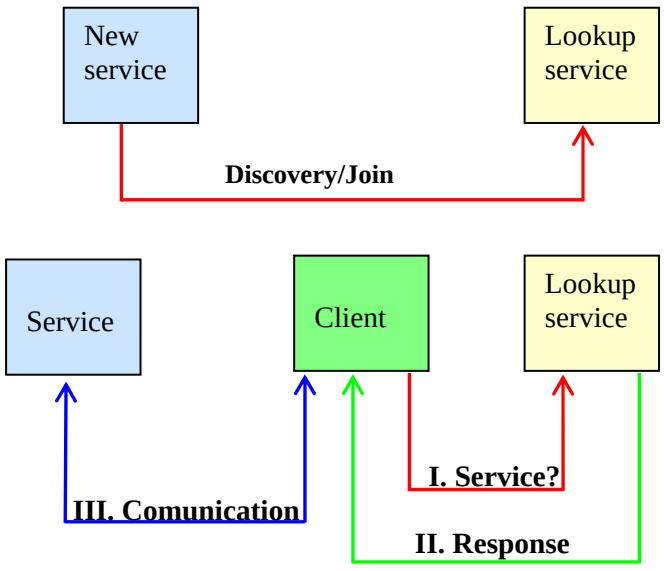


Ilustración 3.3.4-2. Descubrimiento y acceso a un servicio.

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.

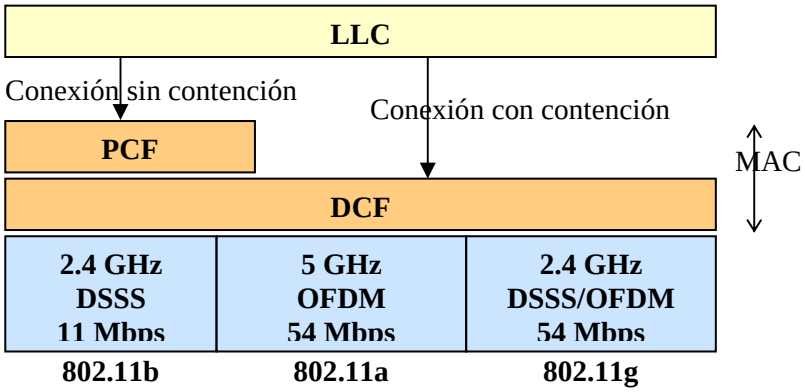


Ilustración 3.4.1-2. Arquitectura Wi-Fi.

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).

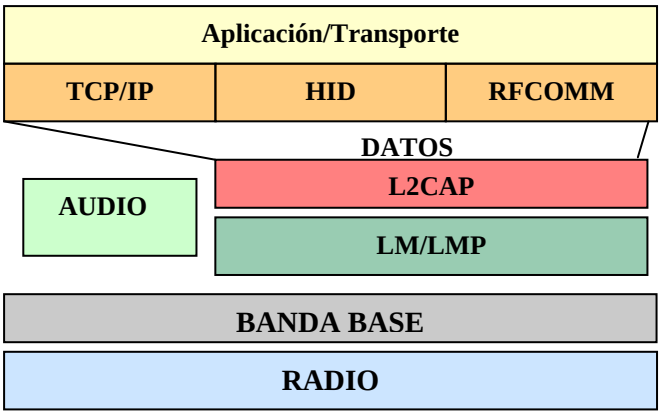


Ilustración 3.4.2-1. Arquitectura Bluetooth.

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.

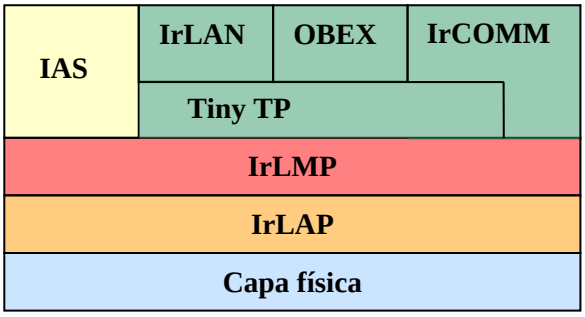


Ilustración 3.4.3-1. Protocolos IrDA.

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.

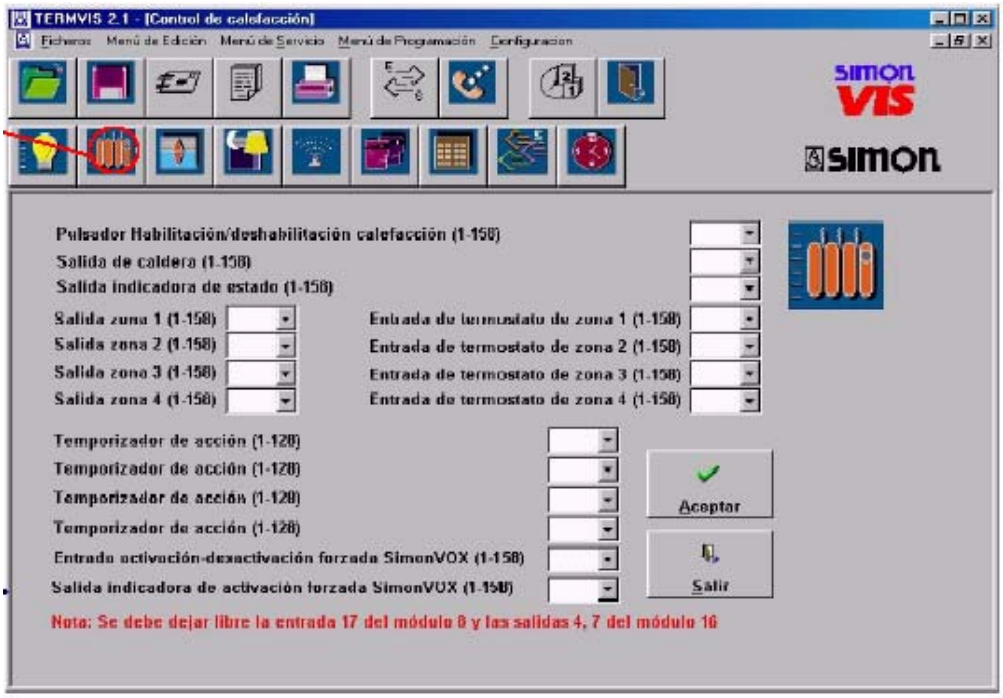


Figura 3.7-1. Simon VIS [3].

- *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.).

4. DISPOSITIVOS DE LOS EDIFICIOS INTELIGENTES

4.1. Introducción.

Como se ha expuesto con anterioridad, una red domótica divide en dos partes diferenciadas, la red que se encarga de interactuar con el medio y controla los equipos domóticos y la red que proporciona al usuario la monitorización de los dispositivos instalados en el edificio y la configuración de los mismos.
Estos dos segmentos encuentran un nexo de unión en los sistemas de control y en las pasarelas de servicios.
También se puede distinguir entre la red interna, que constituye la red inmótica, y la red externa, que proporciona la comunicación con el exterior y la posibilidad de actuar sobre la red interna desde el exterior del recinto donde está implantada la misma, ya sea vía Internet o mediante acceso telefónico.

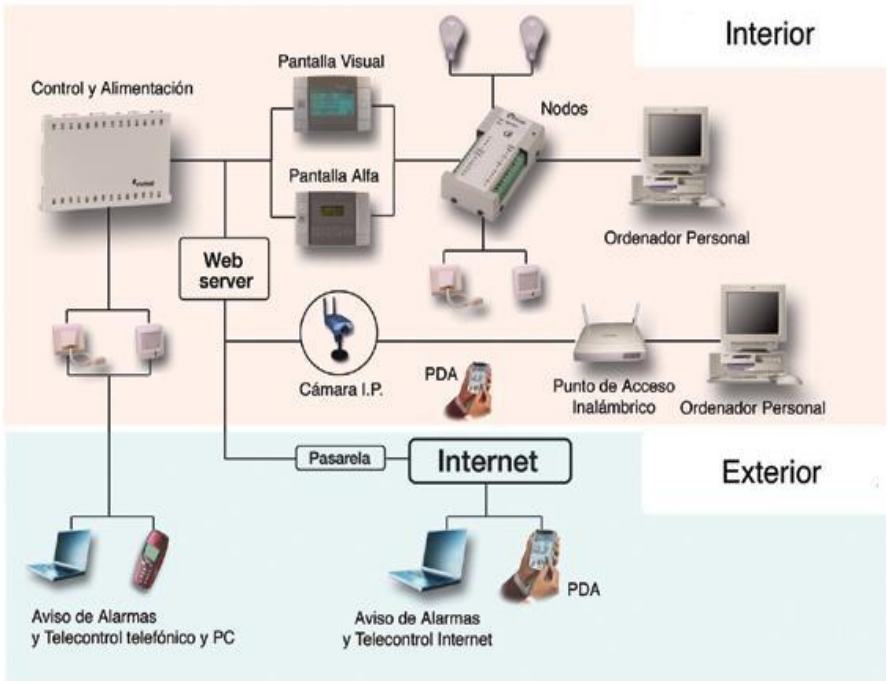


Ilustración 4.1-1. Red domótica.

Los elementos que van a permitir automatizar de forma inteligente un edificio son [4]:

- Sensores. Son los elementos que emplea el sistema para recoger información de diferentes parámetros como pueden ser: la temperatura, el grado de luz, la presencia de personas, etc. Los datos adquiridos son enviados al sistema de control, previo paso por los acondicionadores de señal. De forma general, las señales que entrega un sensor necesitan ser adaptadas al controlador que las recibe. Los acondicionadores de señal se encargan de realizar esta tarea de adaptación.
- Sistema de control. Recoge los datos que le envían los sensores, los procesa y envía las órdenes adecuadas a los actuadores.
- Actuadores. Son elementos que utiliza el sistema para modificar el estado de ciertos equipos e instalaciones. Recibe las órdenes del sistema de control para modificar los parámetros de actuación de los dispositivos que se controlan. Si resulta necesario,

entre el actuador y el controlador se sitúa una interfaz, que permite acondicionar la señal a la entrada del actuador.

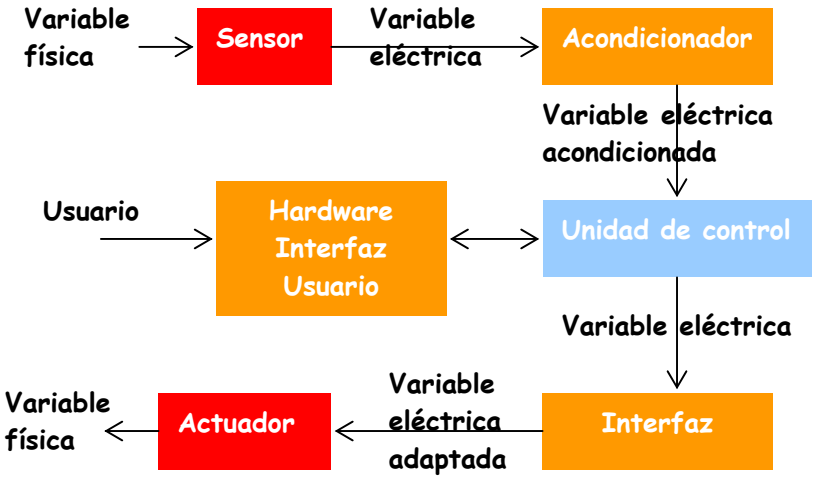


Figura 4.1-2. Componentes básicos [3].

Por otro lado, es necesario que el personal encargado de la instalación pueda comprobar el estado de los dispositivos y cambiar de forma fácil y cómoda los parámetros de configuración de los equipos. Los sistemas de control y la pasarela residencial pueden estar equipados con pequeñas pantallas y teclados, que permiten una instalación, configuración y control local pero que resultan demasiado básicos e insuficientes para realizar operaciones complejas y controlar de forma global y remota los equipos. Por estos motivos resulta adecuado dotar al sistema de elementos como PCs, teléfonos móviles, PDAs o Web Pad, que permiten realizar estas tareas de forma más conveniente.

A continuación se describen con mayor detalle estos elementos básicos, necesarios para llevar a cabo el control de un edificio automatizado. Además se comentarán brevemente algunos productos que se pueden encontrar en el mercado actualmente.

4.2. Sistemas centrales.

4.2.1. Pasarelas de servicios o residenciales.

Una pasarela de servicios es un dispositivo que realiza las funciones de plataforma para la prestación de servicios y constituye la frontera entre las redes de accesos externas y las redes internas del edificio inteligente [1].
Permite la conectividad total del edificio con el mundo exterior y será capaz de controlar el sistema domótico: sistemas de seguridad y de gestión de energía, electrodomésticos, equipos de electrónica de consumo, etc.

Las funciones que lleva a cabo una pasarela de servicios pueden implementarse en un ordenador personal, proporcionándole tarjetas específicas y una aplicación software elaborada para tal fin. Sin embargo, cuando se trata de una instalación en un hogar se opta por una pasarela residencial en sí por motivos de seguridad, fiabilidad y facilidad.
Una posibilidad lógica sería la integración en un único dispositivo de la pasarela y el sistema o los sistemas de control centralizado. En la actualidad esta opción no es llevada a cabo por los fabricantes de pasarelas porque existen en el mercado múltiples sistemas de control destinados a

operaciones específicas. Se prefiere una convivencia con los sistemas de control, permitiendo la gestión desde la pasarela pero sin sustituir ninguno de los actuales componentes.

Las características básicas que debe cumplir una pasarela son:

- Fácil instalación. Cuando se trata de redes del hogar el usuario no debe estar obligado a ser un experto en redes y no debe sentir la necesidad de contratar a un técnico para que instale la pasarela. Por tanto, la instalación y la configuración de la pasarela deben ser sencillas y asequibles. Lo ideal sería que fuese Plug&Play.
- Escalable. Debe ser flexible ante la introducción de nuevos servicios y dispositivos o la actualización de los ya existentes.
- Soporte para distintas redes. Es necesario que la pasarela posee diversas interfaces que permitan la comunicación exterior e interior.
- Segura. Es necesario que ofrezca servicios de protección de datos, autenticación de usuarios, control de accesos, encriptación y cortafuegos. Además debe ser capaz de formar VPN (Virtual Private Networks).
- Potente. En una pasarela de servicios se van a concentrar múltiples servicios y por tanto, será necesario que posea la memoria y la capacidad de procesamiento necesarias para soportarlos. Además, estará dotada de un sistema operativo robusto y multitarea.
- Monitorización empleando páginas web. El usuario debe tener acceso tanto de forma local o como de forma remota a la pasarela, para funciones de monitorización y control del sistema domótico.

Las pasarelas se pueden clasificar en dos grupos:

- De banda ancha. Se trata de routers, hubs o módems que actúan como pasarelas, adaptando los datos de la red interna y la conexión de banda ancha. Poseerán intefaces de diversos tipos: ethernet, USB, etc.
- Multiservicios. Proporcionan varias interfaces para redes de datos y control con diferentes tecnologías. Son más complejas y potentes que las primeras.

En la siguiente tabla se muestran tres tipos de pasarelas comerciales:

Nombre pasarela	OASIS	Connetor 2000	e-box
Fabricante	Amper	Coactive Networks	Ericsson
Características	S.O. Windows98. Amplio disco duro. Simple de instalar y usar. Varias ranuras PCI.	Basada en CORBA. Arquitectura propietaria: IOConnect.	Desarrollado según OSGI. S.O. basado en LINUX.
Acceso al exterior	RTC RDSI ADSL	ADSL Módem de cable	ADSL Módem de cable
Acceso al interior	HomePNA HomeRF IEEE 1394	LonWorks	Bluetooth LonWorks
Principales servicios	Proxy y cortafuegos. Servidor de archivos. Servidor Web. Servidor de correo. Sistemas de seguridad. Control medioambiental.	Telemetría y telecontrol vía Intenent. Telegestión energética.	Cortafuegos. Telecontrol. Acceso único a Internet. Radio Internet.

Tabla 4.2.1-1. Ejemplos de pasarelas comerciales.

4.2.1.1 OSGi.

La Open Services Gateway Initiative (OSGi) Alliance es un grupo de trabajo que fue fundado por quince compañías multinacionales en Marzo de 1999 y cuyo principal impulsor es Sun Microsystems. Actualmente cuenta con unos ochenta socios [30].
Se trata de una organización sin ánimo de lucro, con el objetivo de definir y promover un estándar abierto que permitir conectar los servicios ofrecidos en redes metropolitanas a redes de locales o domóticas.

La especificación OSGi no define ni el hardware ni el medio físico, sino la arquitectura software mínima necesaria para que todos los servicios se ejecuten sobre la misma plataforma. El núcleo de las especificaciones consiste en una colección de API basados en Java que definen la pasarela de servicios.
La especificación OSGi está orientada como complemento y mejora de cualquier protocolo domótico existente, tales como CEBus, HomeRF, Jini, etc.

Las principales características de la pasarela OSGi son:

- Estandarizada. Proporciona una plataforma común a fabricantes de equipos y a proveedores de servicios.
- Independiente del hardware. Capaz de funcionar sobre distintas soluciones.
- Abierta. No define ninguna arquitectura de red y no obliga el empleo de ningún protocolo o tecnología concreta.
- Segura. La arquitectura software que se define, proporciona una alta seguridad e integridad para que se puedan ofrecer múltiples servicios sobre la misma plataforma sin interferencias entre ellos.
- Fiable. Es capaza de operar 24 horas al día, evitando las caídas del sistema.
- Escalable. Flexible ante la introducción de nuevos servicios.

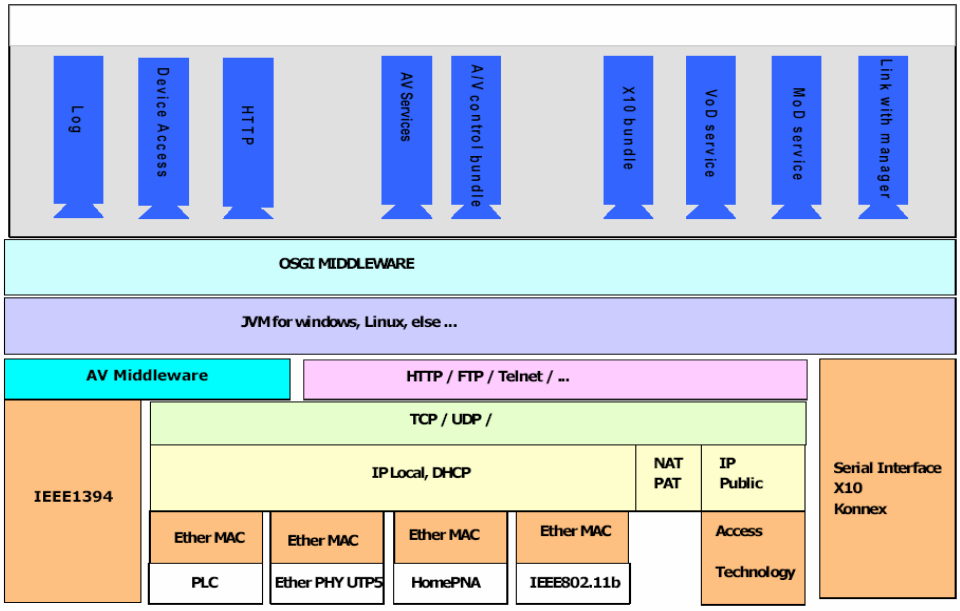


Ilustración 4.2.1-1. Pila de protocolos de la pasarela.

El componente fundamental de la especificación OSGi es el Framework, que proporciona un entorno estandarizado a las aplicaciones. Este elemento central se divide en cuatro capas:

- L0: Entorno de ejecución. Especificación del entorno Java. Las configuraciones Java 2 y los perfiles como J2EE, CDC, CLDC o MDP son todos válidos como entornos de ejecución.
- L1: Módulos. Esta capa define las políticas de clases. Añade clases privadas para un módulo, además de controlar el enlace entre módulos.
- L2: Gestión del ciclo de vida. Gestiona aplicaciones que pueden ser instaladas, iniciadas, detenidas, actualizadas y desinstaladas de forma dinámica. Las aplicaciones dependen de la capa de módulos para el cargado de clases pero en esta capa se añade una API para gestionar los módulos en tiempo de ejecución.
- L3: Registro de servicio. Proporciona un modelo de cooperación para aplicaciones dinámicas. Esta capa permite compartir objetos entre aplicaciones.

Adicionalmente, hay un sistema de seguridad que está profundamente entrelazado con todas las capas. Esta seguridad se basa en el modelo de seguridad de Java y de Java 2.

El Framework de OSGi proporciona tres tipos de servicios:

- Servicio de administración de permisos. Mediante este servicio se pueden manipular los permisos de las actuales y futuras aplicaciones del sistema.
- Servicio de administración de paquetes. Las aplicaciones comparten paquetes con clases y recursos. Este servicio proporciona información sobre los paquetes que se están compartiendo en el sistema y actualiza la compartición de los mismos.
- Servicio de niveles de arranque. Un nivel de arranque es el conjunto de aplicaciones que deben ser arrancadas juntas e inicializadas antes de que las otras comiencen. Este servicio se encarga de establecer el actual nivel de arranque.

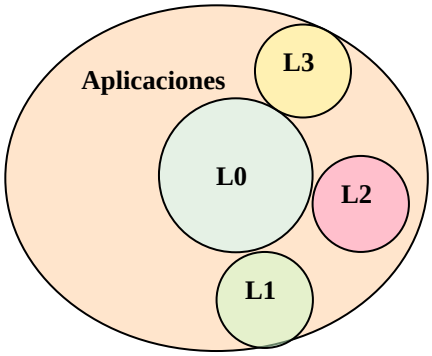


Ilustración 4.2.1-2. Framework de OSGi.

Encima del Framework, la alianza OSGi ha definido diversos servicios. Los servicios están especificados mediante una interfaz Java. Las aplicaciones pueden implementar esta interfaz y registrar el servicio.

4.2.2. Sistemas de control centralizado.

El sistema de control centralizado, también llamado centralita, es el equipo encargado de recoger la información procedente de los diversos sensores distribuidos por el edificio, procesarla y generar las decisiones que ejecutarán los actuadores e interruptores.
La comunicación entre los sistemas de control centralizados y los sensores y actuadores se lleva a cabo mediante los protocolos de control domóticos vistos en el apartado 2 (X-10, LonWorks, Konnex, etc.).

Los componentes que constituyen la unidad de control son [3]:

- Hardware de entrada. Conecta la unidad central con los sensores. Las entradas pueden ser digitales o analógicas
- Hardware de salida. Conecta la unidad de control con los actuadores. Al igual que las entradas, las salidas pueden ser analógicas o digitales.
- Hardware de proceso de datos. Determina como actuar en función de los datos recibidos. Existen distintos tipos de procesadores:

    - Centrales microprocesadoras. Sencillas de instalar pero poco flexible a cambios.
    - Autómatas programables. Poca capacidad computacional.
    - Ordenadores.
    - Controladores embebidos. Elevada inversión en el diseño.

- Hardware de relación con el usuario. El sistema también proporciona una o varias interfaces para que el usuario pueda obtener información del estado de los equipos o intervenir en el proceso de control. Para la configuración local de la centralita se puede emplear una pantalla y un teclado de pequeñas dimensiones que el sistema suele llevar incorporados. Esta interfaz es muy básica, en el ámbito de comandos de texto, y por esto, para una programación más compleja, se incorporan puertos de tipo USB, Ethernet, Bluetooth o WLAN, que permiten la conexión a la centralita de dispositivos como el PC, que dotándolo de un software gráfico específico proporciona el control de la instalación.

Las antiguas instalaciones empleaban diversos sistemas de control para la gestión de los distintos campos de aplicación (iluminación, seguridad, climatización, etc.), sin embargo, la tendencia actual va encaminada a la integración de todas las funciones en un único dispositivo. La unión de estos sistemas de control y la pasarela de servicios parece lógica, pero los fabricantes de estos dispositivos todavía no la ha llevado a cabo. Además, las pasarelas suelen soportar una serie limitada de sistemas de control y cuando la capacidad de las mismas aumente, no sería extraño que éstas sustituyera por completo a todos los sistemas de control del edificio.

4.3. Interfaces con el usuario.

Cualquier sistema automatizado instalado en un edificio necesita una interfaz que permite al usuario actuar sobre el sistema. Además en algunos casos, el sistema necesitará comunicarse con el usuario para notificarle algún problema o aviso.
En el siguiente cuadro se muestran algunas de las interfaces que se pueden encontrar en edificios y viviendas para que la instalación y el cliente interactuen [1]:

Interfaces tradicionales	Interfaces actuales
• Pulsadores e interruptores. • Teclados especiales del sistema. • Llaveros y mandos a distancias. • Software para PC. • Mensajes y sonidos desde central o sirenas. • Teléfono. • Pantallas en la pared.	• Interfaces Web PC. • Web Pads y Tablet PC. • Pocket PC o PDA. • Navegadores y software para PC y PDA. • Televisión. • Teléfono móvil (WAP, SMS, MMS, e-mail).

Tabla 4.3-1. Interfaces con el usuario.

Gracias al avance de las tecnologías y la bajada de precios en dispositivos como PCs, teléfonos móviles o PDAs, estos equipos se están imponiendo a los sistemas tradicionales como mandos a distancia o el teléfono fijo. Además, estos dispositivos permiten realizar operaciones más complejas y el acceso a la instalación desde el exterior vía Internet proporcionando mayor facilidad de uso para el usuario. Por supuesto, la interfaz que se elija para interactuar con el sistema dependerá de la complejidad del mismo y de la inversión que se esté dispuesto a realizar.

Evidentemente estas interfaces se pueden combinar para ofrecer un servicio más eficiente al usuario. Así, por ejemplo, cuando el usuario quiera modificar algún parámetro de la instalación empleará la interfaz Web mediante un PC o una PDA, pero si se produce una alarma, el sistema podría enviar un mensaje SMS al móvil del usuario.

4.3.1. Comunicación mediante PC, Web Pad y PDA.

El ordenador personal es el elemento típico para monitorizar y controlar el sistema domótico instalado en el edificio. En él está cargado un software que permite la programación y la visualización del sistema completo. Se podrán tener disponibles los planos de la edificación con la distribución de los elementos de control sobre ellos y así, sobre cada elemento se podrá obtener y modificar su valor o estado en un momento determinado.
Además, cualquier evento que se produzca en el sistema podrá quedar registrado con fecha y hora, teniendo la posibilidad de almacenarlo en una base de datos o imprimirlo para realizar estudios estadísticos posteriores.

El PC se conectará directamente al sistema central o pasarela a través de puertos tipo USB o Ethernet o empleando tecnologías inalámbricas. Por otra parte se tendrá acceso remoto mediante Internet desde cualquier PC del mundo conectado a la red. Para ello el equipo central deberá tener integrado un servidor Web, que proporcione el acceso a toda la configuración del sistema domótico mediante sencillos menús gráficos.

En cuanto al mercado de ordenadores personales, la oferta actual es tan amplia y personalizada que resulta imposible realizar una comparación válida. Destacar que prácticamente aquello que se necesita se encuentra en un sector que se actualiza cada día con nuevos y mejores dispositivos.

La Web Pad es básicamente una pantalla a color de alta resolución sensible al tacto, que permite comandar el sistema y acceder a Internet al igual que un ordenador personal. Gracias a su escaso peso y tamaño su transporte es fácil y cómodo y por tanto, la utilización desde cualquier punto del edificio es posible. Para ello, estas pantallas suelen disponer de algún tipo de interfaz inalámbrica como Wi-Fi o Bluetooth.

Una agenda personal o PDA es un dispositivo que se asemeja a un ordenador portátil de pequeño tamaño.
En comparación con los teléfonos móviles, presentan mayor capacidad y funcionalidades y desde algunas se permiten realizar llamadas. Además, suelen disponer de pantallas táctiles de mayor tamaño. Todo esto les proporciona más potencia y facilidad que un teléfono móvil para trabajar con herramientas ofimáticas y navegar por Internet, si bien, su precio es más elevado que el del terminal móvil.
Desde una PDA se puede interactuar con la pasarela de servicios mediante tecnologías inalámbricas como puede ser Wi-Fi o Bluetooth, o bien vía Web gracias a que incorporan el protocolo WAP, permitiendo el control del sistema desde el exterior del edificio [1].

En la siguiente tabla se muestran algunos ejemplos de PDA que se pueden encontrar actualmente en el mercado. Existe gran cantidad de modelos y fabricantes y esto se traduce en una disminución de los precios y la posibilidad de encontrar el dispositivo que más se adapte a las necesidades del consumidor.

Nombre PDA	S100	iPAQh6340	Treo 600	Pocket LooX720	PocketPC n50 Premium
Fabricante	Qtek	HP	PalmOne	Fujitsu-Siemens	Acer
Dimensiones (cm)	5,8x10,8x1,8	7,5x2,1x13,8	11,2x6x2,2	12,2x7,2x1,52	11,9x7,1x1,53
Peso (gr.)	150	190	168	170	155
Memoria RAM (Mb.)	64	64	32	128	128
Procesador	Intel Bulverde a 4,16 MHz	Texas Instruments OMAP1510 a 168 MHz	Texas Instruments OMAP a 144 MHz	Intel xScale PX272 a 520 MHz	Intel xScale PXA272 a 520 MHz
Sistema operativo	Windows Mobile 2003 Second Edition	Windows Moblie Phone Edition 2003	Palm OS v5.2.1	Windows Mobile 2003 Second Edition	Windows Mobile 2003 Second Edition
Puertos	USB IrDA Bluetooth	USB IrDA Bluetooth WiFi	USB IrDA	WiFi USB IrDA Bluetooth	Bluetooth USB WiFi IrDA
Pantalla	TFT 240x320 de 2,8”	TFT 240x320 de 3,5”	DSTN 160x160	TFT 480x640 de 3,62”	TFT 240x320 de 3,5”
Características	Teléfono móvil GPRS tribanda integrado. Ranura SDIO.	Teléfono móvil GPRS cuatribanda integrado. Batería extraíble de gran capacidad. Ranura SDIO.	Teléfono móvil integrado. Fácil de usar. Ranura SDIO.	Ranuras CF y SDIO. Cámara digital integrada.	Ranuras CF y SDIO. Disponible SDRAM de 30 Mb.
Precio aprox.	569 €	659 €	635 €	529 €	389 €

Tabla 4.3.2-1. Agendas personales comerciales.

4.3.2. Comunicación mediante móvil.

Los sistemas de control domóticos no son ajenos al boom de las comunicaciones móviles y cada vez más incorporan conexión con la red celular GSM. Para ello, es necesario insertar una tarjeta SIM dentro de la central.
Mediante el uso del móvil cuando se produce algún tipo de problema o alerta en el edificio, el equipo central enviará un mensaje corto SMS al usuario para ser informado de la incidencia. Si la instalación dispone de comunicación con videocámaras, se podrían enviar mensajes con imágenes o sonidos mediante MMS.

Desde el móvil el usuario también puede acceder remotamente al sistema, permitiéndole realizar modificaciones o acciones. Este acceso se podrá realizar mediante llamada al número que contiene la tarjeta SIM de la central, de igual manera que sucede con el teléfono conectado a la RTC. Generalmente cuando se realiza una llamada al equipo central, el usuario deberá autentificarse para poder acceder al sistema y lanzará los comandos a través del teclado del

teléfono. El sistema interpretará las peticiones del usuario y las traducirá en las órdenes para los dispositivos correspondientes.
Otra opción para entrar en el sistema a través del terminal móvil es mediante el protocolo WAP (Wireless Applications Protocol). Empleando este protocolo se puede acceder vía Internet al servidor Web que debe tener integrado el sistema de control o la pasarela. Mediante un menú gráfico el usuario podrá, de manera sencilla y cómoda, monitorizar el sistema para comprobar lo que está sucediendo y realizar cambios.

Por último, destacar que la introducción de la tercera generación (UMTS) en el mercado va a permitir incorporar al móvil todo tipo de servicios, como la transmisión de imágenes en movimiento y el acceso a Internet a gran velocidad [1].

4.4. Dispositivos para la seguridad.

4.4.1. Gestión de la seguridad básica.

4.4.1.1 Dispositivos contra intrusos.

Los detectores de intrusión se clasifican en dos grandes grupos: volumétricos para la detección de presencia o movimiento y perimetrales para la detección de rotura o forcejeo de puertas de acceso o ventanas.

La vigilancia volumétrica permite señalizar la presencia de individuos en el interior del recinto o en una determinada estancia del mismo, activando la alarma cuando detecta el movimiento de las personas. Los detectores volumétricos deben colocarse en una esquina de la estancia, asegurando una orientación que logré la máxima cobertura. A la hora de seleccionar un detector se debe tener en cuenta los siguientes aspectos:

- Ángulo de detección: existen detectores que van desde los 110º a los 360º.
- Distancia máxima de detección: desde los 5 a los 50 metros.

Los sensores de presencia se agrupan en tres grandes grupos [2]:

A) Infrarrojos. Son los más usados y existen dos variantes: activos y pasivos, aunque en el mercado se pueden encontrar también detectores infrarrojos combinados con tecnología microondas o con ultrasonido. El de tipo activo, se basa en la creación, mediante infrarrojos, de una barrera invisible que al ser rota activa la alarma. Está formado por un emisor de infrarrojos, un receptor (fototransistor), un convertidor de señal y un amplificador. Los pulsos de luz recibidos son convertidos a señales eléctricas, que se analizan para determinar si se corresponden con una transmisión de luz. Existen distintas formas de detección, y las características del objeto a ser detectado determinarán el método de detección que se adapta mejor.
   En los de tipo pasivo, se programa el aparato para que detecte variaciones de temperatura con respecto a una de referencia, normalmente la temperatura ambiente; como la temperatura corporal suele ser mayor, la presencia de personas activa el dispositivo (pasiva). Entre sus limitaciones destacan la mala sensibilidad del dispositivo cuando el objeto se acerca directamente al sensor y su reducción en el rango de alcance cuando se dan temperaturas altas.

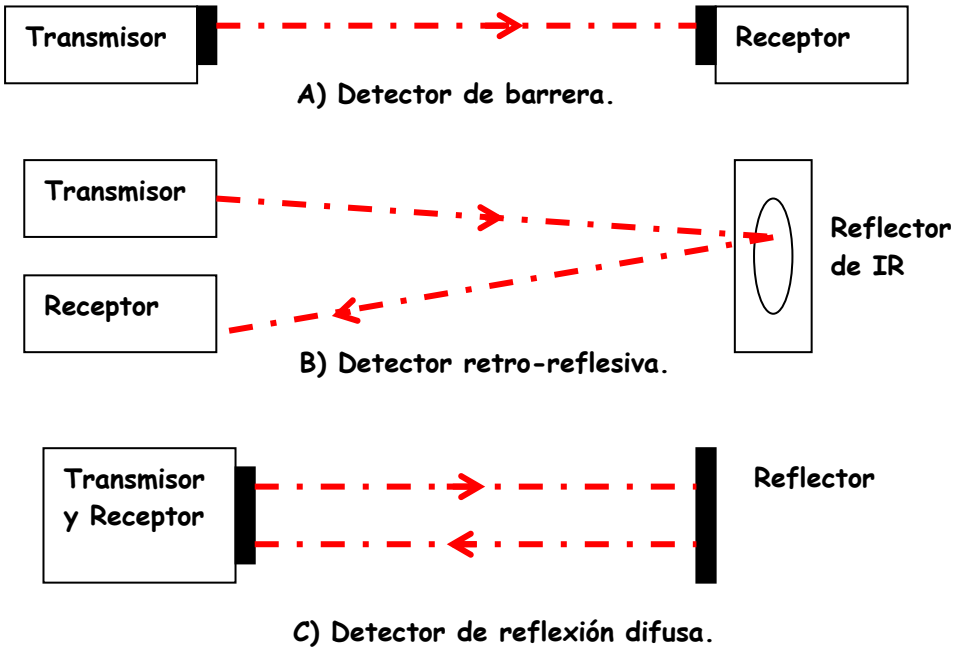


Figura 4.4.1-1. Métodos básicos de detección [2].

B) Ultrasonidos. Emiten ondas de utrasonido y se basan en el efecto Doppler, que provoca que varíe la frecuencia de la onda al rebotar en el objeto en movimiento. El receptor detecta los sonidos procedentes de las reflexiones en el área vigilada, que estarán en fase si no hay ningún objeto en movimiento. Su alcance es de muy pocos metros (0.25 a 13 metros). Son susceptibles al ruido acústico y al viento pero su acción es muy rápida.

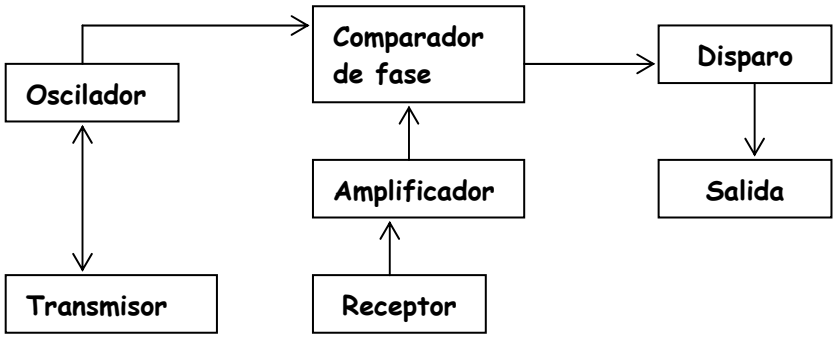


Figura 4.4.1-2. Sensor de ultrasonidos [2].

C) Microondas. Estos sensores emiten ondas electromagnéticas. Trabajan en la banda de los 10 GHz y poseen gran sensibilidad al ser capaces de detectar movimientos muy pequeños en distancias de 50 metros.

Las actuales cámaras IP o de red suelen incorporar detectores de presencia y por tanto, si se tiene una instalación con este tipo de cámaras no sería necesario incorporar este tipo de dispositivos, en las zonas donde estén situadas las mismas.

Detectores de presencia	SRX-1000	C-7300 STE
Fabricante	Crow Electronic	Napco Security Group
Método de detección	Infrarrojo Microondas	Infrarrojo Radar
Cobertura	18m, 105º	18.3m, 85º
Temperatura de trabajo	De -20º a 60º	De -10º a 50º
Protección RFI	30 V/m 10-10000 MHz	30 V/m 10-1000 MHz
Protección EMI	50000V	50000V
Protección luz	30000 lux	30000 lux
Características	Sensibilidad regulable por potenciómetro. Velocidad de detección de 0.3-1.5 m/s.	Microprocesador con 3 memorias EPROM. Sistema SSP para el análisis de la información recibida.

Tabla 4.4.1-1. Detectores de presencia comerciales.

Para la detección de roturas de cristales o forcejeo de puertas y ventanas por parte de intrusos, se emplean dos tipos de sensores [2]:

A) Sensores de contacto. También denominados electromecánicos, son los primeros detectores que se utilizaron y se caracterizan por ser simples, robustos y económicos. Su funcionamiento se basa en la apertura o el cierre de un circuito cuando se actúa sobre el sensor al abrir una puerta o una ventana. Estos sensores suelen constar de dos partes, una fija que se colocará en el marco de la puerta o la ventana y la otra, móvil, que se instalará en el lado contrario a las bisagras en la puerta o la ventana para lograr detección con mínima apertura.
B) Sensores de vibración. Se trata de sensores piezoeléctricos, capaces de detectar las vibraciones del objeto al que están adheridos y transformarlas en variaciones de tensión eléctrica.

4.4.1.2 Control de acceso.

A la hora de controlar la entrada y salida de individuos del recinto existen diversas técnicas que proporcionarán distintos grados de control.
Uno de los sistemas más empleados se basa en tarjetas magnéticas. En este tipo de instalación los usuarios del edificio deben pasar o introducir sus tarjetas de identificación en los lectores situados en las puertas donde se quiere controlar el acceso. Otro método similar es el de lectores de proximidad, en ellos, el usuario sólo debe acercar su tarjeta al lector para poder acceder al lugar deseado. Estos sistemas presentan el problema de la pérdida o robo de la tarjeta, que podría permitir el acceso a personas no autorizadas.
Si se desea un grado mayor de seguridad, se puede optar por sistemas dotados con teclados numéricos que permitan introducir una clave de usuario. En este caso el usuario deberá teclear la contraseña cuando desee acceder al recinto. Problemas que presenta: la memorización y olvido de una clave por parte del usuario y el craqueo de claves.
Si se requiere de un método más sofisticado que proporcione un mayor nivel de seguridad se pueden incluir lectores biométricos de huella digital. En este caso las huellas digitales del personal autorizado están registradas y cuando uno de ellos desea acceder a una zona de la instalación tendrá que poner el dedo encima del lector, que comprobará que el usuario está autorizado a pasar.

Producto	Lector de tarjetas	Lector de proximidad	Teclado	Lector biométrico
Fabricante	RCI Rutherford Controls	Kerisystems	RCI Rutherford Controls	Bioscrypt
Modelo	9310	Serie MS	9212i	V-Station
Características	Verificación de hasta 1000 usuarios. Uso en interiores y exteriores. Memoria EEPROM.	Tres rangos de lecturas: 10, 15 y 35 cm. Tamaño compacto.	Verificación de hasta 120 usuarios. Uso en interiores. Memoria EEPROM.	Verificación de hasta 3000 huellas. Instalación sencilla Plug&Play. Comunicación: RS323, RS485 y Ethernet. Opción de integrar un lector de proximidad.

Tabla 4.4.1-2. Dispositivos comerciales para el control de acceso.

4.4.1.3 Cámaras de vigilancia.

Un elemento tradicional y eficiente para la protección de cualquier edificio es la cámara de seguridad. En este campo se pueden distinguir dos tipos [1]:

A) Cámaras en circuito cerrado de televisión (CCTV). Es el sistema típico de vigilancia, requiere de personal para su observación y permite grabar lo que sucede en la zona para la identificación de posibles intrusos. Estas cámaras se situarán estratégicamente tanto en el exterior como en las zonas interiores y se podrá controlar remotamente para modificar el ángulo de visión. Las imágenes de vídeo procedentes de las distintas cámaras se mostraran en uno o varios monitores de televisión al personal encargado y podrán ser grabadas para un posible análisis posterior.

B) Cámaras IP [5]. Se conocen también como cámaras Web o de red y están diseñadas para enviar las señales de vídeo a través de Internet o a través de un concentrador en una red de área local. Este tipo de cámaras permite la visualización de imágenes tanto desde cualquier navegador de Internet en PC como desde una PDA o un teléfono con el software adecuado. Además, podría ser capaz de enviara un e-mail o un mensaje corto si detecta presencia. Una cámara IP está constituida de los elementos típicos de una cámara de vídeo tradicional, un sistema de compresión de imagen y un sistema de procesamiento que se encargará de la gestión de las imágenes, del envío al módem, de la detección de movimiento, etc.

Las ventajas que aporta una cámara IP frente al sistema tradicional CCTV son:

- Posibilidad de acceder desde cualquier sitio del mundo. Para visualizar las imágenes de un CCTV es necesario estar en el lugar donde se encuentra el sistema.
- Más económico. Instalar un sistema de cámaras IP resulta sencillo ya que es como montar una red local, mientras que las instalaciones de un CCTV resultan caras y complicadas.
- Escalabilidad. Resulta más sencillo añadir nuevas cámaras IP al sistema que en CCTV.

Por otro lado, es posible conectar a la cámara IP sensores convencionales o relés que permitan la actuación de dispositivos de forma remota. Generalmente estas cámaras llevan un mecanismo de detección de movimiento incorporado y no sería necesario dotar al sistema de detectores de movimientos externos.
El principal problema de las cámaras IP es el relacionado con el tema de la seguridad. Al existir conexión a Internet existe la posibilidad de que individuos no autorizados puedan acceder a la configuración de las cámaras de manera más fácil que cuando se tiene un sistema de televisión cerrado. Como medida de seguridad, las cámaras IP disponen de un software interno que permite establecer varios niveles de acceso (administrador y usuario), a los que se tiene entrada mediante un nombre y una contraseña.

Para visualizar las cámaras IP desde un PC lo único que será necesario es tener instalado un navegador web, mediante el cual se tendrá acceso a la dirección propia de la cámara y se mostrará al usuario imágenes de lo que está sucediendo en tiempo real. Además, existe en el mercado software específico que permitirá una visualización simultánea de varias cámaras, control y administración de las mismas y la reproducción de vídeos grabados mediante una grabación programada o como consecuencia de alarmas.

Si se dispone ya de un sistema CCTV se pueden disponer de imágenes del mismo a través de Internet gracias al denominado servidor de vídeo IP. Este servidor se compone de conversores analógico-digital, de sistema de compresión y de un sistema de procesamiento que se conecta por un lado al sistema CCTV y por otro al router que da la conexión a Internet.

En la siguiente tabla se muestra un pequeño ejemplo de cámaras IP que se pueden encontrar en el mercado actual y sus características principales:

Cámaras IP	Axis205	Axis206W	Panasonic WV-NP472	DD-7303
Compresión de imagen	Motion JPEG	Motion JPEG JPEG	JPEG	MPEG4
Accesos	RJ-45: Ethernet 10Base-T/ 100Base-TX	WiFi 802.11b USB	Ethernet10/100Base-T BNC	WiFi 802.11b RJ45
Resolución	640x480 320x240 160x120	640x480 320x240 160x120	640x480	160x120 320x240
Velocidad (imágenes/sg)	25	25	25	25-30
Interior/ Exterior	Interior	Interior	Interior	Interiores
B/N- Color	B/N Color	B/N Color	B/N Color	Color
Características	Sincronización horaria con un servidor NTP. Admite hasta 20 usuarios simultáneos. Capacidad de imprimir y guardar instantáneas.	UPnP. Admite 10 usuarios simultáneos. Capacidad de imprimir y guardar instantáneas.	Detección digital de movimiento. Función de alarma para dispositivos de seguridad externos y activación.	Transmisión de vídeo y audio mediante UDP. Observación y grabación desde PC de 4 cámaras simultáneas en tiempo real.

Tabla 4.4.1-3. Cámaras IP comerciales.

4.4.2. Gestión de alarmas técnicas.

4.4.2.1 Dispositivos contra incendios.

Los sistemas para la detección de incendios que generalmente se emplean en los edificios son [2]:

- Detectores de humo. Sensibles a partículas visibles o invisibles de los productos de combustión.
- Detectores térmicos. Sensibles a las temperaturas anormalmente altas o a la velocidad de aumento de la temperatura.
- Detectores de llamas. Sensibles a las radiaciones infrarrojas, ultravioletas o visibles producidas por el fuego.

A la hora de seleccionar un determinado tipo de detector de humo hay que tener en cuenta distintos factores como pueden ser la altura y volumen de la estancia, los materiales y aparatos contenidos en la misma, la posible generación de falsas alarmas (por ejemplo en una cocina), etc.
La colocación de estos detectores va a depender del tipo de detector empleado y las características del recinto. Se deben seguir una serie de recomendaciones que vendrán impuestas por el fabricante y por las normas referentes a las instalaciones de detección automática de incendios (Norma Básica de la Edificación, Proyecto de Norma UNE 23008/1, Regla técnica de CEPREVEN y Norma Tecnológica de la Edificación).
Existen diversos tipos de los detectores de humos, aunque los más empleados son de dos tipos:

A) Detectores fotoeléctricos u ópticos: el humo visible penetra en el aparato afectando al haz de rayos luminosos que genera una fuente de luz, de forma que varía la luz recibida en una célula fotoeléctrica, y se activa una alarma al llegar a cierto umbral. Existen dos tipos:

   - De haz de rayos proyectados. El humo oscurece el haz proyectado por el emisor, disminuyendo la luz que recibe la célula del receptor situado a cierta distancia. El emisor y el receptor se sitúan en los extremos de la zona a proteger, dando protección a un área máxima de 1400 m^2. Suele emplearse en estancias muy grandes con techos elevados.
   - De haz de rayos reflejados. En este caso el emisor de luz y el receptor están contenidos en un mismo dispositivo. Está formado por una fuente de luz, una célula fotoeléctrica que se tiene que situar en ángulo recto con la fuente y un captador de luz frente a la fuente de luz. Cuando entra humo, parte del haz de luz se refracta y otra se refleja con las partículas de humo. El aumento de intensidad de luz en la célula activa una señal que se transmite al panel de control.
     Se suelen utilizar para la detección de fuegos latentes y fuegos de combustión lenta. Combinándolos con detectores térmicos, se sitúan en salas de ordenadores y salas con material electrónico en condiciones ambientales sin polvo. También sirve para detectar fuegos en los conductos de aire acondicionado.

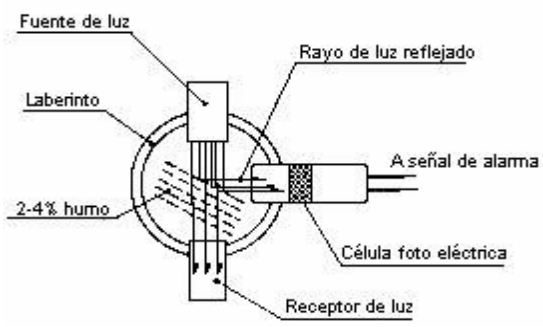


Ilustración 4.4.2-1: Detector óptico de haz de rayos reflejados.

B) Detectores iónicos: al penetrar los productos de combustión de un incendio se produce una disminución en el flujo de corriente eléctrica formada por moléculas de O_2 y N_2 ionizadas por una fuente radiactiva entre dos electrodos y se activa una señal de alarma. Según la fuente radiactiva se dividen en detectores iónicos de partículas alfa y de partículas beta, aunque en España solo se comercializan los primeros. Al incluir una fuente radiactiva estos detectores deben cumplir la Orden del Ministerio de Industria de 20 de Marzo de 1975 sobre Normas de Homologación de Aparatos Radiactivos.
Se emplea tanto para fuegos latentes como para la detección de fuegos abiertos de llama viva.

Dentro del conjunto de detectores térmicos se destacan aquellos que se comercializan en el mercado:

A) Detectores por el principio de temperatura fija. Se basan en que existe un elemento que se rompe, se funde o se deforma a una temperatura prefijada. Cuando sucede esto, se transmite una orden al circuito de alarma. Para que se produzca la alarma el detector debe calentarse hasta la temperatura en la cuál opera, normalmente 60º C. Debido a esto, puede ocurrir que cuando el dispositivo alcance el valor necesario para que la alarma se active, la temperatura del aire que rodea al detector sea más elevada, alcanzando valores mortales para los humanos y equipos.
B) Detectores por el principio de elevación brusca de temperatura. Estos detectores se basan en el hecho que en un incendio, la temperatura ambiente por unidad de tiempo es superior a un valor prefijado (normalmente 7.4 ºC/minuto), provocando que se transmita una orden de alarma. Con este tipo de detectores pueden suceder falsas alarmas debido a incrementos inofensivos de la temperatura como puede ser el caso de nubes intermitentes de vapor procedentes de equipos o pequeños escapes en canalización de vapor, ráfagas de calor procedentes de una zona más caliente o la incidencia de rayos solares durante un pequeño instante durante un día nublado. Por otra parte, con incrementos de temperatura inferiores al valor de referencia, un fuego puede progresar y ocasionar la destrucción completa sin que el sistema lo detecte.
C) Detectores mediante el principio de reacción compensada. Estos detectores tienen la propiedad de actuar siempre que la temperatura del ambiente que rodea al detector alcance la temperatura de referencia independientemente de las condiciones de elevación brusca.

Los detectores de incendios pueden aparecer combinados, distinguiéndose varios tipos:

A) Polisensor inteligente de fuego, humo y CO. Se integra en un único dispositivo un sensor óptico (para el humo), uno térmico para el calor y otro para la detección de monóxido de carbono. El sistema evalúa periódicamente las condiciones del ambiente y cuando éstas cumplen con el patrón de fuego almacenado en el detector, se dispara la alarma.

B) Polisensor inteligente de fuego y humo. Contiene un sensor de ionización que responde mejor a las llamas de rápida iniciación, un sensor fotoeléctrico que responde bien a los fuegos lentos humeantes un sensor de calor que actúa como detector de reserva. La información recogida por los sensores es comparada con la información que posee almacenada y si coinciden se produce la alarma.

La siguiente tabla muestra algunas características de dispositivos que existen en el mercado y que permiten la detección de incendios:

Tipo dispositivo	Detector de incendio IR	Detector de incendio térmico	Detector de incendio iónico	Detector de incendio fotoeléctrico	Detector de calor
Fabricante	System Sensor	Securiton	System Sensor	Notifier	System Sensor
Rango de temperatura de operación	De –30º a 55º	De -20º a 70º	De 0º a 50º	De 0º a 40º	De 0º a 50º
Tensión nominal de operación	24 V DC	24 V DC	12/24 V DC (según modelo)	24 V DC	12/24 V DC (según modelo)
Indicador de alarma	LED rojo	LED rojo	LED on	LED rojo	LED rojo
Características	Ideal para techos altos y temperaturas extremas. Puede operar en modos de corto o largo alcance.	Constante monitoreo de la temperatura. Identificación individual. Respuesta ajustable según hora y evento.	Gran estabilidad y mínimas falsas alarmas.	Combina detección fotoeléctrica y térmica. Auto-ajuste de sensibilidad. Direccionable.	Respuesta adecuada a incrementos lentos y rápidos de temperatura.

Tabla 4.4.2-1. Detectores de incendios comerciales.

Cuando se detecta un posible incendio los detectores envían una señal de alarma. Esta señal permite al sistema de control identificar la localización del siniestro y llevar a cabo una serie de operaciones como puede ser activar una sirena o cortar el suministro de corriente eléctrica. Además, se podrán poner en marcha rociadores de agua pulverizada o de gas argón o halón. Estos últimos se emplean cuando los equipos que contiene el recinto poseen un valor elevado y no se pueden mojar, como es el caso de centros de proceso de datos, archivos históricos o museos. Sin embargo, estos gases no permiten respirar por lo que es necesaria la completa evacuación del recinto antes de proceder a su utilización.

4.4.2.2 Dispositivos contra fugas de gas.

Para prevenir posibles intoxicaciones de los individuos o reducir las posibilidades de una explosión por escape de gases, se distribuyen por las zonas de riesgo los detectores de gases. Estas zonas serán garajes, cocinas o cuarto de calderas.
Hoy en día, los detectores de gas no están sujetos a ningún tipo de norma nacional o europea y por tanto, a la hora de instalar y mantener un detector de este tipo será conveniente seguir las instrucciones del fabricante.

Las pautas a seguir para la colocación de estos detectores son [2]:

- Distancia no superior a 1,5 metros de la caldera de gas o gasodoméstico más empleado.

- Lejos de elementos que puedan interferir en la detección como pueden ser ventanas, conductos de ventilación, extractores, etc.
- Lejos de temperaturas extremas (menores de –10º y mayores de 40º).
- Sin obstáculos entre el detector y el aparato a controlar.

Dentro del grupo de detectores de gas destacan los sensores de monóxido de carbono (CO). El monóxido de carbono es un gas muy venenoso ya que se une a la hemoglobina de la sangre, formando COHb (carboxihemoglobina) que impide el transporte de oxígeno a los tejidos.
Para determinar la presencia de este gas en una habitación se puede emplear tres tipos de sensores [3]:

A) Semiconductor. Se utiliza el dióxido de estaño (SnO_2), semiconductor que cambia su resistencia de forma no lineal cuando es expuesto a un ambiente de CO.
B) Electroquímico. Este tipo de sensor detecta los gases midiendo la electricidad generada por una reacción química de oxidación o reducción en un medio electrolítico.
C) Biomimético o colorimétrico. Estos dispositivos aprovechan las propiedades químicas de un contaminante que produce coloración al entrar en contacto con un agente químico contenido en un tubo detector. Son aparatos de baja exactitud y precisión.

Cuando se detecta una fuga, conviene cerrar el suministro de gas. Para ello se emplean las electroválvulas, que son válvulas cuya apertura se controlas mediante una señal eléctrica. Consta de dos piezas, el cuerpo, que se ajusta a la tubería, y el cabezal, que se encarga de mover el dispositivo de apertura o cierre.

4.4.2.3 Dispositivos contra fugas de agua.

Una fuga de agua se puede detectar mediante una sonda de humedad colocada en las zonas de riesgo, como pueden ser los cuartos de baño [1]. El sistema avisa al inicio de la inundación evitando que los daños ocasionados sean demasiado importantes.
Básicamente, un sensor de inundación consiste en uno o varios electrodos y un relé eléctrico o electrónico que es excitado dando una alarma cuando el agua moja a dichos electrodos.
El sensor se debe situar en contacto directo con el suelo y en zonas donde no puedan producirse falsas alarmas. Se buscará una ubicación que permita una correcta detección, sin molestar a las actividades habituales del usuario y con facilidad para las operaciones de secado y mantenimiento.
Hay que tener en cuenta las prescripciones descritas en el Reglamento Electrotécnico para Baja Tensión cuando se instala una sonda de agua en un cuarto de baño.

Ante la detección de una fuga de agua, se procederá al corte automático del suministro, mediante el uso de electroválvulas. Estas electroválvulas se sitúan tras la llave de paso principal y deben ser capaces de soportar la presión habitual de la red.

4.5. Iluminación y climatización.

4.5.1. Iluminación.

La función del sistema de iluminación es controlar la activación/desactivación y el nivel de intensidad de las luces de una estancia en función de la luz exterior y la presencia o no de personas. Dependerá de factores como la hora del día o la época del año y además, se deberán tener en cuenta la existencia de toldos y persianas, que también se controlarán automáticamente.

La iluminación tradicional de una determinada zona se realiza de dos formas distintas [2]:

- Iluminación todo/nada con pulsadores en modo biestable. En este caso se trata de gobernar una lámpara o grupo de lámparas mediante un pulsador o grupo de pulsadores que trabajaran en modo biestable. Es el sistema típico y no actúa de forma inteligente.
- Iluminación regulada con pulsador/es. Este caso tampoco se trata de forma automatizada al sistema, ya que se regula manualmente el nivel de luz de las lámparas mediante pulsadores reguladores de la intensidad.

Estos dos métodos se mejoran con la incorporación de sensores de iluminación y detectores de presencia que permitirán la regulación de luz de forma automática. El sistema gobernará las lámparas o puntos de luz mediante un regulador de iluminación incorporado, que tendrá en cuenta los valores de los sensores.
Los sensores de iluminación captan la intensidad de la luz (en lúmenes) y se dispondrán tanto en el interior como en el exterior del recinto.
Estos sensores varían de resistencia según la luz incidente. Estos dispositivos pueden tener el coeficiente de resistencia negativo o positivo. Ejemplo típico de sensor de luz es la célula fotoeléctrica de sulfuro de cadmio.
Una célula fotoeléctrica detecta la luz directa y la indirecta en un ángulo llamado ángulo de incidencia, que es el que forma el rayo de luz incidente con la recta horizontal que parte de la superficie de la célula.

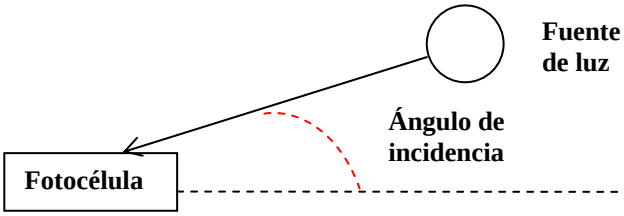


Figura 4.5.1-1. Ángulo de incidencia [2].

Cuando aumenta el ángulo de incidencia, la luz directa detectada por la célula disminuye. Como la fuente de luz más importante en una habitación proviene del techo, el ángulo de incidencia aumenta si la célula se dispone próxima al suelo. Al contrario, si se monta alejada del suelo, el ángulo de incidencia disminuye. Por otra parte, la luz indirecta procede de distintas direcciones y el ángulo de incidencia tiene menor importancia.
Además, la luz directa recibida por la célula disminuye si hay obstáculos tales como personas o muebles. El espacio donde existen estos objetos que crean sombras se denomina zona de interferencia directa (DIZ: Direct Interference Zone). También existe una zona de sensibilidad indirecta (ISZ: Indirect Sensitivity Zone), que es el espacio en la habitación en el que los objetos pueden afectar a la cantidad de luz indirecta. Al aumentar el ángulo de incidencia, el tamaño de la DIZ y de la ISZ aumenta.
Con esto, los criterios para situar idealmente este tipo de dispositivos son:

- Montaje próximo al techo y a la fuente de luz, para que la luz directa supere la indirecta y para que el espacio ocupado por personas y objetos influyan lo menos posible (DIZ e ISZ pequeños).
- Punto de montaje equidistante de todas las fuentes de luz.
- No se recomiendan otras fuentes de luz intermitentes tales como focos de noche próximos a los sensores.

Los lugares a evitar, ya que pueden dar lugar a una disminución en el 50% de la luz detectada, son:

- Puntos a menos de 1 metro sobre el suelo y a menos de 1-2 metros de esquinas.
- Puntos donde hay obstrucciones entre la fuente de luz y las células. Estos obstáculos no tienen que ser permanentes, como por ejemplo, una puerta abierta o cerrada.
- Puntos demasiado próximos a una fuente de luz.
- Puntos próximos a fuentes de luz no controladas.

Los detectores de presencia, también llamados detectores de movimiento o interruptores de proximidad son iguales a los que se emplean para detectar intruso, pero además se utilizan para conectar o desconectar la iluminación de cualquier espacio en función de la existencia o no de personas en el mismo. Con esto se logra que el control de encendido y apagado se realice automáticamente, sin que ninguna persona tenga que accionarlo, de manera que solamente permanecerá encendido un interruptor cuando realmente se requiere que la estancia esté iluminada, logrando a su vez un ahorro energético que puede a llegar a ser de un 20%.
De todas formas hay que valorar de qué superficie se trata para saber si es conveniente tener estos interruptores de movimiento. Por ejemplo, en una sala o habitación de un hogar no interesa su instalación como tampoco en locales muy pequeños donde el bajo consumo de iluminación no justifica la colocación de un detector. Sin embargo, en la escalera de un bloque de viviendas, en estancias y aseos de grandes edificios de oficinas o en los exteriores de jardines sí que resulta interesante, ya que además del ahorro en energía, se reducen los cotes de la contratación de personal para la supervisión del estado de los interruptores.
A la hora de adquirir un modelo de detección de presencia hay que tener en cuenta algunas variables:

- Ángulo de detección.
- Distancia de detección.
- Retardo de desconexión. Es el tiempo entre la salida de la persona y la desconexión de la iluminación.
- Poder de ruptura. Es la carga máxima que el detector es capaz de conectar y desconectar por sí mismo. Si sólo se desea hacer una instalación puntual, no surgen problemas, pero en los casos en los que la instalación es más compleja y se supera el poder de ruptura, el detector debe ir asociado a un dispositivo auxiliar, llamado contactor, que se encarga de efectuar la conexión y desconexión de los circuitos de alimentación.

Para el encendido y apagado de un grupo de luces y la regulación de la luminosidad de las mismas se utiliza un actuador denominado “dimmer”. El control del brillo se basa en ajustar la tensión de alimentación, empleándose tiristores y tricacs como elementos de regulación [2].

4.5.2. Climatización.

El sistema de regulación de la temperatura gobierna el control de temperatura de todas las áreas del recinto, buscando el confort térmico programado y adaptándose en cada caso a las condiciones de ahorro energético. Controla los radiadores y aparatos de aire acondicionado en consonancia con la temperatura interior, exterior y ciertos márgenes debidos a la capa de aislante que se considere que tiene la vivienda (pérdidas de calor). Un sistema de estas características podrá tener asociados uno o varios radiadores o equipos de aire acondicionado y las entradas que tendrá este sistema serán las lecturas de los sensores.
Los elementos que se deben considerar son [1]:

- Termostato de ambiente, destinado a medir la temperatura de la estancia y permitir la modificación de parámetros de consigna por parte del usuario de forma manual.
- Sensor de temperatura interior, destinado a medir únicamente la temperatura de la estancia.

- Sensor de temperatura exterior, destinado a optimizar el funcionamiento de la calefacción a través de una óptima regulación de su carga y/o funcionamiento.
- Sondas de temperatura para gestión de calefacción, necesarias para controlar de forma correcta distintos tipos de calefacción eléctrica (por ejemplo, sondas limitadoras para suelo radiante).

A la hora de situar un termostato o una sonda de temperatura se deben seguir una serie de indicaciones para obtener una lectura adecuada. Estas recomendaciones son [1]:

- Situar el aparato de medida en la pared opuesta a la fuente de calor o frío.
- Evitar que las corrientes de aire y el sol incidan directamente sobre el dispositivo. Las sondas de temperatura exterior deberán por tanto, colocarse en la zona norte del recinto.
- Alejar el medidor de elementos que irradien calor.

4.5.2.1 Sensor de temperatura.

Existen diversas formas de medir la temperatura, las que se suelen usar en las sondas de temperaturas comerciales son [2]:

Detectores de temperatura resistivos (RTD).

Su principio de funcionamiento se basa en que la resistencia eléctrica de metales puros aumenta cuando lo hace la temperatura.
El material que se emplea necesita ser resistente a la corrosión y a ambientes hostiles, presentar un comportamiento lineal, ser estable y proporcionar alta sensibilidad. Los metales que se ajustan a estos requisitos son el cobre, el níquel y principalmente el platino.
Por su elevado rango de temperatura (-200º/500º) se emplea en los edificios para medir la temperatura que permite controlar el consumo de agua caliente y la temperatura de los gases que permiten optimizar la combustión de la caldera.

Termistores.

Se trata de resistores variables con la temperatura, basados en semiconductores. Presenta una dependencia no lineal con la temperatura, por esto, se linealiza en torno al punto de trabajo y su rango de funcionamiento es menor que en el caso anterior. Se emplean para medir la temperatura ambiente.
En estas resistencias, además de las características típicas en resistencias lineales fijas como valor nominal, potencia nominal, tolerancia, etc., hay que destacar:

- Resistencia nominal: en estos componentes este parámetro se define para una temperatura ambiente de 25ºC.
- Autocalentamiento: este fenómeno produce cambios en el valor de la resistencia al pasar una corriente eléctrica a través de él. Hay que tener en cuenta que se puede producir también por una variación en la temperatura ambiente.
- Factor de disipación térmica: es la potencia necesaria para elevar su temperatura en 1ºC.

Dentro de los termistores se pueden destacar dos grupos:

- Resistencias NTC: Esta resistencia se caracteriza por su disminución del valor resistivo a medida que aumenta la temperatura, por tanto presenta un coeficiente de temperatura negativo. Entre sus características se pueden destacar: resistencia nominal de 10 ohmios a 2M, potencias entre 1 microvatio y 35W, coeficiente de

temperatura de -1 a -10% por ºC; y entre sus aplicaciones: regulación, compensación y medidas de temperaturas, estabilización de tensión, alarmas, etc.

- Resistencias PTC: Poseen un coeficiente de temperatura positivo, de forma que su resistencia aumentará como consecuencia del aumento de la temperatura.

Termopares.

Se tratan de sensores activos que se basan en el efecto Seebeck (circula corriente cuando dos hilos de metales distintos se unen y se calienta uno de los extremos). Se mide el voltaje que es proporcional a la diferencia de temperaturas.
Son bastantes lineales y aguantan altas temperaturas aunque se ven afectados por la corrosión.

4.6. Empresas.

Actualmente existen multitud de empresas que se dedican en mayor o menor medida, algunas de forma exclusiva, a la fabricación y venta de productos relacionados con la automatización de edificios.
A continuación, se muestra una breve relación de las compañías más relevantes del sector tanto en el ámbito nacional como internacional.

Empresas españolas
Accede Soluciones
AIKE tecnologies de l'hàbitat S.L.
AKO Electronica
Bioingeniería Aragonesa S.L.
BJC
Cebek
Delta Dore Electrónica S.A.
Dinitel
ISDE Ingeniería Domótica
Logical Design S.A.

Empresas Internacionales
ABB Industrial Systems
Allen-Bradley
AMX Corporate
Andover Controls
Creston
Fermax
Home Director
Honeywell
Schneider Electric
Siemens

Empresas centradas en X-10
ACT/PCC
Home Systems
Home Vision X-10
IntellaVoice&IntellaTest
Leviston
SmartLinc
Wadsworth Electronics
X-10 USA

Empresas centradas en CEBus
Creative Control Concepts
Intellon
ITRAN Communications Ltd.
Smart Corporation

Empresas centradas en LonWorks
Cypress Semiconductor
EBV Elektronik
Echelon
Elva S.A.
K-Lon Control S.A.
Motorola
Toshiba

Empresas centradas en seguridad
CyberTec
Kerisystems
Napco Security Group
Sistemas Integrados de Control Sicon S.L.
System Sensor

Empresas centradas en iluminación
OSRAM
Philips

Empresas centradas en climatización
Airzone S.L.
Carrier
Ciatesa
Danfoss S.A.
Johnson Controls
Schako
Sedical S.A.
Trox
Vemair S.L.

5. CONCLUSIONES Y LÍNEAS DE AVANCE

5.1. Conclusiones.

Tras la realización de este proyecto, se pueden enumerar las siguientes conclusiones:

- Para que un edificio se considere inteligente es característica esencial la integración de todos los dispositivos que constituyen el sistema para lograr una constate comunicación y colaboración entre ellos y así, obtener la información necesaria del medio que les rodea y actuar de forma conjunta para conseguir los objetivos marcados.

- Los propósitos que persigue la instalación de un sistema domótico son la búsqueda del confort, la seguridad del usuario y un ahorro sustancial de la energía. En definitiva, busca mejorar la calidad de vida dentro del hogar y las condiciones de trabajo en donde desarrollar el mismo.

- Aunque sus comienzos datan de los años setenta no es un área tecnológica muy extendida dentro de la sociedad, sobre todo porque siempre se han considerado a estos sistemas productos de lujo. Destacar por un lado, que la mayoría de los edificios no destinados a la vivienda cuenta con algún tipo de sistema inmótico, y por otro, que la bajada de los precios de estos sistemas está animando a los ciudadanos de a pie a instalarlos en sus hogares.

- Existe gran apoyo por parte de empresas, asociaciones y organismos para que se introduzcan elementos que automatizan un edificio, sobre todo en el ámbito de la vivienda en el que estos sistemas no están todavía muy generalizados.

- Existen gran número de estándares, protocolos de comunicación y sistemas destinados específicamente a la automatización de un edificio, aunque la tendencia de asociaciones y organismos de normalización es la integración del sector para aunar esfuerzos y ofrecer así a los usuarios, sistemas fiables, eficientes y que se adapten a sus necesidades.

- La elección a la hora de instalar un sistema inmótico va a depender de diversos factores como puede ser la inversión que se desea realizar, el grado de seguridad que se exige o la complejidad del sistema que se quiere implantar. Por otra parte, hay que destacar que una de las características más valorada es la flexibilidad del sistema ante la introducción de nuevos elementos dentro del sistema y su adaptación ante avances tecnológicos.

- La variedad de dispositivos domóticos que se pueden encontrar en el mercado, cubre la mayoría de las necesidades de los usuarios. Gracias a que cada vez son más las empresas que se dedican a la fabricación y distribución, estos elementos son más económicos y de mejores prestaciones.

- La aparición de la pasarela de servicios supone la unión con el exterior y la posibilidad del usuario de actuar sobre el sistema desde cualquier lugar del mundo.

- A medida que los avances tecnológicos se van desarrollando, los dispositivos que se emplean en un sistema domótico son más fiables, capaces de realizar más funciones y con un coste más razonable.

5.2. Líneas de avance.

Dentro de las líneas de avances que se pueden desarrollar, se destacan:

- Realizar una instalación sobre plano. Escoger un sistema domótico de los vistos en el apartado 3 y realizar una instalación completa sobre el plano de una vivienda o local. Incluiría los dispositivos a emplear, sus posiciones, sus funciones dentro de la red y el presupuesto global de la instalación. Esta instalación podría emplear las herramientas de diseño que aparecen en el cdrom de [2].

- Profundizar en los protocolos domóticos más recientes y que todavía no están del todo implantados, como es el caso de ZigBee y Obix. Estudiar sus posibilidades, las empresas y organismos implicados así como su modelo de funcionamiento.

- Estudiar los dispositivos y protocolos existentes para la red de entretenimiento que puede establecer en una vivienda domótica.

Desde de un punto de vista más técnico, resultaría interesante realizar una aplicación que permitiera el control de dispositivos sobre Jini o UPnP.

6. BIBLIOGRAFÍA

[1] José M. Huidrobro Moya, Ramón J. Millán Tejedor. *"Domótica. Edificios Inteligentes"*. Creaciones Copyright S.L. 2004.

[2] Antonio Creus Solé. *"Domótica para instaladores"*. Cano Pina S.L.- Ediciones Ceysa. 2005.

[3] Cristóbal Romero Morales, Francisco Vázquez Serrano, Carlos de Castro Lozano. *"Domótica e Inmótica. Viviendas y Edificios Inteligentes"*. Ra-Ma. 2005.

[4] Ana Isabel Molina Díaz. Proyecto Fin de Carrera *"Sistema de diseño de entornos virtuales de edificios domotizados con Java 3D"*. Universidad de Castilla La Mancha, 2002.

[5] Francisco Javier Alcázar Rodríguez. Proyecto Fin de Carrera *"Diseño e instalación de sistema wireless de televigilancia y domótica en un entorno agroquímico"*. Universidad de Sevilla, 2004.

[6] Rafael Coomonte Belmonte. *"Jornada sobre hogar digital"*. Foro UPM Universidad-Empresa de encuentro, oportunidades y alternativas tecnológicas, 2005.

[7] Antonio Fernández-Paniagua Díaz-Flores. *"ICT: La llave a la sociedad de la información"*. Foro MINT, 2005.

[8] Ricardo Ferrer Durá, Jorge Fernando Juan, Rafael Riera López. *"Clasificación y proyecto del edificio inteligente"*. Servicio de publicaciones de Universidad Politécnica de Valencia, 1995.

[9] José Mª Quintero González, Javier Lamas Graziani, Juan D. Sandoval González. *"Domótica: sistemas de control para viviendas y edificios"*. Paraninfo Madrid 2003.

[10] EIA-600: *"Cebus Standard"*. 1996.

[11] EIA-709.1: *"Control Networking Protocol Specification"*.

[12] EN-50090: *"Home and Building Electronic Systems"*.

[13] IEEE 802.15.4: *"Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks"*.

[14] IEEE 802.11: *"Wireless Technology for Local Area Network"*.

[15] IEEE 802.3: *"LAN/WAN CSMA/CD Access Method"*.

[16] IEEE 1394: *"Standard for a High Performance Serial Bus"*.

[17] ISO 16484-5: *"Building Automation and control system"*.

[18] ISO/IEC 10192: *"Home Electronic System"*.

[19] BatiBUS Club International: http://www.batibus.com

[20] Bluetooth SIG: http://www.bluetooth.org

[21] Continental Automated Building Association: http://www.caba.org

[22] http://www.domotica.net

[23] Echelon Corp.: http://www.echelon.com

[24] EIB Association: http://www.eiba.org

[25] ETSI: http://www.etsi.org

[26] Home Plug Powerline Alliance: http://www.homeplug.org

[27] Home PNA: http://www.homepna.org

[28] Home RF Working Group: http://www.homerf.org

[29] Jini Community: http://www.jini.org

[30] Modbus: http://www.modbus.org

[31] OSGi Alliance: http://www.osgi.org

[32] UPnP Forum: http://www.upnp.org

[33] USB: http://www.usb.org

[34] Zigbee Alliance: http://www.zigbee.org

7. RECURSOS WEB CONSULTADOS

7.1. Organismos.

- 1394 Trade Association. http://www.1394ta.org
- AENOR. http://www.aenor.es
- Bacnet Association. http://www.bacnetassociation.org
- CENELEC. http://www.cenelec.org
- Cebus Industry Council. http://www.cebus.org
- CEDOM. http://www.cedom.org
- EHSA. http://www.ehsa.com
- EIA. http://www.eia.org
- IEEE. http://www.ieee.org
- ISO. http://www.iso.org
- ITU. http://www.itu.org
- Konnex Association. http://www.konnex.org
- LonMark Interoperability Association. http://www.lonmark.org
- Ministerio de Ciencia y Tecnología. http://www.mcyt.es
- Ministerio de Trabajo y Asuntos Sociales. http://www.mtas.es
- WECA. http://www.wirelessethernet.com
- Wifi Alliance. http://www.wifi.org

7.2. Fabricantes y distribuidores de dispositivos.

- ABB. http://www.abb.com
- Acer. http://www.acer.com
- Ako Electrónica. http://www.ako.com
- Andover Controls. http://www.andovercontrols.org
- Amper. http://www.amper.es
- Axis Communications. http://www.axis.com
- BJC. http://www.bjc-dialogo.es
- Coactive Network. http://www.coactive.com
- Crow Electronics. http://www.crowelec.com
- Delta Dore. http://www.deltadore.es
- Ericsson. http://www.ericsson.es
- Freescale. http://www.freescale.com
- Home Systems. http://www.homesystems.com
- Homeywell. http://www.honeywell.com
- HP. http://www.hp.com
- Kamstrup. http://www.kamstrup.com
- Kerisystems. http://www.kerisys.com
- LG Electronics. http://www.lge.es
- Napco. http://www.napcosecurity.com
- Notifier. http://www.notifier.es
- PalmOne. http://www.palm.com
- Panasonic. http://www.panasonic.com

- Qtek. http://www.qtek.com
- RCI Rutherford Controls. http://www.rutherfordcontrols.com
- Samsung Electronics. http://www.samsung.es
- Scneider Electric España S.A. http://www.scneiderelectric.es
- Siemens S.A. http://www.siemens.es
- System Sensor. http://www.systemsensor.com
- Sony http://sony.net
- Temper S.A. http://www.temper.es

7.3. Webs de domóticas.

- http://www.aldeadomotica.com
- http://www.automatedbuildings.com
- http://www.casaactiva.com
- http://www.casadomo.com
- http://www.domodesk.com
- http://www.domointel.com
- http://www.domoticaviva.com
- http://www.hogardigital.com
- http://www.hometoys.com
- http://www.lacasadelfuturo.com
- http://www.smarthome.com

7.4. Otras webs.

- http://www.antoniucci.com
- http://www.auna.es
- http://www.automatas.org
- http://www.buildings.com
- http://www.eledificiointeligente.8m.com
- http://www.energuia.com
- http://www.javahispano.com
- http://www.la-fortaleza.com
- http://www.monografías.com
- http://www.revista.unam.mx
- http://www.telefonica.es
- http://www.urbe.edu