ESTUDIO COMPARATIVO DEL INTERNET DE LAS COSAS FRENTE A LOS PROTOCOLOS TRADICIONALES DE LA DOMÓTICA Y PROPUESTA DE UN PROTOCOLO UNIFICADO

CÉSAR ANDRÉS GAVIRIA CUEVAS
JHONATAN LEONARDO ORDOÑEZ OLIVEROS
JULIÁN FELIPE RAMOS FUENTES

TUTOR: Ing. CARLOS ENRIQUE MONTENEGRO

ESPECIALIZACION REDES DE DATOS
UNIVERSIDAD SANTO TOMAS
BOGOTA
2014

Las ideas expuestas en este libro son responsabilidad de los autores.

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del director / Tutor del trabajo de grado

_____
Firma del jurado 1 del trabajo de grado

Bogotá, Septiembre de 2014

CONTENIDO

1. RESUMEN 10
2. INTRODUCCIÓN 11
3. PLANTEAMIENTO DEL PROBLEMA 14
3.1 Pregunta problema 14
3.2 Planteamiento del problema 14
4. JUSTIFICACIÓN 17
5. OBJETIVOS 19
5.1. Objetivo General 19
5.2. Objetivos Específicos 19
6. METODOLOGIA 20
7. MARCO TEÓRICO 21
CAPITULO I 36
8. PROTOCOLOS PROPIOS DE LA DOMÓTICA Y EL INTERNET DE LAS COSAS 36
8.1 PROTOCOLO X-10 36
8.1.1 FUNCIONAMIENTO 37
8.1.2 ESTRUCTURA DEL MENSAJE 39
8.2 PROTOCOLO KNX 41
8.2.1 EIB.TP 41
8.2.2 EIB.PL 41
8.2.3 EIB.net 41
8.2.4 EIB.RF 42
8.2.5 FORMAS DE CONFIGURAR LOS DISPOSITIVOS EN KNX: 43
8.2.6 Topología del par trenzado uno (TP1) 44
8.2.7 Estructura de bus KNX 44
8.2.8 COMUNICACIÓN 47
8.2.9 VENTAJAS DEL KNX FRENTE A OTROS SISTEMAS 52
8.3 PROTOCOLO LONWORKS 52
8.3.1. FUNCIONAMIENTO 53
8.3.2. ELEMENTOS FUNDAMENTALES 54
8.3.3. MEDIO DE TRANSMISIÓN 57
8.4 PROTOCOLO ZIGBEE (IEEE 802.15.4) 57
8.4.1 Nodos y topología de red 58
8.4.2 Características generales de 802.15.4 60
8.4.3 Tipos de tráfico 60
8.4.4 La pila de arquitectura ZigBee 61
8.4.5 Capa Física 62
8.4.6 Capa MAC de 802.15.4 65

8.4.7 Capa de Red ZigBee 69
8.4.8 Capa de Aplicación 73
8.4.9 Seguridad 75
8.5 SISTEMAS RFID, COMO BASE DEL IoT 76
8.5.1 FRECUENCIAS DE FUNCIONAMIENTO RFID. 76
8.5.2 LOS TAGS DE RFID 79
8.5.3 Tipos de etiquetas 80
8.5.4 EL PROBLEMA DE INTERFERENCIAS EN RFID 81
8.5.5 Mecanismos centralizados de RFID 82
8.5.6 Mecanismos distribuidos 83
8.6 EPCGlobal 84
8.6.1 EPCGlobal Network 85
8.6.2 Código de Producto (EPC). 86
8.6.3 Middleware EPC 87
8.6.4 EPC Information Server (EPCIS) 88
8.6.5 Object Name Service – ONS 88
8.6.6 Requisitos técnicos del Protocolo EPC 92
8.6.7 Parámetros de protocolo EPC 93
8.6.8 La gestión de las etiquetas o Tags. 102
CAPITULO II 104
9. FACTORES CLAVE QUE IMPULSAN EL USO DEL PROTOCOLO IP EN LOS DISPOSITIVOS PRESENTES EN EL HOGAR BASADOS EN IOT. 104
CAPITULO III 108
10. CARACTERÍSTICAS DE DISPOSITIVOS DEPENDIENDO DE LOS PROTOCOLOS EN QUE SE BASAN SUS DISEÑOS. 108
10.1 X10 108
10.1.1 Dispositivos 108
10.1.2 Software 109
10.2 KNX 110
10.2.1 Dispositivos 110
10.2.2 Software 119
10.3 LONWORKS 121
10.3.1 Dispositivos 121
10.3.2 Software 123
10.4 ZigBee 124
10.4.1 Dispositivos 124
10.4.2 Software 129
10.5 DISPOSITIVOS IOT 130
10.5.1 Fabricantes de integrados 130

10.5.2 Fabricantes de tags 131
10.5.3 Fabricantes de equipos 132
CAPITULO IV 134
11. IMPACTO DEL INTERNET DE LAS COSAS EN EL DESARROLLO ACTUAL DE LA DOMÓTICA Y LOS BENEFICIOS O DESVENTAJAS. 134
11. 1 DEFINICION TECNICA PARA LA IMPLEMENTACION DE IOT. 134
11.2 INFLUENCIA DEL IoT EN LA DOMOTICA. 136
CAPITULO V 140
12. CARACTERÍSTICAS MÁS ÓPTIMAS PARA UN PROTOCOLO EFICIENTE, BASADO EN LA INTEGRACIÓN DE LOS PROTOCOLOS ANALIZADOS, PERMITIENDO LA INTEROPERABILIDAD DE DISTINTOS DISPOSITIVOS DEL HOGAR INTELIGENTE. 140
12.1 Escalabilidad 142
12.2 Medio de comunicación (alámbrico, inalámbrico) 143
12.3 Tipo de Sistema 143
12.4 Seguridad 144
12.5 Distancia y velocidad 144
12.6 Tipo de comunicación 145
12.7 Procesamiento de información 145
12.8 Interfaz de usuario 145
12.9 Costo y facilidad de uso 146
12.10 Control y direccionamiento 146
12.11 Identificación y detección 147
13. CONCLUSIONES 148
14. BIBLIOGRAFIA 151
15. GLOSARIO 155

LISTA DE FIGURAS

Figura 1. Voltajes y Frecuencias por País 36
Figura 2. Sincronización por cruce por Cero de la Señal AC 37
Figura 3. Envió de un “1” lógico 38
Figura 4. Envió de un “0” lógico 38
Figura 5. Envió de 3 pulsos en cada semiciclo 38
Figura 6. Superposición de los 3 pulsos sobre el semiciclo de la señal AC 39
Figura 7. Estructura del mensaje de X-10 11 ciclos 39
Figura 8. Conexión protocolo Ethernet - KNX. 42
Figura 9.Medios de comunicación KNX 43
Figura 10.Topologías KNX. 44
Figura 11.Segmento de línea.. 44
Figura 12.Línea bus KNX. 45
Figura 13.Configuración Área.. 46
Figura 14.Configuración Backbone KNX. 47
Figura 15.Transmisión de un 1 y un 0 lógico en KNX 49
Figura 16.Paquete de datos KNX. 50
Figura 17.Composición Byte dirección emisor.. 50
Figura 18.Dirección con 2 subgrupos y con 3 subgrupos, respectivamente.. 51
Figura 19.EIB Interworking Standard (EIS).. 51
Figura 20. Logotipo LonWorks. 53
Figura 21. Paquete de Datos Lonworks 53
Figura 22. Neuron 5000 Processor Neuron Chip for Lonkworks 54
Figura 23. Componentes Neuron Chip. 55
Figura 24. Transceptor Marca Echelon 55
Figura 25. Arquitectura del nodo 56
Figura 26. Variedad de Medios Físicos para la Transmisión 57
Figura 27.Distancia de transmisión / Potencia 58
Figura 28.Topologías de Red ZigBee. 59
Figura 29.Red ZigBee. 59
Figura 30.Topologías en IEEE 802.15.4 61
Figura 31.Capas modelo 802.15.4 y ZigBee. 62
Figura 32.Asignación de canales. 62
Figura 33. Calculo Frecuencia Central.. 63
Figura 34.Interface de servicio de datos y de manejo entre capas Física y Control de Acceso al medio 64
Figura 35.Interfaces de la capa MAC. 65
Figura 36.Nodo oculto 67
Figura 37.Topologías ZigBee (Árbol, Estrella, Malla) 71
Figura 38. Representación Acoplamiento inductivo 78
Figura 39.Representación Acoplamiento capacitivo 78
Figura 40.TAG de RFID 79

Figura 41.Operación General EPCglobal 86
Figura 42.Código EPC 87
Figura 43.Componentes Middleware EPC. 87
Figura 44.Esquema de Funcionamiento ONS 88
Figura 45.Modelo ONS basado en DNS 91
Figura 46.Interrogator-to-Tag modulation 95
Figura 47.Datos Codificacion por intervalos de impulso 96
Figura 48.Envolvente de RF Interrogador a Tag 97
Figura 49.Parámetros Envolvente RF 97
Figura 50.Envolvente de RF 98
Figura 51.Envolvente de RF con FHSSS 98
Figura 52.Ejemplo Dense-Interrogator TDM 100
Figura 53.Ejemplo FDM Retro dispersión por Límite de Canal 101
Figura 54.FDM por retrodispersión de canal adyacente 101
Figura 55.Operación y estado del Tag en un proceso de Interrogacion/Tag 102
Figura 56.Ejemplo de un Inventario y acceso de un Tag 103
Figura 57.Modelo objeto dentro de IoT 105
Figura 58.Pioneros en Tecnologias asociadas al IoT 106
Figura 59. Tiempo de adopción del IoT en la industria 107
Figura 60. Tipos de dispositivos X-10 108
Figura 61. Modulo Bidireccional TWO-WAY (TW523) 109
Figura 62. Módulo de transceptor inalámbrico (Modelo RR501) 109
Figura 63. Interface ActiveHome 110
Figura 64.Acoplador KNX. 111
Figura 65.Cable Bus EIB 112
Figura 66.Fuente de alimentación KNX. 112
Figura 67.Conectores bus para bus KNX 113
Figura 68.Terminal de protección contra sobretensiones. 113
Figura 69.Actuadores binarios 114
Figura 70.Acopladores de línea/área. 114
Figura 71.Interface USB 115
Figura 72.KNX IP ROUTER 115
Figura 73.Interface RS232. 115
Figura 74.Pulsador KNX. 116
Figura 75.Termostato KNX 116
Figura 76.Módulos de entradas KNX.. 116
Figura 77.Detectores de movimiento y presencia KNX.. 117
Figura 78.Sensores meteorológicos y de ambiente KNX. 117
Figura 79.Sensores de alarmas técnicas KNX. 118
Figura 80.Interruptores horarios KNX.. 118
Figura 81.Interfaces de sistemas de climatización KNX.. 118
Figura 82.Terminal táctil 119

Figura 83.Servidores WEB Schneider Electric para KNX 119
Figura 84 .Puesta en marcha de una instalación KNX mediante ETS 120
Figura 85. Arquitectura de red Lonworks 121
Figura 86. Módulo de control de LonPoint 121
Figura 87. Router Echelon 122
Figura 88. Módulo Repetidor 122
Figura 89. Interfaz LonMaker 123
Figura 90.Dispositivo EasyBee 124
Figura 91.Dispositivo serie Pixie. 125
Figura 92.Pixie Configuration Tool.. 125
Figura 93.Pixie Evaluation Kit.. 126
Figura 94.ETRX1.. 126
Figura 95.ETRX2 127
Figura 96.ETRX1DVK. 128
Figura 97.ETRX1USB. 128
Figura 98.ETRX1CF y PDA. 129
Figura 99.Internet Of Everything 136
Figura 100. IoT orientado a la domótica, Capas Modelo funcional 138
Figura 101. Convergencia de servicios en Smart Building 139

LISTA DE TABLAS

Tabla 1. Códigos de Casa (House Code) del sistema x10 40
Tabla 2. Código de Numeración y Función 40
Tabla 3 Fabricantes de Integrados RFID 131
Tabla 4. Fabricantes de Tag 132
Tabla 5. Fabricantes de Lectores RFID 133
Tabla 6. Comparación de protocolos, Características 1. (Autores) 140
Tabla 7. Comparación de protocolos, Características 2. (Autores) 141
Tabla 8. Comparación de protocolos, Características 3. (Autores) 142
Tabla 9. Comparación de protocolos, Características 4. (Autores) 142

1. RESUMEN

En el documento se puede observar, el desarrollo investigativo sobre varios de los protocolos enfocados a la prestación de servicios en la domótica, así como el funcionamiento de cada uno de estos y principales características de los dispositivitos que se emplean para realizar las instalaciones domóticas de acuerdo a su protocolo. Por lo cual se plantea la necesidad de una integración de todos estos con los basados en IP, que puedan interoperar con todos los dispositivos que conforman las viviendas inteligentes en Colombia, permitiendo la comunicación y un total control del sistema domótico independiente del fabricante y por ende de la tecnología que el mismo utilice, en pro de monitorear y controlar el uso de servicios públicos.

Por lo tanto se debe tener en cuenta el avance tecnológico a nivel mundial y la innumerable variedad de productos que ofrece la industria domótica, con el fin de satisfacer el control y bienestar de sus usuarios; Que hace necesario el estudio de sus protocolos y del internet de las cosas, ya que las personas por naturaleza buscan tener una mejor calidad de vida que se vea reflejado en su entorno, buscando una revolución que permita mejorar la eco-sostenibilidad, disminuir la contaminación y el gasto de energía, así como proteger sus recursos económicos y valores patrimoniales.

Siendo el objetivo un estudio comparativo del internet de las cosas y los protocolos enfocados en domótica, mediante el análisis de estas tecnologías, y es así como se obtiene a través de investigaciones sobre domótica, conceptos teóricos y prácticos que buscan presentar un protocolo óptimo para el control y monitoreo de servicios en las viviendas colombianas que beneficien la economía y la eco-sostenibilidad del hogar.

Palabras clave:
KNX, ZIGBEE, LONWORKS, X-10, IOT, RFID, EPCGLOBAL, DOMÓTICA, PROTOCOLO.

2. INTRODUCCIÓN

El fenómeno de la globalización, la necesidad de comunicación inmediata, las redes sociales, el desarrollo de redes e internet, el avance tecnológico, entre otros factores han contribuido a la idea de generar una red que permita la interacción, no solo entre humanos, sino entre maquinas, y estas a su vez interactúen con las personas. Es así como en 2005 la ITU menciona por primera vez el termino Internet de las cosas (IoT por sus siglas en inglés – Internet of Things). El término describe el uso de internet para comunicar en tiempo real el estado de los objetos conectados a la denominada red de redes, y dicho estado pueda ser consultado por cualquier otro objeto en red.

Esta idea del IoT abre las puertas al desarrollo de otro concepto ligado como lo es el "Hogar Conectado", que ha tomado fuerza en los últimos años debido al acelerado desarrollo de las tecnologías informáticas y de comunicaciones. En Junio de 2014 en una en encuesta realizada a 1650 expertos en tecnología propietarios de hogares con temas relativos al Internet de las Cosas, afirman que el hogar conectado es una realidad. El 61%de los encuestados considera que es altamente probable que una casa en la cual los aparatos electrodomésticos y electrónicos, los servicios, las personas y demás están conectados a Internet, pueda convertirse en una realidad en los próximos cinco años.[1] China es el líder en desarrollo de este tipo de tecnologías y por demás ha implementado políticas y proyectos en pro de la consecución de ciudades, servicios y edificios que conecten todos sus objetos con las personas de manera que pueda crear un entorno de red de interacción continua.

Según lo mencionado el hogar conectado es una idea altamente desarrollada, y basa su modelo en el uso de protocolos de internet. Sin embargo esta idea hoy en día se da sin soporte por la carencia de direcciones IP capaces de sustentar miles de millones de objetos conectados, por lo que la implementación del protocolo de IPv6 y su pronta proliferado es una necesidad inminente. Pero hay que tener en cuenta que el hogar conectado no es una idea del IoT, sino más bien otra perspectiva de su idea original que se remonta a la domótica, que pretende dotar de cierto grado de inteligencia algunos elementos del hogar en busca de seguridad, comodidad y confort. Entre la domótica se pueden distinguir otros conceptos propios que van más allá del hogar como la inmotica que no es más que la domótica enfocada en edificios, conocidos como "Edificios inteligentes". Por otro lado está el

[1] Fortinet ® (NASDAQ: FTNT), Diario TI 02/07/14 16:14:24

concepto de agroinmótica, que se refiere a la inteligencia de los elementos usados en la agronomía y trabajos relacionados a campos y cultivos.

La domótica basa su funcionamiento en protocolos que buscan comunicar datos entre distintos dispositivos, permitiendo ya sea que el usuario realice control remoto o que los mismos accionen mecanismos al detectar una alarma previamente programada. La base de la domótica está desarrollada en el protocolo X10, que utiliza la red eléctrica para la transmisión de datos. Este constituyo el primer protocolo estructurado para ser usado en hogares automatizados. Sin embargo no sería el único, tras la aparición de protocolos como KNX, LonWorks, y ZigBee. Por otro lado, en el desarrollo del IoT, han parecido protocolos como el RFID, que se constituye como regulación técnica bandera para la implementación del internet de las cosas. Así mismo el EPC, que nace para cubrir la necesidad de identificación y comunicación de productos en la industria, se perfila como protocolo complementario a la identificación por radiofrecuencia antes mencionada.

Cada uno de estos protocolos mencionados pretende dar la mejor solución para el uso de objetos con cierto grado de inteligencia dentro del hogar. Y como solución propia, no se tiene interoperabilidad de protocolos, por lo cual un objeto de una marca X desarrollado bajo un estándar del protocolo X, no podrá operar en conjunto con un objeto de marca Y que usa especificaciones técnicas del protocolo Y. Esto se convierte en una limitante importante, por lo cual se hace necesario establecer la posibilidad de unificar los protocolos, o la creación de un protocolo único que logre interoperabilidad, de manera que se aprovecha la mejor característica de cada estándar en pro del desarrollo de un mundo conectado.

Esta necesidad de un protocolo unificado es inminente y es de prioritaria solución, por lo que es objeto de debate en los principales encuentros de fabricantes e investigadores del IoT. A las necesidades técnicas se le suman factores sociales y políticos que pretenden regular el uso del espectro, la seguridad de la información y la privacidad de las personas. Esto se evidencia en la participación que tendrá Colombia en el Foro de Gobernanza de Internet en Turquía, el cual incluye la asistencia a un taller sobre Políticas y prácticas que permiten el Internet de las Cosas. El taller ofrecerá una importante interacción debatiendo 6 áreas de interés[2] como la apertura al desarrollo y la innovación promoviendo la competencia. O como la confianza de los dispositivos que recopilan y almacenan los datos de los objetos

[2] MINTIC, Sala de Prensa, 31 de Agosto 2014. http://www.mintic.gov.co/portal/604/w3-article-6983.html

que están en la red, los cuales estarían auditados por los más altos estándares de seguridad y protección de la información personal. Otras áreas de importancia son el acceso a información y la numeración IP teniendo en cuenta el despliegue de IPv6. El uso del espectro, recuero que se creía infinito es tema de preocupación por parte de los gobiernos del mundo, por lo que se ha hecho un espacio para en el mencionado taller. Este punto podría ser definitivo para los estándares que rijan el IoT.

Lo realmente cierto, es que el internet de las cosas nos abre la puerta a un mundo lleno de posibilidades hasta hace poco tiempo inimaginables. La idea del hogar conectado, de los objetos conectados, del mundo conectado está cada vez más cerca, pero dependerá tanto del desarrollo de tecnologías más acordes, la proliferación de IPv6, y la regulación legislativa y de protocolos técnicos universales.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 Pregunta problema

¿Qué metodología es posible estructurar para unificar los protocolos tradicionales en domótica con los basados en IP para obtener una operación óptima y que satisfaga QoS de los dispositivos usados en los hogares inteligentes, en pro de monitorear y controlar el uso de servicios públicos?

3.2 Planteamiento del problema

Aunque no lo parezca, en la actualidad la domótica ha venido creciendo a la par con otro tipo de tecnologías, ya sea tomando lo que iba surgiendo a nivel mundial adaptando las soluciones tecnológicas a las necesidades de los hogares, así como desarrollando protocolos y dispositivos propios con el fin de obtener no solo un lugar que sea confortable para vivir y agradable a la vista gracias a los lujos, sino que mejore la calidad y forma de vida.

Pero, ¿cuál es la razón de que la gente desconozca estos temas y piense que puede ser un tanto futurista, aun en un mundo donde la revolución de las comunicaciones ha cambiado nuestra cotidianidad y nuestra mentalidad? Según Loja Guarango (2013) uno de los grandes problemas que presenta la domótica hoy en día, y que a su vez indirectamente frena su desarrollo, es la falta de conocimiento por parte de las personas y más grave aún por parte de los mismos ingenieros, que ignoran, cómo trabajar en estos campos por la falta de acceso a los diferentes dispositivos, a pesar de existir en el mercado, pero que las empresas fabricantes no se han encargado de dar a conocer mediante la publicidad.

En el ámbito de la ingeniería electrónica se reconocen y usan muchos dispositivos electrónicos, pero no es el caso de aquellos desarrollados para el uso en los hogares, a pesar de usar dispositivos con tecnología de punta como smartphones o computadoras portátiles que comercialmente han abarcado gran parte de los distintos mercados globales, ignorando que estos pueden ser usados en domótica, por lo que Loja Guarango (2013) se plantea que los ingenieros eléctricos son actores muy importantes ya que son los encargados de la planificación, programación, diseño, implementación, distribución y posterior mantenimiento de estos sistemas.

---

[3] Loja Guarango Milton Javier (2013), Estudio y diseño Inmótico para el edificio de biblioteca de la Universidad Politécnica Salesiana sede cuenca, implementando la tecnología Konnex (KNX) para el control de iluminación, control de accesos y control de seguridad técnica. Páginas 314, 315
Ibid

[4] Romero Morales, Cristóbal, Vázquez Serrano, Francisco. Javier De castro Lozano, Carlos. (2011). Domótica e Inmotica. Viviendas y Edificios Inteligentes 3ª Edición. Editorial Alfaomega. Páginas 120, 119, 118, 117

Otros aspectos importantes a mencionar es la falta de software como simuladores, páginas web que permitan dar un vistazo de forma muy general de cómo funcionan los dispositivos y los protocolos usados como X-10 o KNX entre muchos otros, sin mencionar la falta de bases de datos de los dispositivos. Aunque Romero, Vázquez y Lozano (2011), nos muestra una variedad de páginas web y actualmente aplicaciones para iOS y Android donde se puede observar cómo son estos sistemas.

No en todas partes la domótica es un término que pase desapercibido, en países Europeos ya son bastante utilizados y por lo tanto Loja (2013), propone que este hecho debe ser aprovechado y promovido a países de Sudamérica entre los que se encuentra Colombia. Por supuesto, lo anterior implica un progreso tecnológico y que en pocos años su excesivo precio disminuya considerablemente para generar empleo y aumentar la sana competencia entre los pocos que ya están incursionando en estos temas.

Respecto a domótica es importante plantear la integración de varios protocolos de funcionamiento junto a sus mejores características puesto que al no tener un estándar para el implantación de esta tecnología, es importante primero analizar todos los puntos de vista de los usuarios y las necesidades que se deben abarcar, como la comunicación y medios de transmisión, gasto de energía y espacio que se deben tener en cuenta al momento de implementar todo el sistema, de tal manera que garantice el control sobre toda la red domótica y no sea un problema para el usuario. Siendo los actuadores electrónicos una parte importante a analizar puesto que estos deben realizar la tarea a la cual están asignados sin ocupar un gran espacio ni cantidad de energía relevante puesto que se busca es una solución al usuario y no un problema; además es necesario el pensar en la integración no solo de protocolos si no de tecnologías con energías renovables, lo cual podría llegar a presentar un ahorro aún más relevante que el solo sistema domótico, puesto que la energía generada de forma renovable podría abastecer el funcionamiento de la red y a partir de esta el control total de varias o todas las necesidades que pueden cubrirse son la implementación de la domótica.

En cuanto al IoT, son varias las barreras que podrían retrasar su desarrollo tal como lo manifiesta la empresa Cisco[5] las tres barreras de mayor magnitud son la implementación de IPv6, la energía para alimentar los sensores y el acuerdo sobre las normas.

En la implementación de IPv6, se hace referencia a una necesidad inherente, dado que en febrero de 2010 se agotaron las direcciones IPv4 del mundo. Esta migración de direcciones tomará un tiempo de adaptación diferente en cada país, lo que posiblemente impida la operatividad de los dispositivos en todo lugar cuando se visite una red externa a la red local del dispositivo. Si bien no se ha observado un impacto real, esta situación podría lentificar el progreso de IoT, ya que los posibles

[5] Cisco IBSG, 2011. Pag 5

miles de millones de sensores necesitarán direcciones IP exclusivas. Además, IPv6 facilita la administración de las redes gracias a las capacidades de autoconfiguración y sus características de seguridad mejoradas. Esta seguridad, en un futuro sería la cuarta barrera del IoT, dada la necesidad de mantener la privacidad tanto de las personas como de los dispositivos que usan.

El tema de la energía para los sensores limita el máximo potencial de IoT, ya que estos sensores deberán ser autosustentables, debido a que se estima miles de millones de dispositivos funcionando en red, consumiendo potencia y degenerando el ambiente.

Por otra parte de manera similar a los protocolos domóticos tradicionales se necesita una unificación de normas, tanto a nivel de protocolos (modos de transmisión, arquitecturas, velocidades, bandas de operación etc.) como en áreas de seguridad y privacidad. Haciendo énfasis en los protocolos, y teniendo en cuenta el avanzado desarrollo de la tecnología RFID como pionera en el IoT, aún deben ser resueltos varios temas en cuanto a QoS que permita apoyar la prestación de servicios de manera eficaz,[6] haciendo referencia a la elección de la prioridad del servicio, el uso interoperable del lector de RFID, y la definición de una infraestructura de servicios IoT basado en RFID que permita el uso del protocolo IPv6.

Finalmente en cuanto normatividad cabe la necesidad de plantear una legislación que permita mantener la privacidad y la seguridad en una red que se pretende para "Un mundo, donde todo lo que se mueve puede hablar con todo el mundo, en todas partes, todo el tiempo"[7]. Estas leyes deberán regir a nivel mundial y no solo local, por lo que se deberá tener un organismo mundial que rija los asuntos del IoT y la integración con la domótica.

[6] Chunling Sun, Application of RFID Technology for Logistics on Internet of Things, 2012 AASRI Conference on Computational Intelligence and Bioinformatics

[7] Karl Prince, Michael Barrett, Eivor Oborn, Dialogical strategies for orchestrating strategic innovation networks: The case of the Internet of Things, Information and Organization 24 (2014) 106–127.

4. JUSTIFICACIÓN

El avance tecnológico a nivel mundial y la búsqueda de bienestar y control hace necesaria la aplicación del estudio de la domótica y del internet de las cosas, ya que las personas por naturaleza buscan tener una mejor calidad de vida que se vea reflejado en su entorno, buscando una revolución que permita mejorar la eco-sostenibilidad, disminuir la contaminación y el gasto de energía, así como proteger sus recursos económicos y valores patrimoniales. Por ende suele verse a la domótica, como un lujo exclusivo de pocos, y no como una herramienta de confort que agregue valor a la calidad de vida de las personas. Partiendo de esta idea, enfocar el desarrollo de dispositivos y redes de domótica en el monitoreo y control de los servicios públicos hace que de una manera u otra se retribuye la inversión económica del hogar en el hogar mismo. Sin embargo la introducción de estos factores es un proceso que tomará tiempo pues los índices de desarrollo económico en los hogares por localidades en Bogotá, muestran según el Dane, que un total de 13.832 90 (0,7%) de viviendas que no cuentan con necesidades cubiertas adecuadas. Así mismo 4.635 (0.2%) viviendas sin los servicios adecuados. Esto abre la necesidad de adaptar los hogares a mayores comodidades, y satisfacer las necesidades de servicios.

La industria de la domótica ofrece innumerable variedad de productos que pretende satisfacer desde necesidades biológicas básicas, como el control de la temperatura, hasta llegar a controlar la salud de una persona mediante dispositivos especializados. Por esta misma variedad de productos, y la competencia entre las diferentes empresas por posicionar sus marcas en un mercado globalizado, existe la necesidad de un protocolo que interopere con todos los dispositivos que conforman las viviendas inteligentes en Colombia permitiendo la comunicación y un total control del sistema domótico independiente del fabricante y por ende de la tecnología o protocolo que el mismo utilice. Actualmente entre las organizaciones más importantes a nivel mundial que buscan estandarizar el uso de tecnología enfocada en la domótica se encuentran: la IEEE, CENELEC, CEDOM, KNX Association, Modbus Organization que han desarrollado diversos protocolos específicos para promocionar el uso de su tecnología en ciertos países, entre los cuatro (4) protocolos más importantes entre los que se encuentran X10, KNX/EIB, ZigBee y Modbus. Esta guerra por el dominio del sector de la domótica puede afectar su desarrollo inmediato, y hasta el momento no se ha desarrollado un estándar a nivel mundial que generalice y facilite el desarrollo de la domótica.

Por otra parte con este estudio se pretende obtener las bases de investigación para el desarrollo de la domótica como idea de negocio, brindando innovación en la consecución de un servicio interoperable y orientado a estabilizar la economía del hogar, ofreciendo hasta un 30% en la reducción del consumo de energía eléctrica, y entre un 15% y 25% en otros servicios como gas y agua, de manera que nos permita ingresar en un mercado en auge en los últimos años. Teniendo en cuenta que los desarrollos tecnológicos y los mercados apuntan hacia las megatendencias

actuales, como Movilidad, Cloud Computing y Colaboración, es preciso buscar soluciones que integren dichas características. Por esto mismo se ha ideado el estudio sobre la posibilidad de acceder a un aplicativo de control de los dispositivos domóticos desde cualquier parte del mundo con una conexión a internet, el almacenamiento de análisis de los consumos de servicios públicos en bases de datos almacenadas en la nube, y la constante interacción del usuario con los dispositivos de su hogar de manera intuitiva. Igualmente con la propuesta de un protocolo unificado la posible empresa a conformar podrá tener distintos proveedores sin preocuparse por la operación en conjuntos de los productos, aventajando a la competencia en este sentido.

Finalmente basados en las noticias publicadas a raíz de la feria internacional CES (Consumer Electronics Show) 2014, de electrónica de consumo, celebrada en el mes de enero en Las Vegas, auguran que el mercado del hogar conectado va a alcanzar los 10 mil millones de dólares americanos, cifra que aumentará a 44 mil millones en 2017[8]. Es así como el auge y penetración que ha tenido internet a nivel mundial ha dado como resultado el incremento de los dispositivos que se conectan a la denominada red de redes siendo que la proliferación de los smartphones y las tablet PC elevó a 12,5 mil millones en 2010 la cantidad de dispositivos conectados a Internet, en tanto que la población mundial aumentó a 6,8 mil millones, por lo que el número de dispositivos conectados por persona es superior a 1 (1,84 para ser exactos) por primera vez en la historia[9]. Estos factores facilitarán la implementación de tecnología en el hogar y será un gran impulso en cuanto a lo que se espera para domótica en los próximos años.

[8] International Conference Consumer Electronics Show, Vegas 2014
[9] Cisco IBSG, 2010; Oficina de Censos de EE. UU., 2010.

5. OBJETIVOS

5.1. Objetivo General

Realizar un estudio comparativo del internet de las cosas y los protocolos enfocados en domótica, mediante el análisis de estas tecnologías, que permita proponer un protocolo óptimo para el control y monitoreo de servicios en las viviendas colombianas que beneficien la economía y la eco-sostenibilidad del hogar.

5.2. Objetivos Específicos

1. Recopilar la información correspondiente a las aplicaciones y protocolos propios de la domótica, incluyendo el Internet de las Cosas, mediante el estudio de los últimos desarrollos, que facilite la adquisición de conocimientos, y su posterior investigación.

2. Estudiar los factores clave que impulsan el uso del protocolo IP en los dispositivos presentes en el hogar basados en IoT.

3. Analizar las características de dispositivos desarrollados por algunas de las marcas más reconocidas del mercado domótico, su facilidad en la implementación, el uso de energía, del espacio físico, el software que permite su control y los protocolos en que se basan sus diseños.

4. Estudiar el impacto del internet de las cosas en el desarrollo actual de la domótica y los beneficios o desventajas en las viviendas inteligentes.

5. Proponer las características más óptimas para un protocolo eficiente, basado en la integración de los protocolos analizados, permitiendo la interoperabilidad de distintos dispositivos del hogar inteligente.

6. METODOLOGIA

La metodología utilizada en este trabajo es la investigación documental, que se basa en la recolección de información mediante la consulta de artículos y elementos bibliográficos como punto de referencia para la selección de información que permita cumplir con los objetivos establecidos. De esta forma la recopilación de información pertinente para conocer el funcionamiento de los protocolos desarrollados para su uso en domótica, entre lo que se encuentre los aspectos más importantes como estructura y elemento que permiten su implementación, demás información sobre el desarrollo que tiene en la actualidad el internet de las cosas IoT basado en el protocolo IP. Posteriormente se realiza un análisis de la información recopilada como características, beneficios, restricciones de dichos protocolos y del impacto que podría suponer la integración de los mismos con IoT. Por último se propone un protocolo que sea óptimo para suplir con las necesidades que tienen los hogares en la actualidad que sea interoperable y unifique las mejores características que poseen los protocolos más difundidos.

7. MARCO TEÓRICO

Las empresas fabricantes que están incursionando en el mundo de la domótica tienen un buen número de protocolos en los cuales basarse para desarrollar sus dispositivos, con diferentes características que dependiendo el uso que van a tener facilitan su desarrollo e implementación pero con limitantes ya sea que el estándar sea propietario, libre o que el país donde se desenvuelva la empresa se encuentre en una región donde se use o esté más difundido un determinado protocolo.

X-10

Es uno de los protocolos más antiguos ya que sus comienzos fueron en el año 1970 y para la época ya buscaba hacer un uso robusto y eficiente de la estructura del hogar disminuyendo costos de instalación al usar las instalaciones eléctricas como medio de transmisión de las señales de control de los dispositivos de automatización que se conectan a la red. Desde entonces según Botero y Londoño (2003), se ha convertido en la tecnología y medio más difundido pero el menos eficiente. Las razones por las cuales es uno de los protocolos más reconocidos, es gracias a su implementación ya que no es necesario instalar o hacer uso de una nueva red de comunicaciones sino que usando la red eléctrica 220V o 110V existente en todos los hogares se facilita su puesta en marcha.

Entonces porque Botero y Londoño (2003), afirman que no es un protocolo eficiente si tiene puntos positivos como la facilidad y economía en su implementación, las razones son de mucho peso para quien desarrolla este tipo de tecnología domótica. Este es un protocolo propietario es decir no está abierto a terceras partes por lo que hay que pagar para poder desarrollar los dispositivos con dicho protocolo. El protocolo es restringido ya que las operaciones que permite se limitan al tipo encendido/apagado, más la necesidad de utilización de módulos externos que sirvan de intermediario para posibilitar la conexión entre los dispositivos y la red eléctrica.

Romero, Vázquez y Lozano (2011), afirman que X-10 es un protocolo descentralizado, pero no es un sistema propietario, es decir cualquiera puede producir dispositivos para usar con esta tecnología pero está obligado a usar los circuitos del fabricante, es decir que no podría hacer un diseño más abierto.

---

[10] Botero Valentina, Londoño Diana Marcela. (2003). Domótica: Protocolo X10, Página 7

[11] Romero Morales, Cristóbal, Vázquez Serrano, Francisco. Javier De castro Lozano, Carlos. (2011). Domótica e Inmotica. Viviendas y Edificios Inteligentes 3ª Edición. Editorial Alfaomega Páginas 120, 119, 118, 117

Si X-10 ha sido como un primer protocolo que los demás protocolos toman como el punto de partida, esto quiere decir que se toma lo mejor de uno y se mejoran los puntos más débiles. Es el caso de los demás protocolos que fueron surgiendo.

EHS

El EHS (European Home System) es un sistema de red completo, con todas las funciones domóticas, de forma modular, expansible y configurable y distribuido. Cada nodo conectado a la red domótica establece automáticamente su dirección, dándose a conocer y buscando otros dispositivos que pueden estar interesados en en establecer una comunicación con el. Está avalado entre otros estándares por la Comisión Europea.

Romero Vázquez y Lozano (2011), hace énfasis en un aspecto muy importante y es que entre sus características se nota la implementación de estándares creados para comunicaciones pero que no fueron desarrollados específicamente para domótica, es decir que se basan en otros protocolos y en otros avances tecnológicos para su desarrollo que además permite una posterior interoperabilidad entre tecnologías y dispositivos, ya que presenta todos los niveles del modelo OSI, niveles de direccionamiento jerárquico y las unidades se auto configuran al conectarse al bus de datos.

EIB

EIB (European Installation Bus) es un estándar orientado a la gestión técnica de edificios. Según lo expuesto por la investigación de Romero Vázquez y Lozano (2011), es un sistema por bus de datos Europeo al igual que EHS. Es un sistema descentralizado, la programación de los elementos se realiza de forma individual mediante el uso de un ordenador. Claramente diferenciado al protocolo anterior ya que este EIB es mucho más complicado en cuanto a tiempo de implementación y configuración.

Konnex o KNX

Como hemos visto existen una variedad de protocolos europeos, que en los últimos años han optado por combinar lo mejor de estas tecnologías buscando un protocolo más robusto, más fácil de implementar, con más prestaciones y sobretodo que sea interoperable para disminuir la limitante de los distintos fabricantes que diseñan y fabrican sus dispositivos en base a las característica y beneficios que les que les entrega un protocolo y que otro no puede.

Tal intento de convergencia mencionado se dio entre las asociaciones europeas EHSA (European Home Systems Association), EIB (European Installation Bus Association) y BatiBus también conocido como BCI (Batibus Club Internacional) para dar origen a Konnex también conocido como KNX. Tal como nos comenta

Romero Vázquez y Lozano (2011), esta unión busca que Konnex pueda competiren aspectos como calidad, precios y servicios con otros sistemas o protocolos como LonWorks, que aumente la oferta de productos europeos hacía su propio mercado y los internacionales.

Entre los objetivos que deja en claro sobre el porqué crear un único estándar europeo es:

• Concebir un estándar para la domótica que cumpla con las necesidades y especificaciones de sus instalaciones residenciales.
• Además de Implantar nuevos tipos de funcionamiento del tipo Plug-and-Play a muchos de los dispositivos característicos de una red domótica.

LonWorks

Ya que hemos hablado del mercado europeo también debemos hablar de otros de los mercados más fuertes a nivel mundial, por supuesto nos referimos a Estados Unidos. El estándar LonWorks (Local Operationg NetWork) se basa en la utilización del protocolo Lontalk (ANSI/EIA 709) para redes de control, que implementa las siete capas del modelo OSI.

Según la investigación realizada por Romero, Vázquez y Lozano (2011), se trata de un sistema de control distribuido, basado en un conjunto de nodos, independientes, interconectados entre sí, y cuya red está formada por nodos. Cada uno de ellos dispone de un Chip, un circuito integrado con tres procesadores, memoria de lectura/escritura RAM, memoria de solo lectura ROM y subsistemas de comunicación y entrada y salida. Es independiente del medio de transmisión, aunque el más usado es el par trenzado o Link Power.

La comunicación se realiza mediante paquetes. Cada dispositivo dispone de una dirección y analiza todos los paquetes para determinar si corresponde con su dirección. Cada dispositivo tiene un transceptor para conectarse físicamente a la red, que es la interfaz de comunicación y está disponible para par trenzado, línea eléctrica, radiofrecuencia, fibra óptica, etc., con velocidades de 1,25 Mbps.

En el desarrollo de la domótica es importante la integración tecnológica así como de sus protocolos promoviendo un mejor avance y facilidad de uso, así como lo proponen Vera, Alarcón, Polanco, Nieto, & Bernal, (2004). “Un modelo que permite el control de electrodomésticos a través de la integración de los protocolos X-10 y WAP. Donde se ha definido que un usuario puede modificar el estado de sus electrodomésticos por medio de un teléfono móvil celular. Además, de mostrar su diseño e implementación de los módulos electrónicos, que se ajustan a las

características establecidas por el protocolo X-10".[12] Para lo cual es importante su integración y una comunicación eficaz teniendo como punto presente el control inalámbrico o remoto de todos los elementos que pueden conformar una red domótica, dando un enfoque para el acceso remoto a la información, tomando las mejores características de ellos e integrándolos podemos realizar una red de control remoto mejorada con el fin de satisfacer las necesidades principales en cuanto a confort y seguridad del hogar , garantizando que los datos se transmitan óptimamente para crear un buen funcionamiento sobre la red domótica y que esta sea segura, estableciendo como punto principal el control por medio del dispositivo móvil y un servidor con un login y password, haciendo una comunicación desde el móvil – servidor - electrodomésticos a controlar todo a través de la red eléctrica.

Entonces a partir de la integración de protocolos podemos crear una red domótica más robusta y porque no llevarla a una forma más consiente no solo que se adapte a las necesidades del usuario sino también a su rutina diaria como lo plantea Henríquez y Palma (2011). "En un sistema de consiente de autoconfiguración para domótica, en un entorno de oficina el cual se adapta a la rutina del usuario asumiendo un control sobre (iluminación, temperatura, humedad) en el cual se utilizan redes neuronales para el control del sistema domótico para clasificar y adaptar el estado de cada una de las variables controladas llegando a reconocer patrones de forma acertada en más de un 90%."[13], también "es importante que la adquisición de los datos relacionados con las acciones del usuario se realice tanto de manera implícita como de forma centralizada, es decir por un lado de manera que el usuario no perciba el proceso de captura de los datos, interactuando de forma normal con los dispositivos de la oficina, mediante las técnicas empleadas, se explota la información registrada de las actividades del usuario, con lo cual se deducen los patrones en un proceso completamente automático."[14] Es necesario hacer esas consideraciones con el fin de realizar un sistema autónomo que se adapté al usuario y su forma de vivir lo cual lo podríamos definir como un confort total en su ambiente y adaptable a cualquier entorno.

Aparte de la necesidad de un protocolo o tecnología única que conforme una red domótica integrada y adaptable a las necesidades del usuario, es importante abarcar la seguridad y el ahorro energético, puesto que estamos implementado una nueva tecnología que controlara un entorno y para ello es prescindible tomar parte de lo observado en una red domótico por Morales (2011) "donde se sustenta con el uso adecuado de los electrodomésticos, la gestión de tarifas, el uso de energías renovables, así como el control y regulación sobre la iluminación automatizando distintos sistemas integrados al hogar, además de brindar seguridad y un control vía

[12] Vera, A., Alarcón, A., Polanco, O., Nieto, R., & Bernal, A. (2004). Aplicación de las Comunicaciones Inalámbricas a la Domótica
[13] Henríquez, M. & Palma, P., (2011). Control Automático de Condiciones Ambientales en Domótica usando Redes Neuronales Artificiales.
[14] Ibíd.

internet, buscando crear una tele gestión y accesibilidad para el usuario llegando a representar gran cantidad de ventajas sobre esté, definiendo cada una de las variables necesarias para el bienestar y confort de las personas dentro del hogar"[15]. Donde no solo debemos ver lo que podemos llegar a implementar o tecnologías que renovarían el hogar; es decir podríamos dar un punto de vista donde esto ya viniera incluido en hogares los cuales podríamos habitar o los diferentes entornos en los cuales desarrollamos nuestras rutinas es de allí que es importante que el desarrollo también provenga del "área de construcción como el ámbito arquitectónico y los ingenieros de obras, donde aplicaran un verdadero estudio de factibilidad de estas variables (confort y ahorro energético) en sus proyectos hubiese una significativa relevancia; Asimismo ayudará a la promoción del desarrollo tecnológico por su impulso en varias de las ramas de la computación como lo es la Domótica"[16].

Pasando así a los sistemas inalámbricos como solución al control de la red domótico y por lo tanto a su entorno como lo puede llegar a ser una aplicación móvil implementada sobre el celular del usuario que simplemente por autentificación permita interactuar con el entorno y adaptarlo a sus necesidades; así como lo proponen en una pequeña escala por medio de un módulo Bluetooth y un PIC para el control de la red domótica[17]. Llegando a tener un control no solo manual de la red sino también de forma inalámbrica o promedio de un control remoto gracias a las aplicaciones móviles.

Y entrando no solo a la integración de diferentes tecnologías que tengan que ver con la domótica; también es necesario tener en cuenta el desarrollo tecnológico en cuanto a electrónica o dispositivos que hacen parte de la red es decir sus actuadores y sensores que realizan la parte importante sobre las necesidades del usuario, como lo presenta Márquez & Cárdenas (2011). Dicen que es necesario tener en cuenta los "Sistemas Micro-Electro Mecánicos (MEMS), está tecnología se está convirtiendo rápidamente en una de las tecnologías más promisorias, con un potencial aparentemente ilimitado para dominar los desarrollos tecnológicos futuros, donde los MEMS poseen una serie de ventajas frente a los sistemas de mayor tamaño. Sin embargo, la confiabilidad de estos dispositivos tiene que ser evaluada meticulosamente y éste es un requerimiento vital para mayores mejoras y una adopción más general"[18]. Es decir tenemos que tener en cuenta todo los puntos de desarrollo que destacan a la red domótica como la integración de diferentes dispositivos en un amplio rango instrumental y automatizado es por ello que se plantea que "el potencial de los MEMS apenas se está comenzando a explotar, su aplicabilidad en la industria es inevitable, la evolución de los sensores actualmente utilizados tienden a converger en el uso de tecnologías más pequeñas y la

[15] Morales, G. (2011). La domótica como herramienta para un mejor confort, seguridad y ahorro energético.
[16] Ibíd.
[17] Hernández, J. & Borromeo, S. Sistema Inalámbrico para Aplicaciones Domóticas.
[18] Márquez, D. & Cárdenas, O. (2011). Estado del arte de los sistemas microelectromecánicos.

nanotecnología representa el próximo paso hacia la miniaturización de los sistemas y procesos de medición." [19]

Pero para todo esto es necesario primero analizar las necesidades a cumplir y como se puede adaptar una red domótica y su funcionamiento al entorno pasivo o a controlar en el cual se trabaja, y esto se ve reflejado en el análisis que presentan Penagos, Castellanos, Alarcón, Weiss, Laverde, Rodríguez, & Rincón. (2006). que proponen una solución por medio de la implementación de una red domótica para el laboratorio de electrónica de su universidad "la propuesta de aprovechar el tendido de distribución eléctrica para crear una red domótica que ofrezca facilidades de acceso, control de los equipos del laboratorio, ahorro de energía y mejore la calidad de servicio para los estudiantes. Para ello se aplicó la tecnología Power Line Communications (PLC) y se exploraron mejores alternativas de modulación digital, codificación y detección de errores, protocolos de transmisión de datos y nuevas aplicaciones. Todo el proceso estuvo basado en la estimación del canal (tendido eléctrico) como medio de transmisión, donde se facilita el desarrollo y avance en la aplicación de nuevas tecnologías de comunicaciones para la solución de una necesidad" [20]

Al realizar toda la conceptualización de las necesidades y parámetros necesarios para que una red domótica sea integrada, cumpla las necesidades de los usuarios y se adapta al diario vivir, también se debe tener en cuenta el mantenimiento de está de tal amanera que no represente gastos innecesarios y que no se tiene contemplados, es decir un gasto tanto de implantación como mantenimiento, para lo cual se debe garantizar la vida útil de cada uno de los dispositivos que conforman la red domótica. Es así como "es necesario a lo largo del tiempo garantizar la vida útil de las instalaciones y de los equipos se hace necesario elaborar un plan semanal, mensual o anual que garantice el ciclo adecuado de mantenimiento, así como la correcta planeación y programación de la fuerza de trabajo combinadas con el eficiente manejo; Mediante el FMS (Facility Managment Systems), no solo se evalúan las acciones que se llevan a cabo en el tiempo correcto, sino que se detectan posibles fuentes de problemas"[21] , entonces no solo es el tener o haber implementado la red domótica en cualquier entorno, también es necesario estar pendiente de su correcto funcionamiento y operabilidad en todo el sistema, ya sea por mantenimiento correctivos o preventivos o así como se propone anteriormente con la misma red por medio de un software.

Aparte del desarrollo tecnológico y el control de los entornos para satisfacer las necesidades de los usuarios, es importante y primordial el tener en cuenta la

[19] Ibíd.
[20] Penagos, H., Castellanos, G., Alarcón, R., Weiss, V., Laverde, A., Rodríguez, J. & Rincón, L. (2006). Diseño e implementación de una red domótica para un laboratorio de ingeniería electrónica
[21] Soberanes, M. (2008). El mantenimiento de un edificio inteligente.

construcción eco sostenible y el uso de las energías renovables junto a una integración de la domótica como meta para los hogares inteligentes como "La construcción sostenible está basado en el desarrollo de un modelo que permita a la construcción civil enfrentar y proponer soluciones a los principales problemas ambientales de nuestra época, sin renunciar a la moderna tecnología y a la creación de edificios que atiendan a las necesidades de sus usuarios; donde se promueve alteraciones conscientes en el entorno, de forma a atender las necesidades de habitación y uso de espacios del hombre moderno, preservando el medioambiente y los recursos naturales, garantiendo calidad de vida para las generaciones actuales y futuras"[22] o llevando la vivienda a una vivienda sostenible y autoeficiente por medio de sistemas domótico y la integración de energías renovables, "hacia donde realmente nos dirigimos es hacia la domótica, que no es más que la automatización de cualquier actividad dentro de un edificio. Consiste en sistematizar la entrada de luz natural, el encendido o apagado de aparatos electrónicos según las necesidades de consumo y la regulación de la luz artificial, entre otros"[23]. Donde necesario el utilizar energías limpias y renovables, buscando un mejor futuro para nuestro planeta, sin afectar el desarrollo tecnológico ni la implantación de esté.

Todo lo que abarca la domótica también nos llevaría a una nueva tendencia (control de entornos) y cómo afectaría social y racionalmente a las personas este tipo de tecnología en su entorno, quizá facilitando la vida o tareas cotidianas pero hasta donde llegarían estos; "La inteligencia ambiental presenta problemas especulativos relacionados con el empleo de razonamientos y el despliegue de procesos inferenciales e interpretativos a través de los cuales interactuamos con el entorno social tanto individual como colectivamente."[24] Demostrándonos las claras diferencias entre los entornos artificiales e inteligentes creados por la tecnología y desarrollo de hoy en día llegando a preguntarse si ellos son "capaces de amplificar la capacidad cognitiva y motriz de las personas, el llegar a representar un entorno pertinente para la vivienda, confort y cumplimiento de las necesidades de las personas que habitan en ellos; y hasta donde puede afectar su raciocinio como expresión del procesamiento de la información a partir de un conocimiento adquirido y de unas características subjetivas y fisiológicas específicas, no siempre es correcto ni siempre es consistente en el habitad del ser"[25]; es decir el avance tecnológico en que nos puede afectar y hasta donde nos puede llevar un control total o dependencia de ellos, presentándose como una solución tecnológica a l vida cotidiana o representando un problema a futuro.

[22] O'R sutainables strategies. (2010). Diez Pasos para la Construcción Sostenible.
[23] Chireno, K. (2011). Hacia una vivienda sostenible en Santo Domingo.
[24] Navarro, M. (2011).Inteligencia ambiental: entornos inteligentes ante el desafío de los procesos inferenciales.
[25] Ibíd.

Cabe entonces la necesidad de reformular un protocolo que integre todos los servicios del hogar que permita mantener constantemente comunicado y controlando lo que allí sucede mediante la conexión de todo con todo, de allí parte el IoT.

Por lo que se podría afirmar que "esta es una visión que se inició en la década de 2000 comúnmente conocido como 'El Internet de las Cosas '. En esencia, se reformuló el Internet no sólo como la conexión de las computadoras, sino como la visión de un futuro en el que objetos cotidianos pasarían a formar parte de las redes informáticas"[26]. Estas nuevas visiones de un mundo conectado con sus objetos, comunicado todo con todo, ha generado enfoques casi surrealistas en el que la más mínima herramienta tanto en los hogares, en la industria, en la empresa, o en la vida cotidiana pueda ser controlados desde cualquier parte del mundo y comunicada con las personas.

Según CISCO IBSG "Actualmente, el internet de las cosas (IdC, por sus siglas en español) está compuesta por una colección dispersa de redes diferentes y con distintos fines. Por ejemplo, los automóviles actuales tienen múltiples redes para controlar el funcionamiento del motor, las medidas de seguridad, los sistemas de comunicación y así sucesivamente. De forma similar, los edificios comerciales y residenciales tienen distintos sistemas de control para la calefacción, la ventilación y el aire acondicionado, la telefonía, la seguridad y la iluminación. A medida que IdC evoluciona, estas redes y muchas otras estarán conectadas con la incorporación de capacidades de seguridad, análisis y administración"[27] a través de internet.

Es entonces el uso del Internet de las cosas una herramienta eficaz en todo proceso y ámbito de desarrollo. Por ejemplo, basados en RFID se crean nuevas formas inéditas de dar valor, cambiando la manera como las empresas e industrias operan. Estas innovaciones constituyen lo que se conoce como la innovación estratégica, que se centra en la captura de un alto crecimiento y la generación de valor significativo a través de la redefinición de los mercados, los clientes y los modelos de negocio operativo.

Para todos es conocido que la información es el valor más alto de toda empresa y la manera como se utilice por la organización es fundamental. Desde este punto de partida una red que proporcione tanto la centralización de la información como la disponibilidad de la misma, y a su vez conecte todo objeto utilizado en la operación, hará de la misma un proceso más eficiente. Tal es el Caso del Centro ConnectNet quien desarrolla una herramienta corporativa que conecta tanto objetos como personas a través de internet.

---

[26] Karl Prince, Michael Barrett, Eivor Oborn, Dialogical strategies for orchestrating strategic innovation networks: The case of the Internet of Things, Information and Organization 24 (2014) 106–127.

[27] Cisco IBSG, 2011. Pag 5

El enfoque del Centro ConnectNet fue el desarrollo de la PhysNet, que fue concebido por el Centro como Internet unificado de las cosas, capaces de identificar miles de millones de productos de forma exclusiva en una red interconectada que incluía objetos físicos cotidianos. La innovación se basa en la identificación por radiofrecuencia (RFID). De manera similar a un código de barras, una etiqueta RFID, que consta de un chip de circuito integrado y una antena, es colocada en un objeto con el fin de identificar de forma única y facilitar el seguimiento del objeto.[1] A diferencia de un código de barras, una etiqueta RFID no presenta inconvenientes en una línea de visión directamente muchos menos en orientaciones particulares, pero es más complicado su funcionamiento en cuanto respecta a obstáculos entre etiquetas y lectores, así como las orientaciones de las etiquetas. Además, la creación de una red de conexión de la etiqueta podría estar relacionado con las bases de datos que contienen información sobre el producto. De esta manera, los objetos ordinarios harían parte de la red de redes, Internet. Después de unos años de desarrollo inicial de la innovación PhysNet se ha vuelto ampliamente conocida. La adopción generalizada de PhysNet probablemente resultaría en un aumento en la recolección de datos, un aumento en el número de eventos transitorios que se está grabando de forma permanente, y los datos que se reunió en casi cualquier lugar, en cualquier tiempo, haciendo más eficiente el proceso empresarial al poder obtener en tiempo real cualquier información del estado del producto.

Internet de Las cosas IOT

En su definición más simple, el IoT pretende conectar todo objeto, en todo momento y en todo lugar, “la idea fundamental es que todos los elementos se conecten a Internet mediante dispositivos sensores tales como RFID (Radio Frequency Identification) con el fin de lograr el reconocimiento inteligente y gestión de red. Fue propuesto por primera vez por el laboratorio Auto-ID en el MIT (Instituto de Tecnología de Massachusetts) en 1999”.[28] Su tecnología da soporte a una red de sensores inalámbricos y de identificación por radiofrecuencia, como se mencionó anteriormente.

El concepto de Internet de las cosas se aborda en el Informe sobre Internet de la ITU en 2005 denominado: *El Internet de las cosas,* que se publicó en la Cumbre Mundial sobre la Sociedad de la Información (CMSI) de la Unión Internacional de Telecomunicaciones (UIT) en Túnez el 17 de noviembre de 2005. En ella se informa de que “todo se puede conectar entre sí en cualquier lugar y en cualquier momento por la tecnología de identificación por radio frecuencia, sensores inalámbricos, tecnología de redes, tecnología de la inteligencia integrada, y la nanotecnología”.[29]

[28] Xian-Yi Chen, Zhi-Gang Jin, Research on Key Technology and Applications for Internet of Things

[29] ITU Strategy and Policy Unit (SPU). ITU Internet Reports 2005: The Internet of Things[R]. Geneva: International Telecommunication Union (ITU), 2005.

Dado que no existe una definición uniforme del Internet de las cosas, puede ser definido desde una perspectiva técnica como lo siguiente: Internet de las cosas es la red que puede lograr la interconexión de todas las cosas en cualquier lugar, en cualquier momento con gestión completa, una transmisión fiable, preciso control, procesamiento inteligente y otra características de las tecnologías de apoyo, tales como micro-sensores, RFID, redes de sensores inalámbricos, tecnologías integradas inteligentes, tecnologías de Internet, procesamiento inteligente integrado, y la nanotecnología.

Tecnología RFID

La identificación por radiofrecuencia (RFID), es una red de sensores infrarrojos, sistemas de posicionamiento global, escáneres láser y otros dispositivos de detección, interoperables con el protocolo, o cualquier artículo conectado a Internet para el intercambio de información y la comunicación, a fin de lograr identificar, localizar, rastrear inteligentemente , supervisar y gestionar una red.

RFID es una tecnología con un importante valor comercial y un enorme potencial. RFID promete sustituye al antigua código de barras y contribuye a la visibilidad en tiempo real de los bienes, con independencia de la ubicación de la cadena de suministro. Encontramos aplicaciones RFID en varios campos, pero su uso principal aplicación está en el seguimiento e identificación de objetos.

La tecnología RFID (Radio Frequency Identification, identificación por radiofrecuencia) se originó en los años 40 's, y se usaba principalmente en el reconocimiento de las máquinas de aviones enemigos y amigos en combate aéreo. Después de varias décadas de desarrollo, que puede ser utilizado para la gestión de la producción, la seguridad, el transporte, gestión de la logística, y otras áreas. El Sistema RFID utiliza etiquetas de radio frecuencia para dar información.

Para identificar de forma automática, la etiqueta RFID y lector deben comunicarse por medio de sensores sin contacto, las ondas de radio o microondas. La característica más prominente de la tecnología RFID es la lectura sin contacto y la escritura, distancia de algunos centímetros a decenas de metros, a reconocer objetos a alta velocidad, una gran seguridad en movimiento, y puede identificar varios objetivos al mismo tiempo. Las tecnologías clave de RFID incluyen tecnología de comunicación inalámbrica adaptativa, de alta confidencialidad, bajo consumo de energía, alta confiabilidad de los dispositivos RFID, pequeño volumen, y alta eficiencia.[5]

Las tecnologías RFID (Radio Frequency Identification) se utilizan principalmente para identificar objetos a corta distancia, comunicándose de forma inalámbrica con las etiquetas asociadas a los objetos mediante un lector. Además de ofrecer dos funciones básicas para el Internet de las cosas, la identificación y comunicación. Las etiquetas RFID también se pueden utilizar para determinar el estado del

producto al que están asociadas, los niveles de temperaturas o de luz por los que ha pasado, la humedad, el campo magnético o eléctrico al que ha estado expuesta, así como la ubicación aproximada de los objetos siempre que la posición del lector sea identificada.

Otra tecnología complementaría a RFDI es el Código Electrónico de Producto EPC (Electronic Product Code), que fue desarrollado por el Auto-ID Center en el Instituto de Massachusetts Tecnología (pioneros del IoT), que puede utilizarse para construir una red inteligente global de intercambio de información en tiempo real y establecer un identificador único para cada artículo, y luego utiliza RFID para su identificación, y conexión a través de Internet.

El Auto-ID Center del MIT y su organización sucesora EPC global han aplicado sistemáticamente una visión de Identificadores RFID baratos y estandarizados para la identificación de miles de millones de objetos de uso cotidiano. Vale aclarar, que la red de Auto-ID Labs es un grupo de investigación en el campo de la identificación por radio-frecuencia (RFID) y las nuevas tecnologías de detección que se dedica a la creación de protocolos del Internet de las cosas, utilizando la tecnología RFID y Redes Inalámbricas de Sensores. Estos laboratorios están integrados por siete universidades de investigación situados en cuatro continentes diferentes. Estas instituciones fueron elegidas por el Auto-ID Center para diseñar la arquitectura del Internet de los objetos, con el fin de crear un sistema mundial de seguimiento de mercancías por medio de un sistema único de numeración llamado Código Electrónico de Producto (EPC). Los Laboratorios Auto-ID son la principal red mundial de laboratorios de investigación académica en el campo de tecnologías RFID y por ende del IoT. Por otra parte en cuanto al desarrollo de protocolos basados únicamente en IP se encuentra como pionera la IEEE, quien ha forjado una lucha por establecer normatividad de operación clara para la inserción de IoT en el mundo.

“El desarrollo de la RFID en los últimos años se refleja no sólo en el progreso técnico, sino también en la reducción de costes y en la estandarización. Por ejemplo, el consumo de energía de la última generación de identificadores es menos de 30 mW, con posibilidad de lectura a distancias de hasta diez metros, en condiciones favorables”[30]. El aumento de la miniaturización, con la nanotecnología ha llevado a campos impensados de aplicación, como la inserción de ID en personas. También se han hecho grandes avances en el ámbito de la estandarización, con el protocolo ISO 18000-6C RFID, emitido por el EPCglobal, que es la organización que domina el mercado y pretende entregar interoperabilidad.

Los microchips basados en tecnologías RFID no utilizan baterías sino que están alimentados de forma remota por un dispositivo de lectura. “Debido a que el suministro de potencia puede verse interrumpido por lo que se conoce como “field

[30] Alejandra García Salvatierra, El Internet de las Cosas y los nuevos riesgos para la privacidad, 2012

nulls" o nulos de campo, estos dispositivos evitan la transmisión de paquetes de datos de gran tamaño, a 128 bits que son normalmente más pequeños que los paquetes IP. Por lo tanto los dispositivos que forman parte del Internet de las Cosas y están basados en RFID no se comportarán exactamente igual que los nodos del Internet convencional."[31] Por cuanto las redes actuales deberían sufrir un cambio para adaptarse a las implicaciones del IoT, o por otro lado, los dispositivos adaptarse a una nueva red. Estas adaptaciones vendrán implícitas en la implementación mundial del protocolo IPv6. Además al utilizar protocolos distintos, el lector RFID debería actuar como puerta de enlace entre ambos protocolos, los utilizados en el Internet de las Cosas y los empleados tradicionalmente.

Para entornos RFID se han desarrollado protocolos TCP y protocolos basados en http que se usan para configurar los lectores y distribuir los datos capturados a través de Internet. RFID juega entonces, un papel fundamental en la revolución tecnológica, junto con el Internet y los dispositivos móviles, que se conectan al mundo.

Todos los sistemas RFID, contienen tres componentes básicos. La primera es la etiqueta RFID que se adjunta a un elemento. La etiqueta contiene información acerca de ese elemento y también puede incorporar sensores. El segundo componente es el elemento encargado de identificar el RFID, que se comunica con las etiquetas RFID. El tercer componente es el sistema base, que une los identificadores RFID a una base de datos centralizada. La base de datos centralizada contiene información adicional, como el precio, para cada elemento etiquetado RFID.

Las tecnologías RFID se pueden clasificar en tres categorías: RFID pasiva, RFID activa y RFID semi-pasiva. Sobre la base de la frecuencia de radio, las tecnologías RFID pasivas suelen clasificarse en baja frecuencia (LF) de RFID, de alta frecuencia (HF) de RFID, de ultra alta frecuencia (UHF) de RFID, y RFID de microondas[32]

Por otro lado, el Código Electrónico de Producto (EPC) forma parte de la próxima generación de identificación de objetos complementaria a RFID. Se trata de un ID que identifica los objetos de forma única en la cadena de suministro. El EPC se crea a partir de una idea básica de sistemas de numeraciones jerárquicas para la identificación de una gran variedad de objetos. Al igual que muchos de los actuales sistemas de numeración utilizados en el comercio, el EPC se divide en números que identifican al fabricante y el tipo de producto. Además, este sistema emplea un conjunto de dígitos seriales extra asociados a identificar artículos únicos.

[31] Alejandra García Salvatierra, El Internet de las Cosas y los nuevos riesgos para la privacidad, 2012
[32] Chunling Sun, Application of RFID Technology for Logistics on Internet of Things, 2012 AASRI Conference on Computational Intelligence and Bioinformatics

Gracias a este sistema se puede asociar una gran cantidad de información al producto, como la fecha de caducidad, la fecha y lugar de fabricación, sus dimensiones, y otros datos que pueden ser consultados mediante bases de datos globales, a las que se puede tener acceso usando una simple conexión a Internet.

Calidad de servicio (QoS) para el Internet de las cosas.

Debido a la complejidad de las redes de computación y la movilidad de aplicaciones IoT, más y más tareas no pueden ser terminadas por un solo dispositivo. Así que la IP destino deberá estar incluido a la colaboración de más de un dispositivo, y la forma de elegir un servicio adecuado de todos los servicios utilizables independientemente del usuario y el objeto de ubicación es muy importante en el entorno IOT. El controlador de servicio en IoT puede hacer uso de las preferencias del usuario y la información de recursos que se resumen a partir de muchos tipos de recurso dentro de un contexto, y emplear un modelo nuevo de QoS para evaluar la calidad del servicio. Después de evaluar la calidad de servicio, el mejor servicio puede ser seleccionado por el controlador de servicio y será proporcionado al usuario y satisfaciendo las necesidades reales en el momento indicado.[33]

Cuando un evento ocurre en el entorno de IoT, el mejor servicio con los recursos adecuados debe ser elegido para tratar con él. Por lo tanto se necesita un modelo de evaluación de calidad de servicio para la evaluación de los servicios y la selección adecuada. La evaluación de QoS puede considerarse como un problema de toma de decisión multi-objetivo por ende se debe usar un modelo de evaluación de calidad de servicio basada en modelo de evaluación la toma de decisiones multiobjetivo (MODM)[8], para seleccionar el mejor servicio para el evento y satisfacer así la QoS de la aplicación realmente.

Por otro lado, en el ámbito de un solo componente, la IoT se basa en la noción de objetos inteligentes, desde un punto de vista conceptual, la IoT se basa en tres pilares, relacionados con de los objetos inteligentes, empezando por que sean identificables, mediante un ID digital permitiendo una relación entre las cosas pueden ser en el dominio digital siempre que sea sin una conexión física prestablecida. La segunda característica fundamental es que puedan comunicarse con todo, teniendo la capacidad de comunicarse de forma inalámbrica entre sí, y mediante redes ad hoc de objetos interconectados. Finalmente el tercer pilar es que tengan la capacidad de interactuar ya sea entre ellos mismos, creando redes de entre objetos, con los usuarios finales u otras entidades de la red, Con base en las anteriores consideraciones, se plantean retos previstos para la IoT que requieren el desarrollo de técnicas avanzadas capaces de integrar la computación, capacidades de comunicación y de identificación en cada objetos. En los últimos años, varios aspectos han sido investigados en los campos relacionados. Sin

[33] Fan Shaoshuai, Shi Wenxiao, Wang Nan, Liu Yan, MODM-based Evaluation Model of Service Quality in the Internet of Things, Procedia Environmental Sciences 11 (2011) 63 – 69.

embargo el campo de mayor investigación es el bajo costo de consumo de la potencia micro / nano-electrónica tanto para la computación, así como los puntos de comunicación, para avanzar en campo cercano a comunicaciones con fines básicos de identificación. Las comunicaciones de baja potencia es un bien pretendido dentro de la comunidad de redes de sensores, evidenciado en la investigación activa, realizada en la última década para el desarrollo de protocolos de acceso al medio conscientes del consumo de energía[34]. El enfoque típico seguido son los patrones de activación de RF front-end, es decir, los períodos de sueño o inactividad en el patrón de tráfico cuando no se usa el dispositivo. El uso de tales protocolos, sin embargo, en la actualidad no proporciona una optimización del consumo de energía frente problemas de escalabilidad y tamaño de los dispositivos, siendo la fuente de energía quien genere la robustez del objeto. Estos aspectos son de vital importancia para escenarios de la IoT, por tanto la miniaturización de la batería es un proceso costoso que debe realizarse tanto como sea posible.[35] Además, la idea básica de tales protocolos es realizar ciclos de trabajo activo / inactivo, con el fin para ahorrar energía dispersa en la inactividad. El aumento en la latencia de mensajes a su vez tiene que ser objeto de estudio para otorgar el equilibrio entre la actividad de la red y el rendimiento en cuanto a QoS de la comunicación.

En particular, se ha demostrado que es posible integrar diversas fuentes de captación de energía en sensores, incluyendo piezoeléctrico, termoeléctricos y radio ondas dispositivos de recarga[36].

MARCO LEGAL PARA EL ESTABLECIMIENTO DEL IoT

La necesidad de abordar las cuestiones de reglamentación que normalice el IoT ha sido reconocida por la Comisión de la Unión Europea en 2006, en particular en el marco de un taller titulado “De RFID a la Internet de las Cosas”. Comparativamente, los esfuerzos de la Unión Europea en el estudio de las necesidades normativas de la IoT están más avanzados que los esfuerzos de cualquier otro órgano institucional[37]. Como su mayor contribución al creciente debate público y para llegar a un entendimiento mutuo sobre la IoT y su relación hacia el futuro de Internet, la Unión Europea publicó un documento que relaciona los desafíos en relación con la Internet de las cosas. En Particular, han sido abordadas temas como el desarrollo y la importancia de la IoT, la arquitectura de la RFID y sus aplicaciones como un primer ejemplo de la IoT y las políticas y retos en arquitecturas de RFID, tales como la seguridad, privacidad, protección de datos, el control de crítico de los recursos,

[34] W. Ye, J. Heidemann, D. Estrin, An energy-efficient MAC protocol for wireless sensor networks, in: Proceedings of IEEE INFOCOM, vol. 3, 2002, pp. 1567–1576.
[35] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, Internet of things: Vision, applications and research challenges, Ad Hoc Networks 10 (2012) 1497–1516.
[36] G. Merrett, N. White, N. Harris, B. Al-Hashimi, Energy-aware simulation for wireless sensor networks, in: Proceedings of IEEE SECON, Rome, Italy, 2009, pp. 64–71.
[37] Amcham EU, Response to ‘‘Internet of Things’’ Public Consultation, supra note 25, at p. 7.

gestión de identidad, denominación, interoperabilidad, fomento de la innovación, manejo del espectro y la normalización en general. Entre otras, las cuestiones de política, incluyen la sensibilización de todos los interesados, la reducción de las barreras del IoT y la garantía de los derechos fundamentales de las personas respecto a la privacidad, protección de los datos personales y la protección del consumidor. Entre distintos organismo liderados por la Unión Europea, se estableció una lista de principios esenciales para el futuro desarrollo del IoT, incluyendo la apertura, la interoperabilidad, la neutralidad, la confianza, la transparencia, la protección de la privacidad y los derechos fundamentales, la seguridad, el control del usuario, la representatividad, la responsabilidad, y el respeto del medio ambiente. De estos aspectos se determinó que como críticos el manejo de la privacidad y protección de datos, siendo los principales retos de la el desarrollo del IoT. [38]

Teniendo en cuenta el momento de tomar decisiones de política y normatividad eficaces, en el futuro de la IoT, la Unión Europea recomienda destinar una comisión para evaluar cuidadosamente los aspectos técnicos, económicos y sociales del desarrollo de IoT y su impacto en el equilibrio global. En el aspecto técnico EPCglobal siendo el mayor desarrollador de tecnología RFID orientada al IoT juega un papel vital siendo uno de los más interesados en el mercado.

[38] Rolf H. Weber, Internet of things – Need for a new legal environment?, computer law & security review 25 (2009) 522–527

CAPITULO I

8. PROTOCOLOS PROPIOS DE LA DOMÓTICA Y EL INTERNET DE LAS COSAS

8.1 PROTOCOLO X-10

Como se ha menciona con anterioridad el protocolo X-10 se basa en la utilización de la red eléctrica como medio de comunicación que permitirá transmitir datos entre los dispositivos creados específicamente para el uso en este tipo de red domótica, tales dispositivos tiene la característica de poder conectarse directamente al toma corriente y realizan el procesamiento necesario para la obtención de los datos. El sistema puede funcionar en redes de corriente alterna (AC) monofásica o trifásica con diferentes tensiones dependiendo del país donde se implemente como se muestra en la Figura 1, por lo tanto en Colombia los dispositivos del sistema X-10 deberán trabajar a 110V y 220V (Voltios) a 60Hz (Hertz).[39]

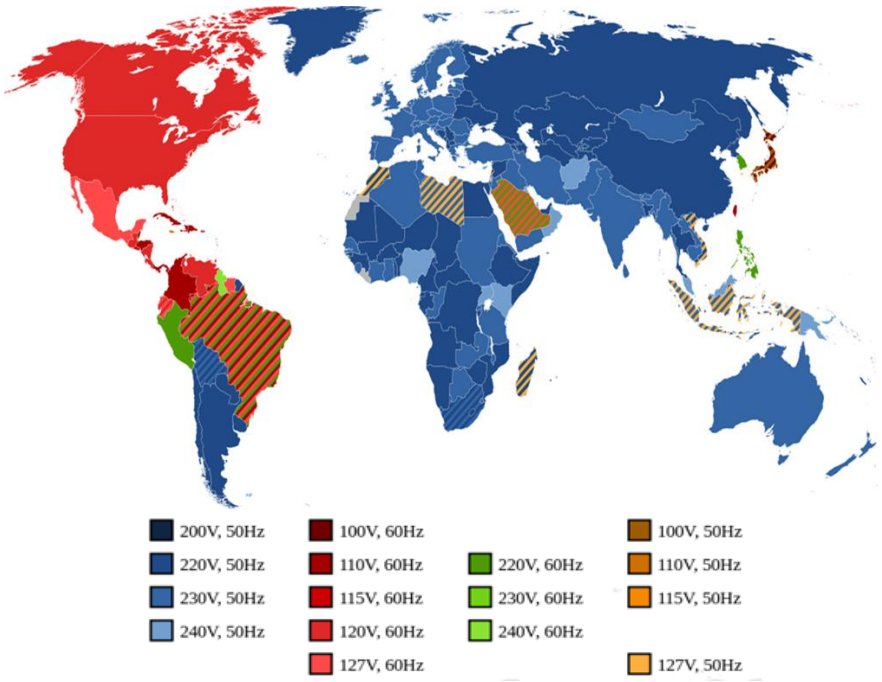


Figura 1. Voltajes y Frecuencias por País
(http://www.kb.barnlightelectric.com/assets/ble_international_voltage_chart.png)

Aunque la red eléctrica no este diseñada para transmitir información y no sea un medio óptimo para su uso en comunicaciones, ya sea problemas de inestabilidad como variaciones de voltajes y la presencia de ruido, presenta ventajas que las empresas no pueden desaprovechar, ya sea la facilidad de implementación, la

[39] VERA, Alexander. ALARCÓN, Andrés. POLANCO, Oscar. NIETO, Rubén. BERNAL, Álvaro. Aplicación de las Comunicaciones Inalámbricas a la Domótica. pág. 2

reducción en el uso de equipos y costos. Por esta razón se desarrolló la técnica denominada "comunicación por corrientes portadoras" (PLC)[40], que es usada por la tecnología X-10 al utilizar la señal alterna de la red eléctrica como una portadora de la información enviada en ráfagas de pulsos de muy baja potencia (3V) y frecuencia superior a la de la red (120KHz)[41], que representan señales codificadas para distribuir la información a los diferentes módulos conectados a la red domótica.[42]

8.1.1 FUNCIONAMIENTO

Para establecer la comunicación entre los dispositivos estos se deben sincronizar mediante la detección de cruces por cero de la señal eléctrica, con lo cual el sistema conoce cuando tiene que enviar o recibir un bit, Figura 2, pero estos no distinguen el cruce por cero de la señal desde el semiciclo positivo al semiciclo negativo que desde el semiciclo negativo al semiciclo positivo siendo interpretado de la misma forma.[43]

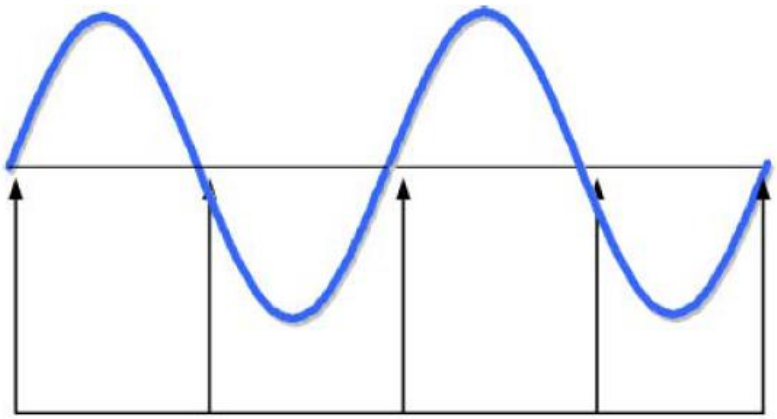


Figura 2. Sincronización por cruce por Cero de la Señal AC (Introducción al sistema X10. pág. 8)

Un “1” lógico se representa por la presencia pulsos de 1ms (milisegundo) de duración con frecuencia anteriormente mencionada de 120KHz en el semiciclo positivo, a partir de un cruce por cero, seguido por un la ausencia de un pulso en el siguiente semiciclo o semiciclo negativo, como se observa en la Figura 3. Mientras que un “0” lógico se representa por la ausencia de un pulso en el semiciclo positivo y presencia de pulsos en el semiciclo negativo como se observa en la Figura 4. Cada orden se transmite 2 veces, con lo cual toda la información transmitida tiene redundancia.[44]

[40] Introducción al sistema X10. pág. 3
[41] MARSAL, Luis. Protocolo X10. pág. 4
[42] Introducción, op. cit, pág.3.
[43] INFANTES D, Juan Antonio. Descripción de X-10. pág. 5
[44] MARSAL, op. cit, pág.4.

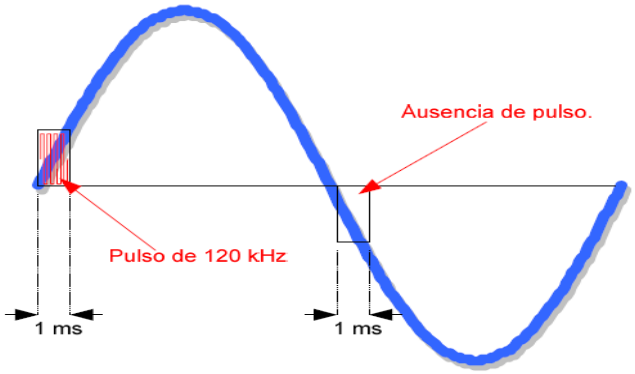


Figura 3. Envió de un “1” lógico (Introducción al sistema X10. pág. 8)

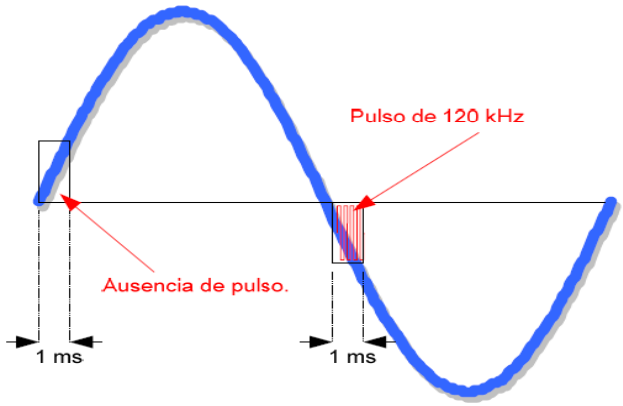


Figura 4. Envió de un “0” lógico (Introducción al sistema X10. pág. 8)

Para redes trifásicas el pulso o tono se repite tres veces por cada semiciclo de modo que permita coincidir el cruce por cero de las tres señales alternas[45] como se observa en la Figura 5. Pero en realidad las señales se superponen sobre la señal portadora de 60 Hz de modo que en realidad es como se muestra en la Figura 6.[46]

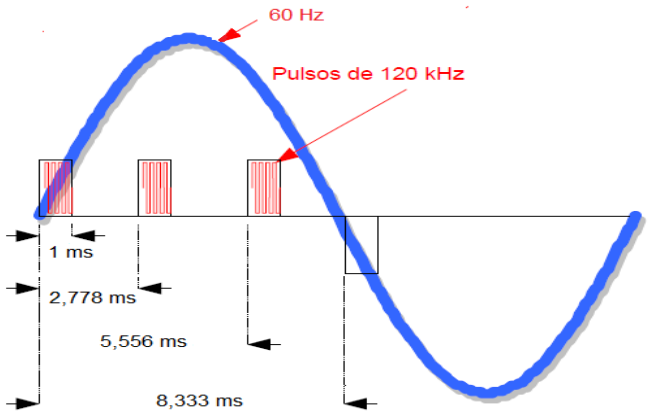


Figura 5. Envió de 3 pulsos en cada semiciclo (Introducción al sistema X10. pág. 9)

[45] Introducción, op. cit, pág.9.
[46] INFANTES D, op. cit, pág. 7.

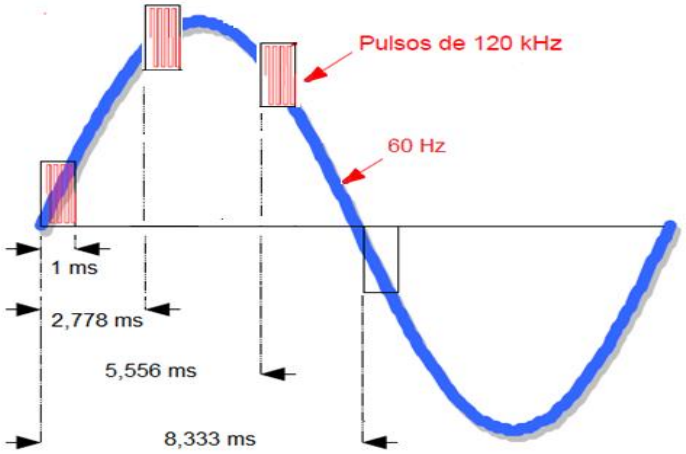


Figura 6. Superposición de los 3 pulsos sobre el semiciclo de la señal AC (Introducción al sistema X10. pág. 9) (modificado por el autor)

8.1.2 ESTRUCTURA DEL MENSAJE

La estructura de datos de un código X-10 está compuesto por 11 ciclos de red como se observa en la Figura 7, con una duración de 183,33 ms.[47] Cada estructura de datos empieza, al menos con seis cruces por cero sin pulsos, es decir que cada trama de datos se separa por seis cruces en los que no envía información que evitan los problemas de corrimiento en los bits de la trama[48].

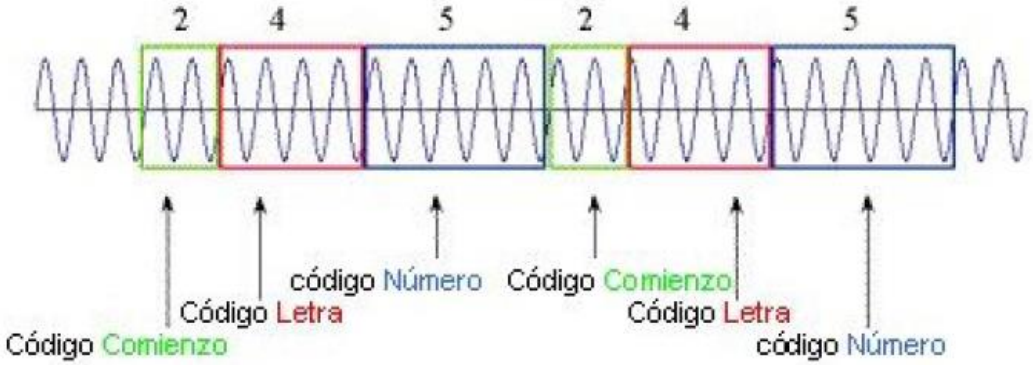


Figura 7. Estructura del mensaje de X-10 11 ciclos (INFANTES D, Juan Antonio. Descripción de X-10. pág. 9)

Los primeros 2 ciclos representan el Código de Inicio constituido por tres pulsos y ausencia de pulso.[49] Los siguientes cuatro ciclos representan el Código de Casa que asocia un código de letras que comprende las letras desde la A hasta la P con cuatro bits como se observa en la Tabla1. Por esta razón, el sistema X-10 no es un

[47] MARSAL, op. cit, pág. 4.
[48] Introducción, op. cit, pág. 10.
[49] Ibíd., pág. 10.

sistema programable, sino que es “configurable”. [50] Estos codigos seran escogidos por el usuario mediante un selector.

A = 0110	I = 0111
B = 1110	J = 1111
C = 0010	K = 0011
D = 1010	L = 1011
E = 0001	M = 0000
F = 1001	N = 1000
G = 0101	O = 0100
H = 1101	P = 1100

Tabla 1. Códigos de Casa (House Code) del sistema x10 *(Introducción al sistema X10. pág. 10)*

Los siguientes 5 ciclos representan el Código Numérico (1-16) o el Código de Función entre lo que se encuentran encender, apagar, aumentar o disminuir la intensidad de luz de los dispositivos entre otras tareas.[51] Los códigos de Numeración y de Función se presentan en la Tabla2, y se observa que se diferencian por el último bit, que en el primer caso es 0 y en el segunca caso es uno para todas las opciones.

Código	Bits				
1	0	1	1	0	0
2	1	1	1	0	0
3	0	1	1	0	0
4	1	0	1	0	0
5	0	0	0	1	0
6	1	0	0	1	0
7	0	1	0	1	0
8	1	1	0	1	0
9	0	1	1	1	0
10	1	1	1	1	0
11	0	0	1	1	0
12	1	0	1	1	0
13	0	0	0	0	0
14	1	0	0	0	0
15	0	1	0	0	0
16	1	1	0	0	0
All Units Off	0	0	0	0	1
All lights On	0	0	0	1	1
On	0	0	1	0	1
Off	0	0	1	1	1
Dim	0	1	0	0	1
Bright	0	1	0	1	1

Tabla 2. Código de Numeración y Función (Introducción al sistema X10. pág. 12)

[50] Ibíd., pág. 10.
[51] DURÁN, Ana. Instalación Domótica de una Vivienda Unifamiliar. pág. 31.

8.2 PROTOCOLO KNX

Fue fundado en 1999 como fusión de tres asociaciones europeas de aplicaciones domóticas y de los sistemas más importantes del mundo, partiendo del más conocido EIB (Bus de Instalación Europeo), BCI: Sistema Batibus y el European Home System Association o sistema EHS. KNX es el único estándar mundial de comunicación abierto e independiente de fabricantes y dominios de comunicación[52], además de utilizar diferentes medios de transmisión como cable bus, línea de fuerza, radio frecuencia o IP/Ethernet, siendo de uso para proyectos de gestión de viviendas, edificios o cualquier tipo de instalación en la que se quiera realizar un control o un eficiente uso de la energía[53]. Llegando a obtener, por medio de la combinación de estos sistemas varios tipos de transmisión en un nivel físico, como lo son:

8.2.1 EIB.TP

Sobre par trenzado alcanzando una velocidad máxima de hasta 9600 bps. Además de suministrar 24 Vdc para la alimentación de los dispositivos como para transmitir información, pero no dispone de potencia para alimentar los elementos controlados (calefacción, electrodomésticos, luces) por lo que los controladores deberán tener, además, una conexión a la red eléctrica; hace uso de la técnica CSMA/CA (Acceso Múltiple por Detección de Portadora) que evita las colisiones y maximizando el ancho de banda disponible para la comunicación de dispositivos[54].

8.2.2 EIB.PL

Utiliza la red eléctrica, con corrientes portadoras sobre 230 Vac/50 Hz (powerline) a 1200/2400 bps en PL-110 (línea eléctrica, 110 kHz) y PL-132 (línea eléctrica, 132 kHz), respectivamente. Usando una modulación SFSK (Spread Frequency Shift Keying), alcanzando distancias sin repetidor de máximo 600 metros[55].

8.2.3 EIB.net

“Utiliza el estándar Ethernet a 10 Mbps, sirve de backbone entre segmentos EIB además de permitir la transferencia de telegramas EIB a través del protocolo IP a viviendas o edificios remotos; las redes LAN pueden utilizarse para transportar (en modo "routing" o en modo "tunneling") telegramas KNX”[56], donde se le asigna una dirección IP de forma automática (DHCP), permitiendo el uso a través de una LAN o cualquier dispositivo conectado a internet como lo muestra la siguiente imagen.

---

[52] Curso iniciación al KNX. pág. 7.
[53] Eficiencia Energética con KNX.
[54] LÓPEZ, Diego. Domótica y eficiencia en edificios. pág.7.
[55] Curso, op. cit, pág.10.
[56] LÓPEZ, op. cit, pág.8.

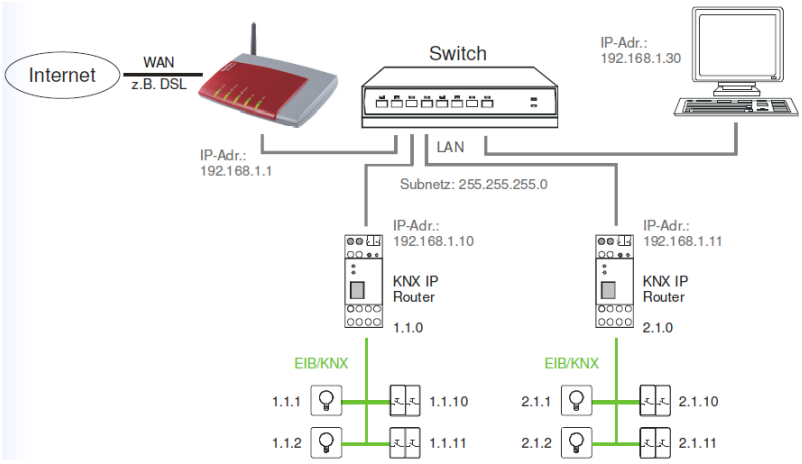


Figura 8. Conexión protocolo Ethernet - KNX. (LÓPEZ, Diego. Domótica y eficiencia en edificios.)

8.2.4 EIB.RF

EIB.RF o r radiofrecuencia utiliza varias portadoras, para lograr distancias de hasta 300 metro. Mediante el uso de repetidores puede abarcar mayores distancias; empleando señales de radio para transmitir telegramas KNX en la banda de frecuencia 868 MHz (corto alcance), con una potencia máxima irradiada de 25 mW, además de presentar un bajo nivel de consumo energético a velocidades de transmisión de 16.384 kbps.[57]

8.2.5 EIB.IR

EIB.IR o infrarrojo, se utiliza mediante el uso con mandos a distancia para controlar los dispositivos EIB instalados.

Para elegir entre algunos de estos medios de transmisión en un nivel físico es importante tener en cuenta el tipo de edificio o construcción en la cual se implementara la red domótica, además de las instalaciones que las que cuente este, identificando así el medio más óptimo para crear la comunicación entre los dispositivos que conforman la red (Par trenzado, línea de potencia o radiofrecuencia).

[57] Ibíd., pág.8.

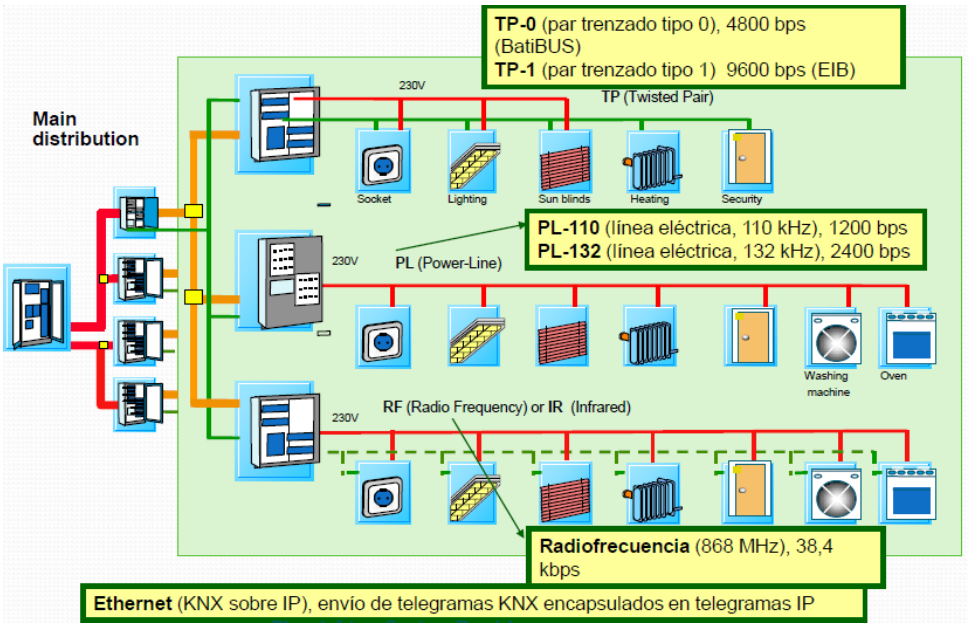


Figura 9.Medios de comunicación KNX (LÓPEZ, Diego. Domótica y eficiencia en edificios)

8.2.5 FORMAS DE CONFIGURAR LOS DISPOSITIVOS EN KNX:

Modo fácil (E-Mode):

- Los dispositivos se encuentran pre – programados con sus parámetros.
- La configuración se realiza con el software ETS3 – Starter.
- La configuración se realiza a través de un controlador central sin necesidad de un PC[58].

Modo automático (A-Mode):

- La configuración se realiza automáticamente cuando se conecta el dispositivo, que adaptan su comunicación al resto de los componentes.
- Usado para aplicaciones de usuario final.
- Cada componente posee unos parámetros fijos además de una librería de instrucciones para comunicarse con otros dispositivos.
- Realización de instalaciones pequeñas, así como el control de dispositivos de audio, video y electrodomésticos[59].

Modo sistema (S-Mode):

- La organización y configuración de la instalación se realiza con el software ETS (EngineeringToolSoftware).
- Se programan los dispositivos de acuerdo a la base de datos de cada uno.

[58] Curso, op. cit, pág.13.
[59] Ibíd., pág.13.

- Mayor grado de funcionabilidad y flexibilidad de la red.
- Utilizado principalmente para grandes instalaciones[60].

8.2.6 Topología del par trenzado uno (TP1)

Permite diferentes tipos de topología en red de comunicación domótica como línea, estrella o árbol, además posee:

- Bus de control descentralizado y controlado por eventos.
- Cada dispositivo conectado al bus tiene su propia unidad de control.
- La información es enviada en forma de telegramas a través del bus de comunicación, a partir de un sensor a sus determinados actuadores.
- Cada receptor de la red envía acuse de recibo de haber recibido la transmisión de forma correcta, de no ser recibido se repite la comunicación, para ello utiliza CSMA/CD.
- La información dentro de la red se transmite de forma simétrica a 9600bps.

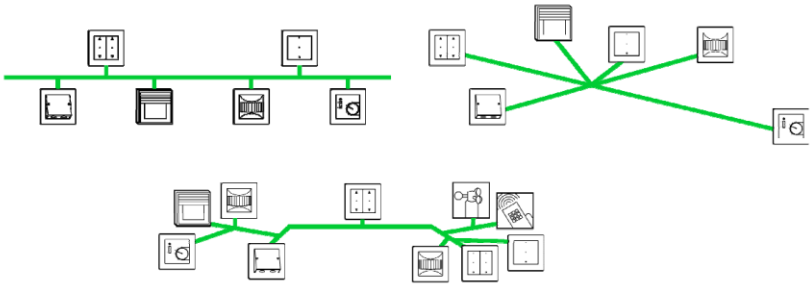


Figura 10.Topologías KNX (línea, estrella, árbol). (Curso iniciación al KNX).

8.2.7 Estructura de bus KNX

8.2.7.1 Segmentos de líneas

Es la unidad más pequeña del bus KNX, compuesto por una fuente de alimentación adecuada y un máximo de 64 componentes o dispositivos[61].

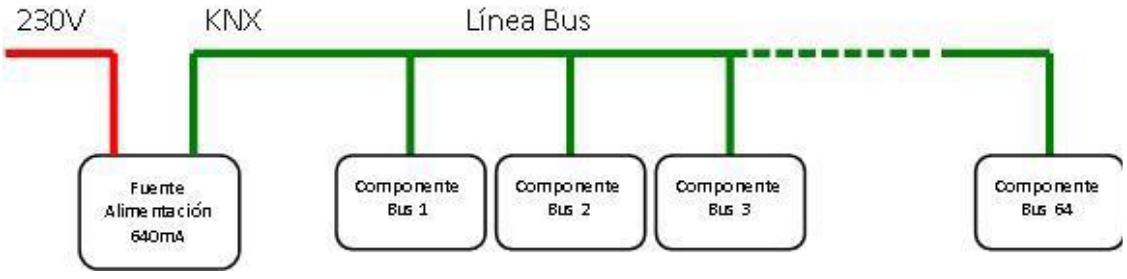


Figura 11.Segmento de línea. (Curso iniciación al KNX).

[60] Ibíd., pág.13.
[61] Ibíd., pág.18.

8.2.7.2 Líneas

Puede disponer o componerse de hasta cuatro segmentos de línea, cada uno de ellos con su respectiva fuente de alimentación y un máximo de 64 componentes bus o dispositivos. Para dividir la línea en varios segmentos de línea es necesario el uso de amplificadores de línea[62].

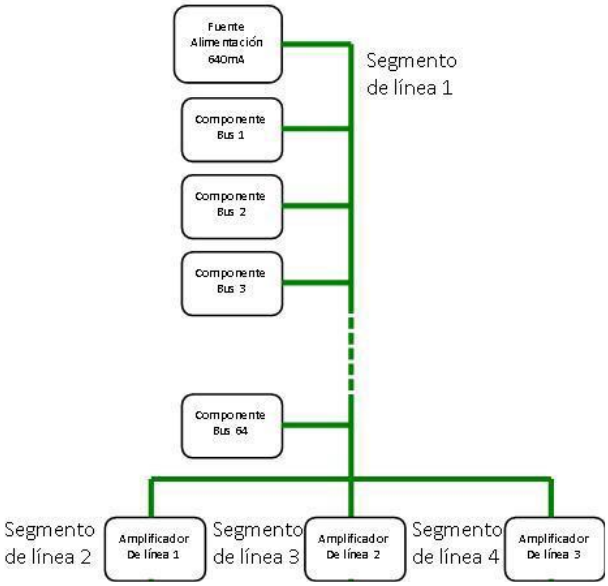


Figura 12.Línea bus KNX. (Curso iniciación al KNX).

8.2.7.3 Áreas

Si es necesario utilizar más de una línea todas se pueden conectar a una línea principal por medio de acopladores de línea y se denomina área; siendo el número máximo de líneas que pueden conectarse a la línea principal 15 (960 dispositivos por área). También es posible conectar hasta 64 dispositivos en la línea principal pero disminuiría este número en función de cada acoplador de línea que se esté utilizando[63].

[62] Ibíd., pág.19.
[63] Ibíd., pág.20.

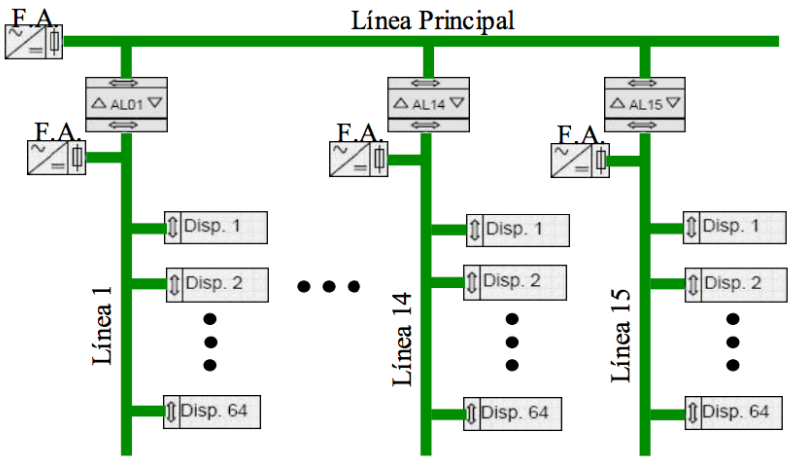


Figura 13.Configuración Área. (PEÑA, Manuel. Comunicaciones en el entorno doméstico).

8.2.7.4 LINEA DE AREAS "BACKBONE":

De igual manera se pueden utilizar más de un área todas ellas conectadas a en una línea de áreas o "backbone" por medio de acopladores de área. A esta estructura se le denomina línea de áreas, donde el número máximo de áreas que pueden conectarse a la línea de áreas son 15 y de esta manera el número máximo de elementos o dispositivos que pueden conformar la red domótica será de 14.400. También es posible conectar hasta 64 dispositivos en la línea de áreas pero disminuiría este número en función de cada acoplador de área que se tenga en uso[64]; por medio de repetidores se podrán acoplar hasta 256 aparatos por línea lo que permitirá un total de 57600 dispositivos[65].

[64] Ibíd., pág.21.
[65] PEÑA, Manuel. Comunicaciones en el entorno doméstico comparación knx – lonworks, (2012).pág.6.

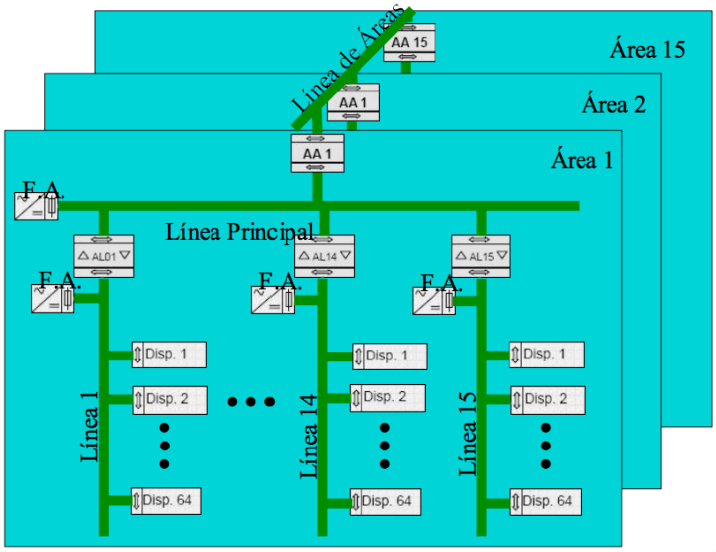


Figura 14.Configuración Backbone KNX. (Peña, Manuel. Comunicaciones en el entorno doméstico).

Para el desarrollo de las topologías se deben tener en cuenta las siguientes restricciones[66]:

- Debe disponer de mínimo una fuente de alimentación.
- No superar los 1000 metros (1Km) el total de la instalación o red domótica.
- La distancia entre un dispositivo y una fuente de alimentación no debe superar los 350m.
- Ente los diferentes elementos de la línea no se deben superar los 750m.
- Separación de 200m mínimo entre cada fuente de alimentación.

8.2.8 COMUNICACIÓN

8.2.8.1 TRANSMISION DE DATOS[67]

- La transmisión de señales se realiza por medio de un bus de datos donde se conectan todos los dispositivos.
- Los datos se transmiten en serie y se empaqueta en forma de telegramas a través del bus.
- En cada receptor se envía un acuse de recibo si se realiza correctamente la transmisión de datos, si no se recibe, la transmisión se repite hasta tres veces. Si el acuse sigue sin recibirse, la transmisión se interrumpe y se notifica un error en el transmisor.
- Los telegramas se modulan y un “cero lógico” se transmite como un pulso y un “uno lógico” como ausencia de pulso.
- La información se transmite de forma simétrica al par de conductores y el componente se controla mediante la diferencia de tensión entre los dos. Las

[66] Ibíd., pág.5.
[67] Curso, op. cit, pág.27.

radiaciones perturbadoras actúan sobre ambos conductores con la misma polaridad y, por tanto, no influyen en la diferencia determinante de la tensión de la señal.

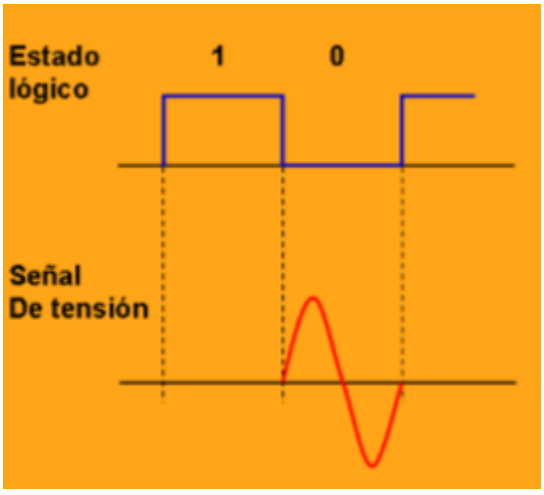
8.2.8.2 REGULACION DE ACCESO AL BUS

Es necesario regular el acceso al bus de transmisión de la información en la red y garantizar un intercambio ordenado de información entre los componentes del bus y el tráfico de telegramas, para ello se utiliza el procedimiento CSMA/CA (Acceso Múltiple por Detección de Portadora/Evitación de Colisiones; garantizando un procedimiento aleatorio libre de colisiones al bus. Todos los dispositivos conectados al bus de comunicación reciben las señales, pero sólo aquellos actuadores a los que se les está hablando reaccionan y efectúan su tarea[68].

"Si un sensor, quiere transmitir, primero debe comprobar el bus y esperar a que ningún otro dispositivo esté transmitiendo. Si el bus está libre, cualquier dispositivo puede comenzar la emisión. Si dos dispositivos comienzan a emitir en el mismo instante, sólo tendrá acceso al bus aquél de ellos que tenga la prioridad más alta. El otro tendrá que esperar y transmitir después. En caso de igualdad de prioridad, comenzará aquel cuya dirección física sea más baja".[69]

8.2.8.3 TELEGRAMAS Y FORMATO DE TRAMAS

En el protocolo KNX, los datos se transmiten de forma simétrica además de usar una trasmisión diferencial, asegurando de esa manera que el ruido afecte por igual a todo el sistema, como también el uso de señales binarias y transmitidas en banda base, donde un 1 lógico se caracteriza o representa con la usencia de señal y un 0 lógico se representa con un impulso AC[70], como se muestra en la siguiente figura.



[68] Ibíd., pág.28.
[69] Ibíd., pág.28.
[70] Peña, op. cit, pág.7.

Figura 15.Transmisión de un 1 y un 0 lógico en KNX. (Curso iniciación al KNX).

Este tipo de transmisión se complementa por medio de los telegramas que contienen la información transmitida entre los dispositivos y no influye el medio físico por el cual es transportado; es aquel que se produce cuando hay un evento en el bus y hace reaccionar un actuador dentro del sistema y se envía un telegrama al bus.

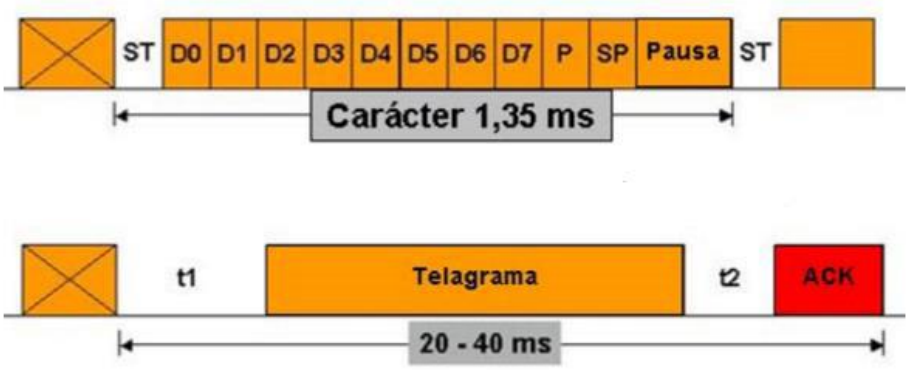
El envío de un telegrama se produce de la siguiente manera[71]:

- Se espera que el bus esté desocupado por lo menos durante un periodo “t1 (50 Bit)”.
- Se envía el telegrama y se espera un tiempo “t2 (13 Bit)” en que los dispositivos que lo reciben envían un acuse de recibo (ACK).
- El tiempo total del telegrama ronda entre los 20 y 40ms.
- El telegrama es transmitido a una velocidad de 9600 bps, es decir, un bit ocupa el bus durante 104µs (1/9600).

Transmisión datos KNX. (Peña, Manuel. Comunicaciones en el entorno doméstico).

El telegrama está formado o agrupado por paquetes de caracteres, cada uno de ellos lo componen 11 Bit + 2 de pausa distribuidos de la siguiente forma[72]:

- ST: 1 bit de inicio, encargado de dar comienzo a un nuevo carácter.
- 8 bit de datos.
- P: 1 bit de paridad par.
- SP: 1 bit de parada, indica el final del carácter enviado.
- Pausa: tiempo de espera equivalente a 2 bits para continuar con el siguiente carácter.



[71] Curso, op. cit, pág.30.
[72] Ibíd., pág.30.

Conformación de un carácter KNX. (Curso iniciación al KNX).

La longitud total del telegrama constara de entre 8 y 23 caracteres, dependiendo de la longitud de la información. Un telegrama de conmutación ocupa en el bus unos 20ms y uno de transmisión de texto unos 40ms. Estos caracteres van dentro de un paquete de datos formado por la siguiente estructura[73]:

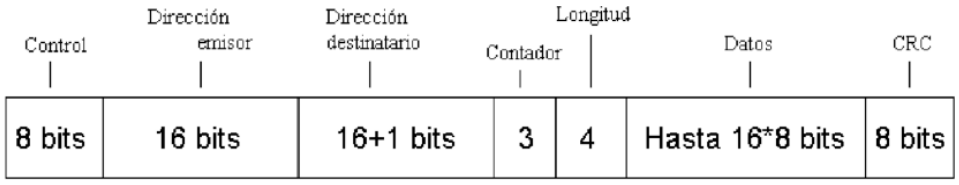


Figura 16.Paquete de datos KNX. (Peña, Manuel. Comunicaciones en el entorno doméstico).

Byte de control: 8 bits que indican la prioridad del mensaje, y expresa el tipo de función del telegrama KNX (alarma, servicios del sistema o servicios habituales)[74].

Byte de dirección emisor: Indica la dirección física del dispositivo que envía el telegrama (4 bits con el área, 4 bits con la línea y 8 bits con el número de dispositivo). Para que posteriormente se puedan comunicar dentro de la red domótica.[75]

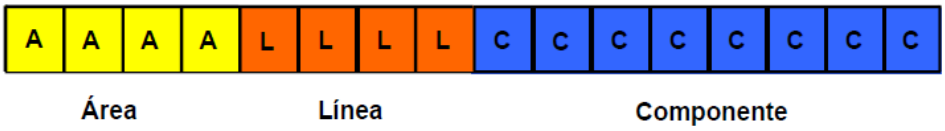
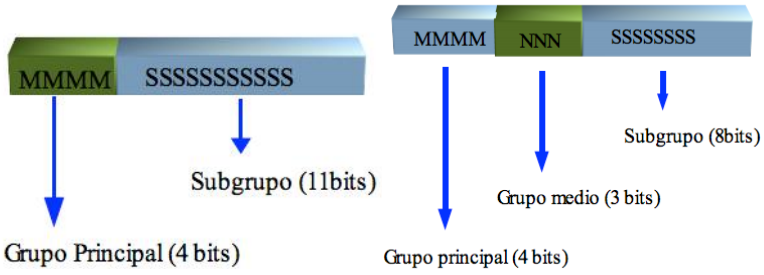


Figura 17.Composición Byte dirección emisor. (Curso iniciación al KNX).

Byte de dirección destinatario: En función con el valor que tome el bit de mayor peso (bit 17) podemos decir que, si toma el valor “0” es una dirección física y se envía únicamente a un dispositivo; si toma el valor “1” es una dirección de grupo y trasmite a todos los dispositivos que tengan esa dirección de grupo[76].



[73] Ibíd., pág.32.
[74] Ibíd., pág.33.
[75] Ibíd., pág.34.
[76] Ibíd., pág.35.

Figura 18.Dirección con 2 subgrupos y con 3 subgrupos, respectivamente. (Peña, Manuel. Comunicaciones en el entorno doméstico).

Byte de contador: Contador de ruta para funciones de enrutamiento, donde realiza el conteo de saltos que ha realizado el paquete hasta llegar a cero, donde el paquete se descarta de la comunicación[77].

Byte de longitud: Indica cuantos bytes contiene el campo de datos (0=1 byte, 15 = 16 bytes)[78].

Datos: Contiene el tipo de comando y los datos de acuerdo con la información de la red domótica en el EIB Interworking Standard (EIS)[79].

EIS (EIB Interworking Standar).			
N°EIS	Función EIB	N° bit	Descripción
EIS 1	Interruptor	1 bit	Encendido/apagado, habilitar/deshabilitar, alarma/no alarma, verdadero/falso.
EIS 2	Regulación	4 bit	Se puede utilizar de 3 formas, como interruptor, como valor relativo y como valor absoluto.
EIS 3	Hora	3 bytes	Día de la semana, hora, minutos y segundos.
EIS 4	Fecha	3 bytes	Día, mes, año (el margen es desde 1990 a 2089).
EIS 5	Valor	2 bytes	Para enviar valores físicos con representación.
EIS 6	Escala	8 bit	Se utiliza para enviar valores relativos con una resolución de 8bit.
EIS 7	Control motores	1 bit	Tiene dos usos: mover, arriba/abajo o extender/retraer y paso a paso.
EIS 8	Prioridad	1 bit	Se utiliza en conjunción con EIS 1 ó EIS 7.
EIS 9	Coma flotante	4 bytes	Codifica un valor en coma flotante según el formato definido por el IEEE 754
EIS 10	Contador 16bit	2 bytes	Representa valores de un contador de 16bit.
EIS 11	Contador 32bit	4 bytes	Representa valores de un contador de 32bit.
EIS 12	Acceso	4 bytes	Se usa para conceder accesos a distintas funciones.
EIS 13	Carácter ASCII	8 bit	Codifica según el formato ASCII
EIS 14	Contador 8bit	8 bit	Representa los valores de un contador de 8bit.
EIS 15	Cadena	14 bytes	Transmite una cadena de caracteres ASCII de hasta 14 bytes.

Figura 19.EIB Interworking Standard (EIS). (Curso iniciación al KNX).

CRC: Es el último byte, se utiliza para comprobar que los anteriores datos se han trasmitido correctamente. “Se obtiene por medio de cálculo de la paridad par de todos los bytes anteriores incluidos en el telegrama. Cuando un dispositivo recibe el telegrama, comprueba si este es correcto a partir del byte de comprobación. Si dicha recepción es correcta, se envía un reconocimiento, de lo contrario se envía un no reconocimiento (NACK) para que el emisor repita el envío. Si el dispositivo está ocupado envía un código Busy para que el emisor reintente la transmisión tras un pequeño retardo”.[80]

Acuse de recibo del telegrama: El componente bus acude al byte de seguridad del telegrama para asegurar la recepción correcta de la información y, de acuerdo con ella devuelve un acuse de recibo. Si se recibe un acuse incorrecto “NACK” el telegrama se repite hasta 3 veces. Si se recibe un acuse de bus ocupado “BUSY” se espera un corto tiempo y se vuelve a enviar el telegrama. Si el componente

[77] Ibíd., pág.37.
[78] Ibíd., pág.39.
[79] Ibíd., pág.40.
[80] Ibíd., pág.43.

emisor no recibe acuse de recibo se envía el telegrama hasta 3 veces antes de interrumpir la transmisión[81].

8.2.9 VENTAJAS DEL KNX FRENTE A OTROS SISTEMAS

- Mayor seguridad.
- Disminución en el uso de la energía.
- Fácil adaptación de la instalación eléctrica.
- Mayor confort.
- Instalaciones preparadas para escalamiento.
- Amplio abanico de productos disponibles de los distintos fabricantes.
- Flexibilidad de implementación en tamaño (edifico- hogar), como de escalabilidad en el sistema domótico.
- Permite el uso de diferentes tipos de dispositivos y fabricantes por medio de acopladores al bus EIB – KNX.
- Permite una instalación sencilla con conocimientos básicos sobre el protocolo.
- El bus de datos EIB – KNX va junto a la red eléctrica lo que permite reducir los costos.
- Permite una gran tasa de transmisión de datos ya que utiliza un bus dedicado para ello.
- Permite la conexión con computadores para su control, configuración y mantenimiento, ampliando así la red de comunicaciones con diferentes tipos de protocolos.

8.3 PROTOCOLO LONWORKS

Lonworks es una plataforma de control creada por la compañía norteamericana Echelon, que fue pensada para dar soluciones a problemas de diseño, construcción, instalación, y mantenimiento de redes de control[82] usado en varios sectores como el transporte (desde aviones hasta ferrocarriles), el control industrial, la automatización de viviendas y edificios, siendo el control de este último el principal enfoque de trabajo. Echelon Corporation ha convertido a LonWorks en un estándar abierto dentro de la familia ANSI/EIA 709 que recibe el nombre de LonTalk como el protocolo propiamente dicho dentro del sistema, que hace necesario de un NeuronChip para su funcionamiento[83]. Por lo tanto Lonworks se diferencia al basarse en dispositivos idénticos sin una jerarquía, un sistema de control distribuido, más potente y flexible, que facilite la instalación y sean más económicos evitando los sistemas centralizados y los sistemas propietarios que garantice la interoperabilidad para impulsar el desarrollo de este protocolo.

---

[81] Ibíd., pág.45.
[82] CALAFAT, Cristhian. Introducción a la Tecnología Lonworks. pág. 2.
[83] GUERRERO M, José A. Diseño de una Instalación Domótica con Tecnología Lonworks. pág. 61

Figura 20. Logotipo LonWorks. (www.Lonworks.es)

8.3.1. FUNCIONAMIENTO

Lonworks mediante el protocolo estandarizado LonTalk está basada en las 7 capas del modelo OSI siendo este muy parecido a una Red de Área Local LAN, en el que los ordenadores conectados a través de otros dispositivos de red como routers, se pueden comunicar gracias al uso del Protocolo TCP/IP.[84] . Estas redes están optimizadas para el manejo de grandes cantidades de datos y la conexión de un buen número de dispositivos. Los nodos conectados se comportan como iguales entre sí, de forma que no existe el concepto de cliente-servidor.[85]

Las comunicaciones entre los dispositivos se basan en el intercambio de paquetes, siendo cada paquete un número variable de bytes que consta de las cabeceras propias de las 7 capas entre lo que se tiene, información de la dirección, tipo de servicio, los datos propiamente dichos y por último un código de detección de errores CRC de 16 bits.[86] Cada dispositivo conectado al canal observa constantemente todos los paquetes para ver si alguno lleva su dirección, si los datos llevan su dirección, el dispositivo los recibe y si es necesario responderá al dispositivo emisor con otro mensaje para hacer saber que recibió el paquete.[87]

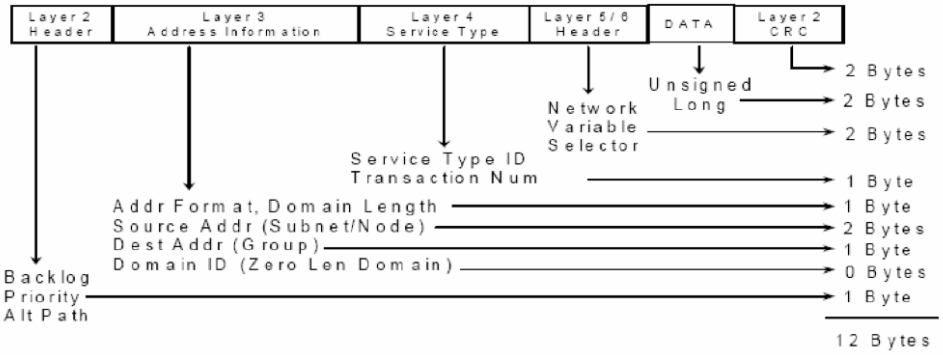


Figura 21. Paquete de Datos Lonworks (Peña, Manuel. Comunicaciones en el entorno doméstico).

[84] Ibíd., pág. 52.
[85] Ibíd., pág. 54.
[86] Ibíd., pág. 55.
[87] Ibíd., pág. 55.

8.3.2. ELEMENTOS FUNDAMENTALES

8.3.2.1. Neuron Chip

Todos los dispositivos presentes en una red Lonworks requieren de la utilización de "Neuron Chip" que sigue siendo la manera más efectiva para implementar este protocolo, pero esto no quiere decir que sea un sistema propietario, recordemos que Lonworks es un estándar abierto dentro de la ANSI/EIA 709, por lo que es de libre disposición para todo el que quiera trabajar con él o desee fabricarlo.[88]

Figura 22. Neuron 5000 Processor Neuron Chip for Lonkworks

El "Neuron Chip" está constituido internamente como tres microprocesadores en uno. Dos de los microprocesadores se encargan de ejecutar el protocolo de comunicación mencionado "LonTalk", mientras que el tercero está dedicado a ejecutar el programa de control del nodo, es decir que se encarga de la aplicación, asegurando de esta forma que la complejidad del programa no afecta negativamente en los tiempos de respuesta de la red y viceversa.[89] El 'Neuron Chip' incluye las primeras 6 capas del modelo OSI/ISO, por lo que el desarrollador sólo tiene que preocuparse del programa de aplicación.[90]

El Neuron Chip tiene un número de identificación Neuron ID asignado de fábrica único de 48 bits grabado en la memoria EEPROM que permite direccionar cualquier dispositivo en forma precisa dentro de la red Lonworks.[91] La memoria de solo lectura (ROM) del Neuron Chip presenta el sistema operativo llamado 'Neuron Chip Firmware' que incluye las especificaciones del protocolo Lonworks, la librería de funciones de Entrada/Salida (E/S)[92] como se observa en la figura 22.

[88] Ibíd., pág. 6.
[89] CALAFAT, op. cit, pág. 5.
[90] GUERRERO, op. cit, pág. 62.
[91] DURÁN, Ana. Instalación Domótica de una Vivienda Unifamiliar. pág. 48.
[92] GUERRERO, op. cit, pág. 63.

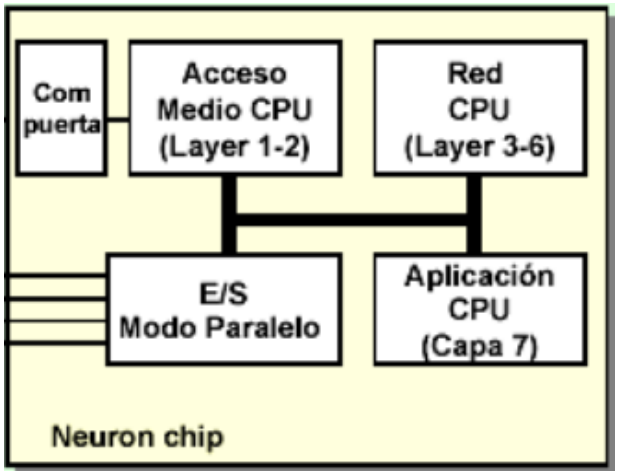


Figura 23. Componentes Neuron Chip. (Sistema Lonworks)

Un Neuron Chip inicia el intercambio de datos entre los dispositivos, gracias a que contienen la dirección de destino, información para el enrutamiento (routing), datos de control así como las instructoras de datos de la aplicación del usuario y un código detector de errores. [93]

8.3.2.2. Transductor Dispositivos emisores/receptores "LonWorks Transceivers".

Cada dispositivo de red contiene un transceptor. Estos proporcionan una interfaz de comunicación física entre un dispositivo Lonworks y una red Lonworks. Dependiendo del fabricante se ofrecen diferentes tipos de transceptores dependiendo de su conexión si es por ejemplo por par trenzado, línea de potencia o radio frecuencia.[94]

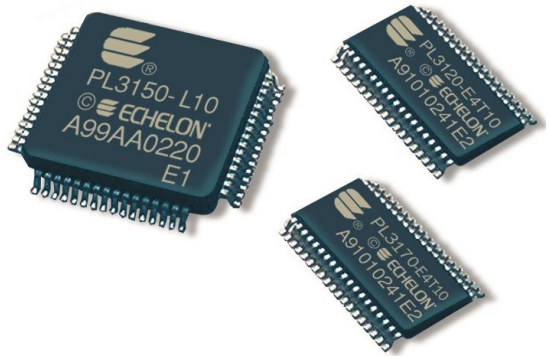


Figura 24. Transceptor Marca Echelon (http://store.echelon.com/item.asp?PID=181)

[93] DURÁN, op. cit, pág.48.
[94] GUERRERO, op. cit, pág. 64.

8.3.2.3. ARQUITECTURA DE NODO

Un nodo está compuesto por los elementos mencionados anteriormente, es decir, un Neuron Chip, un transceptor (transmisor – receptor) para unir el medio de transmisión con el nodo, además de los puertos de conexión a la red donde se conecta al medio de transmisión para efectuar la comunicación entre los dispositivos, los puertos de entrada y salida donde se conectan con los sensores o los actuadores dependiendo de la función que estén cumpliendo los circuitos integrados o nodos y las entradas para la alimentación del dispositivo. Algunos nodos dependiendo de sus características o fabricante tienen una memoria externa aparte de la que presenta el Neuron Chip, que almacena la aplicación como se plasma en la Figura 24.

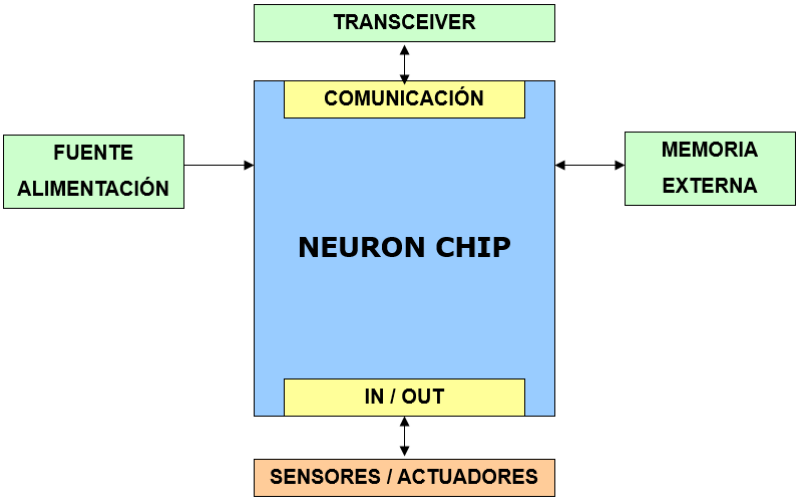


Figura 25. Arquitectura del nodo (CALAFAT, Cristhian. Introducción a la Tecnología Lonworks)

8.3.2.4. SNVT

Son Variables de red, predefinidas y estandarizadas que garantizan la interoperabilidad de distintos dispositivos LonWorks, brindando flexibilidad a los sistemas ya que existen gracias a que hay una gran cantidad de variables que se pueden controlar, citando un ejemplo tenemos, la temperatura, es decir los sensores de cada nodo miden la temperatura utilizando en SNVT correspondiente, con la unidad de medida que en este caso sería grados centígrados y un rango, para luego ser transmitido a otros dispositivos en la red.[95]

[95] Introducción a LonWorks, La Salle. pág. 17.

8.3.3. MEDIO DE TRANSMISIÓN

El sistema LonWorks se caracteriza por ser muy flexible. El modelo de comunicaciones es independiente del medio físico sobre el que funciona, de modo que los datos pueden transmitirse sobre cables de par trenzado, radio frecuencia (RF), fibra óptica, infrarrojos (IR), cable coaxial y línea de potencia PLC como se muestra en la figura 25, permitiendo la mejor solución para cada aplicación.

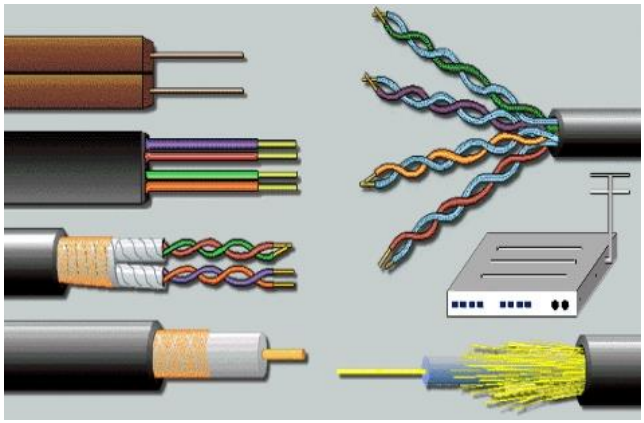


Figura 26. Variedad de Medios Físicos para la Transmisión
(http://monitorealo.blogspot.com/2012/08/medios-de-transmision.html)

Todas las topologías de red son posibles en este sistema (estrella, anillo, topología libre y línea de bus). Una red puede tener un máximo de 255 áreas con 127 nodos por área.[96]

8.4 PROTOCOLO ZIGBEE (IEEE 802.15.4)

ZigBee es considera como una tecnología inalámbrica de corto alcance y poco consumo de energía, definiéndose como la solución para aplicaciones en el hogar como automatización seguridad y confort (domótica) [97], definido como un protocolo para las redes inalámbricas de corto alcance de 10 a 75 metros, bajo consumo energético y transmisión - recepción de baja velocidad de datos operando en las bandas de los 868 MHz hasta los 2.4 GHz con velocidades de 20 a 250Kbps.[98] Desarrollando y utilizando así el uso de sensores con un muy bajo consumo energético. Alcanzando hasta 2 años con una alimentación de pilas AA. Por tanto, dichos dispositivos pasan la mayor parte del tiempo en un estado latente, es decir, en standby para consumir menos energía, hasta recibir algún tipo de señal que modifique su estado actual.[99]

---

[96] DURÁN, op. cit, pág.49.
[97] MORENO, Javier. FERNÁNDEZ, Daniel. Informe Técnico: Protocolo ZigBee, (Jun, 2007). pág.4.
[98] DIGNANI, Jorge. ANÁLISIS DEL PROTOCOLO ZIGBEE, (2011), pág.2.
[99] MORENO, op. cit, pág.4.

Gracias a todo ello, contiene las siguientes características:[100]

- Bajo consumo energético.
- Utiliza un protocolo asíncrono, half duplex y estandarizado, permitiendo a productos de distintos fabricantes trabajar juntos.
- Usar equipos con batería, a largo plazo.
- Bajo costo de dispositivos, instalación y mantenimiento.
- Alcance corto (50 metros).
- Ciclo efectivo de transmisión menor a 0.1 %.
- Velocidad de transmisión de 20 a 250Kbps.

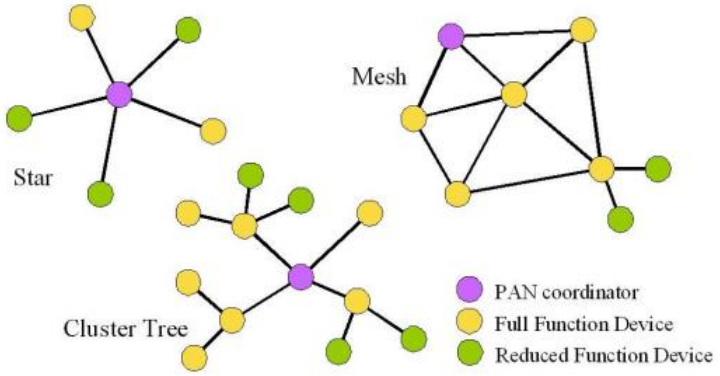
Utiliza CSMA/CA, para gestionar el acceso al medio, además del uso de TDMA para aplicaciones de baja latencia[101]. Por medio del de la banda de 2.4Ghz puede utilizar la modulación de espectro expandido DSSS, con una velocidad de transmisión de 250Kbps y a una potencia de 1mW cubriendo así cortas distancias (13 metros de radio)[102], como se puede observar en la siguiente imagen:

Potencia(mW) / Velocidad(Kbps)	1mW	10mW	100mW
28 Kbps	23m	54m	154m
250 Kbps	13m	29m	66m

Figura 27.Distancia de transmisión / Potencia (Moreno, Javier. Fernández, Daniel. 2007)

8.4.1 Nodos y topología de red

Según la topología utilizada en una red ZigBee se pueden establecer hasta 254 nodos, crear hasta 255 conjuntos/clusters de nodos con lo cual se puede llegar a tener 64.770 nodos. Las topologías de red que se pueden usar son estrella, en malla o árbol, como se puede ver a continuación[103]:



[100] DIGNANI, op. cit, pág.2.
[101] MORENO, op. cit, pág.5.
[102] Ibíd., pág.5.
[103] Ibíd., pág.6.

Figura 28.Topologías de Red ZigBee. (Moreno, Javier. Fernández, Daniel. 2007)

También permite un enrutamiento de saltos múltiples (multi-hop), que permitiendo abarcar una mayor superficie. Donde existen tres tipos de dispositivos característicos para la red ZigBee[104]:

- Coordinador
  - Uno por red.
  - Inicia la formación de la red.
  - Coordinador de PAN (Personal Area Network).
- Router
  - Se asocia con el coordinador de la red o con otro router ZigBee.
  - Puede actuar como coordinador.
  - Encargado del enrutamiento de saltos múltiples de los mensajes (multi-hop).
- Dispositivo final
  - Elemento básico de la red.
  - No realiza enrutamiento.

Teniendo en cuenta estos tres tipos de dispositivos característicos se puede realizar una configuración de red como la siguiente:

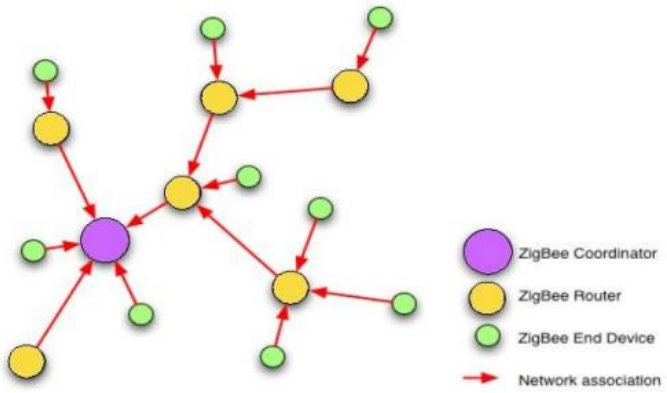


Figura 29.Red ZigBee. (Moreno, Javier. Fernández, Daniel.2007)

Otro punto importante de la red ZigBee es el soporte y la disponibilidad sin importar su topología, ya que si se presenta la caída de cualquier nodo, esta busca rutas alternativas para el intercambio de información[105].

La pila de arquitectura ZigBee consta de varios componentes en capas como IEEE 802.15.4 , entre las que se encuentran la capa de Control de Acceso al Medio (MAC), la capa física (PHY) y la capa de red Zigbee (NWK), para lo cual será necesario su estudio, como:

[104] Ibíd., pág.6.

[105] Ibíd., pág.7.

8.4.2 Características generales de 802.15.4[106]

Entre las características más importantes se pueden mencionar:

- Funcionamiento en las bandas de 2.4GHz como en la de 868/915MHz.
- Tasa de transmisión de hasta 250 kbps en la banda de 2.4 GHz.
- Optimizado para aplicaciones con ciclo efectivo menor a 0.1 %.
- Usa CSMA-CA para acceso de canal.
- Produce alto rendimiento y baja latencia para dispositivos de bajo ciclo de trabajo.
- Baja potencia.
- 64 bits de direccionamiento para una gran cantidad de dispositivos.
- 16 bits para identificar redes (65536 redes).
- Permite el uso de ranuras de tiempo (time slots) para aplicaciones de baja latencia.
- Protocolo con handshake (diálogo) para mejorar la seguridad en las transferencias.
- Rangos de corto alcance.

8.4.3 Tipos de tráfico

Las aplicaciones usadas en el protocolo ZigBee se pueden clasificar según[107]:

- **Datos periódicos (continuo):** La aplicación define una tasa de datos. Es un caso típico de sensores en donde por ejemplo un sensor necesita transmitir en periodos de tiempo cortos (10 segundos).
- **Datos intermitentes (por eventos):** En este caso la aplicación junto a los dispositivos responden a estímulos externos y definen la tasa de datos. Como en un sistema domótico, los interruptores de luces transmiten solo ante un cambio. Mientras tanto están desconectados (Standby) y consumiendo una energía de batería mínima.
- **Datos periódicos con comunicación garantizada (GTS) (Guaranteed time slot):** Aplicaciones de baja latencia que requieren comunicación libre. Es un método de calidad de servicio que garantiza la atención por un cierto Δt dentro de un período, llamado Supertrama. Donde se provee un modo de trabajo denominado “con baliza” que sirve como multiplexación temporal para la comunicación.

El estándar 802.15.4 define 2 tipos de dispositivos con el objeto de minimizar el costo del sistema[108]:

[106] DIGNANI, op. cit, pág.7.
[107] Ibíd., pág.7.
[108] Ibíd., pág.7.

a) **FFD (Full Function Device):** Dispositivos capaces de funcionar en cualquier topología, pueden ser coordinadores de red. Este tipo de dispositivo puede dialogar con cualquier otro, Requerido mínimo uno por red.
b) **RFD (Reduced Function Device):** Son dispositivos de baja complejidad con bajo procesamiento y memoria. Miembros de una red con topología estrella. Establecen comunicación únicamente con el coordinador de red.

Distintas topologías de red con dispositivos FFD y RFD:

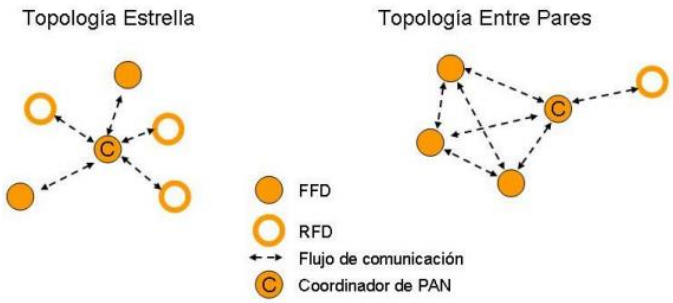


Figura 30.Topologías en IEEE 802.15.4 (DIGNANI, 2011)

Modos de direccionamiento:

Todos los dispositivos tienen direcciones de 16 hasta 64 bits.[109]. "En cuanto a seguridad, Utiliza la encriptación AES de 128bits, que le permite la autentificación y encriptación en las comunicaciones. Además, de existir un Trust Center (Centro de validación) que proporciona un mecanismo de seguridad como la clave de enlace y la clave de red".[110]

8.4.4 La pila de arquitectura ZigBee

Cuenta con 7 capas pero ZigBee usa solo 4 capas para el desarrollo de una red de baja transmisión y consumo. En cuanto a la capa física (PHY) y la capa de acceso al medio (MAC) son las definidas por el estándar IEEE 802.15.4. Las capas de red (NWK) y de aplicación (APL) están definidas por el protocolo ZigBee. Conectadas con las capas adyacentes por medio de un SAP (Service Access Point), una capa superior que permite el requerimiento de un servicio a una capa inferior[111], Además de la capa ZDO (Zigbee Device Objects), donde se encuentran los objetos de aplicación definidos para este protocolo[112].

[109] Ibíd., pág.8.
[110] MORENO, op. cit, pág.8.
[111] DIGNANI, op. cit, pág.9.
[112] MORENO, op. cit, pág.8.

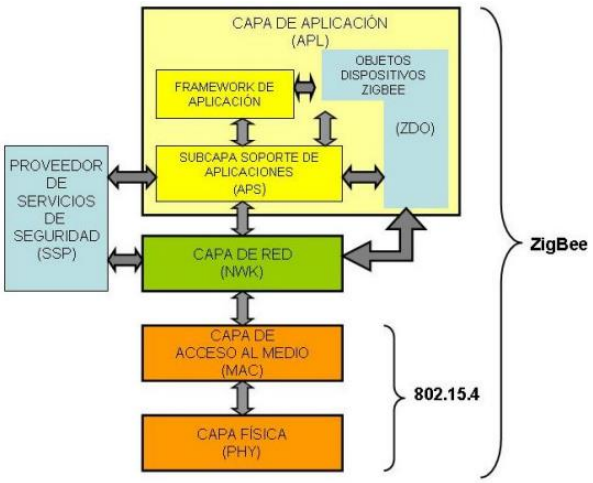


Figura 31.Capas modelo 802.15.4 y ZigBee. (DIGNANI, 2011).

8.4.5 Capa Física

Define las funciones y la relación con la capa MAC, además de aspectos como la potencia del transmisor - receptor y su sensibilidad. Encargada de[113]:

8.4.5.1 Asignación de canales

Donde se definen canales y cada uno de ellos representa una frecuencia. Además de introducir el concepto de página para permitir la incorporación de nuevas formas de tecnologías a la capa física[114].

Nº de página	Nº de Canal	Descripción
0	0	868 MHz. (BPSK)
	1-10	915 MHz (BPSK)
	11-26	2.4 GHz (O-QPSK)
1	0	868 MHz (ASK)
	1-10	915 MHz (ASK)
	11-26	Reservado
2	0	868 MHz (O-QPSK)
	1-10	915 MHz (O-QPSK)
	11-26	Reservado
3-31	Reservado	Reservado

Figura 32.Asignación de canales. (DIGNANI, 2011).

8.4.5.2 Numeración de canales

Cada canal se identifica con un número de canal, y número de página. Se asigna a la banda de 868 MHz con frecuencia central en 868.3 MHz; la frecuencia central del canal de 915MHz se obtiene de la siguiente forma.[115]

[113] DIGNANI, op. cit, pág.9.
[114] Ibíd., pág.10.
[115] Ibíd., pág.10.

FREC. central [Mhz]= 906 + 2 * (Nº canal -1)
Con 1 ≤ Nº canal ≤ 10

Para la banda de 2.4 GHz la frecuencia central se calcula:

Frecuencia central [MHz]= 2405 + 5 * (Nº canal -1)
Con 11 ≤ Nº canal ≤ 26

Figura 33. Calculo Frecuencia Central. (DIGNANI, 2011).

8.4.5.3 Detección de energía

Antes de realizarse la transmisión en un canal, el dispositivo debe medir el nivel de energía para ese canal. Para ello se cambia a modo de recepción y calcula valor medio de las medidas que corresponden a la duración de 8 símbolos; indicando si el canal está ocupado. La sensibilidad del receptor se define como la energía mínima necesaria de la señal entrante que permita ser detectada y demodulada con un error en los paquetes menor al 1 %. Admitiendo una diferencia de 10dB de sensibilidad del receptor y el nivel mínimo de energía detectable. La capa física provee el servicio de detección de energía en un canal determinado y lo envía a la MAC por medio de una trama de 8 bits.[116]

8.4.5.4 Sensado de Portadora (CS) (Carrier Sense)

Consiste en demodular la señal recibida para determinar si esta es compatible con el estándar, y considerarlo ocupado solo cuando hay una señal compatible.[117]

8.4.5.5 Indicador de calidad del enlace (LQI) (Link Quality Indicator)

Indica la calidad de los paquetes recibidos por el receptor. Se puede determinar por la intensidad de señal ó la relación señal ruido, cuanto más alta sea esta relación habrá más garantía de que el mensaje llegue a destino. El LQI puede ser usado en una red ZigBee como mecanismo de ruteo en una malla, para elegir las rutas de LQI más alto. Pero también teniendo en cuenta el gasto de energía de las baterías y la cantidad de que intervengan.[118]

8.4.5.6 Evaluación de canal libre (CCA) (Clear Channel Assessment)

El mecanismo CSMA-CA hace que la MAC le pida a la capa Física que haga una evaluación del canal para saber si esté se encuentra libre. Es allí donde opera la CCA, en los siguientes modos:[119]

- Modo 1: Se usa el nivel de energía y un umbral a partir del cual el canal está ocupado.

[116] Ibíd., pág.10.
[117] Ibíd., pág.11.
[118] Ibíd., pág.11.
[119] Ibíd., pág.11.

- Modo 2: Se usa el nivel CS para determinar la ocupación del canal.
- Modo 3: Combinación AND u OR de los 2 modos anteriores.

AND: La energía pasa de un umbral Y la señal cumple con el estándar

OR: La energía supera a un umbral O es censada una señal que cumple con el estándar.

8.4.5.7 Concepto de cliente – servidor entre capas

La capa superior usa un servicio de puntos de acceso (SAP) para requerir servicios de la capa inferior; dicha capar da la confirmación de la transmisión exitosa a la capa superior, realizando 3 etapas para su comunicación, que son: Pedido, Confirmación, Respuesta e Indicación.[120]

8.4.5.8 Interface entre capa Física y MAC

En la siguiente figura se muestra las 2 capas (Phy- Mac) con 2 bloques SAP: Un SAP de datos (PD-SAP) y un SAP administrativo (PLME-SAP) que comunica a la administración de la capa física (PLME) con la administración de la capa MAC (MLME). Los datos recibidos en el receptor pasan a la MAC a través del PD-SAP, realizando así la comunicación entre las capas.[121]

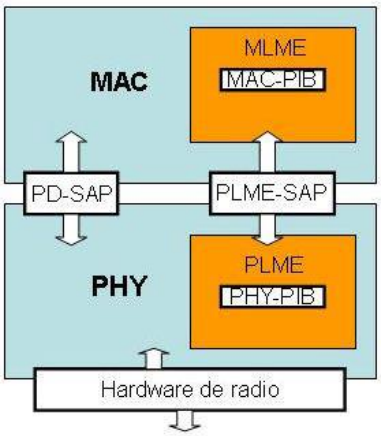


Figura 34.Interface de servicio de datos y de manejo entre capas Física y Control de Acceso al medio (DIGNANI, 2011)

8.4.5.9 Área Datos de la capa Física (PPDU: Physical PDU)

Para el caso de la transmisión de datos a otro dispositivo, estos provienen desde el área datos de la capa MAC, donde la MAC local genera el pedido de servicio, la capa física intenta satisfacerlo y responde indicando el resultado (transmisión exitosa ó fallida[122]. Para el caso de la recepción, la unidad de datos de la capa física

[120] Ibíd., pág.11.
[121] Ibíd., pág.12.
[122] Ibíd., pág.14.

envía un aviso de la llegada de datos a la capa MAC. Además de enviar datos relacionados con la calidad del enlace (LQI).[123]

8.4.6 Capa MAC de 802.15.4

Crea una interface entre la capa física y la capa de red y se compone de especificaciones para las capas PHY y MAC. En la siguiente figura, se ve el modelo de referencia con la subcapa MAC entre PHY y NWK. Conformada por la MLME que es la encargada de manejar los servicios y una unidad de datos e interactúa con la NLME y PLME por medio de las SAP. Además de poseer una base de datos llamada MAC-PIB.[124]

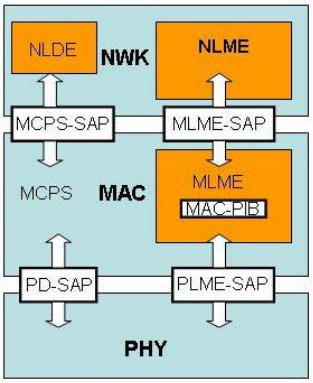


Figura 35.Interfaces de la capa MAC. (DIGNANI, 2011).

8.4.6.1 Operación de la PAN usando balizas

El uso de balizas en la red permite disponer de ranuras de tiempo garantizadas (GTS). Para eso se crean tramas especiales MAC llamada tramas de baliza permitiendo usar una supertrama.[125] Que tiene tres tipos de períodos: Período de acceso en contienda (CAP), período libre de contiendas (CFP) y período inactivo.

Los nodos que quieran realizar una comunicación durante el período CAP deben usar CSMA-CA para acceder a un canal que esté disponible, El primero que lo encuentre libre lo usará y lo tendrá disponible hasta que cese su transmisión. Si el dispositivo encuentra el canal ocupado, iniciará un período de espera aleatorio (back off) e intentará nuevamente usarlo, pero no hay una garantía para que el dispositivo pueda usar el canal en el momento en que lo necesita pues está en competencia con los otros dispositivos que conforman la red.[126]

[123] Ibíd., pág.14.
[124] Ibíd., pág.14.
[125] Ibíd., pág.15.
[126] Ibíd., pág.15.

8.4.6.2 Espaciado entre tramas

Es una espera que hace el transmisor entre tramas para que el receptor tenga tiempo de procesarlas, conocido como IFS (Interframe spacing). De acuerdo al largo del MPDU se realiza un IFS corto (SIFS: Short IFS) o largo (LIFS: Long IFS). Donde existen dos formas de comunicación entre emisor y receptor del mensaje, esto es comunicación con confirmación (ACK) o sin confirmación.[127]

8.4.6.3 CSMA-CA

Cuando un dispositivo desea transmitir, previamente verifica que el canal no esté en uso por otro dispositivo. Si está libre comienza a transmitir. Hay transmisiones que se hacen sin verificación previa. Estas son:

- Transmisión de balizas
- Transmisión durante el período CFP
- Transmisión después de ACK a un comando de pedido de datos.

El uso del CSMA-CA tiene en cuenta si la red está trabajando con supertrama, es decir que el tiempo activo se divide en 16 ranuras iguales, entonces el tiempo de back off debe ser sonorizado con el CAP (CSMA-CA ranurado); o cuando no se trabaja con supertrama, no se necesita sincronizar el back off (CSMA-CA no ranurado). [128]

8.4.6.4 Problemas del nodo oculto y del nodo expuesto.

"El algoritmo de CSMA-CA tiene problemas cuando aparece un nodo oculto. Si los nodos A y C están fuera de alcance entre ellos pero existe un nodo B que puede comunicarse tanto con A como con C. Entonces cuando A transmita algo a B, el nodo C no enterará. Análogamente cuando C transmita a B, A no lo recibirá. Si por alguna razón transmiten A y C en el mismo canal y en el mismo momento, esto creará una colisión de paquetes en B. Una forma de resolver este problema es aumentando la potencia en los nodos A y C de modo que A reciba a C y viceversa"[129].

[127] Ibíd., pág.16.
[128] Ibíd., pág.16.
[129] Ibíd., pág.16.

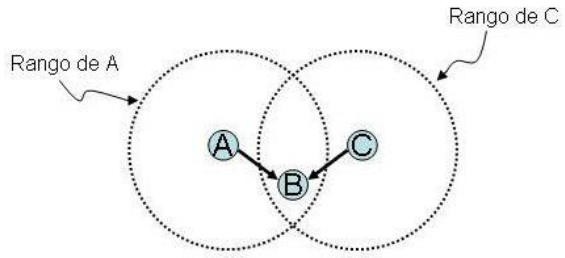


Figura 36.Nodo oculto. (DIGNANI, 2011).

8.4.6.5 Servicios de MAC

La MAC está compuesta principalmente por el área de datos (MCPS) encargada de la comunicación de información hacia las capas vecinas de red y física y el área de manejo (MLME) o a parte de control encargada de recibir los comandos desde la capa de red y decodificarlos, también para la capa física[130].

8.4.6.5.1 Servicios de Asociación y Desasociación

La asociación es el proceso mediante el cual un dispositivo se une a una red. La capa de red (NWK) es la que maneja la formación de la red e instruye a la capa MAC para hacerlo. Donde se utilizan 4 capas primitivas, como:

- MLME-Associate.request
- MLME-Associate.indication (opcional para RFD)
- MLME-Associate.response (opcional para RFD)
- MLME-Associate.confirm

La capa de red hace el pedido al coordinador de red para unirse, en ese pedido le se especifica si es un dispositivo FFD ó RFD, la capa MAC del dispositivo hace el pedido hasta que llega hasta la MAC del coordinador (pasando por la capa física); El proceso de desasociación puede ser originado por el dispositivo que quiere irse de la red ó bien por el coordinador que desea expulsar al dispositivo. [131].

8.4.6.5.2 Servicio de Notificación de Baliza

Cuando la capa MAC recibe una señal de baliza, la MLME manda todos los parámetros a la capa de red indicando el LQI y el tiempo en que se recibió[132].

[130] Ibíd., pág.17.
[131] Ibíd., pág.18.
[132] Ibíd., pág.19.

8.4.6.5.3 Servicio de Habilitación y deshabilitación del receptor

La capa de red puede pedir que se habilite el receptor durante un cierto intervalo. Opcional tanto para FFD como RFD y así poder crear una comunicación o acceso de nuevos dispositivos a la red[133].

8.4.6.5.4 Servicio para generar GTS cuando se trabaja en modo baliza

Se utiliza para reservar ranuras de tiempo cuando se trabaja en modo baliza[134].

8.4.6.5.5 Servicio de Reset

Resetea a la capa MAC llevando los parámetros a los valores por defecto de la PIB[135].

8.4.6.5.6 Servicio de Arranque

Arranca a la capa MAC e inicializa el dispositivo. Utilizado generalmente después del reset[136].

8.4.6.5.7 Servicio de Notificación de orfandad

Un dispositivo debe pertenecer a una red para poder establecer una comunicación con otros. Cuando el dispositivo se desacopla de la red sin el proceso de desasociación se lo considera huérfano. Cuando la capa de red recibe repetidas fallas en la comunicación ó no recibe ACK (Confirmación), concluye que está huérfana. En ese caso instruye a la MAC a resetearse e intentar una nueva asociación ó bien iniciar un nuevo procedimiento de acople de dispositivo. Que consiste en el uso de una trama broadcast para encontrar a sus “padres”. Si el coordinador lo tenía registrado lo reacopla a la red[137].

8.4.6.5.8 Servicio de Barrido de Canales

Es un servicio de la MAC para darle información a la capa de red, sobre la actividad que se realiza sobre esta. Hay 4 tipos de barridos:

- Barrido de energía: Con esto determina la energía de cada canal.
- Barrido de nodo huérfano: Cuando el nodo está huérfano trata de encontrar a qué PAN está asociado enviando una notificación en cada canal y esperando que le contesten en alguno.

---

[133] DIGNANI, op. cit, P.19.

[134] Ibíd., pág.19.
[135] Ibíd., pág.20.
[136] Ibíd., pág.20.
[137] Ibíd., pág.20.

- Barrido activo: El dispositivo manda una trama de baliza y espera respuesta. Utilizada por los coordinadores para para descubrir los identificadores que se están usando en su área.
- Barrido pasivo: Similar al caso anterior pero no hay una señal previa de baliza[138].

8.4.6.5.9 Servicios de Sincronismo y notificación de Pérdida de Sincronismo

Cuando se trabaja con baliza el dispositivo debe sincronizarse al coordinador. Entonces enciende el receptor en determinado momento justo antes del comienzo de la baliza. Si no escucha la baliza en un cierto intervalo entonces la capa de red le ordenará a la MAC que informe al coordinador de la pérdida de sincronismo[139].

8.4.6.5.10 Formato de la trama MAC

Hay 4 tipos de tramas MAC: de baliza, de dato, de confirmación (ack) y de comando. Todas las tramas contienen esencialmente 3 partes: un encabezado (MHR), una carga útil (payload) y un pie (MFR). El encabezado contiene información sobre el tipo de trama, campos de direcciones y banderas de control. La carga útil tiene un largo variable y contiene comandos o datos. El MFR contiene una secuencia de chequeo (FCS) para verificar los datos basada en CRC[140].

8.4.6.6 Responsabilidades de la capa MAC

Las responsabilidades de la capa MAC se puede resumir como:

- Puede generar balizas si es coordinador.
- Usa CSMA-CA como método de compartir el canal.
- Provee el manejo, sincronización y GTS cuando se usa balizas.
- Provee un enlace seguro entre las MACs de dos dispositivos.
- Provee servicios de asociación y desasociación.
- Provee un mecanismo de seguridad cuyo nivel estará determinado por lo solicitado desde las capas superiores[141].

8.4.7 Capa de Red ZigBee

La capa de red provee funciones para el armado y manejo de redes además de una interfaz simple para el uso de aplicaciones. Al igual que las otras capas provee 2 tipos de servicios: de datos a través de la NLDE y de control por medio de la NLME. Cada una de estas entidades se comunica con sus homólogas en las capas MAC y APL por medio de los respectivos puntos de acceso (SAP). La capa de red tiene

[138] Ibíd., pág.21.
[139] Ibíd., pág.21.
[140] Ibíd., pág.21.
[141] Ibíd., pág.22.

sus propios atributos y constantes que se guardan en una base de datos (NIB) dentro del NLME[142].

La capa de red del coordinador asigna direcciones de 16 bits a cada miembro de la PAN. Esa dirección asignada esta capa debe ser idéntica a la dirección de la MAC 802.15.4. Además de llevar la cantidad de saltos máximos que esta puede llegar a realizar, decrementando en uno en cada salto; cuando llega a cero, esa trama no será retransmitida a otro dispositivo.[143]

8.4.7.1 Tipos de nodos ZigBee

El estándar especifica 3 tipos de nodos que pueden estar en una red: coordinador, ruteador y dispositivo final.[144]

8.4.7.1.1 Coordinador

Es obligatoria la presencia de uno que actúa como nodo raíz en la topología árbol y es responsable de:

- Arranque de la red.
- Configuración de la red.
- Admisión de nodos a la red.
- Asignación de direcciones de red.

El coordinador requiere de un dispositivo de función completa (FFD) ya que necesita más potencia de cómputo. También es importante que la fuente de alimentación sea permanente y segura ya que este dispositivo nunca entrará en modo “Standby”.[145]

8.4.7.1.2 Ruteador

Es un nodo de tipo FFD que extiende la cobertura de la red y aumenta la confiabilidad con la creación de rutas adicionales de datos.[146]

8.4.7.1.3 Dispositivo final

Estos nodos se comunican con un nodo ruteador ó un nodo coordinador. Estos nodos tienen menos potencia de cómputo y usualmente son alimentados a batería y son de tipo RFD.[147]

8.4.7.2 Topologías

ZigBee usa las topologías de IEEE 802.15.4 para la transferencia de datos pro medio de diferentes topologías. Debido al poco alcance de cada nodo, frecuentemente un paquete debe ser retransmitido varias veces por intermedio de ruteadores. Pero el ruteo en cualquier topología usada se hace en la capa de red y

[142] Ibíd., pág.23.
[143] Ibíd., pág.23.
[144] Ibíd., pág.23.
[145] Ibíd., pág.24.
[146] Ibíd., pág.24.
[147] Ibíd., pág.24.

entonces no es necesaria ninguna programación adicional en la capa su aplicación[148].

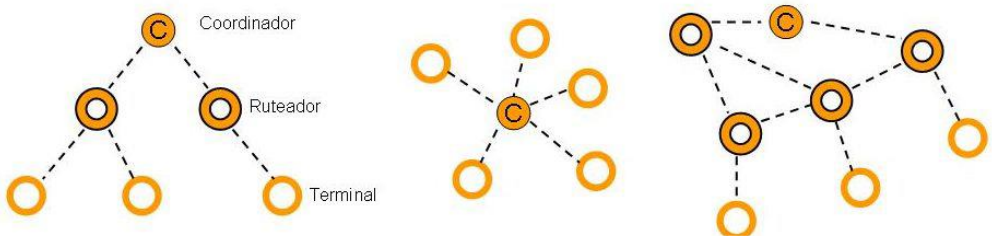


Figura 37.Topologías ZigBee (Árbol, Estrella, Malla). (DIGNANI, 2011).

8.4.7.2.1 Características Topología árbol[149]:

- Los nodos ruteadores pueden tener nodos adicionales “hijos”.
- Hay comunicación directa solo a través de la relación padre-hijo.
- Ruteo jerárquico con un único camino posible entre 2 nodos.

8.4.7.2.2 Características Topología estrella[150]:

- Un coordinador con uno ó varios nodos adicionales “hijos”.
- El rango de la red está limitado al rango de transmisión del coordinador.
- La red es fácil de configurar.
- El coordinador es el único nodo que rutea paquetes.

8.4.7.2.3 Topología malla

Es una extensión de la topología de comunicación entre pares (peer to peer). Características[151]:

- Los nodos ruteadores pueden tener nodos hijos.
- Comunicación directa entre dos nodos FFD siempre que estén separados a una distancia menor al rango de transmisión entre ellos.
- Los nodos terminales solo pueden intercambiar datos con sus respectivos nodos padres.
- Es posible el ruteo dinámico (gasto energético, tiempo, seguridad y confiabilidad).

[148] Ibíd., pág.24.
[149] Ibíd., pág.25.
[150] Ibíd., pág.24.
[151] Ibíd., pág.27.

8.4.7.2.4 Relación padre-hijo

Los ruteadores y dispositivos finales se asocian con nodos presentes en la red. El nodo hijo es el que recientemente ha entrado en la red. El nodo padre es el nodo que le ha dado al hijo acceso a la red[152].

8.4.7.2.5 Propiedades de la relación padre-hijo[153]:

- Solo pueden ser padres el nodo coordinador ó los nodos ruteadores.
- El nodo hijo tiene solo un padre.
- Un hijo puede cambiar de padre.
- Se usa la jerarquía ZigBee.

8.4.7.3 Parámetros para configurar la red ZigBee

- Número máximo de hijos directos: Es la máxima cantidad de ramas que puede tener cada nodo.
- Direccionamiento de nodos: Cada nodo que entra a una red recibe una dirección de 16 bits. Esta dirección se usa en comunicaciones a nivel red.
- Cada ruteador sabe cómo encaminar cada mensaje hacia su destino comparando su propia dirección con la del destino.[154].

8.4.7.4 Mecanismos de ruteo

"En el algoritmo implementado en la capa de red hay un balance entre costo por unidad, gasto de batería, complejidad de implementación para lograr una relación costo desempeño adecuada a la aplicación. Un algoritmo muy utilizado por su simplicidad y bajo requerimiento de procesamiento es el AODV (Ad hoc On-Demand distance Vector). En AODV los nodos mantienen una tabla de ruteo para los destinos conocidos. En el comienzo esta tabla la integran sus vecinos. Solo se agrandará la tabla cuando aparezca algún nodo con camino desconocido. En este caso se envía mensajes de descubrimiento que se propagan entre los nodos hasta llegar al destino. Desde el destino se inicia el camino inverso hasta llegar al nodo origen. Todos los nodos actualizarán sus tablas"[155].

8.4.7.5 Responsabilidades de la capa de red

Las tareas más importantes de la capa de red son[156]:

- Establecer una nueva red por medio de diferentes topologías.
- Agregar o quitar a un dispositivo a/de la red.
- Garantizar la comunicación dentro de toda la red más allá del alcance de un único nodo.

---

[152] Ibíd., pág.25.
[153] Ibíd., pág.25.
[154] Ibíd., pág.25.
[155] Ibíd., pág.27.
[156] Ibíd., pág.27.

- Configurar a un nuevo dispositivo para que pueda operar en la red.
- Asignar direcciones de red a los dispositivos.
- Sincronización entre dispositivos usando balizas.
- Proveer seguridad.
- Rutear tramas a sus destinos (ruteo dinámico).

8.4.8 Capa de Aplicación

Consiste en la subcapa APS (Application Support) y la ZDO (ZigBee Device Object). Encargada de mantener las tablas para los enlaces y balancear o adaptar los dispositivos entre ellos basados en los servicios y necesidades. Cada subcapa se puede definir con[157]:

- APS: trata de descubrir también a otros dispositivos que están operando en su mismo espacio operativo.
- ZDO: Define el rol de un dispositivo dentro de la red.

En esta capa se inicia o responden pedidos de enlace estableciendo una relación segura entre los dispositivos que conforman la red, además de seleccionar un método de seguridad[158].

8.4.8.1 Subcapa de soporte de aplicación (APS)

"Proporciona un interfaz entre la capa de red y la capa de aplicación por medio de los servicios que se utilizan junto a los ZDO, ofrecidos por la entidad de datos APS (APSD) a través del servicio de punto de acceso APSDE (APSDE-SAP) proporcionando el servicio necesario para la transmisión de datos y el transporte de datos de aplicación entre dos o más dispositivos en la misma red y la entidad gestora del APS (APSME-SAP) a través de un servicio que ofrece el punto de acceso que proporciona el servicio de descubrimiento, enlace de dispositivos y mantiene una base de datos de los objetos llamado "APS Information Base (AIB)""[159].

8.4.8.1.1 Servicios

- **Descubrimiento:** Determina qué otros dispositivos operan en el espacio del dispositivo (POS).
- **Enlace:** Enlaza los dispositivos basados en sus servicios, necesidades y comunicación entre ellos.

La capa de aplicación es la que se encarga de las aplicaciones específicas de los usuarios, facilitando su desarrollo por medio de interfaces a la capa RED.

---

[157] Ibíd., pág.27.
[158] Ibíd., pág.27.
[159] MORENO, op. cit. pág.9.

- **Perfiles**

En esta capa existen perfiles que se realizaron con el fin de unificar el intercambio de datos y caracteriza el formato de los mensajes, acciones y funciones que se usarán en ciertas aplicaciones. Los perfiles pueden ser, perfiles públicos y privados.

- **Enlace:**

Es un procedimiento en el que se realiza la conexión virtual entre puntos finales de aplicación. Los enlaces pueden ser:

- Uno a Uno: punto a punto, sensor que se conecta a un nodo central.
- Muchos a Uno: Ejemplo: muchos sensores del mismo tipo se conectan a la misma central.
- Uno a muchos: como un interruptor que controla muchas luces dentro de la red.

8.4.8.2 Objetos de dispositivos ZigBee (ZDO)

Los ZDO representan "una interfaz entre los objetos de aplicación, el perfil del dispositivo y el APS. Los ZDO se encuentran entre el framework de aplicación y la subcapa de soporte de aplicación. Permite así que se cumplan todos los requisitos de las aplicaciones que operan con la pila de protocolo ZigBee. Los ZDO son responsables de"[160]:

- Inicializar la subcapa de soporte de aplicación (APS), y la especificación de servicios.
- Descubrimiento de dispositivos
- Gestión de seguridad,
- Red y enlace.

Los ZDO proporcionan interfaces públicas en la capa del framework de aplicación para tener el control del dispositivo y realizan la gestión de direcciones de los dispositivos que se encuentran dentro de la red ZigBee, así como, el descubrimiento, el enlace (binding) y las funciones de seguridad[161].

Los ZDO creados para simplificar el manejo de la red por las aplicaciones, contienen perfiles de dispositivos ZigBee (ZDP: ZigBee Device Profile) que permiten el manejo de la red. De tal forma que puede proveer un conjunto de comandos y respuestas para[162]:

- Realizar una exploración del canal.
- Descubrir dispositivos.
- Manejo de la potencia de transmisión.

[160] Ibíd., pág.12.
[161] Ibíd., pág.13.
[162] DIGNANI, op. cit, pág.29.

8.4.9 Seguridad

8.4.9.1 Seguridad en ZigBee

ZigBee soporta el uso de protocolos de encriptación y autenticación, por lo que en el diseño de la red se debe tener en cuenta la relación entre seguridad, complejidad y costo de los dispositivos ya que mejorar el nivel de seguridad requiere más capacidad de procesamiento, memoria que aumenta el gasto energético[163].

ZigBee utiliza AES (Advance Encryption Standard) como técnica de encriptación. Un punto fundamental es el mecanismo por el cual cada dispositivo obtiene la clave, como[164]:

a) Preinstalación: El fabricante embebe la clave en el dispositivo y el usuario puede seleccionar luego alguna de estas.
b) Transporte de clave: El dispositivo pide a un servidor él envió de una clave.
c) Establecimiento de clave sin comunicación: Es un método de generar claves al azar para dos dispositivos sin necesidad de comunicarlos. Basado en el protocolo SKKE (Symmetric-Key Key Establishment). Los dispositivos destino de la clave ya tienen que tener una clave común por medio de a) ó b).

La principal limitación que existe en la implementación de mecanismos de seguridad para las topologías ZigBee, es la escasez de los recursos. Los nodos en su mayoría son alimentados a batería, teniendo así poco procesamiento y poca memoria, ya que son de bajo costo; delimitando así la capacidad de su seguridad. Agregando un poco más de complejidad a los dispositivos se puede lograr una defensa contra la lectura directa de información sensible; Teniendo 2 modos de operación[165]:

- Modo comercial: en este modo mantiene una lista de dispositivos, claves maestras, claves de enlaces y claves de red. El espacio de memoria requerido aumenta con la cantidad de dispositivos en la red.
- Modo residencial: La única clave que es obligatoria mantener en el centro de confianza es la clave de red.

En la red ZigBee cada capa del protocolo (APS, NWK y MAC) es responsable de la seguridad de las tramas iniciadas en esa capa. Por simplicidad se usa una misma clave para todas las capas[166].

8.4.9.2 Autenticación

ZigBee soporta autenticación de dispositivos y de datos. El propósito de la autenticación de datos es asegurar que los mismos sean válidos y que no se hayan modificado de alguna forma. Para eso el transmisor incluye un código especial

[163] Ibíd., pág.29.
[164] Ibíd., pág.29.
[165] Ibíd., pág.29.
[166] Ibíd., pág.30.

ZigBee llamado Código de Integridad de Mensaje (MIC), que se genera con un método conocido por emisor y el receptor. Cuando recibe el mensaje el receptor calcula el MIC y si éste coincide con el que envía el transmisor, el mensaje se considera auténtico. El nivel de seguridad en el control se incrementa con el número de bits del MIC.

ZigBee y 802.15.4 soportan MIC de 32, 64 y 128 bit con la posibilidad de encriptación de mensajes. EL MIC se genera usando el protocolo CCM que se utiliza junto a AES de 128 bits y comparten la misma clave de seguridad y así lograr autenticación y encriptación del mensaje[167].

La AES-CCM posee 3 entradas: los datos, la clave y la cadena especial de 13 bytes construido a partir de datos de un header auxiliar, que contiene bits de control de seguridad, bits del contador de trama (frame) y el campo dirección fuente de un encabezado auxiliar. El AES lo usa como parte del algoritmo puesto que no se repite para dos mensajes transmitidos con la misma clave porque se va incrementando el contador de trama, impidiendo así el uso mal intencionado o captación de la trama de datos dentro de la topología ZigBee[168].

8.5 SISTEMAS RFID, COMO BASE DEL IoT

Actualmente los sistemas de identificación por radio frecuencias están trabajando en frecuencias distintas, las cuales presentan unas serie de ventajas y desventajas, lo que hace necesario analizar la aplicación y su mejor adaptación a las condiciones exigidas.

8.5.1 FRECUENCIAS DE FUNCIONAMIENTO RFID.

Según Alan Gidekel las bandas de operación caracterizadas son[169]:

- *125 KHz, operando en la banda de LF (low frequency)*, es el sistema menos susceptible a los líquidos y metales, su velocidad de comunicación es baja, lo que lo hace deficiente para operar en entornos donde haya más de un tag presente en el campo de la antena. Su rango máximo de lectura no supera los 50cms y su utilización más frecuente está asociada a controles de accesos, identificación de animales, y control antirrobo.[170]

- *13.56 MHz, utiliza la banda de HF (High frequency),* su respuesta en presencia de fluidos es aceptablemente buena, la velocidad de comunicación

[167] Ibíd., pág.30.
[168] Ibíd., pág.30.
[169] Alan Gidekel, Introduccion a la identificación por radio frecuencia, Revista Telectronica, Universidad de Palermo, ISBN 987-23017-0-0.
[170] Ibíd., pág.76.

es buena para sistemas de baja velocidad, su rango máximo de lectura es alrededor de un metro, y sus principales aplicaciones se encuentran en bibliotecas, identificación de contenedores y equipaje aeroportuario.[171]

- *868 - 928 MHz, opera en la banda de UHF (ultra high frequency)*, sus principales problemas se encuentran en la interferencia provocada por metales y líquidos. Otro punto inconveniente es la imposibilidad de estandarizar la frecuencia operativa, dado que cada país legisla esta banda con distintas limitaciones. Entre sus puntos positivos está el rango de lectura que alcanza hasta 9 metros, muy superior a las demás frecuencia. Su velocidad de lectura que alcanza los 1200 Tags/seg y el bajo costo de los tags para esta frecuencia de operación. Sus principales aplicaciones se encuentran en la cadena de abastecimientos, tele-peajes e identificación de objetos y equipajes, instrumentación de procesos, y control de antifalsificacion.[172]

- *2.4 - 5.8 Ghz, trabaja en la banda de UHF*, si bien su velocidad de transmisión es buena, su rango de lectura no es mayor a 2 metros. Este tipo de sistemas no se encuentran muy difundidos y su aplicación principal se encuentra en sistemas de peaje y rastreo de vehículos. Sin embargo muchos dispositivos operan en esta banda de frecuencias y abre la puerta a su uso para los protocolos orientados al control de objetos inteligentes.[173]

La frecuencia de operación del Tag, y de los lectores condiciona las características físicas de propagación del campo electromagnético y, por tanto, las de la transmisión. Estas características incluyen el tipo de acoplamiento, distancia máxima de lectura, velocidad de transmisión, sensibilidad a los materiales. Según la banda de frecuencias utilizada en la transmisión, la comunicación entre lector y antena se realiza de dos formas distintas, el acoplamiento inductivo (Inductive Coupling), y el acoplamiento capacitivo (*Passive Backscatter*) [174].

El acoplamiento inductivo. Se usa tanto para comunicaciones a baja frecuencia (LF) como a alta (HF). La corriente eléctrica que circula por la antena del lector genera un campo magnético que, cuando alcanza a la antena de la etiqueta, induce en ésta una corriente que la alimenta. El *tag* conmuta entonces la impedancia de carga de su antena para crear una modulación que le permita la transmisión de datos. [175]

[171] Ibíd., pág.76.
[172] Ibíd., pág.77.
[173] Ibíd., pág.77.
[174] LIBERA WP-RFID-001 © 2010 RFID: TECNOLOGÍA, APLICACIONES Y PERSPECTIVAS
[175] Ibíd., pág.17.

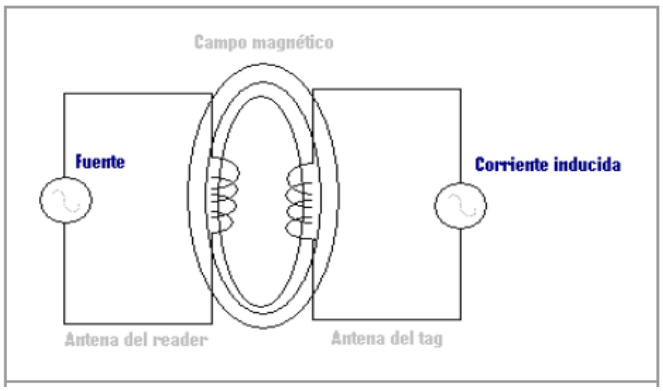


Figura 38. Representación Acoplamiento inductivo, Libera wp-rfid-001 © 2010 rfid: tecnología, aplicaciones y perspectivas

El acoplamiento capacitivo. Se usa únicamente para la comunicación en frecuencias UHF y microondas. En este caso, el lector transmite una señal de radiofrecuencia que la etiqueta recibe, modula y transmite un reflejo hacia el lector de nuevo. Dependiendo del tipo de alimentación de las etiquetas, ya sean pasivas o activas, éstas tomarán de la señal que les llega del lector su alimentación o no, antes de retransmitirla en respuesta.[176] Algo similar a la tecnología PoE que genera su energía por el mismo cable de datos Ethernet.

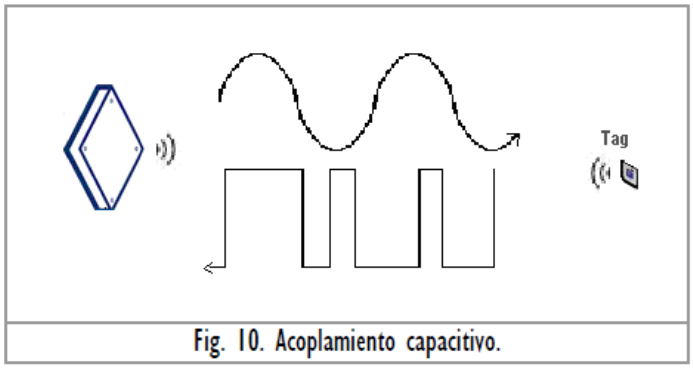


Figura 39.Representación Acoplamiento capacitivo, LIBERA WP-RFID-001 © 2010 RFID: TECNOLOGÍA, APLICACIONES Y PERSPECTIVAS

Entre las características físicas dada la frecuencia de transmisión se presenta una alta sensibilidad para materiales con superficies metálicas o líquidos que afectan la propagación desintonizando la antena. Esto influye también directamente en los problemas de sintonización que se presentan en presencia de varios tags por interferencia, fenómeno que se estudia más adelante. Por otro lado, las ventajas de operar en altas frecuencias se reflejan en las grandes distancias que pueden obtener. Para UHF se pueden alcanzar entre 1 a 8 metros para etiquetas pasivas y

[176] Ibíd., pág.17.

hasta 100 metros para las activas. Así mismo, la tasa de transferencia de datos puede ser más alta si es más alta la frecuencia, ocasionando mayor velocidad de lectura y cantidad de información transmitida.

La legislación internacional establecida hasta ahora, especifica que los equipos RFID utilicen la banda de frecuencias de uso libre ISM (Industrial, Scientific and Medical) para UHF, como ocurre con otras tecnologías como WiFi y Bluetooth[177]. Sin embargo, éste es uno de los problemas de compatibilidad a nivel mundial de la tecnología, ya que dentro de esta banda, para la frecuencia UHF existen distintos rangos permitidos por las diferentes entidades nacionales encargadas de regular el espectro. La unificación internacional de las frecuencias a utilizar o el desarrollo de lectores y etiquetas "multibanda" será necesario para que la tecnología se pueda utilizar en todo el mundo sin problemas de compatibilidad.[178]

8.5.2 LOS TAGS DE RFID

En su parte física constitutiva, una etiqueta RFID consta de un microchip montado sobre un sustrato flexible, con una antena incorporada. A pesar del reducido tamaño de los microchips, las antenas mantienen un tamaño considerable, puesto que necesitan ser lo suficientemente grandes en proporción de la necesidad de captar la señal del lector. La antena funciona en muchos casos como repetidora, permitiendo que una etiqueta pueda leerse a una distancia de tres metros o más, incluso a través de distintos materiales. El tamaño de la antena es proporcional al tamaño de una etiqueta RFID. Un ejemplo de una etiqueta de RFID se presenta en la figura 39.

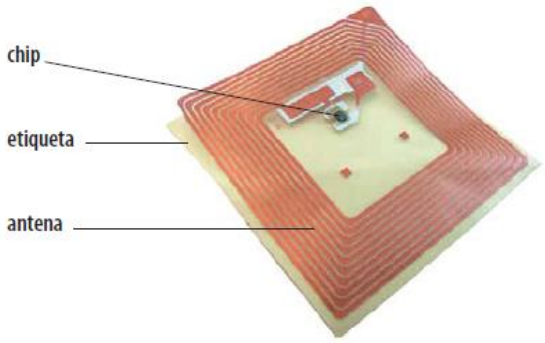


Figura 40.TAG de RFID, Introducción a la identificación por Radio Frecuencia – RFID, Telectronica.

Las antenas son fabricadas de aluminio, cobre u otros materiales conductores, y son creadas a partir de técnicas de inyección de material. La cantidad de este

[177] Harrison B. Chung, Heesook Mo, Naesoo Kim, Cheolsig Pyo, "An advanced RFID system to avoid collision of RFID reader, using channel holder and dual sensitivities". Microwave and Optical Technology Letters, Vol. 49 Issue 11, pp.2643–2647, 2007.
[178] Ibíd., pág.8.

material conductor inyectado y las dimensiones de la antena determinan la sensibilidad de la etiqueta tal como se mencionó anteriormente. La sensibilidad de la etiqueta, su ubicación, la orientación, y la ubicación del lector son vitales para obtener confiables rangos de lectura y minimizar la influencia de otros objetos sobre el Tag.

Las antenas de las etiquetas pueden ser diseñadas en una gran variedad de configuraciones para lograr distintos rendimientos según las necesidades de la aplicación, y el entorno donde suelen utilizarse sistemas RFID con varios lectores ubicados estratégicamente a manera de red, que permita identificar todo objeto que entre en la misma.

8.5.3 Tipos de etiquetas

Un Tag consta básicamente de un inductor que puede ser LF o HF, o antena con recuencias de operación en las bandas UHF, μW y de un circuito integrado de distintas características según el fabricante. Atendiendo a las distintas características de los tags, se pueden realizar las siguientes clasificaciones[179]:

Tag Por Acceso:

- RO, Sólo lectura
- WORM, escrita una vez y múltiples lecturas.
- Escritura y lectura múltiples

Tag por Memoria:

- Sólo Tag ID (64 / 96 bits)
- Tag ID (64 / 96 bits) + User Memory (0-8Kbits, según el fabricante del integrado).

Tag por modo de Alimentación

Pasivas: Realiza la comunicación y la alimentación de los Tag por la misma señal de RF emitida por el lector.

Semi-pasivas: Tienen una batería de reducido tamaño, que alimenta su circuito integrado pero la comunicación de respuesta hacia el lector se hace con la misma señal RF que le llega del lector.

[179] Harrison B. Chung, Heesook Mo, Naesoo Kim, Cheolsig Pyo, “An advanced RFID system to avoid collision of RFID reader, using channel holder and dual sensitivities”. Microwave and Optical Technology Letters, Vol. 49 Issue 11, pp.2643–2647, 2007.

Activas: Cuenta con una carga que no sólo les permite alimentar su circuitería interna sino que también actúa como repetidora, reforzándose la señal que le llega del lector,

8.5.4 EL PROBLEMA DE INTERFERENCIAS EN RFID

En los sistemas RFID con varios lectores dentro de una misma red se producen problemas de colisiones e interferencias que reducen significativamente el throughput del sistema, dado el número de tags identificados por lector. Estos problemas se caracterizan por dos tipos de interferencias:

Interferencias lector-tag (RTI): Se producen cuando en un sistema RFID las áreas de cobertura de dos o más lectores se solapan, independientemente de si trabajan en la misma o distinta frecuencia.

Interferencias lector-lector (RRI): Suceden cuando dos o más lectores de un sistema RFID trabajan a la misma frecuencia y las señales de al menos uno de ellos alcanza a uno o varios lectores. En este caso, si un lector está leyendo a un tag que tiene en cobertura y, al mismo tiempo percibe las señales electromagnéticas de un lector, éstas interferirán en la débil señal de respuesta del tag.

RTI y RRI dependen directamente del rango de lectura de los lectores, que a su vez depende de la potencia de transmisión configurada. En la mayoría de los sistemas RFID, los lectores se configuran a la máxima potencia permitida por el estándar y las regulaciones del país. En Europa, esta potencia alcanza los 2 W. Este valor garantiza el rango de cobertura máximo lector-tag (dRT), pudiendo identificar tags situados a 10m de distancia del lector. Sin embargo, la potencia de transmisión también afecta al rango de cobertura lector-lector (dRR), por lo que, a 2 W, los lectores interfieren entre ellos hasta una distancia de aproximadamente 1000m. [180]

Durante los últimos años se han desarrollado diversos estándares que obvian los problemas asociados a RTI y concentran esfuerzos en proponen soluciones para las interferencias RRI.

Estas soluciones se basan en FDMA (Frequency Division Multiplexing Access), asignando a cada lector una frecuencia de trabajo, según la solicite. El estándar para FDMA propone dividir la frecuencia de trabajo en 15 subportadoras. Cada lector escucha en una subportadora durante un tiempo determinado. Siguiendo el esquema CSMA (Carrier Sense Multiple Access), principio utilizado en el protocolo Ethernet, en el cual el lector accede a la transmisión si encuentra el canal libre. En caso contrario el lector sigue escuchando el canal.[181]

---

[180] K.S. Leong, M.L. Ng, P.H. Cole, “The reader collision problem in RFID systems”, in Proc. of IEEE International.
[181] Ibíd., pág.7.

Cada 4 segundos los lectores dejan libre el canal durante al menos, 100ms. En el EPC global Class-1 Gen-2, también basado en FDMA, se utiliza la técnica de FHSS (Frequency Hopping Spread Spectrum) para dividir el espectro en subportadoras, como lo analizaremos más adelante. Y por el contrario que en FDMA los lectores cambian de subportadora de forma aleatoria, reduciendo la probabilidad de colisión. Los lectores no utilizan CSMA y transmiten únicamente en los canales impares, mientras que las respuestas de los tags se alojan únicamente en los canales pares.[182]

Por otro lado, se han desarrollado diseños de red, procurando reducir la interferencia en redes con varios Tagn mediante posicionamiento estratégico de los elementos, que sugiere como mínimo un estudio de Site Survey. Con este fin se implementan los mecanismos centralizados de RFID.

8.5.5 Mecanismos centralizados de RFID

Los mecanismos centralizados proponen una entidad centralizada o master que coordina y sincroniza los lectores a través de una conexión de cable o inalámbricamente. El master reparte los recursos disponibles en la red entre los lectores operativos, tal como lo haría un administrador y gestor de red con los host de la red, balanceando la carga.

Los ingenieros de la IEEE, Wang, D., Wang, J., y Zhao Y, propone un dispositivo centralizado que reparte los recursos entre los lectores y coordina la comunicación entre ellos y los tags a través de una técnica de multiplexación de peticiones de lector. Los autores asumen que las RRI no suceden. Además, los lectores deben ser capaces, no solo de almacenar toda la información referente a los tags identificados, sino también deben comunicarse con sus lectores vecinos para compartir información. El mecanismo requiere hardware extra en los lectores y un hardware específico, no comercial, en el master.[183] Lo que le hace de difícil implementación en un plano real, pues es necesario centrarse en el desarrollo del hardware mencionado, del cual lo grandes fabricantes de Tag y Lectores RFID, no están dispuestos a asumir los gastos de desarrollo que ello implica.

Otras teorías de mecanismo centralizado, consideran la existencia de las RRI que son minimizadas con el empleo de la técnica de acceso por división de Frecuencia FDMA. Tal es el caso de la propuesta planteada por Harrison B. Chung, Heesook Mo, Naesoo Kim, y Cheolsig Pyo, donde el mecanismo centralizado distribuye las frecuencias entre los lectores en función de la distancia entre ellos, cuanto más

[182] K.S. Leong, M.L. Ng, P.H. Cole, “The reader collision problem in RFID systems”, in Proc. of IEEE International

[183] Wang, D., Wang, J., and Zhao, Y.,“A novel solution to the reader collision problem in RFID system”. In Proc. of IEEE Int.

cerca estén, las frecuencias se asignan lo más separadas posibles, de manera que no se solapen, al complementar la técnica con la disminución de la potencia de transmisión de los lectores, lo que implica disminuir el rango de cobertura entre el lector y el tag, minimizando la probabilidad de identificar mayor cantidad de tags[184].

Por otro lado, basados en conceptos similares, se realizan planteos sobre sistemas distribuidos que eviten colisiones y solapamientos causando interferencias, como es analizado a continuación.

8.5.6 Mecanismos distribuidos

Los mecanismos distribuidos no trabajan con una entidad centralizada, sino que se obliga a los lectores para que se comunican entre ellos mediante comunicación inalámbrica distribuyendo los recursos de la red. Estos mecanismos requieren que los lectores mantengan y controlen la sincronización de la red, lo que incrementa su complejidad a nivel de software y programación de los circuitos integrados y microprocesadores de los lectores y los tags.

Ching-Hsien Hsu, Yi-Min Chen, Chao-Tung Yang, proponen un mecanismo donde cada lector detecta el máximo número de lectores vecinos que solapan coberturas y cada uno de ellos decide si alguno de sus vecinos debe desconectarse para disminuir las RTI sin degradar la funcionalidad de la red. Una vez realizadas las desconexiones oportunas, los lectores comienzan la identificación. Se plantea entonces un algoritmo similar al del protocolo STP, eligiendo los lectores base para la identificación[185]. Este sistema es funcional dentro de una red de lectores fijos, puesto que de lo contrario sería necesario configurar cada vez que haya un nuevo lector la identificación del mismo. Una solución a este problema sería la introducción de un identificador de agente externo, de manera que permita identificar si el lector pertenece a una red conocida, y si no es así será necesario la reconfiguración y elección de los lectores base de identificación.

Otro de los protocolos madre que son usados para evitar las colisiones e interferencia basadas en sistemas distribuidos, es el protocolo de Ethernet. La relación se da en la procura de evitar las colisiones. En el estudio de Shailesh M. Birari y Sridhar Iyer denominado “PULSE: A MAC Protocol for RFID Networks”, se propone un mecanismo basado en CSMA. Utiliza un canal de control y otro de datos. Los lectores pueden recibir de ambos canales a la vez, pero no transmitir simultáneamente en ambos. Los lectores, escuchan el canal de control para conocer si el canal de datos está libre. El lector que utiliza el canal de datos transmite

[184] Harrison B. Chung, Heesook Mo, Naesoo Kim, Cheolsig Pyo, “An advanced RFID system to avoid collision of RFID reader, using channel holder and dual sensitivities”. Microwave and Optical Technology Letters, Vol. 49 Issue 11, pp.2643–2647, 2007.

[185] Ching-Hsien Hsu, Yi-Min Chen, Chao-Tung Yang, "A Layered Optimization Approach for Redundant Reader Elimination

periódicamente un paquete en el canal de control para avisar a los lectores que el canal sigue ocupado.[186]

Similar al uso del protocolo MAC para redes RFID, Sungjun, K., Sangbin, L., Sunshin, A., proponen para el canal de control que se realice mediante una red de sensores, lo que implica hardware extra.[187]

Un estudio conocido como Colorwave, es un mecanismo basado en TDMA, donde cada lector elige un slot para transmitir. Si dos o más lectores eligen el mismo slot, se dara la colisión, y los lectores involucrados eligen de nuevo un slot. Si vuelven a colisionar, uno de ellos deberá elegir un nuevo slot y transmitir un paquete de control indicando lo cual ha sido el slot ocupado, disminuyendo así, significativamente las RTI.[188]

Por último, el mecanismo distriuido conocido HiQ reduce las RTI utilizando patrones de colisión. Los lectores, se comunican entre ellos a través de un canal de control y se intercambian información de las colisiones que han tenido de acuerdo a la frecuencia y al slot que han elegido, de manera que se genere información e indicadores. Existe entonces una entidad centralizada que tiene información de todo lo que sucede en la red, y es capaz de asignar recursos a los lectores.[189]

8.6 EPCGlobal

EPCGlobal es una organización sin ánimo de lucro apoyada por la industria, para establecer y mantener la red EPCGlobal como el estándar mundial para la identificación de objetos. El estándar EPC Clase 1 Generación 2 (C1G2) se ha publicado como estándar ISO 18000-6C reconocido internacionalmente. Por tanto, EPCGlobal define diversos estándares reconocidos para RFID. Entre ellos están[190]:

- El formato lógico de los datos contenidos en una etiqueta EPC.
- El protocolo de comunicación de las etiquetas
- Middleware de recogida y tratamiento de datos incluyendo la comunicación con los equipos lectores.
- La especificación PML (Physical Markup Language), lenguaje basado en XML que define el formato de la información de intercambio entre componentes dentro de la red EPC.

[186] Shailesh M. Birari and Sridhar Iyer. “PULSE: A MAC Protocol for RFID Networks” 1st International Workshop on RFID
[187] Sungjun, K., Sangbin, L., Sunshin, A., “Reader Collision Avoidance Mechanism in Ubiquitous Sensor and RFID
[188] J. Waldrop, D.W. Engels, and S. E. Sarma, "Colorwave: an anticollision algorithm for the reader collision problem," in
[189] Ho, J., Engels, D., Sarma, S., “HiQ: a hierarchical Q-learning algorithm to solve the reader collision problem”. In Proc.
[190] LIBERA WP-RFID-001 © 2010, RFID: Tecnología, Aplicaciones Y Perspectivas.

- La especificación ONS (Object Name Service), para la red global, que retiene la información sobre cualquier objeto etiquetado con un tag EPC en el mundo.

8.6.1 EPCGlobal Network

La EPCGlobal Network es un medio para usar la tecnología RFID en una cadena global de suministros y compartir la información obtenida entre usuarios autorizados a través de internet sobre cada producto identificado.[191]

La EPCGlobal Network está compuesta por varios elementos los cuales proporcionan la habilidad de obtener y compartir información dentro de la red. Los objetos se etiquetan con *tags* de bajo coste que contienen su código de identificación único *EPC*. En cada compuesto de la red, se suministra un sistema de identificación conocido como el *ID System*, que a su vez está formado por lectores y antenas, que recogen los códigos *EPC* de todos los objetos. Estos datos son gestionados por el Middleware EPC, el cual los entrega a los sistemas corporativos y a los Sistemas de Información EPC.[192]

Para obtener información adicional sobre un *EPC*, el agente autorizado, a través de sus Sistemas de Información *EPCIS*, acudirá a los Servicios de Información centralizados mediante el servicio de Nombres de Objeto conocido como ONS, *Object Naming Service*, que funciona similar a un servidor DNS otorgando a una identificación EPC un nombre único. De una forma más extensa se presenta el esquema de bloques sobre la operación del EPCglobal.[193]

[191] Ibíd., pág.10.
[192] Ibíd., pág.10.
[193] Ibíd., pág.12.

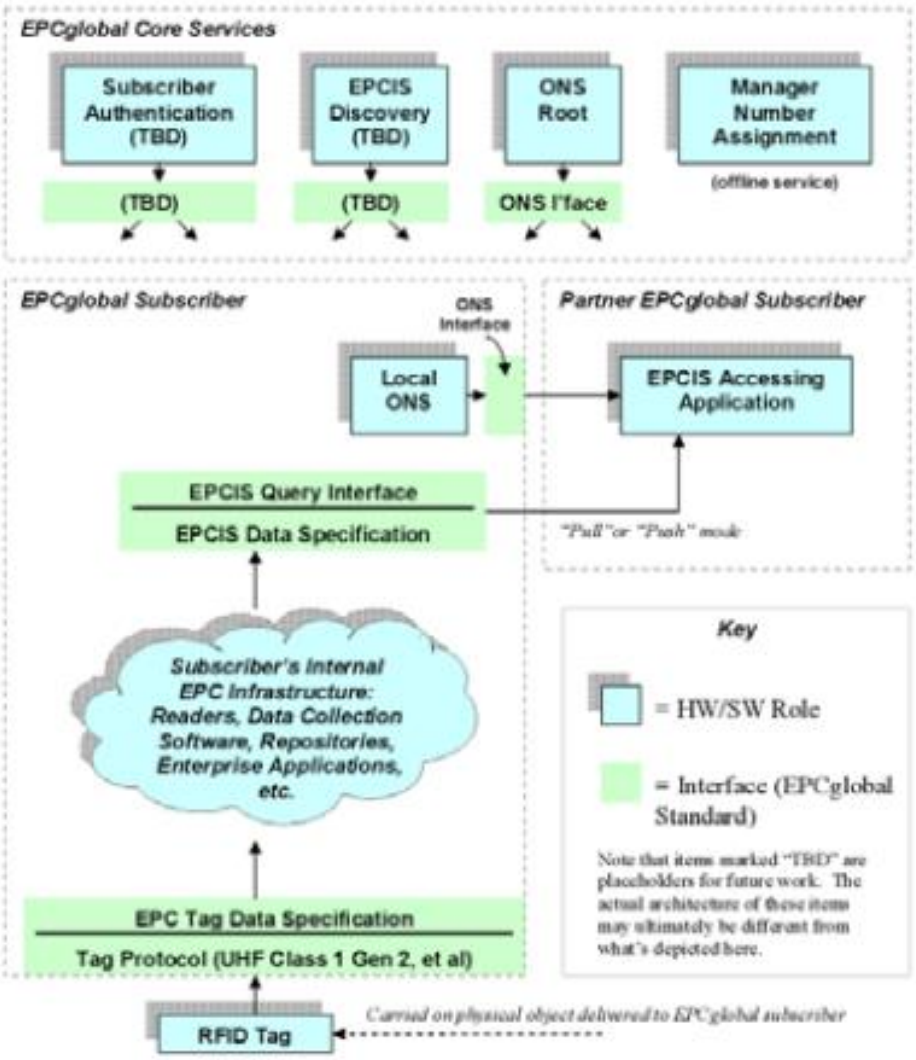


Figura 41.Operación General EPCglobal. Fuente EPCGLOBAL.

8.6.2 Código de Producto (EPC).

El EPC es el código numérico estandarizado de 96 bits que identifica de forma única un objeto. Este código no contiene ninguna información específica sobre el objeto al que etiqueta, por lo que únicamente es un código de identificación para la red EPC, distribuido como se muestra en la figura 41. En esta se observa que los 96 bits están en formato hexadecimal distribuido entre los bits de cabecera (0 a 7 bits), los bits de gestión de EPC que van desde 8 a 35 bits, la identificación de la clase de objetos desde el 36 a 59 bits, y finalmente del 60 a 95 bits para el numero serial del objeto dentro de la red EPC.[194]

[194] LIBERA WP-RFID-001 © 2010, RFID: Tecnología, Aplicaciones Y Perspectivas.

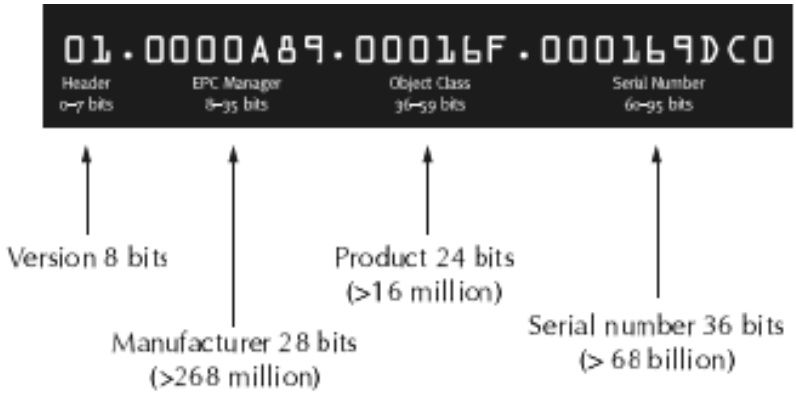


Figura 42.Código EPC, Fuente: EPCGlobal

8.6.3 Middleware EPC

El Middleware EPC es un componente fundamental dentro de la red EPCGlobal ya que, debe asegurar la integración de los equipos RFID de los distintos fabricantes, y además gestiona a los datos recogidos por los lectores. Dado que los lectores pueden estar recogiendo datos de cientos de *tags* por segundo, el middleware debe filtrar y consolidar adecuadamente los datos según corresponda antes de enviarlos a los sistemas corporativos.El Middleware EPC esta compuesto por la interface del lector, el sistema ONS y otros serivicios propios de la indentificacion, el procesamiento de la información obtenida, y finalmente un Gateway hacia la interface de aplicaccion coporativa.[195]

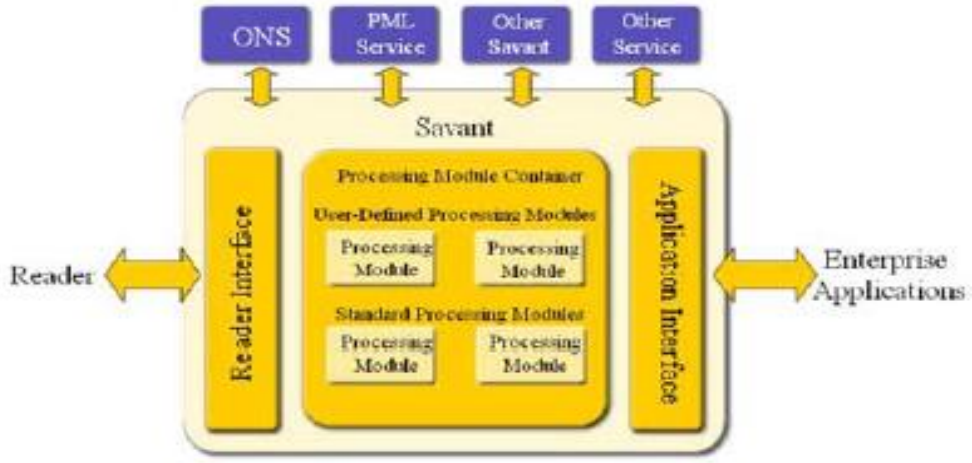


Figura 43.Componentes Middleware EPC, Fuente: EPCGlobal.

[195] LIBERA WP-RFID-001 © 2010, RFID: Tecnología, Aplicaciones Y Perspectivas

8.6.4 EPC Information Server (EPCIS)

Es el gateway para el intercambio de información entre aplicaciones remotas, que se encarga de imterpretar los servicios e interfaces que son necesarios para facilitar dicho intercambio. Una de sus principales características consiste en la existencia de un almacenamiento central de datos compartido, cuya información es actualizada por todos los partners que componen la red.[196]

El proceso de comunicación se realiza mediante servicios web (SOAP) utilizando el Lenguaje de Marcado Físico ("PML, *Physical Markup Lenguaje*"), de forma que cualquier aplicación local pueda comunicarse con sistemas remotos.[197]

8.6.5 Object Name Service – ONS

La función del Servidor de Nombres de Objetos dentro de la red EPCGlobal es identificar la localización del servidor que contiene la información que necesita una aplicación. Como se muestra en la figura 43, el ONS utiliza la información del código EPC para obtener la localización de un servicio perteneciente a un servidor EPCIS de su base de datos local o de un servidor ONS raíz[198] Este servidor ha sido diseñado utilizando los conceptos de los servidores DNS para que ofrezca escalabilidad y funcionalidades similares.

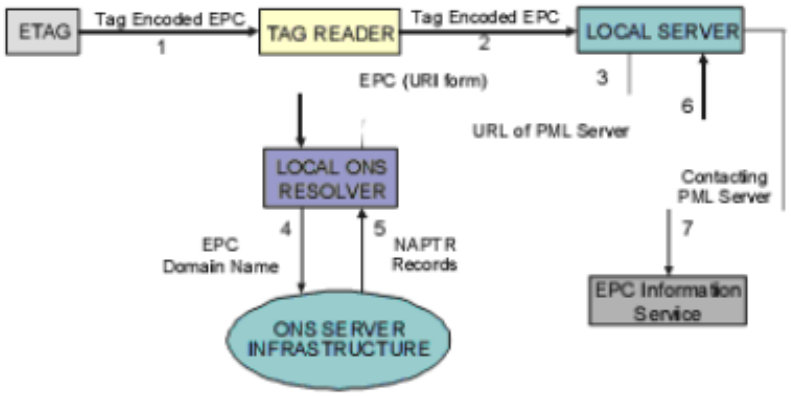


Figura 44.Esquema de Funcionamiento ONS. Fuente: EPCGlobal.

Como se ha mencionado, el servicio de nombres de objetos (ONS) es un servicio de red automatizado similar al Servicio de Nombres de Dominio (DNS). (Por lo que más adelante se analiza su función). Cuando un interrogador RFID lee la etiqueta de un producto, el código electrónico del producto se pasa a un middleware, que a

[196] Ibíd., pág.12.
[197] LIBERA WP-RFID-001 © 2010, RFID: Tecnología, Aplicaciones Y Perspectivas
[198] Karakostas, B. "A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics", The 4th International Conference on Ambient Systems, Networks and Technologies (ANT 2013), Procedia Computer Science 19 (2013) 594 – 601.

su vez hace una consulta ONS en una red local o en Internet, para encontrar donde se almacena la información sobre el producto. El resultado de esa consulta se almacena en un servidor con un archivo del producto.

8.6.5.1 Servicio Dominio de nombres (DNS)

DNS es un servicio de Internet de alto nivel de infraestructura utilizado para el descubrimiento de información sobre un nombre de dominio y para la asignación de un nombre de host a una dirección IP. El DNS tiene tres componentes principales:[199]

- *Registros del espacio de nombres de dominio y de recursos,* que son un árbol estructurado espacio de nombres y datos (direcciones de red) asociados con los nombres. El DNS de Internet utiliza algunos de sus nombres de dominio para identificar hosts. Una consulta basada en un nombre de dominio puede devolver direcciones de host de Internet.

- *Los servidores de nombres,* que contienen información acerca de la estructura del árbol de dominio. Los servidores de nombre conocen las partes del árbol de dominio para los que tienen la información completa.

- *Resolvers* que son aplicaciones de cliente que extraen información de los servidores de nombres en respuesta a peticiones.

La red de servidor ONS tiene una arquitectura que es similar a la DNS actual de Internet. Una de las diferencias entre el DNS para los objetos (ONS) y el DNS actual es que los servidores autorizados de los primeros no pueden ser fijos, debido a la naturaleza móvil de los objetos, por tanto el tiempo de vida (TTL) varía desde unas pocas horas hasta varios días o incluso semanas según los movimientos del objeto[200].

Por otra parte de manera similar al DNS de Internet actual, el sistema ONS para los objetos necesita tener una organización jerárquica a fin de hacer frente al tamaño del dominio. Una posible jerarquía de servidores ONS implica un nivel superior (nivel 0) de Servidor DNS gestionado por un organismo internacional como la ONU / CEFACT[201], es decir una entidad responsable de la legislación del nombre de dominio. Los grandes Carrier podrían ser responsables de la infraestructura básica DNS, para proveer el Nivel 1 de los nombres de dominio que se les

[199] RFC 1034, Domain Names - Concepts and Facilities, P. Mockapetris, The Internet Society (November 1987)
[200] RFC 1034, Domain Names - Concepts and Facilities, P. Mockapetris, The Internet Society (November 1987)
[201] Karakostas, B. “A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics”, The 4th International Conference on Ambient Systems, Networks and Technologies (ANT 2013), Procedia Computer Science 19 (2013) 594 – 601.

asignan. Subdominios de nivel inferior podría corresponden a la organización empresarial. Por ejemplo, los grandes centros de distribución y unidades se podrían asignar subdominios de tipo tier 2, mientras que las instalaciones más pequeñas, conseguirían asignados subdominios de nivel cada vez más bajos.

De acuerdo con este enfoque y en línea con la visión de la IoT, una consulta enviada al servidor de nivel superior podría estar formado como[202]:

TopDomainName / serviceofobjectrequired /? = ID de objeto

Donde *ID* es el identificador único del objeto rastreado.

Se requiere esta consulta para resolverse una dirección URL completa como:

TopDomainName / subdominio / sub-subdominio /.../ serviceofobjectrequired /? ObjectID = ID, mediante la transmisión a los servidores autorizados para cada sub-subdominio.

Correspondientemente, el nivel 0 posee servidores con muchos consultas de nombres acerca de los servidores de nivel 1, mientras que el los servidores de Nivel 1 se ocuparía de las consultas DNS que corresponden a las consultas de seguimiento manejados hoy por las páginas web. Los servidores de nivel 1 tienen entonces que delegar las consultas a la subred apropiada de servidores Nivel 2, dependiendo del tipo de objeto consultado. Los servidores de nivel 2 y los inferiores serán responsables de resolver la consulta mediante el trazado del objeto a la ubicación del equipo adecuado.

En última instancia, los servidores de nivel más bajas tendrían que interactuar con las diferentes puertas de enlace que actúan como proxy para la objetos. Por tanto, la puerta de enlace actúa como los servidores autorizados para las consultas ONS. Ellos suministrarían el *registro de servicio* (SRV).

8.6.5.2 Requerimientos red ONS

El diseño de una arquitectura de ONS adecuado para la IoT debe tener en cuenta el tamaño de la red de la vida real, en términos de aspectos tales como el número esperado de consultas ONS. Si bien no es fácil obtener un panorama global y una cifra precisa para el total de objetos manipulados por la industria, una estimación se puede extrapolar a partir de los datos proporcionados por las grandes empresas de logística

El tráfico total de Internet de 500 millones de consultas por día (sólo en los EE.UU., y para el seguimiento de paquetes pequeños solamente) es comparable, por

[202] Ibíd., pág.598.

ejemplo, a de 3 mil millones de consultas por día. A su vez, este gran número de consultas podría generar una cantidad significativa de tráfico de red que suponiendo un 1kB promedio por consulta / respuesta, podría potencialmente llegar a niveles de varios petabytes por día. Ese cálculo de tráfico excluye el tráfico interno generado por la sincronización de los servidores DNS.[203]

Cada uno de los servidores de nivel 2 mencionados anteriormente, mantiene los registros de servicio (SRV) de varios objetos. (Figura 44). Un registro SRV contiene información tal como el TTL, nombre de host, número de puerto, etc, del servidor al que el objeto está asociado, así como los servicios proporcionado por el objeto por ejemplo, su ubicación física, temperatura y otra información relevante.

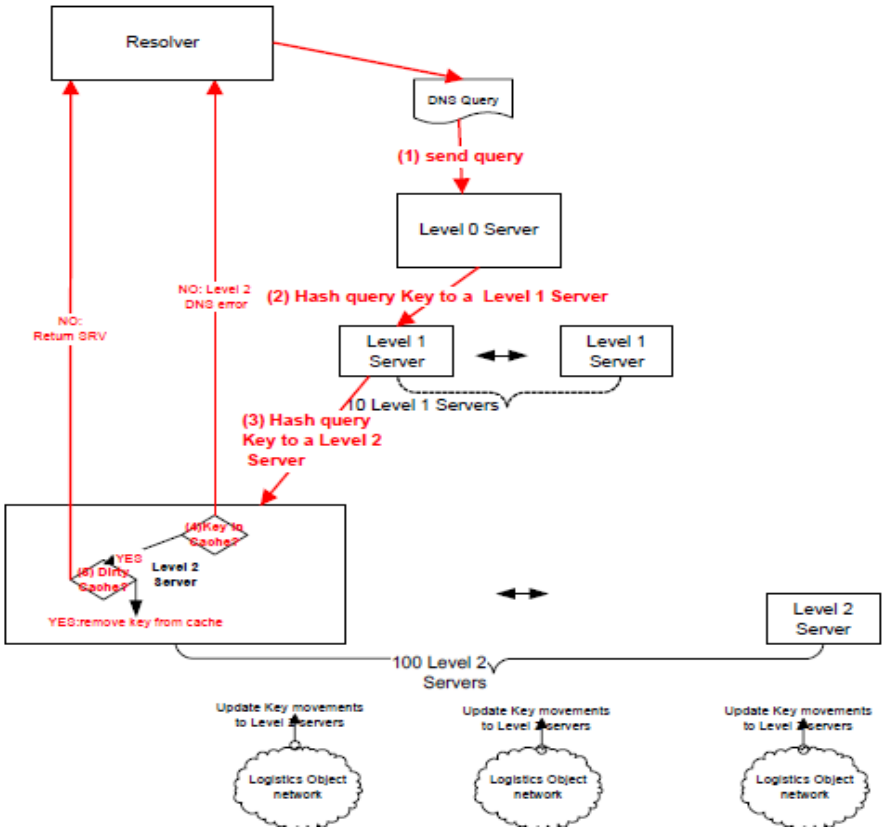


Figura 45.Modelo ONS basado en DNS, Karakostas, B.

Los registros de caché de nivel 2 para el SRV en función de su tiempo de vida (TTL), donde, como en el DNS existente, un TTL de 0 significa que el registro no debe almacenarse en caché. Como consecuencia de esta política de almacenamiento en caché, los cambios de registros ONS no se propagan por toda la red de inmediato,

[203] Karakostas, B. "A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics", The 4th International Conference on Ambient Systems, Networks and Technologies (ANT 2013), Procedia Computer Science 19 (2013) 594 – 601.

pero requieren que todos los cachés expiren y se actualice después el TTL, permitiendo que no haya información redundante de los objetos en la red y optimizar el throughput.

8.6.6 Requisitos técnicos del Protocolo EPC

Información general del Protocolo

La información presentada a continuación, hace referencia al EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.

8.6.6.1 Capa física

Para el protocolo RFID, según lo definido por el EPCglobal Inc., un lector o interrogador envía información a una o más etiquetas mediante la modulación de una portadora de RF usando amplificación de doble banda lateral, modulación por desplazamiento (DSB-ASK), modulación de banda lateral con único desplazamiento de amplitud (SSB-ASK), o inversión de fase por desplazamiento de amplitud (PR-ASK) utilizando un formato de codificación de intervalos de impulsos (PIE). Las etiquetas reciben su energía de funcionamiento de esta misma portadora de RF modulada.[204]

Un interrogador recibe información de una etiqueta mediante la transmisión de una portadora de RF modulada y escuchando el respuesta de retro dispersión. Las etiquetas comunican información por retrodispersión, la modulación de la amplitud y / o fase de la Portadora de RF. El formato de codificación, seleccionado en respuesta a los comandos del interrogador, es o bien FM0 o subportadora modulada Miller. El enlace de comunicaciones entre los interrogadores y etiquetas es half-duplex,es decir, que a las etiquetas no se les exigirá que demodular comandos del lector o interrogador. Una etiqueta no deberá responder a una orden usando comunicaciones full-duplex.

8.6.6.2 Tag-identificación

Un interrogador maneja poblaciones de códigos utilizando tres operaciones básicas[205]:

a) **Seleccionar.** El funcionamiento de la elección de una población Tag para el inventario y el acceso. El comando *Select* puede ser aplicado sucesivamente para

[204] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.
[205] Ibíd., pág.17.

seleccionar una población Tag particular basada en criterios especificados por el usuario. Esta operación es análoga a la selección de registros de una base de datos.

b) **Inventario.** La operación de identificación de Etiquetas. Un interrogador comienza una ronda de inventario mediante la transmisión de un comando de *Consulta* en cuatro sesiones. Uno o más etiquetas pueden responder. Si el interrogador no detecta una sola Respuesta Tag revisa el código EPC, y la identificación de errores mediante el CRC de la etiqueta. Un Inventario comprende múltiples demandas. Una ronda de inventario opera en sólo una sesión a la vez.

c) **Acceso.** Para la funcionalidad de la comunicación de leer y/o escribir en una etiqueta. Una etiqueta individual debe identificarse de forma única antes del acceso. El Acceso comprende múltiples comandos, algunos de los cuales emplean de una sola etiqueta de encubrimiento de codificación.

8.6.7 Parámetros de protocolo EPC

8.6.7.1 Señalización - control físico y de acceso a medios (MAC).

El procedimiento operativo define los requisitos físicos y lógicos para un interrogator-Talk-Fisrt (ITF), y define el arbitraje de colisión. El sistema RFID opera en la 860 MHz - 960 MHz rango de frecuencia.

Señalización

La interfaz de señalización entre un interrogador y una etiqueta puede ser vista como la capa física en una red jerárquica en un sistema de comunicación. La interfaz de señalización define frecuencias, la modulación, la codificación de datos, la envolvente de RF, velocidades de datos, y otros parámetros requeridos para las comunicaciones RF.

Frecuencias operacionales

Las etiquetas recibirán energía al comunicarse con los lectores o interrogadores en el rango de frecuencias de 860 MHz a 960 MHz. La decisión de frecuencia de funcionamiento de un lector o interrogador, será determinado por las regulaciones de radio locales y por el entorno de radio frecuencia local.

8.6.7.2 Comunicación Entre el Interrogador y el Tag

Un interrogador se comunica con uno o más etiquetas modulando una portadora de RF usando DSB-ASK, SSB-ASK, o PR-ASK con codificación PIE. Los interrogadores deberán utilizar un formato de modulación fija y velocidad de datos

para la duración de una ronda de inventario, previamente definido. El interrogador establece la velocidad de datos por medio del preámbulo que inicia la ronda.[206]

8.6.7.2.1 Interrogador precisión de frecuencia

Los interrogadores certificados para operar en ambientes simples o con múltiples interrogadores tendrán una frecuencia exacta que cumpla con las normas locales. Los interrogadores certificados para su uso en entornos densos deberán tener una precisión de frecuencia de +/- 10 ppm sobre el rango de temperatura nominal (-25 ° C a +40 ° C) y 20 ppm +/- en todo el rango de temperatura ampliado (-40 ° C a +65 ° C) durante la transmisión, a menos que las normas locales especifican una precisión más estricta, en cuyo caso la precisión de frecuencia del lector o interrogador deberá cumplir con los reglamentos locales.[207]

8.6.7.2.2 Modulación

Los lectores se comunicarán usando modulación OSD-ASK, SSB-ASK, o PR-ASK.

8.6.7.2.3 Enlace para modulación Interrogador-a Tag

Formas de onda de RF

La Figura 45 muestra R => T de banda base con las formas moduladas generada por un interrogador, y la envolvente detectada por una etiqueta, para modulación DSB-o SSB-ASK, y para modulación PR- ASK.

[206] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.
[207] Ibíd., pág.22.

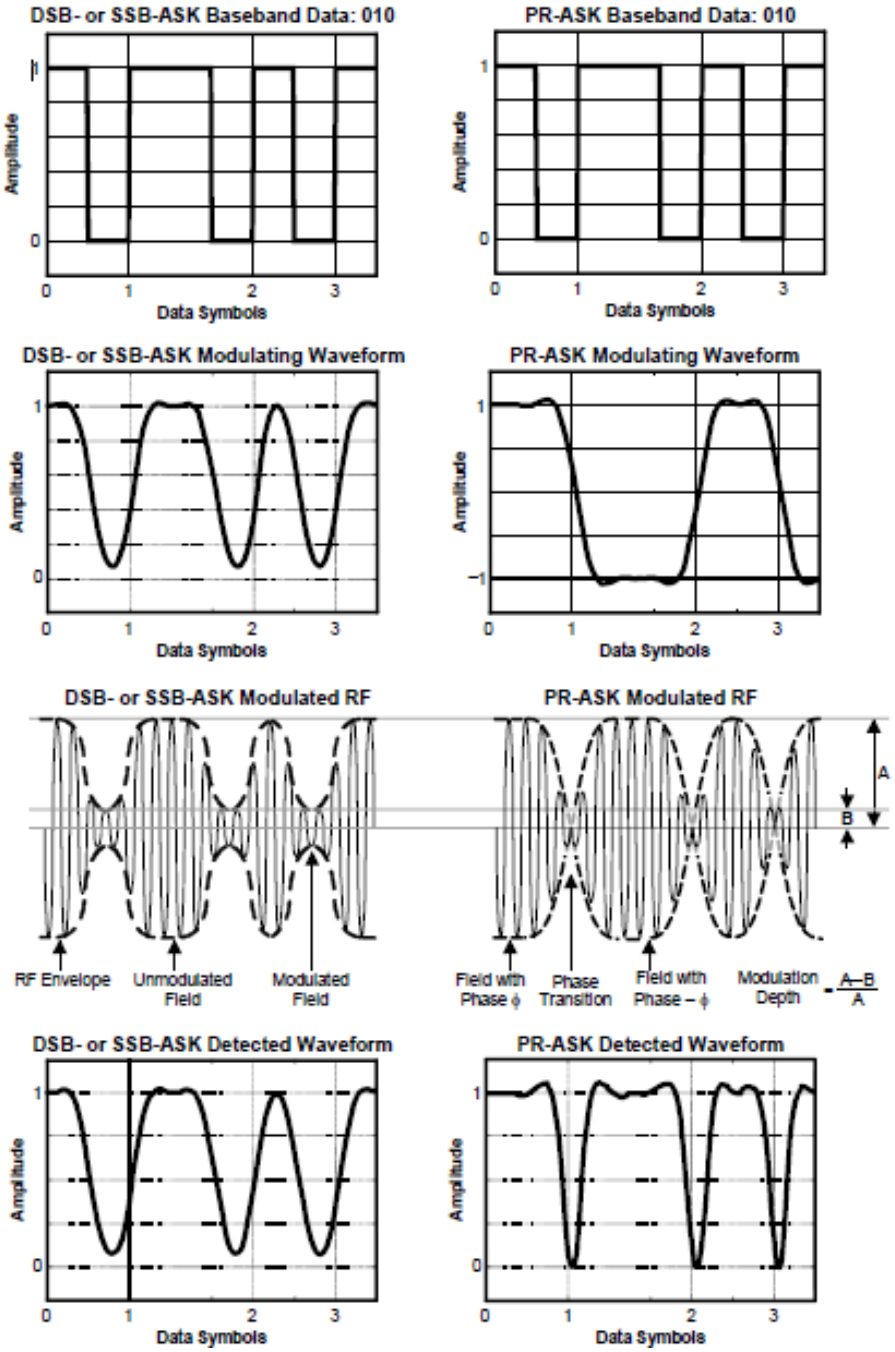


Figura 46.Interrogator-to-Tag modulation, EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz, Version 1.1.0

8.6.7.2.4 Codificación de datos

La codificación está dada por modulación de pulsos de profundidad de tiempo de subida, tiempo de bajada, y PW será la especificada por el protocolo, y será el mismo para datos-0 y datos-1. Los interrogadores deberán utilizar un coeficiente de modulación fija, tiempo de subida, tiempo de bajada, PW, Tari, Longitud datos-0, y

longitud de los datos-1 para la duración de una ronda de inventario. La envolvente de RF será la especificada.[208]

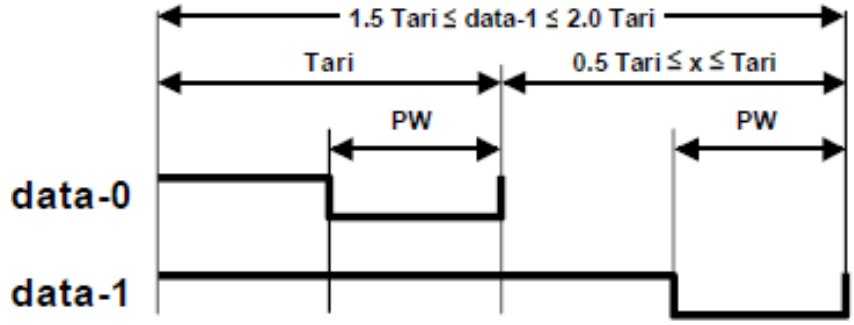


Figura 47.Datos Codificacion por intervalos de impulso, interrogator-to-tag modulation, epc™ radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz – 960 mhz, version 1.1.0

8.6.7.2.5 Valores Tari

Los interrogadores se comunicarán utilizando valores Tari en el rango de 6.25µs a 25µs. Cumplimiento interrogador ser evaluado utilizando al menos un valor Tari entre 6.25µs y 25µs con al menos un valor del parámetro *x*. La tolerancia en todos los parámetros especificados en unidades de Tari será +/- 1%. La elección del valor de Tari y *x* será de conformidad con las regulaciones locales de radio.[209]

8.6.7.2.6 Envolvente de RF

La envolvente de RF => T R deberá está regida por los principios físicos del campo eléctrico, donde la fuerza un campo eléctrico es la máxima amplitud de la envolvente de RF (Figura 47). El ancho de pulso se mide en el punto donde se alcanza el 50% del pulso. Un interrogador no podrá cambiar los valores R => T ni el tipo de modulación (es decir, no podrá cambiar entre DSB-ASK, SSB- ASK, o PR-ASK) sin eliminar primero la forma de onda de RF.

[208] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.
[209] Ibíd., pág.23

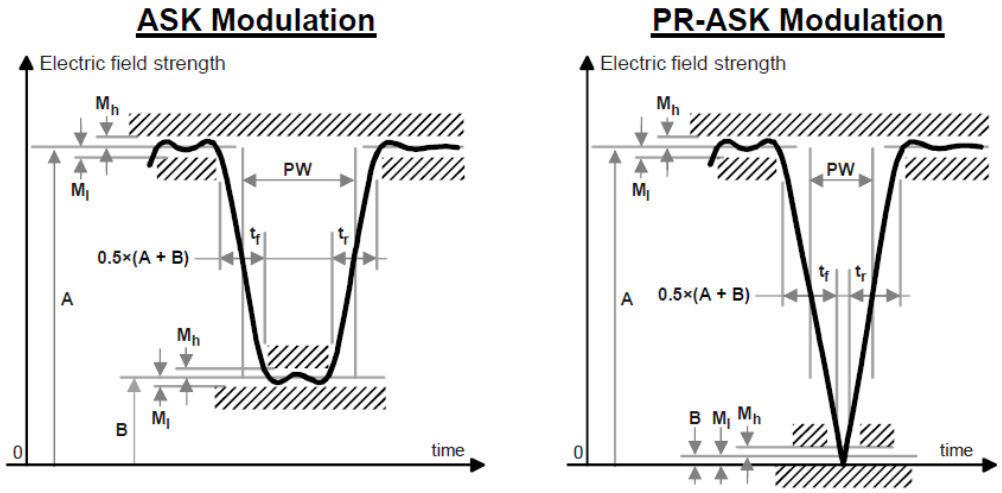


Figura 48.Envolvente de RF Interrogador a Tag, epc™ radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz – 960 mhz, version 1.1.0

Tari	Parameter	Symbol	Minimum	Nominal	Maximum	Units
6.25 µs to 25 µs	Modulation Depth	(A–B)/A	80	90	100	%
	RF Envelope Ripple	$M_h = M_l$	0		0.05(A–B)	V/m
	RF Envelope Rise Time	$t_{r,10-90\%}$	0		0.33Tari	µs
	RF Envelope Fall Time	$t_{f,10-90\%}$	0		0.33Tari	µs
	RF Pulsewidth	PW	MAX(0.265Tari, 2)		0.525Tari	µs

Figura 49.Parámetros Envolvente RF, epc™ radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz – 960 mhz, version 1.1.0

8.6.7.2.6 Energía en modo Power-Up

El modo Power-up ó forma de onda encendido, se da una vez que el nivel de la portadora se eleva por encima del 10%, de manera que el power-up se levantará de forma monótona hasta por lo menos el límite de ondulación. El RF no caerá por debajo del 90% durante el intervalo Ts (Figura 49). Los interrogadores o lectores no realizaran demandas antes de que finalice el intervalo máximo de tiempo de asentamiento en T, es decir, antes de que finalice Ts.[210]

8.6.7.2.7 Energía en modo Power-down

Una vez que el nivel de la portadora esta caído por debajo del nivel del 90%, la onda de energía caeré continuamente hasta el límite de apagado Ms (Figura 49). Una vez

[210] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.

apagado, un interrogador deberá permanecer apagado durante al menos 1 ms antes de encender de nuevo.[211]

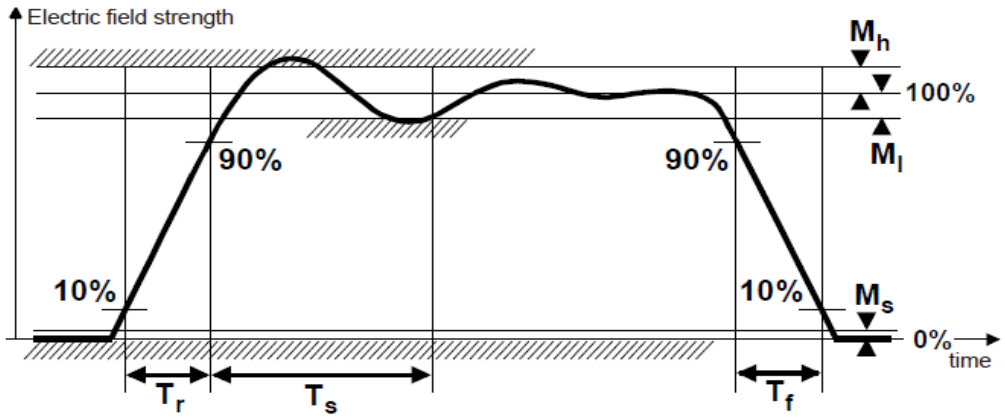


Figura 50.Envolvente de RF, Power-up y Power-down, epc™ radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz – 960 mhz, version 1.1.0

8.6.7.2.8 Forma de onda de espectro disperso con salto de frecuencia

Cuando un interrogador utiliza espectro ensanchado por salto de frecuencia (FHSS) de señalización, la envolvente de RF no caerá por debajo del punto de Undershoot (Mhl) durante el intervalo del 90% (Figura 50). Los interrogadores no podrán emitir comandos que finalice el intervalo máximo de tiempo de asentamiento, es decir Ths. El tiempo máximo entre saltos de frecuencia y el tiempo de RF.off mínimo durante un salto comenzara conociendo los requerimientos locales.[212]

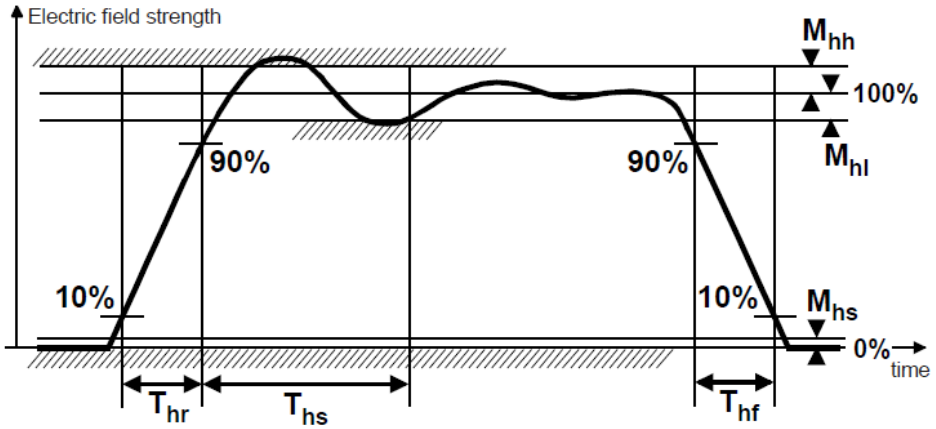


Figura 51.Envolvente de RF con FHSSS

[211] Ibíd., pág.23.
[212] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.

8.6.7.2.9 Canalización con salto de frecuencia de espectro ensanchado.

Los interrogadores certificados para funcionar en entornos con un único interrogador deberán cumplir la normativa local sobre el cálculo de la canalización del espectro. Los interrogadores certificados para la operación en redes con múltiples interrogadores deberá cumplir con las regulaciones locales para la canalización de ensanchamiento de espectro, a menos que la canalización no este regulada, deberán tomar el modelo de canalización conocido como Dense-Interrogador definido para TDM y FDM según corresponda, y que se describe a continuación. [213]

8.6.7.2.10 Dense-Interrogator

En entornos que contienen dos o más interrogadores, la distancia y la velocidad a la que los interrogadores gestionan sus etiquetas o Tags se puede mejorar mediante la prevención de las transmisiones del interrogador de chocar con las respuestas de la etiqueta, ya sea temporal o espectralmente. Para tal efecto se describe la multiplexación por división de tiempo (TDM) y multiplexación por división de frecuencia (FDM), métodos que pueden minimizar las colisiones interrogador-on-Tag. Si lo permiten los reglamentos locales, los interrogadores certificados para el funcionamiento en entornos dense-interrogator se podrá apoyar a uno de los métodos de TDM o FDM se describen a continuación. Si un interrogador utiliza la modulación SSB-ASK, el espectro de transmisión se centra en el canal de señalización durante R ≦T, y la CW será centrada en el canal durante la retro dispersión del Tag.

TDM: Las transmisiones del interrogador y las respuestas de la etiqueta estarán separados temporalmente, mediante sincronismo preestablecido, un único interrogador transmiten primero hacia las etiquetas, entonces todos los demás interrogadores que transmiten CW podrán escuchar las respuestas de la etiqueta.

FDM: Las transmisiones del interrogador y las respuestas de la etiqueta estarán separadas espectralmente, usando una de las tres escalas descritas a continuación:

***Retrodispersión por Limite de Canal*:** Las transmisiones del interrogador se centran en los canales, y la respuesta del Tag de por dispersión se encuentra en los límites del canal.

Retrodispersión por canale adyacente: Las transmisiones del interrogador se centran en los canales de número impar, y la retrodispersión del Tag se encuentra en los canales de número par.

[213] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.

Retrodispersión por canal: Las transmisiones del interrogador se centran en los canales, y la retrodispersión se encuentra separa, pero dentro de los límites del mismo canal.

Ejemplo 1: Dense-Interrogator TDM

ERC REC 70-03E Anexo 1 permite que la banda de 869,4 a 869,65 MHz para ser utilizado como un único canal de 250 kHz. El modo denso-interrogador será TDM. Donde se muestra uno operativo posible, donde los transmisiones interrogadoras utilizan DSB-ASK modulación con Tari = 25 ms, y Retrodispersión Tag de 20 kbps de datos en una subportadora de 80 kHz (BLF = 80 kHz, M = 4).

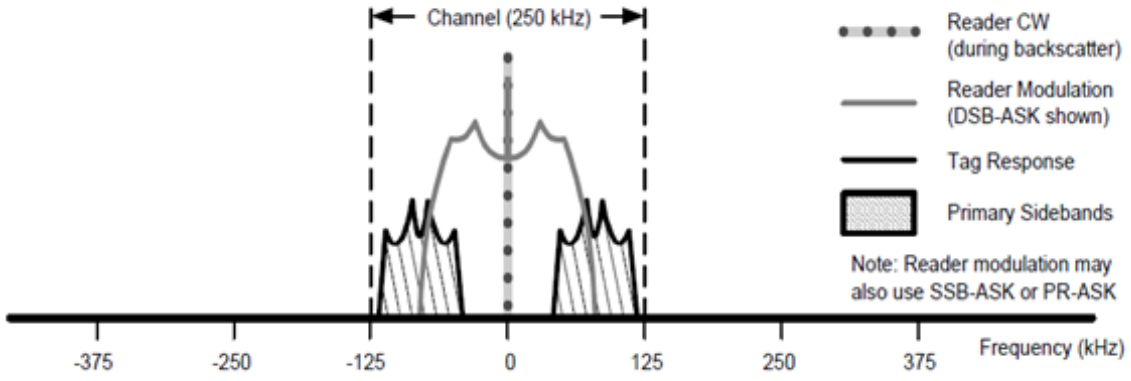


Figura 52.Ejemplo Dense-Interrogator TDM, ERC REC 70-03E Anexo 1

Ejemplo 2: FDM Retro dispersión por Límite de Canal:

FCC 15.247, de fecha octubre de 2000, autoriza la operación de salto de frecuencia en la banda ISM 902-928 MHz con 500 kHz como máximo ancho de canal, y no prohíbe retro dispersión por límite de canal. Los interrogadores utilizarán 500 canales kHz con retro dispersión por límite de canal. Las transmisiones del interrogador están utilizando PR-ASK modulación con Tari = 25 ms y 62,5 kbps Tag data backscatter en una subportadora de 250 kHz (BLF = 250 kHz, M = 4). Los interrogadores centran su R≦ T en la señalización de los canales definidos con transmisiones no sincronizadas en el tiempo, saltando entre los canales.[214]

[214] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.

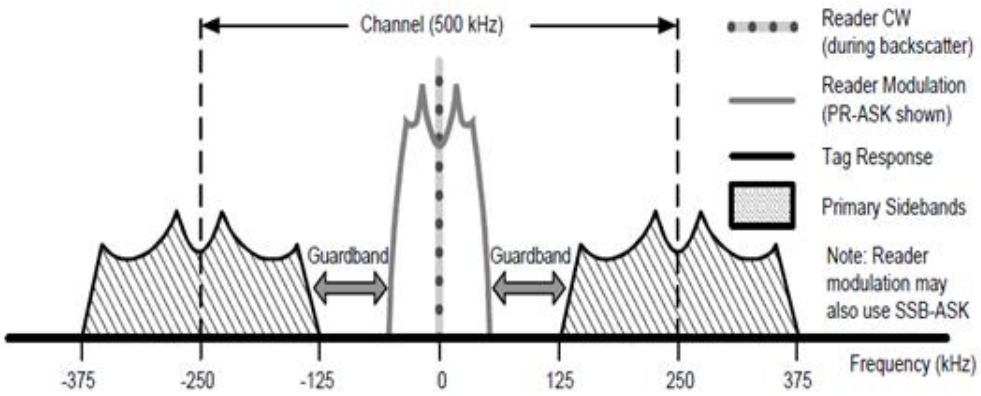


Figura 53.Ejemplo FDM Retro dispersión por Límite de Canal, FCC 15.247, octubre del 2010

Ejemplo 3: FDM retrodispersión de canal adyacente

ERC REC 70-03E Anexo 11 especifica quince canales de 200 kHz en la gama de frecuencias 865-868 MHz y no prohíbe la retro dispersión de canal adyacente. Los interrogadores utilizarán como ancho de canal 200 kHz y utilizan modulación SSB-ASK con Tari = 25 ms, y 50 kbps en una subportadora 200 kHz (BLF = 200 kHz, M = 4) para la respuesta del Tag.[215]

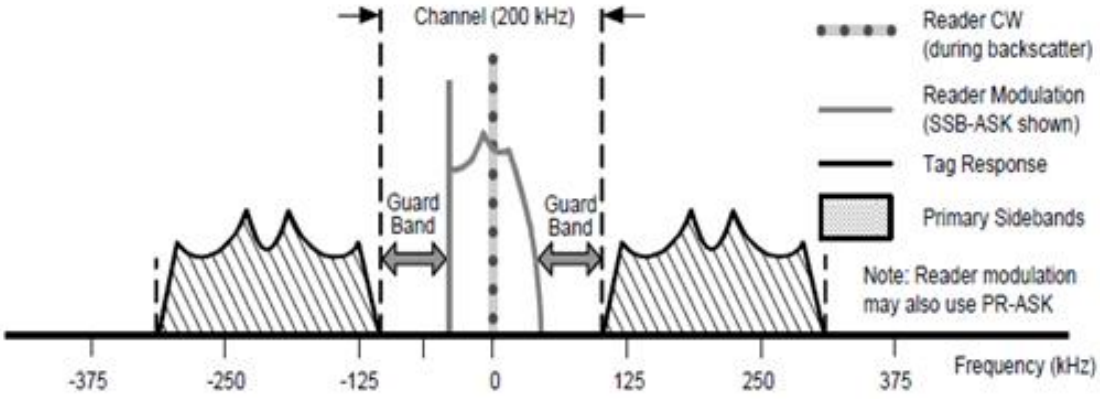


Figura 54.FDM por retrodispersión de canal adyacente, ERC REC 70-03E Anexo 11

Ejemplo 4: FDM retro dispersión en canales

Un entorno normativo hipotético asigna cuatro canales de 500 kHz y rechaza un canal adyacente y retrodispersión por límite de canal. Los interrogadores utilizará 500 canales kHz con retrodispersión de canal. Se muestran transmisiones del

[215] Ibíd., pág.94.

interrogador utilizando modulación PR-ASK con Tari = 25 ms, y 25 kbps sobre una subportadora 200 kHz (BLF = 200 kHz, M = 8).[216]

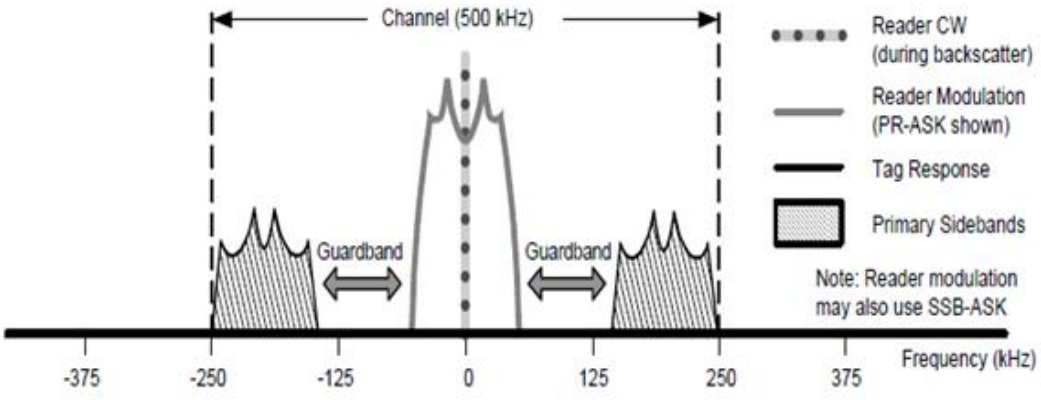


Figura. Ejemplo FDM retro dispersión en canales, epc™ radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz – 960 mhz, version 1.1.0

8.6.8 La gestión de las etiquetas o Tags.

Finalmente se analiza la forma como los interrogadores pueden gestionar la información operacional del Tag, utilizando las tres operaciones básicas[217] que se muestran en la Figura 54. Cada uno de estas opciones opera entre uno o más estados.

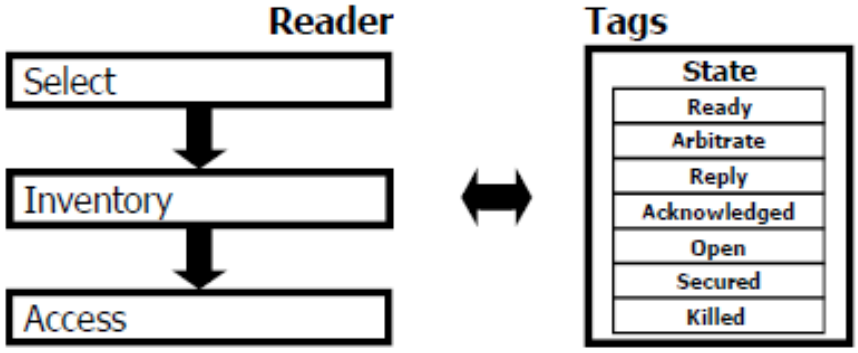


Figura 55.Operación y estado del Tag en un proceso de Interrogacion/Tag, epc™ radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz – 960 mhz, version 1.1.0

a) Select: El proceso por el cual un interrogador selecciona una población de Tag para el inventario y el acceso. Pueden utilizar uno o más comandos Select para seleccionar una población Tag determinada antes de un inventario.

[216] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.
[217] Ibíd., pág.94.

b) Inventory (Inventario): El proceso por el cual un interrogador identifica Etiquetas. Un interrogador se mantiene transmitiendo una consulta de comandos en una de las cuatro sesiones. Uno o más etiquetas pueden responder. El Interrogador detecta una única respuesta Tag.

c) Access: El proceso por el cual un interrogador realiza transacciones de lectura o escritura individuales en las etiquetas. Un Tag debe ser identificado antes del acceso. Acceso comprende múltiples comandos, algunos de que emplean una sola vez, basado en cubrimiento de codificación del enlace de R ≦ T.

Cabe destacar que en cada uno de las Query y sus respectivas Request se realiza una compracion de errores por redundancia cíclica de 16 bits. (CRC 16 Bits). El proceso para la gestión de las etiquetas por parte del interrigador se describe en la figura 55 a continuación.

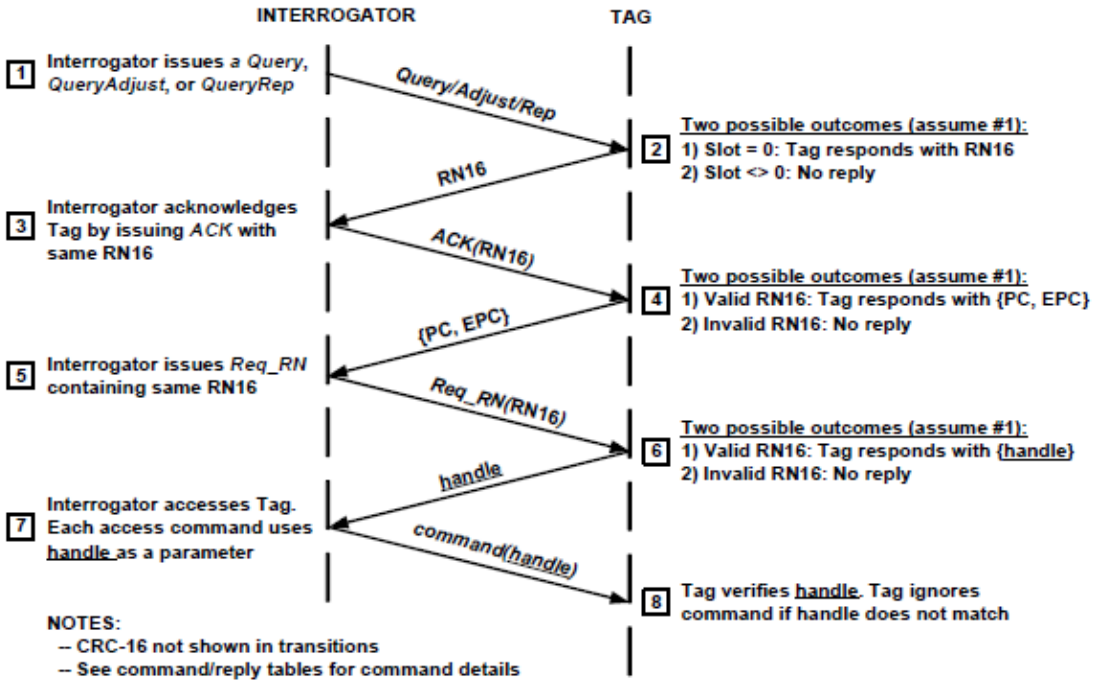


Figura 56.Ejemplo de un Inventario y acceso de un Tag. Fuente: epc™

CAPITULO II

9. FACTORES CLAVE QUE IMPULSAN EL USO DEL PROTOCOLO IP EN LOS DISPOSITIVOS PRESENTES EN EL HOGAR BASADOS EN IOT.

Como se mencionó anteriormente el uso del Internet en el término "Internet de cosas" significa que según distintas visiones no solo se puede llegar a un entorno de red que permita un uso similar al de la web que se le da hoy en día, sino que las cosas pronto también se comunicarán entre ellos, utilizando servicios, proporcionando datos y así generando valor agregado a todo servicio, en todo momento y en todo lugar. Por otra parte puede interpretarse de forma más técnica como un stack de protocolos que basados en el protocolo IP para cosas inteligentes, aunque el uso de IP no sea el primer camino para lograr la interconexión de todo con todo, sino que se enfoque mediante el uso de otro tipo de protocolos que formen una red,

Para finales del año 2012 y principios de 2013, los visionarios de un mundo conectado esperan que más de 60 millones de dispositivos en Europa estén conectados entre ellos y compartan información utilizando tecnología que comunica una máquina a otra conocida como machine-to machine (M2M), que no es otra cosa que dotar a la máquina de sistemas y lenguajes estándar para su comunicación.

Para el IoT, el Future Trends Forum[218], ha definido una pirámide con capas funcionales similares a las capas de modelos de referencia como el OSI o TCP/IP. Como se observa en la figura 56, en la base de la pirámide (Capa 1), el objeto obtiene una identidad única mediante una etiqueta RFID. En la segunda capa, se utiliza la tecnología GPS para localizar la posición o trayectoria del objeto, tal como sucede hoy en día con todos los smartphone. Una capa más arriba, se dota al objeto de estado propio, previamente definido y estandarizado que identifique su condición, es decir, que sea capaz de comunicar su estado actual y sus propiedades. Por último, y en la capa más alta, se otorga al objeto un contexto para que sea consciente y conozca el entorno en el que está y aplique inteligencia propia según la labor que desempeña.

[218] Ibíd., pág.6.

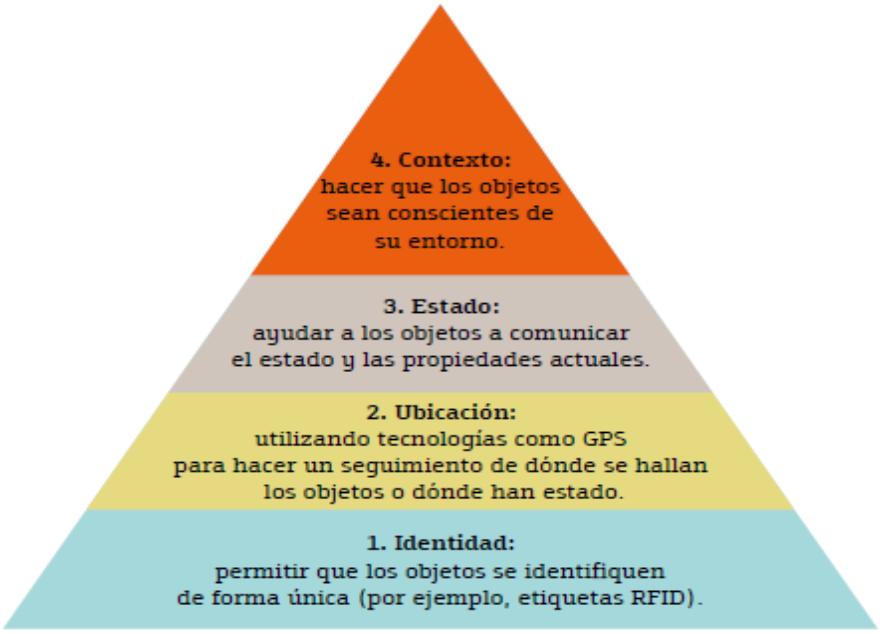


Figura 57.Modelo objeto dentro de IoT, Sensor Telemetry, Accenture,2005

Los expertos del Future Trends Forum sitúan a Estados Unidos como preferida entre las regiones que van a ser precursoras del IoT en las distintas industrias[219]. No obstante, los países de economías emergentes poco a poco han empezado a sobresalir en áreas como la innovación de tecnología, área reservada hasta ahora a los países más desarrollados. Como se muestra en la figura 57, el área del Internet de las Cosas no es la excepción a esta tendencia. China está a la par, e incluso lo supera cuando se trata de telecomunicaciones y equipos. Sobresale por otro lado, la presencia de África en sectores como tecno medicina, domótica e inmotica, así como se destaca Suramérica en energía y medio ambiente.

Por otro lado se tienen proyectos que pretenden dotar de inteligencia las grandes ciudades usando IoT. Tal es el caso de Amsterdam, donde para convertir la capital de Holanda en una ciudad inteligente, se creó el proyecto Amsterdam Innovation Motor (AIM). Un sistema que pretende la co-creación del proyecto y pedir sugerencias al usuario sobre cómo ahorrar energía y monitorizar el consumo. Otra iniciativa interesante es i-Japan Strategy 2015, que pretende construir una sociedad digital, impulsada por los ciudadanos que aplique el IoT en gestión gubernamental, sanidad y educación. Por su parte, Italia ya tiene el proyecto de smart metering más grande hasta el momento, y el Reino Unido tiene planes de equipar unos 29 millones de hogares con esa tecnología para el año 2020. Estocolmo implementó con éxito su sistema de peajes que registra las matrículas de los vehículos que pasan los puntos de control y envía una factura al domicilio del conductor o lo cobra

[219] Eva López Suárez, Cynthia Gregsamer, Javier Corsini Ramírez, El Internet de las Cosas En un mundo conectado de objetos inteligentes, Accenture España 2012

automáticamente de la cuenta bancaria on-line. En España ya existen más de dos millones de líneas móviles asociadas a máquinas y los servicios de e-Administración nacionales se sitúan entre los mejores del mundo[220]

Por su parte China tiende a convertirse en el gigante del IoT, cuando en 2010 anuncio un plan agresivo para abarcar en todo sentido el uso del IoT, mediante la creación de fondos y un marco regulatorio afín por parte del gobierno. Tanto es así, que según los miembros del Future Trends Forum, D. Jong Lok Yoon y Thomas Lee, universidades como la Jiangnan University ya incorporan una facultad de Ingeniería IoT con un extenso currículum asociado. China está potenciando una red con inteligencia superior para aumentar la proporción de energía renovable al 15% para 2020[221].

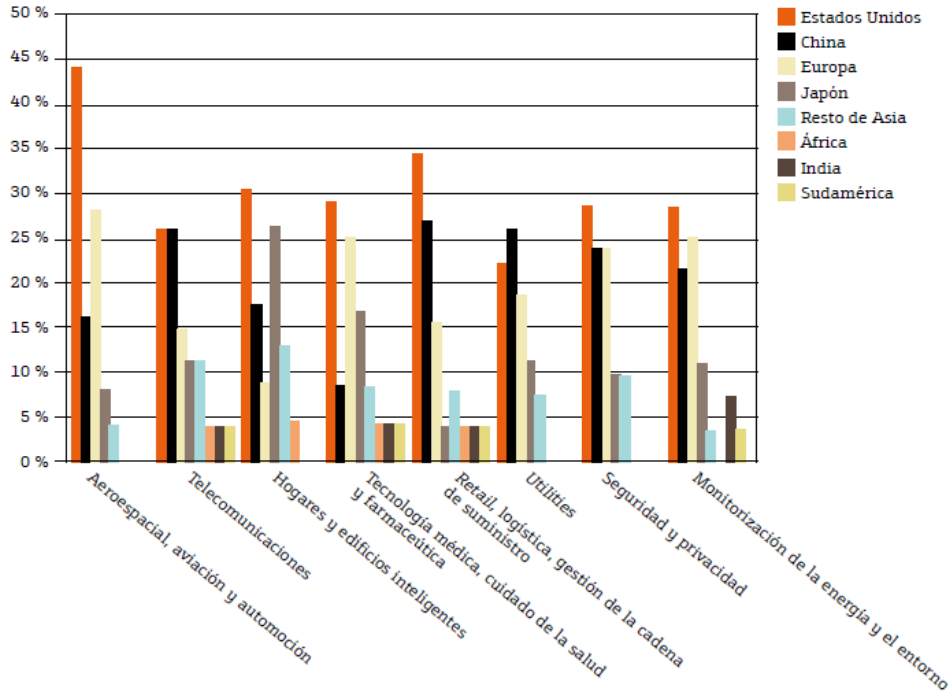


Figura 58.Pioneros en Tecnologias asociadas al IoT, Sensor Telemetry, Accenture,2005

Entonces pues, con el Internet de las cosas, el planeta está siendo instrumentado e interconectado, al tiempo que se vuelve más inteligente. Esto ocurre porque los mil millones de personas y una lista interminable de objetos conectados a Internet (carros, electrodomésticos, teléfonos, cámaras, etc.) ahora pueden interactuar, traspasando las barreras del tiempo y el espacio. A su alrededor, se construyen entornos inteligentes capaces de analizar, diagnosticar y ejecutar funciones. Por

[220] Eva López Suárez, Cynthia Gregsamer, Javier Corsini Ramírez, El Internet de las Cosas En un mundo conectado de objetos inteligentes, Accenture España 2012
[221] Ibíd., pág.16.

ejemplo, una red eléctrica inteligente basada en sistemas SCADA, es capaz de detectar sobretensiones y de dirigir la electricidad por caminos alternativos para minimizar apagones, constituyendo una aplicación de la inteligencia en los objetos y sistemas que causan impacto en la sociedad. Otro claro ejemplo de menor cuantía, es el de la cuchara electrónica que es capaz de calcular la cantidad de calorías y vitaminas que se consume con ella, o la nevera que alerta sobre la falta de un alimento en su interior y es capaz de comunicarse con el almacén para realizar el pedido respectivo, entre otras muchas aplicaciones que comienzan a hacerse más común hoy en día. En la gráfica se ilustra cómo ha sido la adopción del IoT en distintos sectores de la industria.

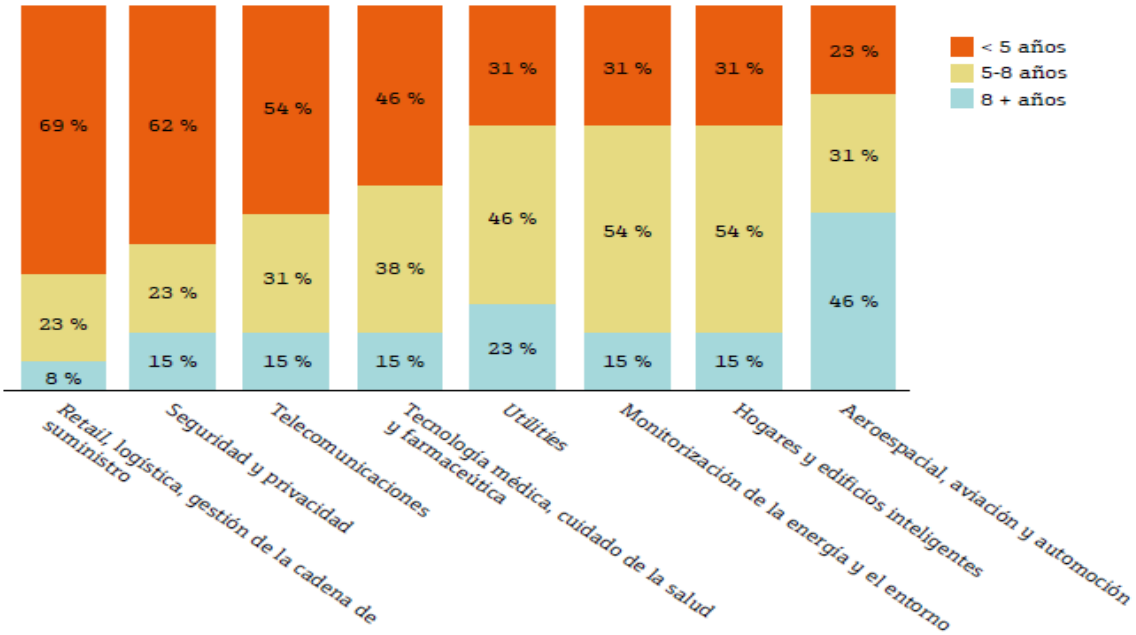


Figura 59. Tiempo de adopción del IoT en la industria, Sensor Telemetry, Accenture, 2005

CAPITULO III

10. CARACTERÍSTICAS DE DISPOSITIVOS DEPENDIENDO DE LOS PROTOCOLOS EN QUE SE BASAN SUS DISEÑOS.

10.1 X10

10.1.1 Dispositivos

Existen 5 tipos de dispositivos que conforman la topología de red del protocolo X-10, unos que se encargan de funciones específicas y otros que pueden cumplir varias de acuerdo al uso que se les vaya a dar. La gama de productos comprende transmisores, Receptores, Transceptores, Bidireccionales y equipos inalámbricos. [222]

Figura 60. Tipos de dispositivos X-10 (MARSAL, Luis. Protocolo X10. Pag. 5)

Transmisores: Solo pueden enviar información, la señal codificada de bajo voltaje (3V) que se superpone con la señal de alta tensión de la línea eléctrica (120V), el transmisor tiene la capacidad de enviar información hasta 256 dispositivos conectados en la misma red domótica. Varios transmisores pueden enviar información a varios dispositivos a la vez. [223]

Receptores: Solo reciben información de los dispositivos transmisores, y pueden comunicarse con 256 direcciones distintas, es decir que pueden recibir información de diferentes nodos.[224]

Bidireccionales: Estos dispositivos reciben la señal enviada por transmisores y tiene la capacidad de responder, si se utilizan ordenadores para el control algunos de estos dispositivos pueden comunicar su estado de igual forma encendiéndose (ON) o apagándose (OFF) confirmando que se recibió el mensaje y que se ejecutó la acción.[225]

---

[222] MARSAL, Luis. Protocolo X10. pág. 5.
[223] INFANTES D, Juan Antonio. Descripción de X-10. pág. 3.
[224] Ibíd., pág.3.
[225] Ibíd., pág.3.

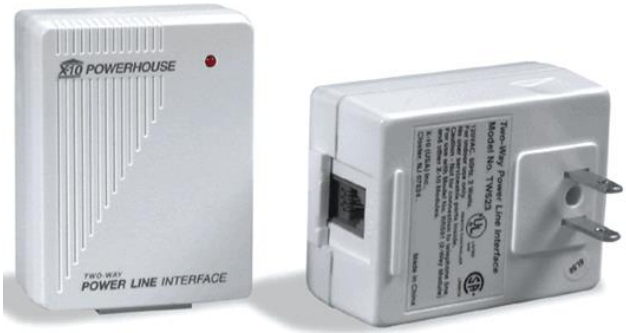


Figura 61. Modulo Bidireccional TWO-WAY (TW523) (http://www.smarthome.com/x10-tw523-x10-two-way-interface-module.html)

Inalámbricos: El protocolo X10 nos da la opción de realizar conexiones inalámbricas, mediante él envió y recepción de señales de radiofrecuencia RF desde módulos especiales con antenas integradas, que luego inyectan la señal en la línea eléctrica.[226]

Figura 62. Módulo de transceptor inalámbrico (Modelo RR501) (http://www.electronicoscaldas.com/alarmas-domotica/189-transceiver-x10-rr501.html)

10.1.2 Software

10.1.2.1 ActiveHome

El Software ActiveHome automatiza las tareas del hogar a través de un ordenador central. Los eventos se pueden programar de acuerdo a un horario, por ejemplo, puede activar cierta tarea dependiendo de la hora del día, como prender las luces cuando anochezca. Otras tareas se ejecutan durante todo el día. El software controla los dispositivos que el usuario desee gracias a los mandos a distancia que activan “macros” o grupos de acciones en el ordenador central, por ejemplo, abrir

[226] Ibíd., pág.4.

las ventanas oprimiendo un botón. ActiveHome responde a señales emitidas por sensores que actúan al detectar movimiento, luz, temperatura, entre otras variables.

Figura 63. Interface ActiveHome (web: http://activehome-pro.software.informer.com)

10.2 KNX

La tecnología KNX está respaldada por KNX Association, además de estar aprobada como estándar internacional, europeo y chino, y ser parte del desarrollo de un conjunto de grandes compañías líderes en el mercado del control, confort y seguridad del hogar (domótica e innatica); conformada por más de 300 empresas miembros, que engloban más del 80% de los dispositivos vendidos en Europa, promoviendo a KNX como el único estándar abierto mundial para el control domótico. A nivel mundial, la KNX Association posee acuerdos y asociaciones con más de 35.000 compañías alrededor de 120 países y distintos centros de formación[227].

10.2.1 Dispositivos

Una instalación KNX consta principalmente de:

- Una fuente de alimentación 29V DC.
- Sensores.
- Actuadores.
- Cable bus.

[227] Formación Estudiantes IKNX Ingeniería.

Una vez se tengan todos los elementos instalados, la programación de ellos se realizara mediante el programa ETS, donde:

- Asigna las direcciones físicas.
- Parametriza sensores y actuadores.
- Crea las direcciones de grupo.

10.2.1.1 Acoplador KNX

Es necesario el uso de acopladores para unir medios distintos o diferentes protocolos de comunicación al bus de datos utilizado por KNX y permitir la interacción, configuración y control de la red domótica.

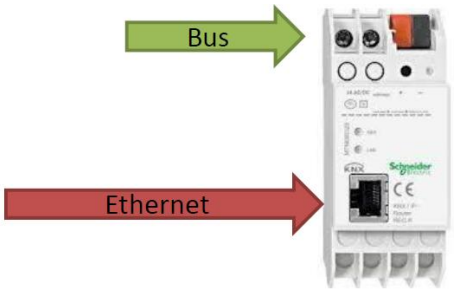


Figura 64.Acoplador KNX. (Curso iniciación al KNX).

10.2.1.2 Cable Bus EIB

Es el elemento principal en la comunicación física a en la instalación domótica y que dispone de su propia inteligencia, por lo que no es necesario una unidad central de control o servidor; además que permite ser utilizado tanto en pequeños proyectos como viviendas o en proyectos mucho más grandes como edificios, etc.[228]

Es el encargado de dar alimentación a los aparatos y transmitir la información. Está compuesto por:

- Par de cables rojo y negro:
  - Rojo: positivo.
  - Negro: negativo.

- Par de conductores de reserva amarillo y blanco:
  - Amarillo: positivo EIB, comunicación KNX.
  - Blanco: negativo EIB, comunicación KNX.

[228] Curso iniciación al KNX, op. cit, pág.12.

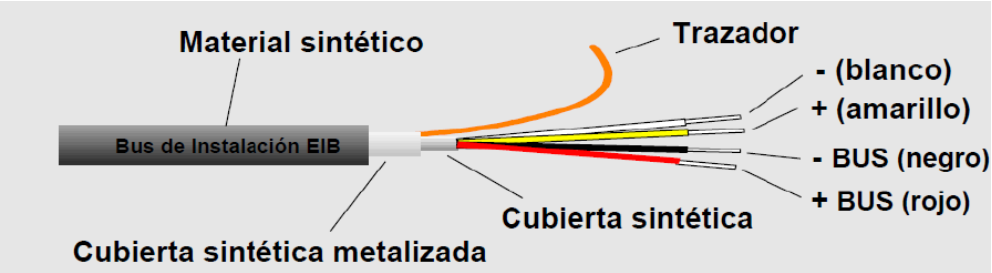


Figura 65.Cable Bus EIB. (Curso iniciación al KNX).

10.2.1.3 Fuente de alimentación KNX

Las fuentes de alimentación KNX producen y controlan la tensión necesaria para el funcionamiento del sistema y los dispositivos que la conforman. Donde se debe tener en cuenta la corriente utilizada que permitirá conectar más o menos dispositivos a la red KNX[229].

Figura 66.Fuente de alimentación KNX. (LÓPEZ, Diego. Domótica y eficiencia en edificios.).

10.2.1.4 Conectores bus para bus KNX

Los conectores para el bus de comunicación KNX permiten:

- Ramificar y extender el cable bus.
- Proteger los extremos del cable bus.
- Conectar el cable bus a otros dispositivos empotrados.
- Conectar el cable bus a dispositivos de montaje superficial.
    - Parte roja: positivo. Parte negra: negativo.

[229] Ibíd., pág.58.

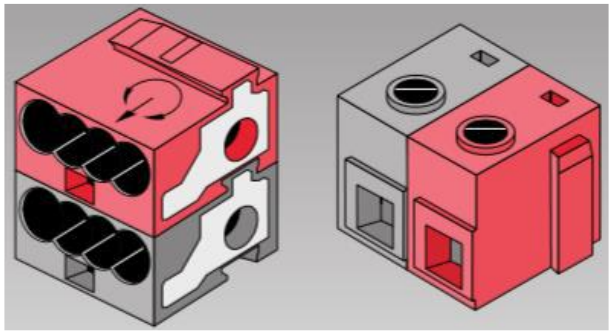


Figura 67.Conectores bus para bus KNX. (Curso iniciación al KNX).

10.2.1.5 Terminal de protección contra sobretensiones

Son dispositivos de seguridad que descargan los dos conductores del bus, evitando grandes diferencias de tensión entre el bus de comunicación y los dispositivos integrados a este[230].

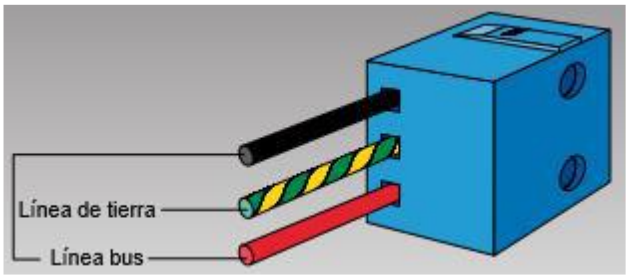


Figura 68.Terminal de protección contra sobretensiones. (Curso iniciación al KNX).

10.2.1.6 Actuadores binarios

Son dispositivos que conectan y desconectan las cargas o actuadores que interpretan este tipo de señal. Existen de varios tipos en función de[231]:

- Composición interna: mecánicos o electrónicos.
- Número de canales.
- Intensidad máxima por canal.
- Con o sin detección de corriente.

[230] Ibíd., pág.61.
[231] Ibíd., pág.62.

Figura 69.Actuadores binarios. (Curso iniciación al KNX).

10.2.1.7 Acopladores de línea/área

Son los encargados de conectar los segmentos de línea a líneas y posteriormente a áreas, permitiendo o filtrando los telegramas a los dispositivos o el paso de unos niveles a otros[232].

Figura 70.Acopladores de línea/área. (Curso iniciación al KNX).

10.2.1.8 Interface USB (programador)

Permite la conexión de un dispositivo por medio de la interfaz USB para el diagnóstico o programación al bus y sus dispositivos[233].

[232] Ibíd., pág.66.
[233] Ibíd., pág.67.

Figura 71.Interface USB. (Curso iniciación al KNX).

10.2.1.9 KNX IP ROUTER

Permite la conexión de un dispositivo por medio de la interfaz Ethernet al bus KNX, para realizar operaciones de diagnóstico o programación en red KNX. Además se puede utilizar como acoplador de líneas o áreas[234].

Figura 72.KNX IP ROUTER. (Curso iniciación al KNX).

10.2.1.10 Interface RS232

Permite la conexión de un dispositivo por medio de la interfaz Serial – RS232 al bus para el direccionamiento, configuración, parametrización de los dispositivos acoplados en la red domótica[235].

Figura 73.Interface RS232. (LÓPEZ, Diego. Domótica y eficiencia en edificios.).

10.2.1.11 Pulsadores

Permiten la pulsación, regulación, conexión, etc., de los distintos que conforman la instalación de la red domótica KNX[236].

[234] Ibíd., pág.68.
[235] LÓPEZ, Diego. Domótica y eficiencia en edificios. Pág.64.
[236] Curso, op. cit, p.69.

Figura 74.Pulsador KNX. (Curso iniciación al KNX).

10.2.1.12 Termostatos

Controlan todas las funciones del clima y es el componente de un sistema de control simple que abre o cierra un circuito eléctrico en función de la temperatura[237].

Figura 75.Termostato KNX. (Curso iniciación al KNX).

10.2.1.13 Módulos de entradas

Son los encargados de captar una señal de entrada para enviar una orden o transferencia de datos al bus, ya sea en función a la tensión de entrada y/o señal analógica[238].

Figura 76.Módulos de entradas KNX. (Curso iniciación al KNX).

[237] Ibíd., pág.70.
[238] Ibíd., pág.71.

10.2.1.14 Detectores de movimiento y presencia:

- Movimiento: si detectan movimiento y las condiciones de luminosidad no son suficientes conectan o desconectan el alumbrado, dependiendo de la configuración establecida en la red KNX.
- Presencia: si detectan movimiento y las condiciones de luminosidad no son suficientes conectan el alumbrado o desconectan el alumbrado, dependiendo de la configuración establecida en la red KNX. En cuanto las condiciones de luminosidad mejoran el alumbrado se desconecta[239].

Figura 77.Detectores de movimiento y presencia KNX. (Curso iniciación al KNX).

10.2.1.15 Sensores meteorológicos y de ambiente:

Captan las señales o magnitudes físicas del medio donde están instalados y envían la información al bus. Nos podemos encontrar entre otros[240]:

- Crepuscular: captan la luminosidad exterior.
- Sensores de CO2, humedad y temperatura: se utilizan para tener valores representativos de estas variables en diferentes entornos en donde actué la red KNX.
- Centrales meteorológicas: recogen datos como velocidad del aire, temperatura y otras variables para su posterior procesamiento en sistema.

Figura 78.Sensores meteorológicos y de ambiente KNX. (Curso iniciación al KNX).

[239] Ibíd., pág.73.
[240] Ibíd., pág.76.

10.2.1.16 Sensores de alarmas técnicas:

Son los encargados de tomar las distintas señales y dar avisos de alarma por humo, inundación, entre otras[241].

Figura 79.Sensores de alarmas técnicas KNX. (Curso iniciación al KNX).

10.2.1.17 Interruptores horarios

Conectan y desconectan los distintos circuitos que conforman la red domótica KNX en función de su programación horaria establecida de forma diaria, semanal o anual[242].

Figura 80.Interruptores horarios KNX. (Curso iniciación al KNX).

10.2.1.18 Interfaces de sistemas de climatización

Son las pasarelas de comunicación entre la domótica KNX y un dispositivo de clima de un fabricante diferente a KNX, permitiendo la interoperabilidad entre estos sistema[243].

Figura 81.Interfaces de sistemas de climatización KNX. (Curso iniciación al KNX).

[241] Ibíd., pág.77.
[242] Ibíd., pág.78.
[243] Ibíd., pág.79.

10.2.1.19 Terminal táctil

Son los elementos que permiten interactuar con la domótica y configurar los sistemas al usuario final, por medio de una interfaz amigable[244].

Figura 82.Terminal táctil. (Curso iniciación al KNX).

10.2.1.20 Servidores WEB

Nos permiten controlar nuestra instalación domótica desde cualquier dispositivo de una forma remota, pues estos se encuentran conectados directamente a la red KNX.

Figura 83.Servidores WEB Schneider Electric para KNX. (Curso iniciación al KNX).

10.2.2 Software

La herramienta de software para la programación de la instalación para KNX/EIB es el ETS (ETS, Engineering Tool Software) que se estructura de forma flexible y modular para poder facilitar futuras ampliaciones en la red domótica KNX[245]; además de ser un software común a todos los fabricantes que sirve para diseñar y configurar instalaciones inteligentes para el control de viviendas y edificios basadas en KNX, además de funcionar en ordenadores con sistema operativo Windows ©.

Estructurado en los siguientes programas[246]:

- **ETS Tester:** Es el programa de aprendizaje del ETS- 3 Starter, y su objetivo es iniciarse en el sistema.

[244] Ibíd., pág.80.
[245] Montaje y puesta en marcha en servicios de instalaciones con bus KNX/EIB. pág.10.
[246] Ibíd., pág.10.

- **ETS Starter:** Está dirigido al diseño de pequeñas redes domóticas KNX (una línea, 64 dispositivos) con aplicaciones limitadas, como control de la iluminación, persianas y control individual de la temperatura.
- **ETS Profesional:** Proporciona un control total de la instalación y dispone de conexión por USB, sistema multitarea, descarga simultánea de diferentes dispositivos y diseño de la red, etc.

Por medio del software se presentan los parámetros en forma de árbol, la versión profesional integra todas las funcionalidades de diseño de proyectos y la parametrización en un solo entorno de trabajo. ETS es una herramienta de software completamente nueva que puede instalarse en un PC para configurar los dispositivos y crear bases de datos para la red domótica, además de realizar todas las funciones de programación, puesta en marcha y diagnóstico de la instalación, sin tener que abrir o cerrar otros módulos del programa, por lo que simplifica el trabajo de diseño del sistema KNX/EIB[247].

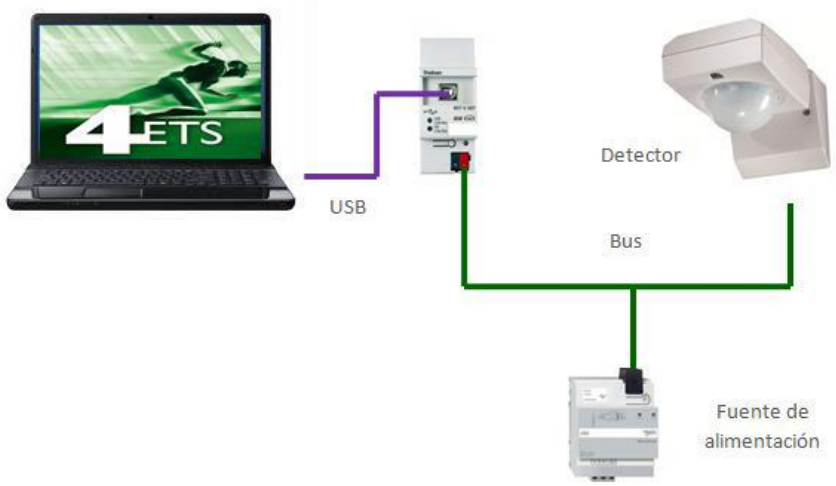


Figura 84 .Puesta en marcha de una instalación KNX mediante ETS. (Curso iniciación al KNX).

[247] Ibíd., pág.10.

10.3 LONWORKS

10.3.1 Dispositivos

La arquitectura de red de los sistemas Lonworks está conformado principalmente por nodos que se encuentra en un segmento de la red. Los repetidores que interconectan dos segmentos, y por ultimo un enrutador (router) en cada línea de la topología.

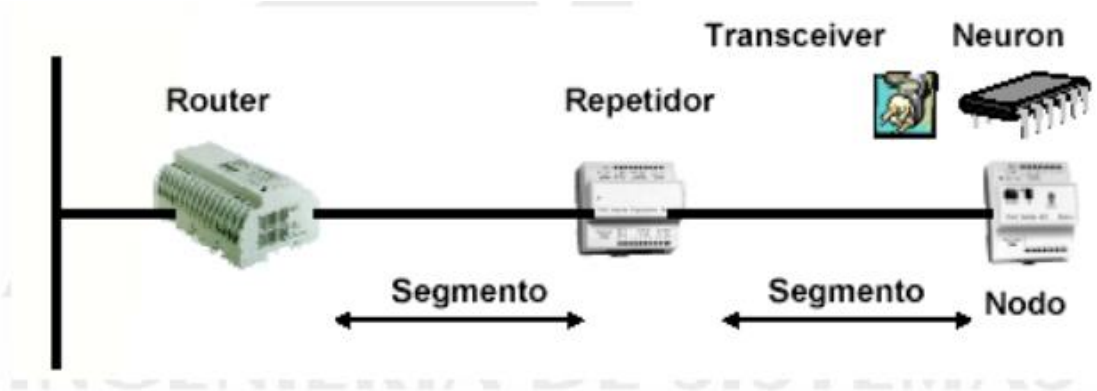


Figura 85. Arquitectura de red Lonworks
(http://isa.uniovi.es/docencia/AutomEdificios/transparencias/LonWorks.pdf)

10.3.1.1 Módulos LonPoint – Nodos

Estos nodos están conformados por Neuron Chip. Los nodos se comunican entre sí utilizando el protocolo LonTalk establecido en el estándar EIA 709.1, garantizando la interoperabilidad entre dispositivos de diferentes fabricantes. Los nodos deben poder ser instalados con una herramienta de gestión de red abierta.[248]

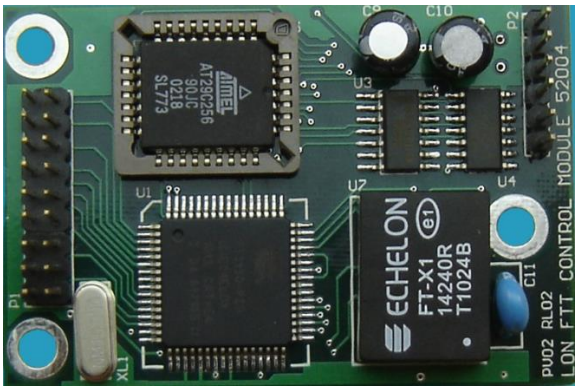


Figura 86. Módulo de control de LonPoint. (http://www.lonworks.org.cn/en/index.html)

[248] Sistema LonWorks. Automatización Integral de Edificios. pág. 27

10.3.1.2 Chip Neuron

En cada chip se encuentra implementado el protocolo LonTalk, el sistema operativo, las funciones de entrada y salida E/S, y un identificador (Neuron ID) único de 48 bit insertado de fábrica.[249]

10.3.1.3 Módulos Routers

Este módulo se encarga de reducir el tráfico de la red ya que tiene en cuenta el destino del mensaje aislando paquetes y restringiendo el tráfico para no congestionar el canal, es la puerta de enlace a otros medios físicos de transmisión.[250]

Figura 87. Router Echelon. (http://www.metz-connect.com/en/system/files/styles/large/private/productfiles/productimage_11021302.png?itok=KgWjaEfJ)

10.3.1.4 Repetidores

Conecta dos segmentos de la línea o bus de datos, diferenciando dos subredes de Lonworks, amplificando la señal en ambas direcciones aumentando el alcance. Envían mensajes sin tener en cuenta el destino y acopla dos medios de comunicación pero estos deben ser el mismo medio de comunicación.

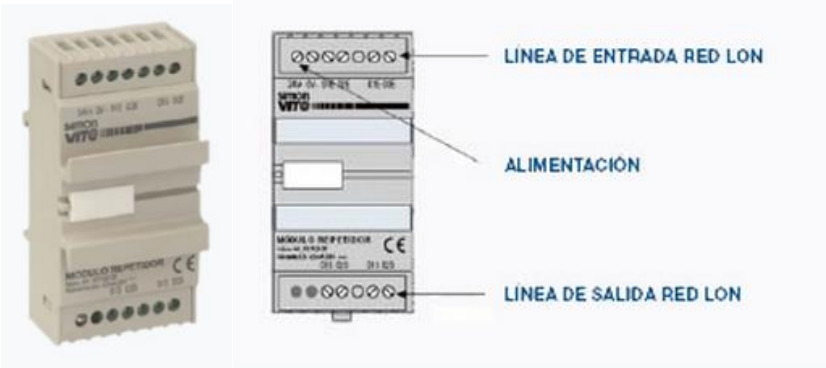


Figura 88. Módulo Repetidor. (http://www.simondomotica.es/images/funcionamiento2%20repetidor.jpg)

[249] Ibíd., pág.20.
[250] Ibíd., pág.29.

10.3.2 Software

10.3.2.1 LonMaker (Turbo Edition) Echelon

LonMaker es un de software de diseño, gestión y mantenimiento de redes LonWorks independiente del fabricante del dispositivo. El software permite el diseñar e instalación de la red de control. Los elementos de LonMark se representan como bloques gráficos funcionales de fácil visualización y diseño del sistema de control y su respectiva lógica de programacion.

CARACTERÍSTICAS:

- Entorno gráfico de diseño, instalación, gestión y mantenimiento de redes LonWorks.
- Incluye Sistema Operativo de red LNS® Edición Turbo y Microsoft Visio® 2010.
- Permite modificación simultánea de múltiples usuarios sobre los diferentes dispositivos.
- Selección automática de tipos de conexiones de red para reducir errores en conexiones.
- Incluye una interfaz simplificada para reducir el tiempo de ingeniería de diseño.
- Incluye los componentes SmartShape® del interface de gestión Visio.
- Es compatible con otras herramientas y aplicaciones con capacidad de importar y/o exportar XML.

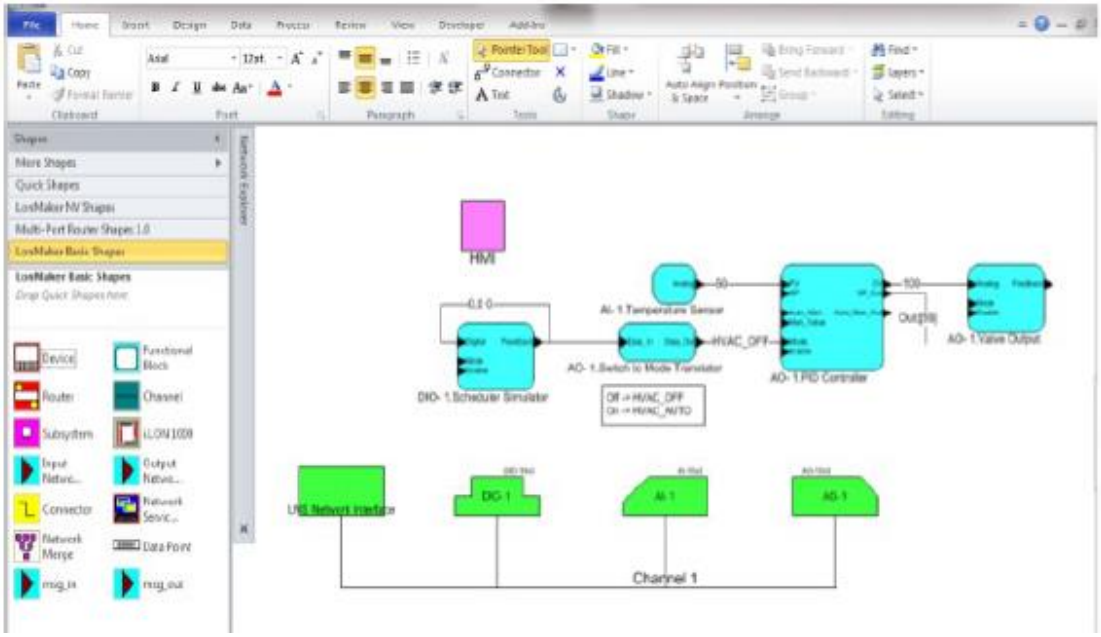


Figura 89. Interfaz LonMaker. (www.aditel-sistemas.com)

10.4 ZigBee

Desde que apareció la primera especificación del protocolo ZigBee, se han desarrollado distintos tipos de dispositivos capaces de utiliza este protocolo, debido a su bajo coste de fabricación, el precio no sería muy costoso a comparación de otros dispositivos domóticos, en cuanto a tecnología es utilizada por muchas empresas por lo tanto, se han desarrollado gran cantidad de dispositivos. Fabricando componentes de bajo nivel, que llevan embebido procesadores y sistemas capaces de trabajar con este protocolo directamente desde cualquier ordenador u otro dispositivo; los que llevaría a esta tecnología a tener gran variedad dispositivos en el campo de la domótica[251].

10.4.1 Dispositivos

10.4.1.1 Dispositivos de Bajo Nivel

Existen varias empresas que ofrecen componentes ZigBee, como también ofrecen paquetes o conjuntos de desarrollos más especializados, y no son del todo compatibles con el resto de dispositivos ZibBee[252].

10.4.1.1.1 EasyBee

Una de las empresas desarrolladoras de dispositivos ZigBee, es una alianza entre rfSolutions y FlexiPanel; desarrollando el dispositivo EasyBee; que es un transceptor RF que cumple la normativa IEEE 802.15.4, que trabaja dentro de una red ZigBee como un dispositivo final[253].

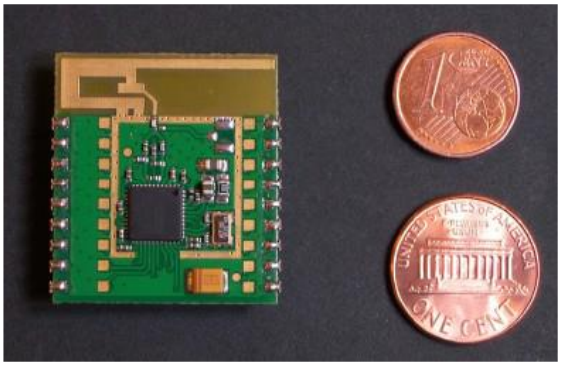


Figura 90.Dispositivo EasyBee. (Moreno, Javier. Fernández, Daniel.2007)

Es un dispositivo pequeño (26mmx20mm), que consume de 2.1V a 3.6V y puede trabajar a temperaturas entre -40ºC y 85ºC. También pueden comunicarse con otros

[251] MORENO, Javier. FERNÁNDEZ, Daniel. Informe Técnico: Protocolo ZigBee, pág.28.
[252] Ibíd., pág.28.
[253] Ibíd., pág.28.

dispositivos de la red ZigBee en el rango de doscientos metros de distancia, con una velocidad de transferencia de 25kbps y sus aplicaciones son[254]:

- Reemplazar el cableado de cualquier red.
- Automatismos en viviendas.
- Redes y control industrial.
- Sensores para redes inalámbricas.

10.4.1.1.2 Pixie

También entre los dispositivos de bajo nivel se encuentra uno más potente llamado Pixie. Este dispositivo es una serie compuesta por dos dispositivos, con funciones de Coordinador y Router, con las mismas características técnicas pero con mayor capacidad de procesamiento que el EasyBee, siendo dispositivos más potentes dentro la red domótica ZigBee[255].

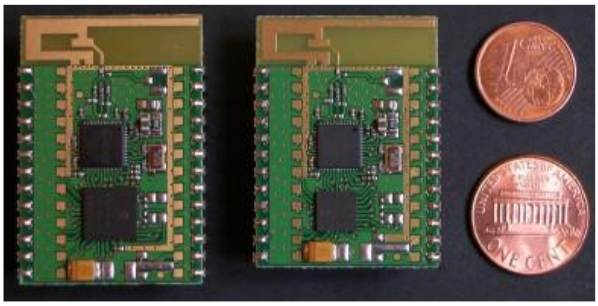


Figura 91.Dispositivo serie Pixie. (Moreno, Javier. Fernández, Daniel.2007).

10.4.1.1.3 Pixie Configuration Tool

Otro elemento interesante es un cable de conexión USB, que permite conectar de forma serial un ordenador a los dispositivos ZigBee; para configurar y manejar los dispositivos de la red.

Figura 92.Pixie Configuration Tool. (Moreno, Javier. Fernández, Daniel.2007).

[254] Ibíd., pág.29.
[255] Ibíd., pág.30.

10.4.1.1.4 Pixie Evaluation Kit

Permite probar los diseños de la red ZigBee y trabajar directamente sobre sus dispositivos; permitiendo su control, programación y análisis de funcionamiento.

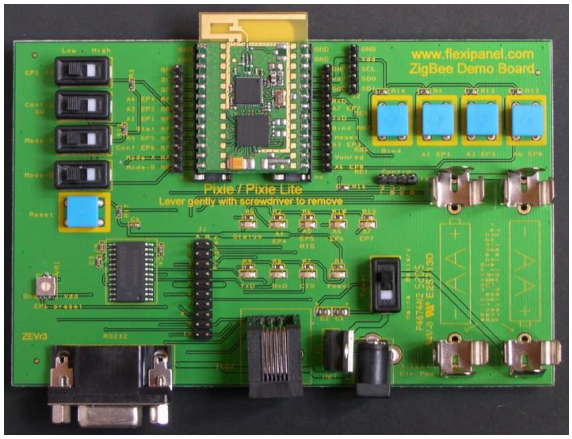


Figura 93.Pixie Evaluation Kit. (Moreno, Javier. Fernández, Daniel.2007).

Telegesis es una empresa que dispone de dispositivos para el protocolo ZigBee, que se pueden utilizar como dispositivos finales, así como de Routers y Coordinadores, es decir un kit todo en uno basado en sus dispositivos[256].

10.4.1.1.5 ETRX1

Dispositivo de bajo costo, con dimensiones 27.75x20.45mm, que consume de 2.1V a 3.6V y puede trabajar a temperaturas entre -40ºC y 85ºC; y ´puede utilizarse como dispositivo final, como de Coordinador de la red ZigBee[257].

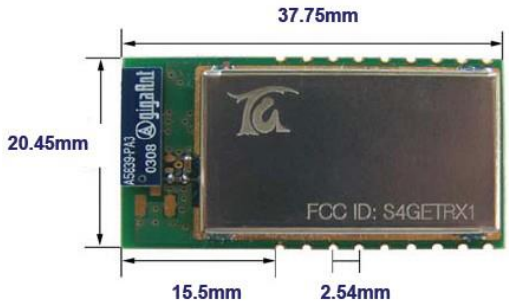


Figura 94.ETRX1. (Moreno, Javier. Fernández, Daniel.2007).

Siendo sus aplicaciones:

- Lectura automática de métricas.

[256] Ibíd., pág.30.
[257] Ibíd., pág.31.

- Alarmas Wireless y Seguridad.
- Automatismos de viviendas.
- Sensores de presencia inalámbricos.
- Control industrial.
- Periféricos de PC.

10.4.1.1.6 ETRX2

Posee una memoria flash de 128k y otros 5kbytes de SRAM, permitiéndole actuar como cualquier tipo de dispositivo dentro de una red ZigBee, "además de la posibilidad de conectar tres tipos de antenas de forma simultánea al dispositivo, lo lleva a abarcar distancias muy superiores que las indicadas en el protocolo, para programar ambos dispositivos (ETRX1-2) se dispone de un interfaz en línea de comandos, que de forma muy intuitiva y sencilla, lo que hace que no sea necesaria mucha experiencia en módulos RF para su programación y sus aplicaciones son"[258]:

- Todas las aplicaciones de los dispositivos anteriores, y unas más potentes:
    - Controles industriales M2M.
    - Sistemas ZigBee futuros.

Figura 95.ETRX2. (Moreno, Javier. Fernández, Daniel.2007).

10.4.1.1.7 ETRX1DVK ó ETRX2DVK Devkit

Kit de desarrollo para trabajar sobre el protocolo ZigBee y sus dispositivos, con la posibilidad de hacer modificaciones, configuraciones, aplicaciones y nuevos desarrollos. Se utiliza el cable serie directamente, sin tener que utilizar un USB de intermediario (USB - Serie). Además de contener dispositivos de tipo ETRX1 o ETRX2 para trabajar desde el primer momento[259].

[258] Ibíd., pág.31.
[259] Ibíd., pág.32.

Figura 96.ETRX1DVK. (Moreno, Javier. Fernández, Daniel.2007).

10.4.1.2 Dispositivos de Alto Nivel

"Son dispositivos totalmente independientes y que no están compuestos sólo por los componentes electrónicos que soportan el estándar, sino que además ya disponen de interfaz que nos permite trabajar con ellos directamente sobre redes ZigBee."[260]

10.4.1.2.1 ETRX1USB

Diseñado por la empresa Telegesis, es un dispositivo totalmente operativo, dentro de una USB. Basado en ETRX1/ETRX2, es un dispositivo que trabaja en la banda de frecuencia de los 2.4GHz, con alcance de hasta 100m de distancia para conectarse y comunicarse con otros dispositivos ZigBee; además de poseer una antena omnidireccional y una capacidad para usar hasta 16 canales para las búsquedas de dispositivos[261].

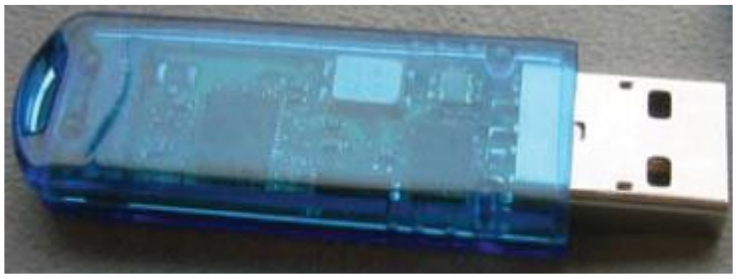


Figura 97.ETRX1USB. (Moreno, Javier. Fernández, Daniel.2007).

[260] Ibíd., pág.33.
[261] Ibíd., pág.33.

10.4.1.2.2 ETRX1CF

Es la evolución del sistema ETRX2 a ETRX2CF también desarrollado por Telegesis, se trata de un dispositivo en tarjeta Compact Flash. Permitiendo que sea utilizado desde un PC, utilizando el mismo sistema que las tarjetas PCMCIA y ser utilizado desde una agenda electrónica o PDA, abarcando las mismas características y especificaciones que el USB[262].

Figura 98.ETRX1CF y PDA. (Moreno, Javier. Fernández, Daniel.2007).

10.4.2 Software

El fabricante añade el sistema operativo embebido sobre los dispositivos pertenecientes a la red domótica ZigBee y permitir la comunicación, programación y operación. Donde actualmente existen dos sistemas operativos[263], como lo son:

Hyperterminal

Es un entorno que permite la comunicación por medio del puerto RS232 con los dispositivos a través de comandos AT. Estos comandos permiten ra realizar las operaciones más básicas, y otros comandos AT especiales, que nos permiten crear, buscar una red, expulsar dispositivos y enviar información dentro de la red, etc. Existen comandos AT propietarios que dependen del fabricante del dispositivo, como es el caso de los dispositivos de Telegesis, que proporciona un entorno de acceso propio, que contiene las opciones más comunes en botones que permiten que la comunicación y las operaciones se realicen en pocos clics[264].

TinyOS

Sistema operativo basado en Unix y de código abierto, orientado a componentes para redes de sensores inalámbricas. Utilizado en los dispositivos ZigBee. Donde es necesario el uso de un puerto serie para su comunicación con el dispositivo o la red ZigBee. Para el desarrollo de aplicaciones puede utilizar varios leguajes de programación entre los que se encuentra Java y el código Bash, aunque el principal

[262] Ibíd., pág.33.
[263] Ibíd., pág.34.
[264] Ibíd., pág.34.

es el lenguaje nesC, orientado y optimizado para las limitaciones de memoria y comunicación de este tipo de redes[265].

Este software proporciona interfaces, módulos y configuraciones específicas e interfaces estándar para entradas y salidas de hardware, es decir interfaces específicas para la programación de los dispositivos de la red ZigBee. TinyOS 2.0 dispone de un entorno de programación para Linux y Windows, además de la versión Boomerang[266].

10.5 DISPOSITIVOS IOT

Los dispositivos de IoT están siendo desarrollados teniendo en cuenta parámetros como la frecuencia de operación que se adapte a las regulaciones impuestas por cada país, la potencia nominal de alimentación de manera que se utilice la menor cantidad posible de recursos de generación, entre otros aspectos técnicos, que se suman a la necesidad de mantener la seguridad y la privacidad de la información de los objetos y personas en la red. La empresa Fortinet en Julio de 2014 afirma que "La batalla por el Internet de las Cosas apenas ha comenzado. De acuerdo con la firma de investigación de la industria IDC, se prevé que este mercado alcance los $7.1 billones de dólares en 2020," donde "Definitivamente los ganadores de los hogares conectados a Internet de las Cosas serán aquellos fabricantes que pueden proporcionar un equilibrio entre seguridad y privacidad versus precio y funcionalidad".[267]

Dentro de los fabricantes más destacados de productos enfocados en satisfacer las necesidades del IoT que basan sus desarrollos en tecnología RFID podemos hacer distinción en varias categorías:

10.5.1 Fabricantes de integrados

La tendencia es la implementación de transponders (interrogadores) de UHF de tamaño reducido pero con alto espacio de memoria de manera que se cumpla con el estándar EPC ClassI Gen2. Hasta la segunda mitad de 2006, este mercado ha estado controlado por el fabricante de integrados Impinj. Actualmente, el mercado ha visto los lanzamientos de los integrados XRAG2 del fabricante ST Microelectronics, y del integrado Gen2 de Texas Instruments. La compañía Philips Semiconductors anunció anteriormente la disponibilidad de su integrado UCODE Gen2.[268]

---

[265] Ibíd., pág.35.
[266] Ibíd., pág.35.
[267] Fortinet ® (NASDAQ: FTNT), Diario TI 02/07/14 16:14:24
[268] LIBERA WP-RFID-001 © 2010 RFID: Tecnología, Aplicaciones Y Perspectivas

Estándar	ISO18006B	EPC Class1 Gen2			
Característica	Philips v.1.19	Philips UCODE Gen2	Monza de Impinj	Texas Instruments	XRAG2 Stmicroelectronics
Tasa de datos	hasta 40 Kbps	HASTA 640 Kbps			
Estructura de memoria	96 bits EPC + 256 User Memory	96 bits EPC+32 bits TID+32 bits KILL password+32 bits. ACCESS password+128 bits	Tres opciones: 1.Monza:96 bits EPC+32 bits TID+32 bits KILL password+32 bits ACCESS password 2.Monza/ ID: dispone de un ID locked único. Factory Programmed Serial Number 3.Monza/64: Dispone de 64 bits de User Memory reescribible	96 bits EPC+32 bits TID+32 bits KILL password+32 bits ACCESS password	Dos versiones: 64 bits TID+ 64 bits RESERVED+(304 ó 176 bits de EPC)+ (0 ó 128 bits de User Memory)
Alcance	Hasta 7 metros (dependiendo de la antena usada y las características del objeto y del entorno)				

Tabla 3 Fabricantes de Integrados RFID, LIBERA WP-RFID-001 © 2010 RFID: TECNOLOGÍA, APLICACIONES Y PERSPECTIVAS

A continuación se presentan las principales características de los integrados para RFID según el tipo de fabricante.

10.5.2 Fabricantes de tags

La evolución actual se dirige a la creación de etiquetas UHF, que puedan contener antenas de tamaño considerable adheridos a la etiqueta, o que hagan parte intrínseca de la forma mecánica de la misma. En la tabla se observan distintos modelos de TAG según el fabricante.

TIPO DE TAG	FABRICANTE TAG	MODELOS	INTEGRADO RFID
PASIVOS	TEXAS		TEXAS IC

	ALIEN		MONZA IMPINJ
	OMRON		EPCglobal Class1/ST Microelectronics
	RAFSEC		Impinj EPC
	INTERMEC		Philips IC ISO180006/EPC Class1 Gen2
ACTIVOS	IDENTEC		Propietario

Tabla 4. Fabricantes de Tag, LIBERA WP-RFID-001 © 2010 RFID: TECNOLOGÍA, APLICACIONES Y PERSPECTIVAS

10.5.3 Fabricantes de equipos

En cuestión de lectores, Symbol, Intermec, Omron y Alien son las empresas con mayor implantación en el mercado. La mayoría de ellas, disponen en el mercado de alguna versión compatible con el estándar europeo ETSI 302-208 que permite un mayor rango de frecuencias y una mayor potencia de transmisión (0.5W).[269]

Todos los lectores no han sido desarrollados para poder interactuar entre distintos fabricantes, sino que están atados a características únicas de los Tags, frecuencias distintas de operación y otros factores que imposibilitan el uso de un lector para cualquier tipo de tag.

Adicionalmente, las antenas utilizadas variarán en ganancia, polarización y radiación, así como en su frecuencia de funcionamiento, según el país y, por tanto, la normativa aplicable en él, la aplicación a implementar y también el lector a usar. La mayoría de los fabricantes de lectores y tags ofrecen también la posibilidad de

[269] LIBERA WP-RFID-001 © 2010 RFID: TECNOLOGÍA, APLICACIONES Y PERSPECTIVAS

adquirir antenas de forma externa al lector moldeándose a cualquier entorno en el que se desempeñe.

Para los lectores, los fabricantes ofrecen modelos independientes de la tecnología de los tags, soportando los distintos estándares disponibles (EPC Class 1 Gen 1, EPC Class 0, EPC Class 1 Gen 2, Clase 0+, ISO18000 6, y Philips UCODE 1.19.)[270]

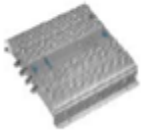
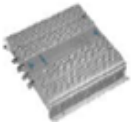
Estándares	SYMBOL	INTERMEC	OMNRON	ALIEN
Multiprotocolo: ISO180006B EPCClass1Gen2 (300-220; 0.5W) Philips v.1.19		Reader Fijo IF5  Reader Portátil IP4 		
EPCClass1Gen2 (USA/Cánada)	Reader Portátil IMC9060-G 		Reader Fijo V750-BA50C04-US 	Reader Fijo AL-9800 
EPCClass1Gen2 (302-208; 2 W)	Reader Fijo XR480 		Reader Fijo V750-BA50C04-EU 	Reader Fijo AL-8800 

Tabla 5. Fabricantes de Lectores RFID, LIBERA WP-RFID-001 © 2010 RFID: TECNOLOGÍA, APLICACIONES Y PERSPECTIVAS

[270] Ibíd., pág.12.

CAPITULO IV

11. IMPACTO DEL INTERNET DE LAS COSAS EN EL DESARROLLO ACTUAL DE LA DOMÓTICA Y LOS BENEFICIOS O DESVENTAJAS.

11. 1 DEFINICION TECNICA PARA LA IMPLEMENTACION DE IOT.

La Internet de las cosas desde un punto de vista técnico, no es el resultado de una sola tecnología novedosa, sino que consiste en varios avances técnicos complementarios que proporcionan capacidades y que en conjunto ayudan a reducir la brecha entre el mundo virtual y físico[271] Según Friedemann Mattern y Christian Floerkemeier, estas capacidades incluyen:

- **Comunicación**: Los objetos tienen la capacidad de estar en red con recursos de Internet (Protocolo IPv6) o incluso con otros, hacer uso de los datos y servicios y actualizar su estado en tiempo real. La tecnologías inalámbricas como GSM y UMTS, 4G (LTE), Wi-Fi, Bluetooth, ZigBee, RFID y varios otros estándares de red inalámbricas son de primordial importancia, sobre todo este último que se constituye como la tecnología pionera para el desarrollo del IoT.

- **Control y Direccionamiento**: Dentro del Internet de las cosas, los objetos pueden ser ubicados y dirigidos a través de servicios de búsqueda, identificación de nombres (ONS) y por lo tanto remotamente gestionados y configurados.

- **Identificación**: Los objetos son identificables de forma única. RFID, y NFC (Near Field Communication) son ejemplos de tecnologías que pueden identificarse incluso si son objetos pasivos que no tienen recursos energéticos integrados. La identificación permite que los objetos estén ligados a información asociada con el objeto concreto y que se pueda recuperar de un servidor.[272]

- **Detección:** Los objetos recopilan información sobre su entorno con sensores, guardan información, envían órdenes o accionan directamente sobre él.

- **Actuación:** Los objetos contienen actuadores propios de su estructura física para manipular su entorno, o por ejemplo, convertir las señales eléctricas en movimiento mecánico. Estos actuadores pueden utilizarse para controlar de forma remota procesos reales, en tiempo real a través de Internet.

---

[271] Friedemann Mattern, Christian Floerkemeier, Desde la Internet de los equipos hacia la Internet de las cosas, Grupo de sistemas Distribuidos, Instituto de computación ubicua, ETH Zurich, 2010.

[272] Alan Gidekel, Introduccion a la identificación por radio frecuencia, Revista Telectronica, Universidad de Palermo, ISBN 987-23017-0-0.

- **Procesamiento de información**: La face inteligente cuenta con una capacidad de procesador o microcontrolador y además capacidad de almacenamiento. Propiedades innatas para poseer inteligencia propia como tal.

- **Localización**: Los objetos inteligentes son conscientes de su ubicación física, o puede ser ubicadas. La red de celular móvil de velocidad avanzada como LTE, o GPS, son tecnologías adecuadas para lograrlo, así como medidas de tiempo de ultrasonido, UWB (banda de Ultra-Wide), radio beacons[273] (por ejemplo, las estaciones base de WLAN o lectores RFID con coordenadas conocidas y tecnologías ópticas.

- **Interfaces de usuario:** Los objetos inteligentes pueden comunicarse con la gente de manera adecuada, directa o indirectamente, por ejemplo a través de un Smartphone, teniendo en cuenta la inteligencia ya integrada en estos dispositivos. Para lo cual es necesario la implantación de paradigmas de interacción innovadores, como interfaces de usuario intuitivas, pantallas flexibles basadas en materiales de polímeros, como los usados en el teléfono Samsung Flexible OLED Display, y métodos de reconocimiento de voz, imagen y demás.[274]

Las aplicaciones más específicas necesitan sólo un subconjunto de las capacidades definidas por Friedemann Mattern y Christian Floerkemeier y que se describió anteriormente, sobre todo porque implementar todo en ellas suele ser costoso y requiere un esfuerzo técnico significativo, teniendo en cuenta que el IoT hoy en día, aún está en desarrollo. Las aplicaciones de logística, por ejemplo, actualmente se concentran en la identificación de costo relativamente bajo de objetos mediante RFID.

Por tanto, una manera de instrumentar objetos es a través de etiquetas RFID (siglas de radio frequency identification, en español, se describe como identificación por radiofrecuencia). En 2010, cerca de 3.000 millones de etiquetas RFID se encontraban en circulación en el mundo. La empresa Violet comercializa TAGs RFID que se adhieren a distintos objetos para que, en contacto con un lector, se abra una página web en un ordenador.[275] Lo que nos acerca a la interacción hombre-máquina (P2M-People to Machine), maquina-maquina (M2M-Machine to machine) y Hombre-hombre (People to people) mediante el uso de protocolos de internet.

---

[273] Chunling Sun, Application of RFID Technology for Logistics on Internet of Things, 2012 AASRI Conference on Computational Intelligence and Bioinformatics

[274] Xian-Yi Chen, Zhi-Gang Jin, Research on Key Technology and Applications for Internet of Things

[275] Eva López Suárez, Cynthia Gregsamer, Javier Corsini Ramírez, El Internet de las Cosas En un mundo conectado de objetos inteligentes, Accenture España 2012

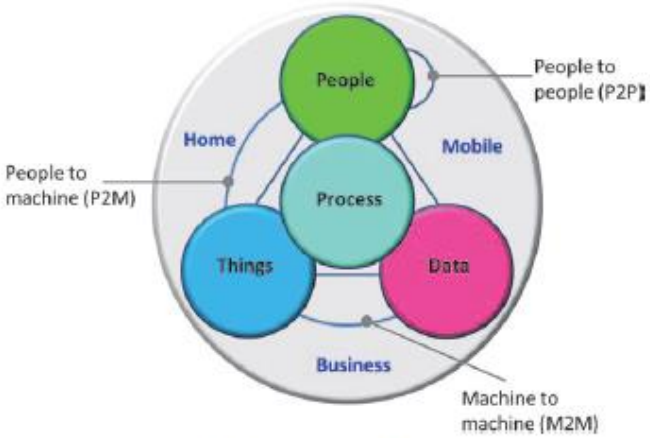


Fig. 2.6 Internet of everything. (*Source*: Cisco).

Figura 99.Internet Of Everything, CISCO

11.2 INFLUENCIA DEL IoT EN LA DOMOTICA.

Según lo mencionado el IoT otorga mayores características al desarrollo del hogar inteligente, y funciona como complemento de los protocolos domóticos. Para el hogar inteligente o "Smart Building", el IoT influye en factores como:

Energía y Uso del Agua: Energía y control del consumo de suministro de agua para obtener consejos sobre cómo ahorrar costos y recursos.

Control remoto de Electrodomésticos: Conexión y desconexión remota aparatos para evitar accidentes y ahorrar energía.

Sistemas de detección de Intrusos: Detección de aperturas de ventanas y puertas y alarmas de violación para evitar intrusos.

Teniendo en cuenta estos factores, las características fundamentales de la IoT orientada a la domótica son las siguientes[276]:

- **Interconexión**: En relación con la IoT, cualquier cosa puede ser interconectado con la infraestructura de comunicación global de la vivienda según los permisos establecidos.

- **Servicios relacionados con los objetos**: La IoT es capaz de proporcionar servicios relacionados, como la protección de la privacidad y la coherencia semántica entre las cosas físicas y sus cosas virtuales asociadas. Con el fin de proporcionar servicios relacionados tanto las tecnologías en el mundo físico y el mundo de la información.

[276] ITU-T, Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

- **Heterogeneidad:** Los dispositivos de la IoT son heterogéneos y basado en diferentes plataformas de hardware y redes. Pueden interactuar con otros dispositivos o plataformas de servicios a través de diferentes redes.

- **Cambios dinámicos:** El estado de los dispositivos de cambiar de forma dinámica, por ejemplo, conectado y/o desconectado, así como el contexto de dispositivos, con la ubicación y la velocidad. Por otra parte, el número de dispositivos puede cambiar dinámicamente.

- **Escalabilidad:** El número de dispositivos que deben ser gestionados y que se comunican entre sí será de al menos los que corresponden a electrodomésticos del hogar.

Con el fin de suplir estas características y los factores mencionados anteriormente, varias organizaciones están trabajando para dotar a los hogares con tecnología que permite a los ocupantes utilizar un solo dispositivo para controlar todos los objetos electrónicos y electrodomésticos. Las soluciones se centran principalmente en la vigilancia del medio ambiente, gestión de la energía, comodidad y confort. Las soluciones se basan en plataformas abiertas que emplean una red de sensores inteligentes para proporcionar información sobre el estado de la casa. Estos sensores supervisan tales sistemas de generación de energía y de medición, calefacción, ventilación y aire acondicionado, iluminación, la seguridad, y los indicadores clave de desempeño ambiental. La información es procesada y puesta a disposición a través de una serie de métodos de acceso, tales como pantallas táctiles, teléfonos móviles y navegadores en 3-D.[277] Los aspectos de redes están trayendo los servicios de streaming en línea o reproducción de la red, convirtiéndose en un medio para controlar la funcionalidad de los dispositivos en la red. Al mismo tiempo, en los dispositivos móviles, los consumidores tendrán acceso a un controlador portátil para los objetos conectados a la red. Ambos tipos de dispositivos pueden ser utilizados como puertas de enlace para aplicaciones de IoT.

[277] Connected Devices for Smarter Home Environments, IBM Data Magazine, 2014,

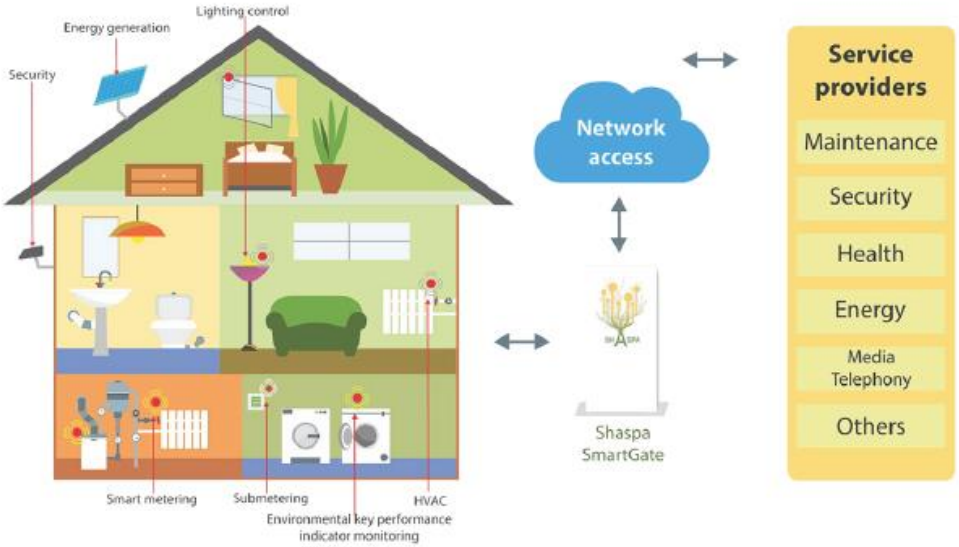


Figura 100. IoT orientado a la domótica, Capas Modelo funcional. “Autonomic Computing: IBM’s perspective on the state of Information Technology”, 2008.

En este contexto, muchas empresas están considerando la construcción de plataformas que integran la automatización de edificios con el entretenimiento, la vigilancia de la salud, monitoreo de energía y monitoreo de sensores inalámbricos en los ambientes del hogar y la construcción.

Las aplicaciones del IoT utilizan sensores para recoger información sobre las condiciones de funcionamiento, combinando software alojado en la nube, que permite el análisis de datos, lo que ayudará en la gestión de los edificios con la máxima eficiencia.

Desde el punto de vista tecnológico, es posible identificar las diferentes capas de un edificio inteligente con más detalle (Figura 99), para entender la correlación de los sistemas, servicios y operaciones de gestión. Para cada capa, es importante entender los actores implicados, los interesados y las mejores prácticas para implementar diferentes soluciones tecnológicas.[278]

Desde las capas de un hogar o edificio inteligente hay muchos servicios integrados que se pueden ver como subsistemas. El conjunto de servicios se gestionan para ofrecer las mejores condiciones para las actividades de los ocupantes de la vivienda. La siguiente figura presenta la convergencia de servicios básicos.

[278] Larios V.M., Robledo J.G., Gómez L., and Rincon R., “IEEE-GDL CCD Smart Buildings Introduction”.

Figura 101. Convergencia de servicios en Smart Building, Larios V.M., Robledo J.G., Gómez L., and Rincon R., “IEEE-GDL CCD Smart Buildings Introduction”.

El uso de Internet, junto con los sistemas de gestión de energía también ofrece la oportunidad de acceder a la información de la energía desde un ordenador portátil o un teléfono inteligente colocado en cualquier parte del mundo. Esto tiene un enorme potencial para la prestación en la retroalimentación del consumo de energía y la capacidad de manejar esa información, hacia planes de ahorro eficientes.

De esta manera el IoT influencia en gran medida el desarrollo de los hogares inteligentes y el uso de la tecnología como fuente de confort, seguridad, regulación energética, control y monitoreo de la vivienda.

CAPITULO V

12. CARACTERÍSTICAS MÁS ÓPTIMAS PARA UN PROTOCOLO EFICIENTE, BASADO EN LA INTEGRACIÓN DE LOS PROTOCOLOS ANALIZADOS, PERMITIENDO LA INTEROPERABILIDAD DE DISTINTOS DISPOSITIVOS DEL HOGAR INTELIGENTE.

Realizando un análisis a cada uno de los protocolos expuestos en los capítulos anteriores, se pueden distinguir ciertas características técnicas para cada uno de ellos resumidas en las tablas a continuación:

MEDIO FÍSICO		
Tecnología	**Alámbrico**	**Inalámbrico**
X10	Línea de Potencia PL	Radiofrecuencia RF
KNX	Línea de Potencia PL Cable Par Trenzado TP	Radiofrecuencia RF Infrarrojo IR
LonWorks	Fibra Óptica Línea de Potencia PL Cable Par Trenzado TP	Radiofrecuencia RF Infrarrojo IR
ZigBee	No aplica	Radiofrecuencia
RFID	No aplica	Radiofrecuencia RF Infrarrojo IR
EPC	No aplica	Radiofrecuencia RF

Tabla 6. Comparación de protocolos, Características 1. (Autores)

Tecnología	**Distancia (m)**	**Velocidad de Transferencia máxima (bps)**	**Número de Dispositivos**	**Topología**	**Potencia de Transmisión**
X10	1.200	50	256	Distribuido	3Vpp
KNX	1.000	PL 1.200/2.400 TP 9.600 Ethernet 10.000.000 RF 16.384	57.600	Estrella Bus Árbol	PL 220 Vac RF 25 mW
LonWorks	TP=2000 IR=10-30 RF=2000	IR=78.000 PL=4800, 5400 TP=1.250.0000	Nodos por dominio: 32,385	Topología Lógica: Distribuida	

	OF=30Km			Topología Físicas: Estrella Anillo Bus Mixta	
ZigBee	154 75	28.000 250.000	65.536	Distribuida Malla Estrella Árbol	100 mW
RFID	10	25.000 en UHF	10	Centralizado	2W
EPC	100	100.000 en UHF	Indeterminado	Distribuido	2W

Tabla 7. Comparación de protocolos, Características 2. (Autores)

Tecnología	**Técnicas de Acceso**	**Modulación**	**Tipo de Comunicación**	**Frecuencia de Operación (Hz)**
X10	No Aplica	ASK 2 Símbolos	Half duplex	PL= 120 KHz Portadora de 310 MHz
KNX	CSMA/CA	FSK	Half-duplex	PL 110 o 132 KHz RF 868 MHz
LonWorks	CSMA/CA	RF=FSK	Full-duplex	PL=125 kHz y 140 kHz RF-10 (49 MHz) RF-100 (433 - 472 MHz)
ZigBee	CSMA/CA TDMA	DSSS	Half-duplex	2.4GHz
RFID	FDMA (Frequency Division Multiplexing Access)	Modulación por desplazamiento de Amplitud (ASK)	Half-duplex	125 KHz 13.56 MHz 868 - 928 MHz 2.4 - 5.8 Ghz
EPC	CSMA (Carrier Sense Multiple Access) FHSS (Frequency Hopping Spread Spectrum)	Modulación por desplazamiento con doble banda lateral (DSB-ASK). Modulación de banda lateral con único desplazamiento de amplitud (SSB-ASK)	Full-duplex.	860 MHz a 960 MHz

		Inversión de fase por desplazamiento de amplitud (PR-ASK)		

Tabla 8. Comparación de protocolos, Características 3. (Autores)

Tecnología	**Escalable**	**Interoperable fabricantes**	**Estándar**	**Software**
X10	Sí	Sí	Sí	NO aplica
KNX	Sí	Sí	Abierto no gratuito	Sí
LonWorks	Sí	Sí	Abierto	Sí
ZigBee	Sí	Sí	Abierto	Sí
RFID	No	Sí	Abierto	No aplica
EPC	Sí	No	Cerrado	Sí

Tabla 9.Comparación de protocolos, Características 4. (Autores)

Tal como lo estudiado anteriormente para obtener un hogar inteligente es necesario que la red cuente con ciertos parámetros referentes a Comunicación, Control y Direccionamiento, Identificación, Detección, Procesamiento de información, e Interfaces de usuario, que permita tanto la interacción entre objetos como la interacción con los usuarios.

Para el análisis de las características referentes a comunicación tenemos que entrar a evaluar algunos factores clave a tener en cuenta, entre lo que tenemos:

12.1 Escalabilidad

En este factor se tiene en cuenta la habilidad del sistema o red domótica para adaptarse, seguir creciendo y reaccionar a su entorno sin perder calidad de servicio, por lo tanto EPC es el protocolo que ofrece mayor escalabilidad en su red, en comparación con los otros protocolos anteriormente descritos, ya que permite direccionar un número indefinido de dispositivos que se pueden comunicar dentro de la red domótica, permitiendo un amplio crecimiento de la red para suplir las necesidades del usuario. En cuanto a la ampliación o modificación, este protocolo permite facilita el poder cambiar o conectar nuevos dispositivos a la red gracias a que requiere sólo de la previa configuración y su identificación en la red ya que esta posee una auto-organización, auto-recuperación y coexistencia operativa dentro de todos sus dispositivos con el fin de poder realizar una comunicación óptima dentro de toda la red dependiendo de sus características.

12.2 Medio de comunicación (alámbrico, inalámbrico)

Para el análisis de este factor se tiene en cuenta el lugar donde se va realizar o implementar la red domótica, puesto que si se instala sobre una estructura como un hogar o edificio que ya esté construido es mejor optar por una comunicación del tipo inalámbrico, ya que de esta forma se evita la modificación de la estructura disminuyendo los gastos de su implementación, por lo cual ZigBee es la mejor opción para una red inalámbrica, ya que la comunicación entre todos sus dispositivos se realiza gracias a la radiofrecuencia en la banda de libre de 2,4GHz, y el protocolo fue diseñado esencialmente para este tipo de comunicación.

Si la red domótica se va a instalar al mismo tiempo que se construye la estructura, lo anterior mencionado pierde relevancia ya que se puede realizar la instalación de la red de forma alámbricamente mediante buses de comunicación. Por lo cual el protocolo que mejor se adapta a estas características es LonWorks ya que puede utilizar los medios de comunicación alámbricos (Fibra Óptica, Línea de potencia, Cable de par trenzado), que se pueden instalar a medida que se construye la estructura, de forma que no se necesiten modificaciones posteriores para la implementación de la red.

12.3 Tipo de Sistema

En cuanto a este factor es importante tener en cuenta si el protocolo permite una de las siguientes topologías de red:

Centralizada: en este tipo de sistema, todos los nodos que hacen parte de la red domótica se comunican a través de un nodo central con otros nodos, que tendría como ventaja un menor costo del sistema ya que solo se necesita de un único controlador, pero tendría una desventaja significativa ya que si el nodo central deja de funcionar el resto de la red también lo haría, perdiéndose la comunicación.

Descentralizada: En este tipo de sistema no existe un único nodo central para la comunicación sino que para ello existen varios de estos nodos, donde la caída de uno de ellos no afecta la totalidad del funcionamiento de la red, solo afectaría los dispositivos que se conectan a este nodo, donde el problema radicaría en que la caída de los dispositivos conectados al nodo por medio de un mismo bus de comunicación y el aumento de costos.

Distribuida: en este tipo de sistema todos los dispositivos se comunican entre sí, estableciendo diferentes caminos para la transferencia de datos, es decir, que si alguno de estos dispositivos deja de funcionar no afectaría la red ni su funcionalidad ya que la red posee una auto-organización que permite el establecimiento de nuevo camino de comunicación hasta que el dispositivo vuelva a funcionar, permitiendo una total versatilidad de configuración entre sus diferentes conexiones. Pero

también presenta desventajas como elevados costos y la complejidad de su instalación y mantenimiento.

Por lo tanto el mejor tipo de sistema de red es la distribuida ya que permite la comunicación entre todos sus dispositivos formando diferentes caminos de comunicación si alguno de estos dispositivos falla dentro de la red se forman caminos alternativos para el intercambio de información, permitiendo el funcionamiento total de la red; como lo realiza el protocolo ZigBee además de sus topologías de tipo en estrella, malla y árbol.

12.4 Seguridad

En cuanto a seguridad es importante tener en cuenta la autentificación de los dispositivos, como también es parte importante la encriptación de los datos transmitidos en la comunicación de la red, con el fin de proteger los datos del usuario de terceras personas al igual que evitar que otros puedan controlar o modificar el funcionamiento de la red domótica como lo realiza el protocolo ZigBee al utilizar uno de los estándares más importantes de cifrado de hoy en día como lo es AES con longitud clave de 128 bits que no es la mejor pero disminuye el procesamiento que tienen que hacer los dispositivos ya que los dispositivos ZigBee no tiene gran capacidad de memoria. También solicita autenticación o validación de los dispositivos y datos transmitidos.

12.5 Distancia y velocidad

Uno de los factores más importantes es el rango o distancia máxima existente entre los dispositivos, que no afecte la comunicación, que dependen del medio de transmisión que no presenta tantas pérdidas de potencia de la señal por atenuaciones y de elementos intermediarios utilizados. En este aspecto el sistema Lonworks que utiliza diferentes medios para la comunicación puede transmitir desde 30 metros con infrarrojo, 2000 metros con par trenzado o radiofrecuencia y hasta 30 Kilómetros mediante fibra óptica. Además del medio gracias al uso de repetidores que amplifican la señal se logra aumentar las distancias entre dispositivos.

En cuanto a velocidad es importante tener en cuenta la tasa de transferencia de datos, es decir, la cantidad de bits por segundo que se pueden enviar en la comunicación, de tal manera que los dispositivos puedan compartir información de una forma más eficiente dentro de la red domótica, disminuyendo la cantidad de recursos utilizados dentro de la misma; como lo realiza el protocolo KNX sobre un medio guiado como Ethernet que alcanza velocidades de hasta 10 Mbps o por medio inalámbrico como lo hace ZigBee con radiofrecuencias, alcanzando velocidades de hasta 250 Kbps.

12.6 Tipo de comunicación

Es importante el método de comunicación utilizado dentro de la red domótica, ya que este permite la comunicación simultánea o no entre los dispositivos, como sensores y sus actuadores, siendo sus principales tipos de comunicación:

Half duplex: el cual permite la comunicación o envío de información entre los dispositivos pertenecientes a la red de una forma bidireccional pero no simultánea
Full duplex: el cual permite que los dispositivos que se encuentran dentro de su red se comuniquen de una forma bidirecc**i**onal y simultánea permitiendo enviar y recibir a la vez información.

Todo esto se deberá tener en cuenta para que la red se pueda comunicar con sus dispositivos de una forma rápida, es decir, en tiempo real, con el fin de actuar por medio de la información recibida de sus sensores. Característica presenta en el sistema LonWorks gracias a los dispositivos que lo integran, el cual permite una rápida respuesta entre sus actuadores y variables, ya que esta red utiliza la comunicación de tipo full duplex.

12.7 Procesamiento de información

LonWorks sobresale en este aspecto ya que todos sus dispositivos o nodos se encuentran conformados por un NeuronChip, que es el corazón de esta tecnología. Este Chip está compuesto por tres procesadores que se encargan de correr el protocolo permitiendo su funcionamiento al mantener los mismos parámetros para establecer la comunicación. Además se encarga de la aplicación de control en los nodos procesando la información de acuerdo a las variables de entrada y salida, tomando los datos de los sensores y controlando los actuadores, de forma que Lonworks sea un sistema distribuido con nodos inteligentes. También facilita el direccionamiento de los mensajes en la red.

El protocolo del EPC utiliza técnicas de modulación que pretenden transportar la mayor cantidad de información con los menores recursos posibles. Es así como con el uso de técnicas como Modulación por desplazamiento con doble banda lateral (DSB-ASK) y técnicas como Espectro ensanchado por salto de frecuencia (FHSS) que permite transmitir señales de radio frecuencia que otras modulaciones no pueden transmitir, si se tienen en cuenta que opera en altas frecuencias de UHF. A su vez entre mayor sea la frecuencia de operación mayor va a ser la capacidad neta de procesar la información.

12.8 Interfaz de usuario

La interfaz de usuario es vital en el funcionamiento de las redes, ya que es el medio con el cual el usuario se puede comunicar con el sistema, observando de esta forma lo que captan los sensores, y dando órdenes para que los actuadores actúan

dependiendo de las variables especificadas. Por esta razón estas interfaces deben ser intuitivas para facilitar su uso por parte del usuario. Por esta razón LonWorks utiliza un paquete de software como herramienta de diseño, instalación, gestión, mantenimiento de las redes LonWorks y accesibilidad y facilidad de uso gracias a la interfaz de Microsoft Visio, reconocido por estar integrado en la suite ofimática de Microsoft Office.

12.9 Costo y facilidad de uso

Un factor que impulsa el desarrollo y la instalación de redes domóticas a nivel mundial es el costo ya que si estos no son muy altos se facilita la adquisición y crecimiento de este mercado. Por lo tanto es un factor a tener en cuenta, así las tecnologías sean nuevas y escasas. Un bajo costo de dispositivos con la tecnología necesaria para que cumplan las necesidades que los usuarios demandan, es una de las características del Protocolo X10, que permite su instalación sin necesidad de realizar modificaciones en las estructuras de los hogares ahorrando tiempo y dinero adicional debido a que es un sistema plug & play, es decir que solo es necesario conectar los dispositivos a la red eléctrica para su puesta en funcionamiento.

Otro protocolo que tiene en cuenta este factor es ZigBee, considerado como una tecnología de poco consumo de energía, ya que posee un corto alcance y baja velocidad de datos, alcanzando hasta 2 años con una alimentación de pilas AA. ya que los dispositivo que conforman la red pasan la mayor parte del tiempo en standby para consumir menos energía, hasta recibir algún tipo de señal que modifique su estado actual, por lo que implica un bajo costo de dispositivos, instalación y mantenimiento.

12.10 Control y direccionamiento

Para el control y direccionamiento se perfila EPC que posee la característica del ONS que permite direccionar cualquier dispositivo conectado a la red a través de servidores.

En cuanto a ONS opera de manera análoga a un traductor de direcciones, de forma tal que a un cierto objeto en la red, entrega un número serial único asociado a una dirección con salida a internet que le permite direccionar hacia otro servidor con gestión de ONS para ser transportado hacia cualquier parte del mundo. Este ONS depende directamente del Middleware, encargado de almacenar y actualizar las tablas de enrutamiento dependiente de la convergencia de la red, y así mismo el estado del objeto direccionado por el Middleware, que actúa como cerebro de la operación, controlando cambios en el estado del objeto en tiempo real.

El ONS utiliza una estructura Jerárquica que permite direccionar un objeto dependiendo del servicio que presta, dándole un código de mayor nivel a servicios

prioritarios predefinidos en el Middleware, de manera que garantiza en parte la calidad de servicio (QoS). Por otro lado el sistema ONS es escalable a un número indeterminado de usuarios, únicamente limitado por las direcciones públicas y privadas asignadas para la salida a internet. Siendo el ONS un servidor más de la red, puede tener backup de información de los objetos que son almacenados en otros servidores dentro de la misma red, lo que le permite una rápida interacción con objetos nuevos identificados.

12.11 Identificación y detección

RFID es sin lugar a dudas el pionero en la detección de objetos, ya que permite su identificación a distancia sin necesidad alguna de contacto, ni de establecer línea de vista directa. Se pueden identificar tramas amplias como la de Ethernet y entre 1500 a 9000 bytes de payload. De igual manera los microchips integrados de la etiqueta permiten que cada objeto adopte un código único estandarizado que de manera inequívoca marca dicho objeto.

RFID opera en distintas frecuencias 125 KHz, 13.56 MHz, 868 - 928 MHz, 2.4 - 5.8 Ghz, lo que según regulaciones del espectro pueden adaptarse a las normativas de cada país. La frecuencia de IMS (2,4-5,8Ghz) además le permite operar con dispositivos bluethooth, Wifi, Wlan.

Las etiquetas transmiten alcanzando una potencia de 2W y las antenas son adaptables a la forma física de la etiqueta. Los tamaños por tanto de los dispositivos RFID son reducidos y adaptables a cualquier tipo de objeto. (Para elementos metálicos y en contacto con líquidos es necesario un diseño especial del Tag). La alimentación de las etiquetas puede ser de tipo pasiva, haciendo uso de la energía emitida por el transceiver a través de las ondas electromagnéticas, por cuanto es innecesario el uso de alimentación externa en el hardware del tag.

13. CONCLUSIONES

El IoT se constituye en una herramienta para la domótica y no en su reemplazo, ya que los desarrollos hasta el momento únicamente incluyen el protocolo IP para el Core de las redes, lo cual sugiere el uso de protocolos complementarios que permita unificar las funciones de los objetos. Por tanto no se puede dejar de lado los protocolos diseñados principalmente para su uso en domótica como X10, Lonworks y KNX, ya que fueron los pioneros en el sector y se encargaron de plantear enfoques de cómo deben encaminarse los futuros desarrollos. Esto se plasma en el estudio de las características y funcionalidades que nos deja ver no sólo las ventajas sino los problemas que presenta cada protocolo respecto de sus homólogos. En caso de ser enfocado a los hogares inteligentes el IoT opera en pro de la seguridad al poder conocer el estado en tiempo real de cerraduras y ventanas, activar alarmas de intrusos, observar mediante cámaras IP la vivienda y demás. Así mismo tener control de todos los ambientes del hogar, regulando la temperatura, los factores de luminosidad, música, colores y olores deseados. Contribuye igualmente al ahorro energético, al monitorear los consumos y evitar excesos. Por último mediante la variedad de ambientes y facilidades que ofrece un hogar inteligente, la calidad de vida de las personas aumentará en cuanto a comodidad y confort en la vivienda.

Algunos países implementan políticas para el desarrollo del IoT, lanzando planes a corto plazo para la construcción de ciudades inteligentes enfocadas en el auto sostenimiento a través de la tecnología. Por tanto el desarrollo industrial de los dispositivos para el hogar es acelerado y se tienen por ejemplo objetos basados en RFID y EPC de fabricantes como Philips, Texas Instrument, Cisco, IBM, entre otros. De igual forma para dispositivos basados en Lonworks entre los fabricantes más importantes tenemos a Echelon que fue el desarrollador de esta tecnología, otras empresas reconocidas a nivel mundial como Philips y Siemens,entre otras, referente a mercados más cercanos tenemos a la empresa española E-Controls; en cuanto a X10 hoy en día es estándar y fabricante con la marca X10 PowerHouse.

De igual forma la implementación del IoT con un protocolo basado únicamente en IP depende en gran medida de la difusión de IPv6. Por otra parte, la falta de unificación de protocolos impide su desarrollo en aspectos técnicos como las frecuencias de operación, velocidades de transmisión, medios físicos de transporte entre otros que dependerá en gran medida de la propuesta de organismos estandarizadores como la ITU, EPCGlobal, IEEE y demás. Si bien en la actualidad hay organismos que se encargan de estandarizar sus propios protocolos para impulsar las ventas de sus productos, este aspecto genera un ambiente de competencia que puede ser positivo para optimizar las prestaciones, pero que a su vez puede generar un problema para el sector en el hecho de la falta de

interoperabilidad y elevados costos de los dispositivos. La idea final es que mediante IoT sea posible comunicar cualquier objeto en cualquier momento y lugar, siempre y cuando este sea capaz de ser identificado, comunique datos de su estado actual, logre gestionar y actuar sobre otros sistemas, e interactúe con otros objetos (Comunicación M2M) y con el ser humano (Comunicación P2M).

Para tales fines, RFID es vital en el proceso de identificación de objetos por cuanto es considerada como tecnología habilitadora del IoT, constituyéndose como protocolo universal de identificación haciendo uso de interfaces de aire, sin necesidad de contacto alguno entre objetos. En cuanto a direccionamiento de la información de los objetos, EPC con el desarrollo de ONS es pieza fundamental, ya que permite a cada objeto identificado, la adopción de un código igualmente inequívoco y transportar su información a través de internet, siendo un direccionamiento escalable, solamente limitado por el IPv4. En cuanto a escalabilidad EPC permite direccionar un número indefinido de dispositivos.

Respecto a la comunicación tenemos en cuenta varios parámetros que ZigBee se ha encargado de integrar, ya que fue pensado para comunicaciones inalámbricas trabaja en la banda libre de 2,4GHz alcanzando velocidades de 250Kbps, su tipo de comunicación es distribuida permitiendo la continuidad a través de diferentes caminos en la red, la seguridad ya que utiliza cifrado AES de 128 Bits y autenticación de dispositivo siendo una tecnología que consume poca energía que lo hace importante en cuanto a la economía del hogar. EPC destaca al transportar una gran cantidad de información utilizando pocos recursos gracias al uso de técnicas de modulación DSB-ASK y técnicas de espectro ensanchado FHSS. En cuanto a distancias Lonworks utilizando alámbricos puede alcanzar distancias de 30 kilómetros mediante el uso de fibra óptica y gracias a repetidores y comunicaciones full duplex, lo que lo convierte en uno de los mejores protocolos para instalar a medida que se va construyendo la estructura ya sea un hogar o un edificio. Lonworks integra un NeuronChip en sus dispositivos que permite el procesamiento de información y el manejo del protocolo, aplicando el concepto inteligente a sus nodos, importante de cara a la continuidad del desarrollo de la domótica.

La parte enfocada en el uso por parte del usuario tenemos Lonworks que se preocupa por este aspecto al integrar un paquete de software LonMaker con interfaz Microsoft Visio para el diseño, instalación y gestión que sea amigable e intuitiva para el usuario. En cuanto a facilidad de uso X10 que es el pionero en la rama de la domótica le da la importancia que se merece a este aspecto con sus característica plug & play, conectar y usar, que no requiere de modificaciones a la estructura del hogar para su uso, con dispositivos de bajo costo.

Para la unificación de estos protocolos es necesario la creación de Gateways capaces de funcionar como puerta de enlace entre los mismos, de manera que su

entrada sea un protocolo base y la salida sea otro protocolo distinto según corresponda.

14. BIBLIOGRAFIA

Alan Gidekel, Introduccion a la identificación por radio frecuencia, Revista Telectronica, Universidad de Palermo, ISBN 987-23017-0-0.

Alejandra García Salvatierra, El Internet de las Cosas y los nuevos riesgos para la privacidad, 2012.

Amcham EU, Response to ‘‘Internet of Things’’ Public Consultation, supra note 25, at.

CALAFAT, Cristhian. Introducción a la Tecnología Lonworks. Asociación LonUsers. España. {En línea}. {Agosto 2014}. Disponible en: (http://www.lonmark.es/www/pdf/articulos/Introduccion%20Tecnologia%20LonWorks__6.pdf).

Ching-Hsien Hsu, Yi-Min Chen, Chao-Tung Yang, "A Layered Optimization Approach for Redundant Reader Elimination.

CHIRENO, Katherine. (2011). Hacia una vivienda sostenible en Santo Domingo.

Chunling Sun, Application of RFID Technology for Logistics on Internet of Things, 2012 AASRI Conference on Computational Intelligence and Bioinformatics

Cisco IBSG, 2011.

Curso iniciación al KNX. {En línea}. {Agosto 2014}. Disponible en: (http://www.iknx.es/).

Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, Internet of things: Vision, applications and research challenges, Ad Hoc Networks 10 (2012) 1497–1516.

DIGNANI, Jorge. Análisis del protocolo ZigBee, (2011).

DURÁN, Ana. Instalación Domótica de una Vivienda Unifamiliar. Madrid: (junio 2009), 183p. Trabajo de grado (Ingeniera Industrial). Universidad Pontificia Comillas. Escuela Técnica Superior de Ingeniería (ICAI).

Eficiencia Energética con KNX. {En línea}. {Agosto 2014}. Disponible en: (http://www.iknx.es/).

EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0 de diciembre de 2010.

Fan Shaoshuai, Shi Wenxiao, Wang Nan, Liu Yan, MODM-based Evaluation Model of Service Quality in the Internet of Things, Procedia Environmental Sciences 11 (2011).

Formación Estudiantes IKNX Ingeniería. {En línea}. {Agosto 2014}. Disponible en: (http://www.iknx.es/).

G. Merrett, N. White, N. Harris, B. Al-Hashimi, Energy-aware simulation for wireless sensor networks, in: Proceedings of IEEE SECON, Rome, Italy, 2009.

GUERRERO M, José A. Diseño de una Instalación Domótica con Tecnología Lonworks. Cartagena: (05 febrero, 2010), 135p. Trabajo de grado (Ingeniero en Automática y Electrónica Industrial). Universidad Politécnica de Cartagena. Facultad de Ingeniería en Automática y Electrónica Industrial.

Harrison B. Chung, Heesook Mo, Naesoo Kim, Cheolsig Pyo, “An advanced RFID system to avoid collision of RFID reader, using channel holder and dual sensitivities”. Microwave and Optical Technology Letters, Vol. 49 Issue 11, pp.2643–2647, 2007.

Harrison B. Chung, Heesook Mo, Naesoo Kim, Cheolsig Pyo, “An advanced RFID system to avoid collision of RFID reader, using channel holder and dual sensitivities”. Microwave and Optical Technology Letters, Vol. 49 Issue 11, pp.2643–2647, 2007.

HENRÍQUEZ, Mauricio. PALMA, Patricio. (2011). Control automático de condiciones ambientales en domótica usando redes neuronales artificiales.

HERNÁNDEZ, J. & BORROMEO, S. Sistema Inalámbrico para aplicaciones domóticas.

Ho, J., Engels, D., Sarma, S., “HiQ: a hierarchical Q-learning algorithm to solve the reader collision problem”.

INFANTES D, Juan Antonio. Descripción de X-10. Málaga: (25 enero, 2009). Universidad de Málaga. Departamento Lenguajes y Ciencias de la Computación

Introducción a LonWorks, La Salle. {En línea}. {Agosto 2014}. Disponible en: (http://www.salleurl.edu/).

Introducción al sistema X10. {En línea}. {Agosto 2014}. Disponible en: (http://trabajosunidrc.arredemo.org/Introduccion%20al%20sistema%20X10.pdf).

ITU Strategy and Policy Unit (SPU). ITU Internet Reports 2005: The Internet of Things[R]. Geneva: International Telecommunication Union (ITU), 2005.

J. Waldrop, D.W. Engels, and S. E. Sarma, "Colorwave: an anticollision algorithm for the reader collision problem,"

K.S. Leong, M.L. Ng, P.H. Cole, “The reader collision problem in RFID systems”, in Proc. of IEEE International.

Karakostas, B. “A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics”, The 4th International Conference on Ambient Systems, Networks and Technologies (ANT 2013), Procedia Computer Science 19 (2013) 594 – 601.

Karl Prince, Michael Barrett, Eivor Oborn, Dialogical strategies for orchestrating strategic innovation networks: The case of the Internet of Things, Information and Organization 24 (2014) 106–127.
LIBERA WP-RFID-001 © 2010 RFID: TECNOLOGÍA, APLICACIONES Y PERSPECTIVAS.

MÁRQUEZ, David. & CÁRDENAS, Oscar. (2011). Estado del arte de los sistemas microelectromecánicos.

MARSAL, Luis. Protocolo X10. Asunción: (septiembre, 2018). Universidad Católica “Nuestra Señora de Asunción”. Facultad de Ciencias y Tecnología. Departamento de Ingeniería Electrónica e Informática.

Morales, Geraldine. (2011). La domótica como herramienta para un mejor confort, seguridad y ahorro energético.

MORENO, Javier., & FERNÁNDEZ, Daniel. Informe técnico: Protocolo ZigBee (IEEE 802.15.4), (Jun, 2007).

NAVARRO, María. (2011).Inteligencia ambiental: entornos inteligentes ante el desafío de los procesos inferenciales.

O’R sutainables strategies. (2010). Diez pasos para la construcción sostenible.

PENAGOS, Hernán., CASTELLANOS, Germán., ALARCÓN, Ronald., WEISS, Viviana., LAVERDE, Ángela., RODRÍGUEZ, Juan. & Rincón, Leonel. (2006). Diseño e implementación de una red domótica para un laboratorio de ingeniería electrónica.

PEÑA, Manuel. Comunicaciones en el entorno doméstico (domótica) comparación knx – lonworks, (2012).

RFC 1034, Domain Names - Concepts and Facilities, P. Mockapetris, The Internet Society (November 1987).

Rolf H. Weber, Internet of things – Need for a new legal environment?, computer law & security review 25 (2009) 522–527.

Shailesh M. Birari and Sridhar Iyer. “PULSE: A MAC Protocol for RFID Networks” 1st International Workshop on RFID.

SOBERANES, María. (2008). El mantenimiento de un edificio inteligente.

Sungjun, K., Sangbin, L., Sunshin, A., “Reader Collision Avoidance Mechanism in Ubiquitous Sensor and RFID.

VERA, Alexander., ALARCÓN, Andrés., POLANCO, Oscar., Nieto, Rubén., & Bernal, Álvaro. (2004). Aplicación de las comunicaciones Inalámbricas a la domótica.

W. Ye, J. Heidemann, D. Estrin, An energy-efficient MAC protocol for wireless sensor networks, in: Proceedings of IEEE INFOCOM, vol. 3, 2002, pp. 1567–1576.

Wang, D., Wang, J., and Zhao, Y.,“A novel solution to the reader collision problem in RFID system”. In Proc. of IEEE Int.

Xian-Yi Chen, Zhi-Gang Jin, Research on Key Technology and Applications for Internet of Things.

15. GLOSARIO

ACK	Acknowledgement
AES	Advance Encryption Standard
AODV	Ad hoc On-Demand distance Vector
APDU	Application Support Sublayer Protocol Data Unit
APL	Application Layer
APS	Application Support
APSDE	Application Support Sublayer Data Entity
APSME	Application Support Sublayer Management Entity
ASDU	APS Service Data Unit
ASK	Amplitud Shift Keying
BACKBONE	Principales conexiones troncales
BIT	Unidad básica del sistema binario
BYTE	Múltiplo del bit, equivale a 8 bits
CAP	Contention Access Period
CCA	Clear Channel Assessment
CRC	Comprobación de Redundancia Cíclica
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOMÓTICA	Conjunto de sistemas capaces de automatizar una vivienda
DSSS	Direct Sequence Spread Spectrum
ECHELON	Echelon Corporation, inventó, vende y da soporte a LonWorks.
ED	Energy Detection
EHS	European Home System Association
EIB	Bus de Instalación Europeo
EIS	EIB Interworking Standard
ETS	Engineering Tool Software

FCS	Frame Check Sequence
FDMA	Frequency Division Multiple Access
FFD	Full Function Device
FHSS	Frequency-hopping spread spectrum
GATEWAY	Pasarela o puerta de enlace, permite interconectar redes con protocolos diferentes
GTS	Guaranteed Time Slot
HEADER	Cabecera en una trama de datos
IB	Information Base
IEEE	Institute of Electrical and Electronics Engineers
IOT	Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IR	Radiación Infrarroja
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
LON	Local Operating Network
LQI	Link Quality Indicator
LR-WPAN	Low-Rate Wireless Persona Area Network
MAC	Medium Access Control
MIC	Message Integrity Code
MLME	MAC Layer Management Entity
MLME-SAP	Mac Layer Management Entity Service Access Point
MPDU	MAC protocol Data Unit
MSDU	MAC Service Data Unit
NACK	Negative Acknowledgement
NLDE	Network Layer Data Entity
NLME	Network Layer Management Entity
NPDU	Network Protocol Data Unit
NSDU	Network Service Data Unit

NWK	Network Layer
ONS	Object Name System
OSI	Open System Interconnection
PAN	Personal Area Network
PD	Physical Data
PDA	Personal Digital Assistant
PHY	Physical Layer
PIB	Pan Information Base
PL	Power Line
PLME	Physical Layer Management Entity
POS	Personal Operating Space
PPDU	Physical Prococol Data Unit
PSDU	Physical Service Data Unit
QOS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RFD	Reduced Function Device
RFID	Radio Frequency Identification
ROUTER	Enrutador o encaminador de paquetes
SAP	Service Access Point
SFSK	Spread Frequency Shift Keying
SKKE	Symmetric-Key Key Establishment
SNR	Signal to Noise Ratio
SNVT	Standard Network Variable Types
TDMA	Time Division Multiple Access
USB	Universal Serial Bus
WLAN	Wireless Personal Area Network
WPAN	Wireless Personal Area Network
ZDO	ZigBee Device Object