

# PROTOCOLOS EN DOMÓTICA: STATE-OF-THE-ART REVIEW

Youssef Moises Abarca Reyes  
yabarcar@est.ups.edu.ec  
José Patricio Campoverde Gárate  
jcampoverdeg2@est.ups.edu.ec  
Universidad Politécnica Salesiana - Cuenca

**Resumen**—En este artículo presenta un visión general del estado del arte de la domótica, para lo cual se analizarán los distintos protocolos que se han implementado en la domótica. Se describirá diversos sistemas para elaborar protocolos y como estos se han desarrollado al transcurrir el tiempo, por lo tanto se realizará una comparación entre protocolos anteriores y actuales, con la finalidad de establecer diferencias entre estos y encontrar el más adecuado para las instalación que se requiera.

**Abstract**—In this article presents an overview of the state of the art home automation, for which the various protocols that have been implemented in the automation will be analyzed. Various systems are described to develop protocols and how they have evolved as time passes, so a comparison of previous and current protocols, in order to differentiate between them and find the right fit for the required installation used to be held .

**Index Terms**—domótica, protocolos de seguridad, review, home automation, etc.

## I. INTRODUCCIÓN

Los diccionarios franceses incorporaron el término “domotique” a partir de 1998. Esta palabra, traducida al castellano por domótica, es originaria de la palabra latina “domus”(de la que ha derivado la raíz que quiere decir casa) y de la palabra francesa “informatique” (de la que se ha derivado la palabra informática) o, según otros autores “robotique” (robótica). Este término de uso común en España, no a conseguido imponerse en diversos países hispanoamérica; donde aún se ha quedado con el término inteligente.[2]

De forma escrita, se define la vivienda domótica como:

“aquella en la que existe agrupaciones automatizadas de equipos, normalmente asociados por funciones , que disponen de la capacidad de comunicarse interactivamente entre ellas a través de un bus doméstico multimedia que las integra”.[1]



Figura 1. Definición teórica de Domótica mediante la disponibilidad de un bus doméstico multimedia. [1]

La domótica se aplica a la ciencia y los elementos desarrollados por ella que proporciona algún nivel de automatización

o automatismo dentro de la casa; pudiendo ser desde un simple temporizador para encender o apagar la luz o aparato a una hora determinada, hasta los mas complejos sistemas capaces de interactuar con cualquier elemento eléctrico de la casa.[2][20] Uno de los principales inconvenientes de la domótica es el factor seguridad, debido a que es controlada mediante dispositivos de comunicación que estan interactuando con la internet, tambien otro factor es el fallo de los sensores que existen en los equipos electrónicos, si estos llegaran a tener algún daño pueden proporcionar y guardar información errónea que puede resultar perjudicial o incluso molesta para el usuario.

Un problema de igual importancia que se presento en la domótica fue el control de los equipos ya que son manipulados de distintas formas: De forma manual o aun estando fuera de casa y controlarlos por medio de un smartphone.

Para esto se crearon protocolos, los cuales fueron diseñados específicamente para el control de los mismos los cuales han evolucionado para evitar los inconvenientes antes mencionados.

## II. PROTOCOLOS DE DOMÓTICA

Los protocolos o procedimientos de comunicación (programas o software) son los recursos que ofrecen que ofrecen los fabricantes para la utilización de los sistemas de domótica por medio de botones, pantallas, o visores.

Los mas difundidos son los siguientes:

### II-A. Datos por cable exclusivo

Centralizado.

Descentralizado.

### II-B. Datos por radiofrecuencia inalámbricos

Wi-fi.

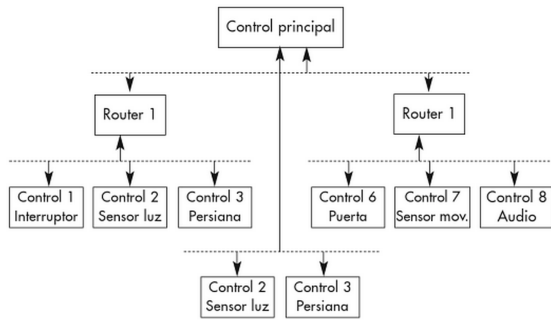


Figura 2. Datos por RF inalámbricos WI-Fi[3]

### Zig-Bee

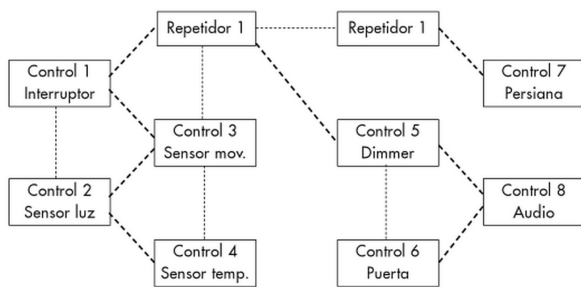


Figura 3. Datos por RF inalámbricos ZIG-BEE. [3]

## II-C. TECNOLOGÍA WIFI

Lo indicado en la Figura [2] es una tecnología inalámbrica digital binaria que transmite datos a través del aire con una velocidad suficiente para aplicaciones domésticas. Cada aplicación en domótica tiene necesidad de diferentes anchos de banda.

Las aplicaciones de domótica para el hogar no necesitan de alta velocidad, ni manejar protocolos o procedimientos que no sean simples o de bajo consumo energético.

El WI-Fi se origina como una solución que permite interconectar computadoras (PC) sin necesidad de cables.

En general esa tecnología se utiliza para acceso a Internet en circuitos cerrados como oficinas, locales comerciales, etc. Para conectar a la web son cables es necesario que los terminales (Laptops y smartphones) cuente con un dispositivo (interfaz), cuya antena (circuito) sintonice alguna señal con estas características. Como esta es una tecnología es simple y de bajo consumo, se han desarrollado otros protocolos que proporcionan un mejor rendimiento tanto en seguridad, como en automatización[3]

## II-D. TECNOLOGÍA ZIG-BEE

Es una nueva tecnología inalámbrica de corto alcance y bajo consumo originaria de la antigua alianza HOMERF y que se definió como una solución inalámbrica de baja capacidad para aplicaciones en el hogar como la seguridad y automatización.

El objetivo de esta tecnología no es obtener velocidades muy altas, ya que solo puede alcanzar una tasa de 20 a 250Kbps en un rango de 10 a 75 metros, si no que es obtener sensores cuyos transceptores tengan un muy bajo consumo energético.

De hecho, algunos dispositivos alimentados con dos pilas AA puedan aguantar 2 años sin el cambio de baterías. Por tanto, dichos dispositivos pasan la mayor parte del tiempo en un estado latente, es decir, durmiendo para consumir mucho menos.[4]

En una red ZigBee pueden haber hasta 254 nodos, no obstante, según la agrupación que se haga, se pueden crear hasta 255 conjuntos/clusters de nodos con lo cual se puede llegar a tener 64770 nodos para lo que existe la posibilidad de utilizar varias topologías de red: en estrella, en malla o en grupos de árboles. En ZigBee hay tres tipos de dispositivos:

- **Coordinador**
  - Sólo puede existir uno por red.
  - Inicia la formación de la red.
  - Es el coordinador de PAN (Personal Area Network).
- **Router**
  - Se asocia con el coordinador de la red o con otro router ZigBee.
  - Puede actuar como coordinador.
  - Es el encargado del enrutamiento de saltos múltiples de los mensajes.
- **Dispositivo final**
  - Elemento básico de la red.
  - No realiza tareas de enrutamiento.

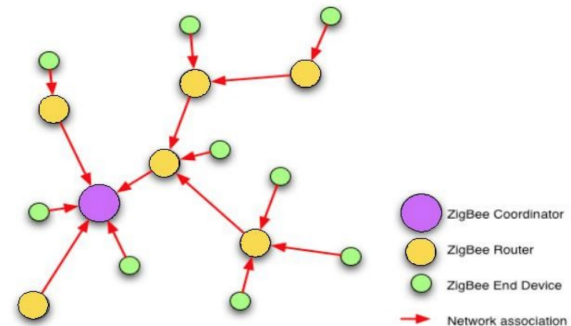


Figura 4. Ejemplo de red Zig Bee. [4]

En cuanto a seguridad, ZigBee puede utilizar la encriptación AES de 128bits, que permite la autenticación y encriptación en las comunicaciones. Además, existe un elemento en la red llamado Trust Center (Centro de validación) que proporciona un mecanismo de seguridad en el que se utilizan dos tipos de claves de seguridad, la clave de enlace y la clave de red.

- El gestor de seguridad determina que seguridad está habilitada o deshabilitada. Si está habilitada debe permitir:
  - Establecer una clave.
  - Transportar la clave.
  - Autenticación.
- Todos los dispositivos ZigBee disponen de dos funcionalidades:
  - Incorporación a una Red.
  - Abandonar una red.

**II-D1. Claves de Seguridad :** La seguridad en una red de dispositivos ZigBee se basa en claves de enlace y de red. En una comunicación por unicast entre pares de entidades

APL la seguridad se basa en claves de 128bits entre los dos dispositivos. Por otro lado, la comunicación existente cuando es por broadcast, también las claves para la seguridad se establecen de 128bits entre todos los dispositivos de la red.

Para el establecimiento de la clave de red hay dos maneras: el transporte de clave y la pre-instalación. El establecimiento de clave se obteniendo previamente una clave de enlace basándose en una clave maestra. Esta clave maestra puede ser obtenida por el transporte de dicha clave o en fábrica.

En establecimiento de clave existen dos elementos: el que inicia la comunicación y el que responde, que normalmente es el que le dará la validación. La información de validación, es decir, la clave maestra da paso a que el elemento iniciador pueda establecer una clave de enlace.

En el establecimiento del protocolo de clave simétrica Symmetric-Key Key Establishment (SKKE), el dispositivo iniciador establece una clave de enlace con el receptor usando la clave maestra. Esta clave maestra, puede venir dada de fábrica o que se implemente desde el centro de validación, que puede ser un tercer elemento o bien puede venir dada como datos introducidos por usuario.

Esta tecnología el transporte de las claves puede ser de forma segura y no segura de un dispositivo a otros. La forma segura significa transportar las claves muestra de la red desde el Trust Center a los dispositivos. Este comando no protege con criptografía la clave que tiene que ser cargada. También proporciona una forma segura para que un dispositivo, como un router, informe al Trust Center, que existe un tercer dispositivo que ha cambiado su estado y que por tanto hay que actualizarlo. De esta manera el centro de validación mantiene una lista precisa de los dispositivos activos en la red.

A continuación se presenta distintos tipos de protocolos en los cuales se encuentran inmersas estas tecnologías.

### III. PROTOCOLOS

#### III-A. PROTOCOLO DE COMUNICACIONES BUSing

Creado por Ingenium, una empresa fundada en el año 1998 en la ciudad de Oviedo (España). su objetivo fue introducir en el mercado un protocolo de comunicaciones asequible para sistemas domóticos que siguiese las bases de protocolos distribuidos ya consolidados, como KNX o LonWorks. De este modo surgió el protocolo BUSing caracterizado por un sistema libre de royalties, abierto a otros fabricantes y cuyos campos principales de aplicación son la domóticas e inmóticas. Es por tanto un sistema de control completo que se adaptará, por presentaciones y por coste, tanto a sencillas viviendas o complejos edificios.[5]

Este protocolo tiene opciones tan diversas como: control de iluminación, gestión de toldos y persianas, gestión de alarmas técnicas, control de temperatura o riego, gestión de sistemas de seguridad y sistemas audiovisuales.

La gran mayoría de los dispositivos de este sistema poseen una versión inalámbrica Wi-Fi al objeto de facilitar su conexión y evitar la adición de nuevo cableado.[6]



Figura 5. Lógo BUSing.[7]

#### III-B. PROTOCOLO KNX

KNX es una realidad desde que en 1999. Esta asociación nació gracias al impulso de las tres asociaciones europeas BatiBUS Club International, EIBA(EUROPEAN INSTALLATION BUS ASOCIATION) que consideraron necesario unir sus experiencias de décadas de años en este mercado.

Este protocolo asegura una relación y presentación adecuada para todas las tipologías de edificios y aplicaciones, de tal manera que garantiza la total interacción de los productos de diferentes constructores y permite realizar una base de datos de los productos certificados. Además para obtener la certificación del estándar KNX, todos los dispositivos son ensayados, según pruebas descritas en las especificaciones del estandar, por una entidad de certificación externa suficientemente acreditada que garantiza al comprador la fiabilidad de los dispositivos.

KNX es un protocolo versátil sumamente escalable y completamente abierto. Posee un campo de aplicación muy diverso y una de sus características más destacables es su escalabilidad: se puede implementar en entornos de muy variado tamaño, desde una vivienda unifamiliar a una gran factoría o edificio administrativo.

Hoy en día, KNX esta presente en 70 países, cuenta con mas de 100 empresas productoras asociadas y mas de 7.000 productos certificados. [6][8][9]

**III-B1. Arquitectura de un sistema KNX:** Está compuesta por áreas y líneas. Las áreas pueden ser hasta 15, interconectadas mediante una línea dorsal principal. En cada área hay una línea principal, de la pueden colgar varias líneas secundarias, hasta un máximo de 15.

En las líneas secundarias estan conectados los dispositivos KNX(detectores, actuadores,...) siendo el número máximo de dispositivos por cada línea de 256 divididos como sigue: 4 segmentos de línea de 64 dispositivos. A continuación se presenta una imagen donde se observa esta arquitectura.[6]

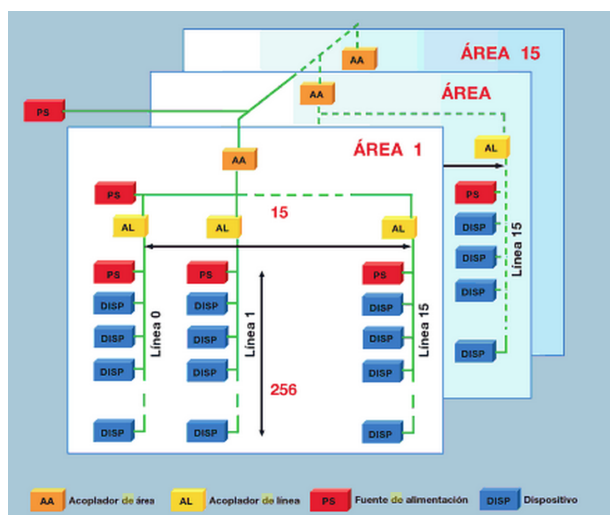


Figura 6. Arquitectura KNX.[6]

### III-C. PROTOCOLO BatiBUS

Es un protocolo de domótica que está totalmente abierto, al contrario de los protocolos como LonTalk de la tecnología LonWorks, el protocolo del BatiBUS lo puede implementar cualquier empresa interesada en introducirlo en su cartera de productos. A nivel de acceso, este protocolo usa la técnica CSMA-CA, (Carrier Sense Multiple Access with Collision Avoidance) similar a Ethernet pero con resolución positiva de las colisiones. Esto es, si dos dispositivos intentan acceder al mismo tiempo al bus ambos detectan que se está produciendo una colisión, pero sólo el que tiene más prioridad continua transmitiendo, el otro deja de poner señal en el bus. Esta técnica es muy similar a la usada en el bus europeo EIB y también en el bus del sector del automóvil llamado CAN (Controller Area Network). Todos los dispositivos BatiBUS escuchan lo que ha enviado cualquier otro, todos procesan la información recibida, pero sólo aquellos que hayan sido programados para ello, filtrarán la trama y la subirán a la aplicación empotrada en cada dispositivo. Al igual que los dispositivos X-10, todos los dispositivos BatiBUS disponen de unos microinterruptores circulares o miniteclados que permiten asignar una dirección física y lógica que identifican unívocamente a cada dispositivo conectado al bus. [10][11]

### III-D. PROTOCOLO X10

X-10 es uno de los protocolos más antiguos que se están usando en aplicaciones domóticas. Fue diseñado en Escocia entre los años 1976 y 1978 con el objetivo de transmitir datos por las líneas de baja tensión a muy baja velocidad y muy bajos costos. Al usar las líneas de eléctricas de la vivienda, no es necesario tender nuevos cables para conectar dispositivos. El protocolo X-10, en sí, no es propietario, es decir, cualquier fabricante puede producir dispositivos X-10 y ofrecerlos en su catálogo, eso sí, está obligado a usar los circuitos del fabricante escocés que diseñó esta tecnología. Aunque, al contrario de lo que sucede con la firma Echelon y su Neuron Chip que implementa LonWorks, los circuitos integrados que implementan el X-10 tienen un royalty muy bajo, gracias a

más de 20 años en el mercado y a la tecnología empleada, los productos X-10 tienen un precio muy competitivo, de forma que son líderes en el mercado norteamericano residencial y de pequeñas empresas (instalaciones realizadas por los usuarios finales o electricistas sin conocimientos de automatización). Se puede afirmar que el X-10 es ahora mismo la tecnología más asequible para realizar una instalación domótica no muy compleja. Habrá que esperar a que aparezcan los primeros productos E.mode (easy mode) del protocolo KNX en Europa para comprobar si el X-10 tendrá competencia real, por precio y prestaciones, en el mercado europeo.[9][12][13]

### III-E. PROTOCOLO EIB

El European Installation Bus o EIB es un sistema domótico desarrollado bajo los auspicios de la Unión Europea con el objetivo de contrarrestar las importaciones de productos similares que se estaban produciendo desde el mercado japonés y el norteamericano.[1]

El objetivo era crear un estándar europeo, con el suficiente número de fabricantes, instaladores y usuarios, que permita comunicar a todos los dispositivos de una instalación eléctrica como: contadores, equipos de climatización, de custodia y seguridad, de gestión energética y electrodomésticos. El EIB está basado en la estructura de niveles OSI y tiene una arquitectura descentralizada. Este estándar europeo define una relación extremo a extremo entre dispositivos que permite distribuir la inteligencia entre los sensores y los actuadores instalados en la vivienda.

#### EIBA

La EIB Association (EIBA) es una agrupación de 113 empresas europeas, líderes en el mercado eléctrico, que se unieron en 1990 para impulsar el uso e implantación del sistema domótico EIB. Las tareas principales de esta asociación son:

- Fijar las directrices técnicas para el sistema y los productos EIB, así como establecer los procedimientos de ensayo y certificación de calidad.
- Distribuye el conocimiento y las experiencias de las empresas que trabajan sobre el EIB.
- Encarga a laboratorios de ensayo las pertinentes pruebas de calidad.
- Concede a los productos EIB y a los fabricantes de estos una licencia de marca EIB con la que se pueden distribuir los productos.
- Colabora activamente con otros organismos europeos o internacionales en todas las fases de la normalización y adapta el sistema EIB a las normas vigentes.
- Lidera el proceso de convergencia (ver Konnex Association en este mismo apartado) de los tres buses europeos de más amplia difusión como son el propio EIB, el BatiBUS y el EHS.

Según la EIBA hay unos 10 millones de dispositivos EIB instalados por todo el mundo, unas 70.000 instalaciones, una gama de 4.500 productos diferentes, 113 empresas asociadas a la EIBA, y 70.000 instaladores cualificados.[13][14]

### III-F. PROTOCOLO CEBus

En 1984 varios miembros de la EIA norteamericana (Electronics Industry Association) llegaron a la conclusión de la



necesidad de un bus domótico que aportara más funciones que las que aportaban sistemas de aquella época (On, Off, Dimmer xx, All Off, etc.). Especificaron y desarrollaron un estándar llamado CEBus (Consumer Electronic Bus). En 1992 fue presentada la primera especificación. Es un protocolo, para entornos distribuidos de control, que está definido en un conjunto de documentos. Como es una especificación abierta cualquier empresa puede conseguir estos documentos y fabricar productos que implementen este estándar. En Europa, una iniciativa similar en prestaciones, teniendo en cuenta el mercado al que va dirigido, es el protocolo EHS (European Home System). [15]

La CIC (CEBus Industry Council) es una asociación de diferentes fabricantes de software y hardware que certifican que los nuevos productos CEBus que se lancen al mercado cumplan toda la especificación. Una vez que el producto pase todos los ensayos, el fabricante paga una tasa y es autorizado a poner el logo CEBus en ese producto.

### III-G. PROTOCOLO LONWORKS

Hoy en día, los protocolos de comunicaciones se diseñan en concordancia con la norma OSI (Modelo de Referencia Abierto para la Interconexión de Sistemas) que engloba un conjunto completo de protocolos, y clasifica a estos según siete categorías funcionales (conocidas como "capas"). De ahí se establece el conocido como "Modelo OSI de 7 capas". El protocolo LonTalk implementa las siete capas del modelo OSI, y los hace usando una mezcla de hardware y firmware sobre un chip de silicio, evitando cualquier posibilidad de modificación casual. Se incluyen características como gestión acceso al medio, reconocimiento y gestión punto a punto, y servicios más avanzados tales como autenticación de remitente, detección de mensajes duplicados, colisión, reintentos automáticos, soporte de cliente-servidor, transmisión de tramas no estándar, normalización e identificación de tipo de dato, difusión unicast/multicast, soporte de medios mixtos y detección de errores.[16]

El protocolo LonTalk tiene dos técnicas para asegurar el correcto envío y recepción de las transmisiones. La fiabilidad de las transmisiones se asegura mediante una confirmación entre emisor y receptor (pueden asegurar que un paquete fue transmitido con éxito, pero no que fue recibido por el destinatario). La integridad de los datos se garantiza por el hecho que todas las transmisiones disponen de un control de errores basado en códigos polinómicos de 16 bits.

Todas las operaciones en la red de control se realizan usando un sistema de "autenticación de remitente" como una Capa de nivel 4 (Nivel de Servicio del modelo OSI). Esta capa proporciona una garantía de autenticidad del remitente, que no puede ser violada por piratas informáticos ("hackers"). Cada transmisión de paquete proporciona autenticación del remitente. Dado que la implementación de esta característica se encuentra a nivel de chip, por una parte no puede ser modificada y por otra está garantizada en todos los productos, independientemente del fabricante del mismo. [16]

### III-H. PROTOCOLO BACnet

El BACnet es un protocolo norteamericano para la automatización de viviendas y redes de control que fue desarrollado bajo el patrocinio de una asociación norteamericana de fabricantes e instaladores de equipos de calefacción y aire acondicionado. El principal objetivo, a finales de los años ochenta, era la de crear un protocolo abierto que permitiera interconectar los sistemas de aire acondicionado y calefacción de las viviendas y edificios con el único propósito de realizar una gestión energética inteligente de la vivienda.[17] Se definió un protocolo que implementaba la arquitectura OSI de niveles y se decidió empezar usando, como soporte de nivel físico, la tecnología RS-485. Incluso a principios de los años 90, cuando apareció el protocolo LonTalk usado en LonWorks, esta asociación se planteó su inclusión como parte del protocolo BACnet, a pesar que Echelon demostró que no pensaba ceder los derechos de patente ni dejar de cobrar royalties por los chips que implementan el LonWorks. Todo ello iba en contra de las bases fundacionales del grupo de trabajo BACnet como protocolo abierto. La parte más interesante de este protocolo es el esfuerzo que han realizado para definir un conjunto de reglas HW y SW que permiten comunicar dos dispositivos, independientemente si estos usan protocolos como el EIB, el BatiBUS, el EHS, el LonTalk, TCP/IP, etc. El BACnet no quiere cerrarse a un nivel físico o a un protocolo de nivel 3 concreto, realmente lo que pretende definir es la forma en que se representan las funciones que puede hacer cada dispositivo llamadas "objetos", cada una con sus propiedades concretas. Existen objetos como entradas/salidas analógicas, digitales, bucles de control, entre otros. Algunas propiedades son obligatorias otras son opcionales, pero la que siempre se debe configurar es la dirección o identificador de dispositivo el cual permite localizar a este dentro de una instalación compleja BACnet. Actualmente existe incluso una iniciativa en Europa para la estandarización del BACnet como herramienta para el diseño, gestión e interconexión de múltiples redes de control distribuido. Este protocolo puede ser utilizado en varios medios de transporte: RS485 a un Mbit/s, RS232, Ethernet 10 Mbit/s, mas usado en redes TCP/IP.[18][17]

### III-I. PROTOCOLO DMX

DMX512 normalmente conocido como DMX (Digital MultipleX), es un protocolo electrónico utilizado en luminotecnica para gestión y control de iluminación espectacular permitiendo la comunicación entre los equipos de control de luces y las propias fuentes de luz. Desarrollado por la Comisión de Ingeniería de USITT, el estándar comenzó en 1986, con posteriores revisiones en 1990 que dieron paso al USITT DMX512/1990. ESTA tomó el control del estándar en 1998 y empezó el proceso de revisión. El nuevo estándar, conocido oficialmente como "Entertainment Technology - USITT DMX512-A - Asynchronous Serial Digital Data Transmission Standard for Controlling Lighting Equipment and Accessories", fue aprobado por ANSI en noviembre del 2004. El actual estándar es también conocido como "E1.11, USITT DMX512-A", o solo "DMX512-A", y es mantenido por la ESTA. DMX aparece como la solución al problema de la incompatibilidad que existía entre marcas

por la utilización de protocolos propietarios, lo cual obligaba a tener un control de manejo por cada marca de luces que se tenía. DMX fue originalmente pensado para usarlo en controladores de enlace y dimmers de diferentes fabricantes, un protocolo que sería usado como último recurso después de probar otros métodos más en propiedad, no GNU. Sin embargo, pronto se convirtió en el protocolo preferido no sólo para controladores de enlace y dimmers, sino también para controlar aparatos de iluminación como scanners, cabezas móviles y dispositivos de efectos especiales como máquinas de humo. Como DMX512 es un sistema de transmisión de datos poco fiable, no debe ser usado para controlar Pirotecnia, para esta tarea se usa a veces controladores MIDI.[5][19]

#### IV. CONCLUSIONES.

A medida que pasan los años cada vez existen nuevos protocolos orientados hacia la domótica las cuales se van adaptando a las nuevas tecnologías existentes hoy en día, pero en cuanto a confiabilidad, se recomienda utilizar los protocolos que ya hayan tenido una gran trayectoria, protocolos como KNX, X10, IBE. Ofrecen dispositivos mucho mas económicos y eficientes que otros competidores recientes, teniendo en cuenta aspectos importantes como es, el factor calidad, la mayoría de los protocolos orientados a la domótica hoy en día, someten a sus dispositivos a rigurosas pruebas y estándares de calidad antes de la salir al mercado, muchos protocolos crean sus propios estándares de seguridad para proteger sus servicios contra hackers o algun tipo de malware. Estos se han perfeccionando y desarrollando en el transcurso del tiempo y sobre todo en el mercado generando confiabilidad y seguridad en los usuarios.

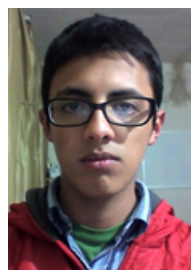
Es importante mencionar que la mayoría de los dispositivos que se implementan en la domótica están controlados mediante Wi-Fi, las cuales han facilitado, economizado la implementación de los mismos.

#### REFERENCIAS

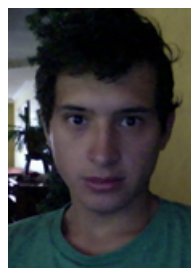
- [1] S. Junestrand, X. Passaret, D Vázquez "Domótica y Hogar Digital," Thomson Ediciones Spain, pp. 4, 2005
- [2] J.M. Huidobro Moya, R.J. Millán Tejedor, "Manual de Domótica," ISBN correspondiente a materias de construcción, pp. 4, 2010.
- [3] J.C. Calloni, "Curso básico de domótica," 1a. ed, Librería y editorial Alsina pp. 30-35, 13 de oct. 2011.
- [4] J.M. Moreno, D.R. Fernández, "informe técnico: protocolo Zig-Bee (IEEE 802.15.4)," IEEE trans.Ind. Electron, pp. 4-27 jun.2007.
- [5] J.M. Maestre, Paraninfo Domótica para ingenieros, (ed.), Ediciones Paraninfo, pp. 65-68. 2015.
- [6] J.M. Rivas Arias, "Manuel Ilustrado Para la instalación Domótica," La tecnología entra en casa, Gewiss Ibérica S.A, pp. 11-15 2010.
- [7] <http://ingeniumsl.com/website/primer-curso-busing-partner-en-ecuador/>
- [8] M.E. Garcia del Puerto, M.J. García Hernández, J.A. Garrido Oliver, "Sistema domótico basado en el protocolo KNX EIB: diseño, programación y puesta en marcha", pp. 17.Project Express, 2006
- [9] M. Moro Vallina, "Instalaciones Domóticas (electricidad-electrónica)," Ediciones Paraninfo, SA 1ª edición, pp. 17-18, 2011.
- [10] C. Romero Morales, Carlos De Castro Lozano, "Domótica e inmótica. Viviendas y Edificios Inteligentes. ," 3ª edición, pp. 20 RA-MA S.A. Editorial y Publicaciones, 2010.
- [11] Instalaciones automatizadas en viviendas y edificios: equipos e instalaciones electrotécnicas, Publisher Thomson, 2001 Author Gil, J. M. and Diéguez, E. R. and Tárraga, D. L. Date-Added 2015-07-05 23:43:27 +0000 Date-Modified 2015-07-05 23:43:27 +0000 Isbn 9788497320245, Electricidad-electrónica, <https://books.google.com.ec/books?id=DJt7vggf8jAC>, <https://books.google.com.ec/books?id=DJt7vggf8jAC>

- [12] Gestión, Publisher Centro de Estudios para el Desarrollo de la Empresa Year 2002, Centro de Estudios para el Desarrollo de la Empresa (Chile) Number v. 28,n."331-342 Date-Added 2015-07-06 00:01:44 +0000 Date-Modified 2015-07-06 00:01:44 +0000, <https://books.google.com.ec/books?id=svOzAAAAIAAJhttps://books.google.com.ec/books?id=svOzAAAAIAAJ>
- [13] R. Hernández Balibrea, "Tecnología Domótica para el control de una vivienda," etsin (escuela técnica superior de ingeniería de telecomunicación), Universidad Politécnica De Cartagena, pp.14-26, Sep. 2012.
- [14] F. Tommasino Juncal, "Guía Técnica de Prevención de Riesgos Laborales para Trabajos en Domótica e Inmótica," Universidad Politécnica de Catalunya, Proyecto Final de Grado, pp. 58-62, Feb. 2011.
- [15] A. Martínez Argote, "Domótica," DEPARTAMENTO DE EXPRESION GRAFICA Y PROYECTOS DE INGENIERIA, Universidad del País Vasco, pp.13-25, 2012
- [16] C.A. Ponce Morquecho, "IMPLEMENTACIÓN DEL SISTEMA INMÓTICO PARA EL CONTROL DE ACCESOS EN EL AEROPUERTO DE LATACUNGA BASADO EN LA TECNOLOGÍA LONWORKS," Escuela Potitécnica Del Ejército, Departamento de eléctrica y electrónica, pp. 18-19, Mar. 2011
- [17] V.E. Cedeño Núñez, J.C. Ruiz Vasco, "DISEÑO E IMPLEMENTACIÓN DE UN MÓDULO DE CONTROL DOMÓTICO DE ARQUITECTURA CENTRALIZADA Y DISTRIBUIDA BASADA EN LONWORKS," Universidad de las fuerzas armadas (ESPE), Departamento de Eléctrica y Electrónica, pp. 11-16, 2013
- [18] S.J. Tontebeller, SENSORES SEM FIOS, Avaliação e Emprego na Automação de Sistemas Prediais. 1ª Edição, Seven System Internacional Ltda. Sao Paulo-SP-Brasil, pp. 50, Maio 2011.
- [19] García, J. F. and Gregorio, C. P. and Segarra, J. G, Control de iluminación con protocolo DMX-512: transmisor-receptor, Date-Added 2015-07-12 22:28:16 +0000 Date-Modified 2015-07-12 22:28:16 +0000 <https://books.google.com.ec/books?id=JZFkMwEACAAJ>, pp. 34-37, 2001.
- [20] Copertina Di Franco Beretta, Introduzione alla DOMOTICA, terza edizione, Milano, Junio 2009. <https://books.google.com.ec/books?id=JWwd35u4gNgC&printsec=frontcover#v=onepage&q&f=false>

#### BIOGRAFÍA



**Youssef Moises Abarca Reyes**, nació el 30 de Agosto de 1994, realizó sus estudios secundarios en el colegio Adolfo Valarezo de la ciudad de Loja, obtuvo el título de Bachillerato físico matemático. Curso sus estudios superiores de Ingeniería Electrónica en la Universidad Politécnica Salesiana sede Cuenca donde desarrolla actividades extracurriculares en el proyecto de Vinculación con la Sociedad, realizando instalaciones eléctricas entre otras actividades en beneficio de la sociedad.



**José Patricio Campoverde Gárate**, nació el 30 de Septiembre de 1993, realizó sus estudios primarios en la escuela Juan Montalvo desde el año 1998 hasta el 2005, posteriormente comienza sus estudios secundarios en el colegio Miguel Moreno Ordoñez en el cual estuvo 3 años, para después continuar el bachillerato en el colegio Pio XII "Hogar de Nazareth" en la ciudad de Cuenca, en el cual obtuvo el título de Bachillerato en Físico-Matemáticas en el año del 2012. Actualmente cursa sus estudios superiores en la Universidad Politécnica Salesiana sede Cuenca en la carrera de Ingeniería Electrónica.