UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA SISTEMAS Y COMPUTACIÓN

"DISEÑO DE UN SISTEMA DOMÓTICO CON TECNOLOGÍA EIB KONNEX PARA GESTIONAR LA SEGURIDAD DEL EDIFICIO DE INGENIERÍA DE LA UNACH"

Trabajo de Titulación para optar al Título de Ingeniero en Sistemas y Computación

Autor:
Bastidas Tituaña Bryan Josue

Tutor:
PhD. Fernando Tiverio Molina Granja.

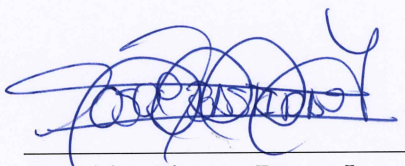
Riobamba, Ecuador. 2022

DERECHOS DE AUTORÍA

Yo, BASTIDAS TITUAÑA BRYAN JOSUE, con cédula de ciudadanía 1723079784, autor (a) (s) del trabajo de investigación titulado: " DISEÑO DE UN SISTEMA DOMÓTICO CON TECNOLOGÍA EIB KONNEX PARA GESTIONAR LA SEGURIDAD DEL EDIFICIO DE INGENIERÍA DE LA UNACH ", certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 02 días del mes de diciembre de 2022.



Bastidas Tituaña Bryan Josue
C.I: 1723079784

DICTAMEN FAVORABLE DEL TUTOR Y MIEMBROS DE TRIBUNAL;

Quienes suscribimos, catedráticos designados Tutor y Miembros del Tribunal de Grado para la evaluación del trabajo de investigación DISEÑO DE UN SISTEMA DOMÓTICO CON TECNOLOGÍA EIB KONNEX PARA GESTIONAR LA SEGURIDAD DEL EDIFICIO DE INGENIERÍA DE LA UNACH, presentado por Bastidas Tituaña Bryan Josue con cédula de identidad número 1723079784, certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha asesorado durante el desarrollo, revisado y evaluado el trabajo de investigación escrito y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba a los 2 días del mes de diciembre del 2022.

MsG. Ana Elizabeth Congacha Aushay
PRESIDENTE DEL TRIBUNAL DE GRADO
Firma

MsG. Luis Gonzalo Allauca Peñafiel
MIEMBRO DEL TRIBUNAL DE GRADO
Firma

PhD. Ximena Alexandra Quintana López
MIEMBRO DEL TRIBUNAL DE GRADO
Firma

PhD. Fernando Tiverio Molina Granja
TUTOR
Firma

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación DISEÑO DE UN SISTEMA DOMÓTICO CON TECNOLOGÍA EIB KONNEX PARA GESTIONAR LA SEGURIDAD DEL EDIFICIO DE INGENIERÍA DE LA UNACH, presentado por Bastidas Tituaña Bryan Josue, con cédula de identidad número 1723079784, bajo la tutoría de PhD. Fernando Tiverio Molina Granja; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba a los 2 días del mes de diciembre del 2022.

Presidente del Tribunal de Grado
MsG. Ana Elizabeth Congacha Aushay — Firma

Miembro del Tribunal de Grado
MsG. Luis Gonzalo Allauca Peñafiel — Firma

Miembro del Tribunal de Grado
PhD. Ximena Alexandra Quintana López — Firma

C E R T I F I C A C I Ó N

Que, **BASTIDAS TITUAÑA BRYAN JOSUE** con CC: **1723079784**, estudiante de la Carrera **INGENIERÍA EN SISTEMAS Y COMPUTACIÓN**, **NO VIGENTE,** Facultad de **INGENIERÍA**; ha trabajado bajo mi tutoría el trabajo de investigación titulado " **DISEÑO DE UN SISTEMA DOMÓTICO CON TECNOLOGÍA EIB KONNEX PARA GESTIONAR LA SEGURIDAD DEL EDIFICIO DE INGENIERÍA DE LA UNACH**", cumple con el 6 %, de acuerdo al reporte del sistema Anti plagio **URKUND**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 23 de noviembre de 2022

Firmado electrónicamente por:
FERNANDO TIVERIO MOLINA GRANJA

PhD. Fernando Tiverio Molina Granja
TUTOR TRABAJO DE INVESTIGACIÓN

AGRADECIMIENTO

"Le pedí a Dios fortaleza,
Dios me dio dificultades para hacerme más fuerte
Le pedí sabiduría,
Dios me dio problemas para resolverlos
Le pedí prosperidad,
Dios me dio mentalidad y fuerzas para trabajar."

Es por ello que deseo expresar mi agradecimiento a Dios por escuchar y contestar cada una de mis plegarias, de igual manera agradezco con todo mi ser a mi madre Magdalena Bastidas y tía Sylvia Bastidas por guiarme a lo largo de mi vida, brindándome su apoyo incondicional y por ser un pilar fundamental en mi vida.

Así mismo a mi tutor el PhD Fernando Molina y a mis colaboradores MSc. Gonzalo Allauca y PhD. Ximena Quintana por la dedicación y dirección que me han brindado en el proyecto de grado.

Finalmente, a mi alma Mater la Universidad Nacional de Chimborazo por permitirme formar parte de tan prestigioso centro de educación superior.

Josue Bastidas

ÍNDICE GENERAL

Contenido

ÍNDICE DE TABLAS.

ÍNDICE DE FIGURAS

RESUMEN

La presente propuesta tiene como objetivo diseñar un sistema domótico basado en tecnología EIB KONNEX para la gestión de la seguridad del edificio del tercer piso de ingeniería de la Universidad Nacional de Chimborazo.

Se procedió inicialmente a analizar las vulnerabilidades de seguridad dentro del tercer piso del bloque A de la Facultad de Ingeniería, donde se seleccionó una herramienta open source NMAP para monitorear la red, e identificar posibles amenazas que pueden poner en riesgo su sistema; seguidamente se procedió a la creación una matriz para cada amenaza, definir un ranking de importancia y definir medidas de corrección en la fase de diseño.

El diseño del sistema domótico para gestionar la seguridad en el edificio de Ingeniería, consistió en el estudio de la tecnología EIB KONNEX. El diseño del sistema domótico consistió en la selección de equipos y esquemas de conexión en el plano para acceso, inundación, sistema de cámaras y sistema contraincendios; posteriormente se elaboró el diagrama unifilar y el presupuesto.

La implementación de 4 escenarios simulados con máximo 5 dispositivos basado con el software ETS y KNX Virtual, consistió en definir la funcionalidad, definir la estructura y topología de la edificación, definir la estructura de grupo direcciones, editar parámetros e insertar dispositivos y establecer las funciones y enlaces; para finalmente pasar a la fase de programación y diagnóstico del sistema simulado.

Los resultados obtenidos de la investigación fueron corroborados por un grupo de expertos, que consideran que la propuesta planteada para mejorar la seguridad del tercer piso del bloque de ingeniería, en lo referente al diseño, simulación y posterior implementación del sistema domótico, se tabulo como muy satisfecho. En este sentido, también se dictamino la hipótesis planteada como verdadera, utilizando el método estadístico ANOVA.

Palabras claves: diseño, domótica, KNX, EIB KONNEX, edificio, seguridad.

ABSTRACT

The objective of this proposal is to design a home automation system based on EIB KONNEX technology for the security management of the third-floor engineering building of the National University of Chimborazo.

We initially proceeded to analyze the security vulnerabilities within the third floor of block A of the Faculty of Engineering, where an open source NMAP tool was selected to monitor the network, and identify possible threats that could put your system at risk; then proceeded to create a matrix for each threat, define a ranking of importance and define corrective measures in the design phase.

The design of the home automation system to manage security in the Engineering building consisted of the study of EIB KONNEX technology. The design of the home automation system consisted of the selection of equipment and connection schemes in the plan for access, flooding, camera system and firefighting system; subsequently the single-line diagram and the budget were drawn up.

The implementation of 4 simulated scenarios with a maximum of 5 devices based on the ETS and KNX Virtual software, consists of defining the functionality, defining the structure and topology of the building, defining the address group structure, editing parameters and inserting devices and establishing functions and links; to finally move on to the programming and diagnosis phase of the simulated system.

The results obtained from the investigation were corroborated by a group of experts, who considering that the proposal raised to improve the security of the third floor of the engineering block, in reference to the design, simulation and subsequent implementation of the home automation system, was tabulated as very satisfied in this sense, the hypothesis raised as true is also dictated, using the Anova statistical method.

Keywords: Design, home automation, KNX, EIB KONNEX, building, security.

1. CAPÍTULO I: INTRODUCCION.

Actualmente la domótica está en auge a nivel mundial, especialmente en los países desarrollados; la automatización de casas o edificios para alcanzar altos estándares tecnológicos y llegar a ser ciudades inteligentes; con la finalidad de brindar servicios automatizados de alta calidad a los usuarios.
EIB Konnex actualmente denominado como KNX, es un sistema de comunicación de control de edificios que permite conectar dispositivos como sensores, actuadores, controladores, terminales de operación y monitores; además esta tecnología abierta permite operar dispositivos KNX independiente del fabricante; cada dispositivo KNX (sensores y actuadores) será utilizado para el control y gestión del sistema de seguridad.

La automatización del edificio de Ingeniería de la UNACH, anteriormente no ha sido posible por falta de recursos económicos; sin embargo, se espera que, este diseño de automatización, pueda ser el punto de partida para gestionar un proyecto factible en beneficio de la Facultad de Ingeniería, considerando los beneficios a la seguridad de personas y bienes, como el ahorro de recursos en agua y luz.

La domótica aplicada a la seguridad del edificio de ingeniería se tomará en cuenta para evitar posibles daños y robos a los bienes del tercer piso del bloque A por parte de actores internos y externos a la facultad, si bien la seguridad dentro de la domótica constituye un factor indispensable para salvaguardar la vida de las personas también busca proteger el inmueble y los enceres de la institución, la domótica permite tener un ambiente seguro, confortable y contar con un gran aporte en las funcionalidades para gestionar los sistemas de climatización, iluminación y control de accesos, y alcanzar una óptima eficiencia energética.
Son pocas instituciones educativas a nivel nacional que han automatizado sus edificios, con la tecnología KNX. A nivel local tenemos la automatización del edificio de laboratorios de la Facultad de Mecánica de la ESPOCH para brindar confort, seguridad y ahorro energético (Baldeón & Congacha, 2014).
Otro edificio educativo implementado con tecnología KNX es el edificio de la Facultad de Odontología UEES, el proyecto permitió alcanzar una eficiencia energética del 60%, obteniendo mayor confort, mayor control de todos los pisos para la iluminación, y climatización (Knx.org, 2022).
El servicio de seguridad domótica es importante en nuestro caso, ya que permitirá controlar remotamente el edificio de ingeniería ante cualquier acontecimiento referente a la seguridad del edificio, de las personas y bienes que en él se encuentran, tales como: intrusiones, escapes de agua o gestión de emergencias. Estos eventos se comunican directamente al cliente o al encargado del sistema de seguridad y dentro de este servicio se incluyen detección, aviso y actuación, si procede.

El diseño del sistema domótico del edificio de la Facultad de Ingeniería se realizará usando la norma KNX (ISO/IEC 14543), para ello se realizó encuestas, entrevistas e investigación de campo, para el estudio de requerimientos de automatización del edificio de Ingeniería. En el diseño se considera el uso de sensores de inundación para las instalaciones hidrosanitarias, sensores para el control de accesos al tercer piso, sensores para dar seguridad a puertas y ventanas, sistemas de cámaras de seguridad y sistema de control de incendios. Se analizó las instalaciones de seguridad existentes y de comunicaciones, con el fin de mejorar los sistemas actuales con la tecnología EIB KONNEX.

El capítulo 1, describe el planteamiento del problema y objetivos de la investigación, seguidamente en el capítulo 2, se realizó un estudio de la norma KNX (ISO/IEC 14543) aplicables al diseño domótico en el tercer piso del edificio del bloque B de la Facultad de Ingeniería para posteriormente trabajar en el capítulo 3, el cual es referente a la metodología aplicable al diseño y simulación del sistema de seguridad basado en KNX, el capítulo 4, se analiza las vulnerabilidades de seguridad de la red implementada, para ello se realizó un estudio del estado del arte de los diversos softwares de monitoreo open source y licencia libre. Seleccionando a Nmap como software para monitoreo que permite verificar las vulnerabilidades de la red, el capítulo 5, se realizó la simulación de la red domótica, en base a los softwares KNX Virtual y ETS 6; se considera que está limitado el diseño a 5 equipos por oficina o laboratorio, debido a las restricciones del software mientras que en el capítulo 6, se procedió a la aplicación de la norma KNX (ISO/IEC 14543) para el diseño de los sistemas de seguridad (accesos, inundación, cámaras e incendios) del tercer piso, en el capítulo 7, muestra los resultados de la simulación de cada uno de los escenarios, los cuales no mostraron errores en los resultados de la simulación y finalmente el capítulo 8, describe las conclusiones y recomendaciones del diseño y simulación del sistema domótico para el tercer piso del edificio de ingeniería.

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Problema

En tanto, el problema de la investigación se determina: ¿cómo el diseño de un sistema domótico basado en la tecnología EIB KONNEX mejorará la gestión de la seguridad del bloque A edificio de Ingeniería?

Actualmente el edificio de Ingeniería (bloque A), carece de un sistema domótico de seguridad que permita controlar el servicio de seguridad de forma automática y remota mediante un dispositivo electrónico, como un teléfono celular o una computadora, esto repercute en que existe falta de control remoto y automático frente a cualquier evento que violente la seguridad del edificio, especialmente en horas no laborales.

Por consiguiente, el diseño de un sistema domótico para la seguridad, permitirá controlar de manera automática intrusiones, fugas de agua o gestión de emergencias; mediante un dispositivo móvil o computador, permitiendo un mejor resguardo del edificio, las personas y bienes que en él se encuentran.

1.2 Objetivos

1.2.1 Objetivo General

Diseñar un sistema domótico con tecnología EIB KONNEX para gestionar la seguridad del edificio de Ingeniería de la Universidad Nacional de Chimborazo.

1.2.2 Objetivos Específicos

- Analizar las vulnerabilidades de seguridad dentro del tercer piso del bloque A de la Facultad de Ingeniería utilizando la tecnología EIB KONNEX.
- Simular un sistema domótico para gestionar la seguridad en el edificio de Ingeniería de la Universidad Nacional de Chimborazo.
- Validar el sistema domótico a través de criterios de seguridad sobre un escenario simulado por medio de la norma KNX (ISO/IEC 14543).

2. CAPÍTULO II: MARCO TEÓRICO.

2.1 ESTADO DEL ARTE DE KNX

La automatización de viviendas y edificios es un esfuerzo tecnológico que tiene como objetivo hacer que las casas y los edificios sean más controlables, autónomos y cómodos. Este sistema requiere una gran implementación de sensores y actuadores para detectar información contextual y luego transferir datos de control a todos los componentes del edificio. Permite que los fabricantes elijan entre varios medios de transmisión, según los requisitos del mercado y los hábitos específicos (Ruta et al., 2022).

2.1.1 Iot KNX

Dweik et al. (2022), presenta y evalúa un caso de uso del esqueleto propuesto integrado con un sistema de automatización de oficinas basado en KNX, a través del sistema integrado, las luces y las persianas se controlan y los sensores se sondean mediante comandos de voz de un personal autorizado.

El término iluminación inteligente describe tres importantes atributos de diseño: control avanzado, estado sólido y amplia conectividad de red de acuerdo con los estándares internacionales. Proporciona una puerta de enlace de red óptica como una función adicional que permite la coexistencia con Wi-Fi tradicional; en este contexto, se están utilizando varias interfaces de comunicación inalámbrica compatibles con IoT para satisfacer las necesidades de iluminación de las viviendas inteligentes (Thirupathi et al., 2022).

Vanus et al. (2022), explica que una nueva solución interoperable que combina la tecnología de automatización de edificios KNX descentralizada existente con una puerta de enlace con aplicación de software KNX/LabVIEW y una nueva puerta de enlace para aplicaciones basadas KNX/IoT que utiliza un protocolo MQTT para la interoperabilidad entre la tecnología KNX y la plataforma IBM Watson IoT.

2.1.2 Seguridad KNX

Los sistemas de gestión de edificios centralizan y automatizan los activos esenciales de un edificio, a menudo están vinculados a la LAN y, a veces, se puede acceder a ellos en Internet, lo que expone dispositivos de automatización de edificios y protocolos de red que generalmente no están diseñados para manejar problemas de ciberseguridad (Vacherot, 2020).

Los edificios inteligentes tienen muchas características positivas, sin embargo, también hay deficiencias en lo relacionado a la seguridad. Los protocolos utilizados se desarrollaron hace algunas decenas de años y, por lo tanto, no están actualizados en cuanto a la seguridad. Reemplazar dispositivos antiguos por otros nuevos utilizando protocolos seguros no es una opción, ya que esto significaría una gran cantidad de costos. Esto significa que se debe encontrar una solución adecuada para contrarrestar este problema y mejorar la seguridad en tales sistemas (Goltz, 2021).

Los edificios inteligentes son redes de dispositivos y software conectados que se encargan de administrar y controlar automáticamente varias funciones del edificio, como aire acondicionado, alarmas contra incendios, iluminación, persianas y más. La seguridad de los edificios inteligentes está creciendo significativamente en complejidad debido a los numerosos protocolos introducidos recientemente y que la comunidad científica ya está estudiando (Ciholas et al., 2022).
La falta de seguridad de KNX lo hace sujeto a una variedad de ataques, el ataque de inyección de datos falsos contra una red de automatización de edificios basado en KNX. El diseño de un ataque man-in-the-middle (MITM) para cambiar los datos de un sensor de temperatura e inyectar datos falsos en la red de edificios. Dado que el ataque MITM puede perturbar el tráfico KNX, diseñamos una estrategia de detección basada en aprendizaje automático (ML) para detectar el ataque de inyección de datos falsos utilizando una función novedosa basada en Jensen Shannon Divergence (JSD). El ataque de inyección de datos falsos tiene un gran impacto en el sistema automatizado de edificios en términos de consumo de energía (Cash et al., 2022).
El impacto de los ataques cibernéticos en los edificios como corrupción de señal, retraso de señal y bloqueo de señal; y los enfoques típicos de detección y defensa de ciberataques se identifican en los tres niveles: nivel de gestión, nivel de automatización y nivel de campo. Las vulnerabilidades generales de edificios y las vulnerabilidades específicas de los cuatro protocolos BAS dominantes (BACnet, KNX, LonWorks y Modbus), Las estrategias de control resilientes ciberseguras para BAS bajo ataque se clasifican en esquemas de control resilientes pasivos y activos (Li et al., 2022).
Los métodos para agregar características de seguridad a las redes de automatización de edificios en forma de detección de intrusión o manipulación mediante el uso de la capa física, se propone métodos que se basan en la toma de huellas eléctricas de los dispositivos y el medio de comunicación, así como en el sondeo activo de radiofrecuencia de la red (Zdziarstek et al., 2022).

La seguridad de los sistemas de control y automatización de edificios están cada vez más interconectados con las redes del edificio e Internet, plantean problemas de seguridad. Considerando que toda la información recopilada a nivel local, en varios puntos de la red de campo, puede ser enviada a sistemas centralizados y más robustos para la detección de anomalías o ataques, aumentando así la probabilidad de detección (Graveto et al., 2022).

En las redes KNX las unidades acopladoras se utilizan para conectar los diferentes segmentos de la red, y para mantener el tráfico de transmisión local, ofrecen configuraciones de filtrado de diferentes acopladores de línea bajo aspectos de seguridad, se diseñó un conjunto de diferentes telegramas para probar la selectividad según los diferentes campos de encabezado de los telegramas. Se encontró que los acopladores solo filtran los telegramas al verificar su dirección de destino y ninguna de las otras características posibles. Esto significa que estos filtros no se pueden utilizar en un concepto de seguridad (Goltz et al., 2022).

Los sistemas de automatización de edificios proporcionan una gran cantidad de datos sobre su estado actual, con este propósito, generalmente se instala una gran cantidad de sensores en el edificio que detectan acciones humanas. Están conectados través de una red de bus de campo KNX, haciendo posible evaluar los eventos en una ubicación central, usando los datos de la automatización de edificios para detectar intrusos físicos y otras anomalías (Mundt et al., 2022).

2.1.3 Tecnologías para KNX

La tecnología Power Line Communication (PLC), disminuye con éxito el consumo de energía de un edificio, se evalúa la reutilización de recursos constructivos existentes mediante PLC; esto permite una ocupación estimada del edificio basada en la tecnología Visible Light Sensing (VLS), que puede detectar el número de personas solo al adquirir los reflejos de la luz visible, para transmitirlos de manera rentable, confiable y respetuosa con el medio ambiente (Ivanov et al., 2022).

2.1.4 Inteligencia artificial en KNX

La aplicación de la inteligencia interficial debe cambiarse hacia la conexión de red inalámbrica, es decir, "Internet de las Cosas" (IoT). El objetivo es crear las condiciones para reducir el consumo energético, mejorar el confort ambiental en los edificios y reducir las emisiones de CO2 (Garlik, 2022).

Las herramientas analíticas de big data de inteligencia artificial ofrecen varias soluciones para la gestión práctica de edificios. Por lo general, pueden ayudar para analizar los datos del equipo conectado y tomar decisiones inteligentes, eficientes y oportunas para mejorar el desempeño de los edificios como la detección de anomalías energéticas en edificios residenciales y de oficinas y la optimización energética y rendimiento en instalaciones deportivas (Himeur et al., 2022).

Por otro lado, un modelo para predecir la calidad del aire interior del edificio inteligente, los datos se recolectan del sistema de control y monitoreo de este proyecto en diferentes días y horas, y la calidad del aire se mide utilizando una red neuronal de la función de base radial, con entradas: temperatura, humedad del aire y dióxido de carbono (Majdi et al., 2022).

2.2 EIB KONNEX

El estándar KNX desarrollado por la Asociación Konnex de Domótica y Control de Edificios (ISO/ICE 14543, CENELEC EN 50090, CEN EN 133211, GB / Z 20965) se basa en los protocolos de automatización Home BatiBus, European Installation Bus (EIB) y European Home System (EHS). KNX admite varios medios de transmisión, como el par trenzado (KNX TP), línea eléctrica (KNX PL), radiofrecuencia (KNX RF) y tunneling IP (KNX IP). Los dispositivos KNX son dispositivos que se conectan a un bus para el control de edificios. Esto permite que los dispositivos KNX utilicen el mismo método de transmisión en una red

con bus común. KNX como estándar abierto para tecnologías de control de edificios en todo el mundo. En este caso, abierto significa que los dispositivos de diferentes fabricantes pueden comunicarse entre sí (Aguilar et al., 2018).

2.2.1 El Sistema de BUS KNX

El sistema KNX es un sistema de bus de control de edificios que permite que cada dispositivo del sistema KNX utilice el mismo método de transmisión e intercambio de datos en una red de bus común. El sistema KNX utiliza un sistema de bus descentralizado, lo que significa que, si un dispositivo falla, los demás continúan funcionando con normalidad (Aguilar et al., 2018).

La mejor solución es conectar todos los sensores y actuadores de un edificio a un solo medio de transmisión y permitir la comunicación entre ellos (Figura 1). Luego, cada dispositivo puede comunicarse con todos los demás; el sensor de botón pulsador, genera un comando y luego transmite datos en forma de telegrama a través del bus a un operador. Tan pronto como el actuador recibe la trama de datos, envía un reconocimiento y luego ejecuta el comando (Merz, 2019).

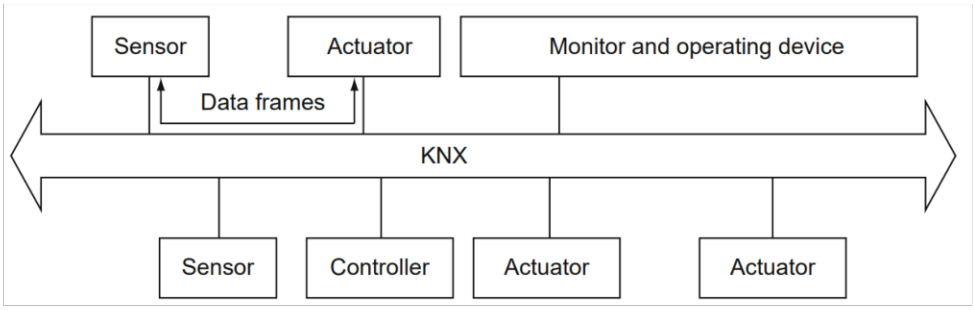


Figura 1: Dispositivos de control de edificios conectados a través de Konnex.
Fuente: (Hermann, 2019)

2.2.2 Medios de Transmisión KNX

El sistema KNX ofrece a los fabricantes la posibilidad de elegir entre varios medios de transmisión, según los requisitos del mercado y los hábitos específicos. Además, también es posible combinarlos para crear configuraciones de red multimedia y multiproveedor. Los medios de comunicación básicos par trenzado (TP) y onda portadora (PL) van acompañados del soporte de radiofrecuencia (RF) para hacer que las redes KNX sean flexibles y adaptables a múltiples dominios de aplicación y situaciones de instalación. Algunas de las características principales de los medios admitidos se presentan a continuación:

- **Par trenzado 1 (TP1):** es el medio básico heredado del protocolo EIB. Aporta una solución para el cableado, utilizando una red de seguridad de muy baja tensión (SELV) y un sistema de alimentación. KNX es compatible con los medios TP1-64 y TP1-256, que difieren en la cantidad de dispositivos conectables por segmento físico (64 o 256). TP1-256 es compatible con versiones anteriores de TPI-64. La velocidad de transmisión de TP1 es de 9600 bit/s con un modo de transferencia de datos asíncrono orientado a caracteres y una comunicación bidireccional semidúplex.

También cumple con el protocolo de acceso múltiple con detección de operador con prevención de colisiones (CSMA/CA). Todas las topologías de red (p. ej., línea o estrella) se pueden usar y combinar.

- **Onda portadora 110 (PL110):** también se hereda del protocolo EIB y admite la comunicación por medio de la red de alimentación principal de un edificio. Se basa en una transmisión asíncrona de paquetes de datos y una comunicación bidireccional semidúplex. PL110 utiliza la frecuencia central de 110 kHz con una tasa de datos de 1200 bit/s; cumple con CSMA.
- RF permite una comunicación vía radio en la banda de 868.3 MHz para dispositivos de corto alcance. Admite la codificación por desplazamiento de frecuencia, un ciclo de trabajo máximo del 1 % y una codificación de datos Manchester (Ruta et al., 2017).

2.2.3 Modos de configuración de los dispositivos KNX

En esta investigación se eligió el modo S porque (Shehata, 2007):

- La configuración y gestión de los dispositivos que funcionan en S-Mode pasan de la configuración y gestión manual a un conjunto de herramientas basado en PC llamado Engineering Tool Software ETS.
- S-Mode admite programación libre, puede tener software complemento de terceros.
- S-Mode ETS utiliza una base de datos para almacenar información sobre todos los dispositivos reales o simulados.
- S-Mode ETS admite de forma libre simulación de hasta 5 dispositivos, utilizado conjuntamente con el software KNX Virtual.

2.2.4 Topología

2.2.4.1 Nodos, Líneas y Áreas

Figura 2, representa un sistema KNX está estructurado jerárquicamente. La topología se basa en la estructura de las instalaciones de edificios convencionales, conocida como topología de árbol (Merz, 2019):

- Los nodos (N) se asignan a una línea (L).
- Varias líneas están conectadas a una línea principal (ML) a través de acopladores (C) y forman un área (A).
- Varias áreas están conectadas entre sí, conectando las líneas principales a la línea troncal o línea backbone (BL) a través de acopladores.

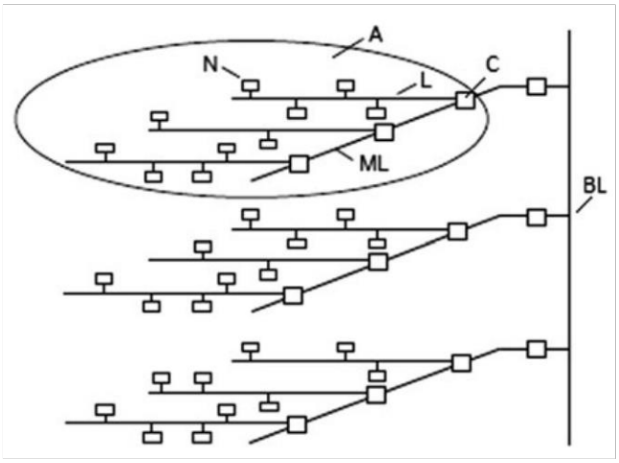


Figura 2: Topología en Árbol KNX.
Fuente: (Merz, 2019)

2.2.4.2 Acopladores

La Figura 3 muestra un acoplador es un componente del sistema y se puede utilizar como repetidor de línea (LR), acoplador de línea (LC) o acoplador de red backbone (BC). Su función como acoplador o repetidor, se define durante la configuración, asignando una dirección física específica. Las líneas y los segmentos de línea que están conectados entre sí por LC, BC y LR están eléctricamente aislados (Merz, 2019).

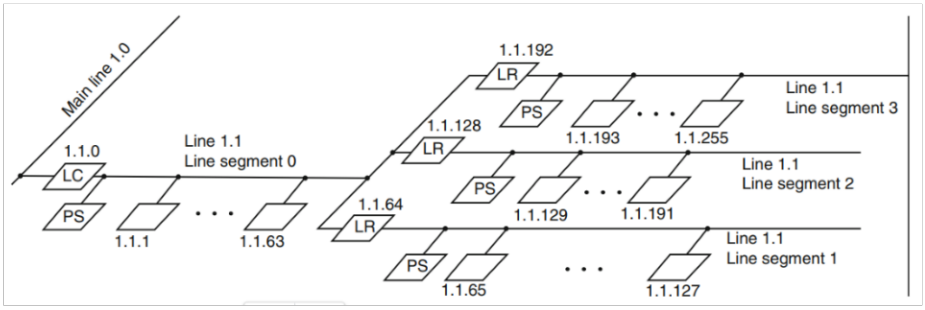


Figura 3: Una línea con tres repetidores de línea y cuatro segmentos.
Fuente: (Merz, 2019)

Para la configuración de una línea se aplican las siguientes reglas:

- El segmento de línea 0 puede tener un máximo de 64 actuadores/sensores, o 63 sensores/actuadores y un LC.
- Los segmentos de línea 1–3 pueden tener cada uno un LR y un máximo de 63 actuadores/sensores.

Una línea en su configuración máxima tiene 253 sensores/actuadores (o 252 si otro LC lo está conectando a la línea principal).
Para la versión TP1-256 de KNX.TP, solo hay un segmento de línea con un máximo de 256 sensores/actuadores o 255 más un LC (Merz, 2019).

La Figura 4, muestra los acopladores de línea (LC) conectan las líneas dentro de un área a la línea principal del área. Para convertir un acoplador en un acoplador de línea, se le asigna una dirección física especial (1.1.0, 1.2.0, etc.). Los acopladores troncales (BC) conectan las líneas principales a la línea troncal. Para convertir un acoplador en un acoplador de red troncal, se le asigna una dirección física especial (1.0.0, 2.0.0, etc.).
Las siguientes reglas se aplican a una línea o a un segmento de línea:

- Una línea no debe tener más de 1000 m de largo.
- La longitud del cable entre los dos dispositivos de bus que están más alejados no debe ser superior a 700 m.
- La longitud del cable entre una fuente de alimentación y un dispositivo no debe ser superior a 350 m.
- Cualquiera de las dos fuentes de alimentación en un segmento debe estar separada por al menos 200 m. No se pueden utilizar más de dos fuentes de alimentación.

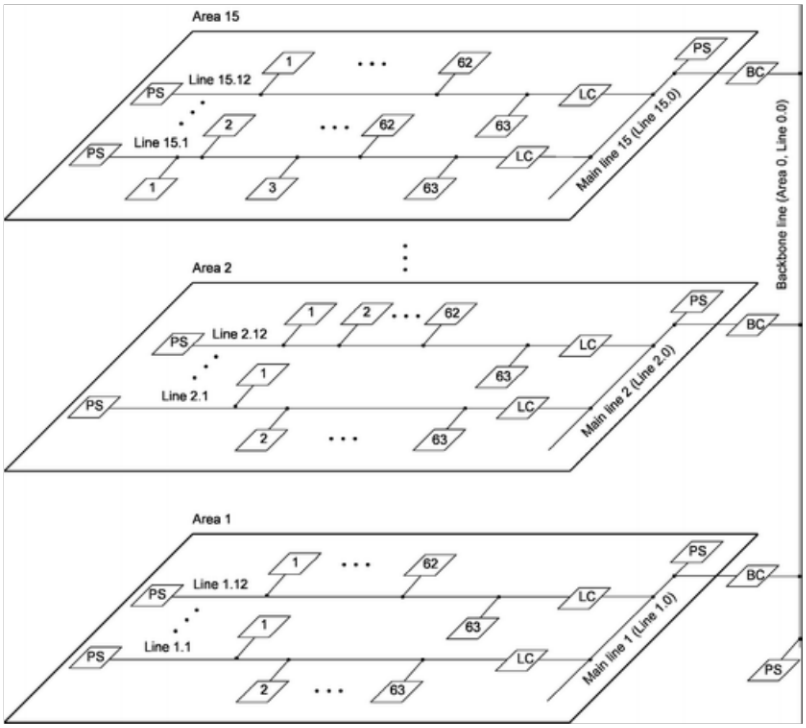


Figura 4: Topología de un sistema KNX.
Fuente: (Merz, 2019)

2.2.5 Direccionamiento de dispositivos (nodos)

Todos los dispositivos KNX que se comunican (sensores, actuadores, acopladores, etc.) deben tener una dirección física única. Los nodos también pertenecen a un grupo para que puedan intercambiar datos entre sí, los nodos de dicho grupo tienen una dirección de grupo además de su dirección física, que se puede utilizar para comunicarse con ellos (Merz, 2019).

2.2.5.1 Direccionamiento Físico

A cada dispositivo de bus (excepto la fuente de alimentación) se le asigna una dirección física única. A continuación, esta dirección se carga en el dispositivo (nodo) y se almacena de forma permanente en su EEPROM durante la puesta en servicio mediante ETS (Engineering Tool Software). Las direcciones deben asignarse de forma aleatoria, pero deben corresponder al diseño de la instalación del edificio. Los nodos (dispositivos) que se encuentran uno al lado del otro se les deben asignar direcciones físicas consecutivas.
La dirección física de un dispositivo lo identifica y proporciona la siguiente información:
Area.Line.Node (A.L.N.): Las partes de área, línea y nodo de la dirección física están separadas por puntos. La dirección física sirve para identificar el aparato o componente bus dentro de una topología o estructura del bus (Merz, 2019). Consta de tres números:

- **Primer número:** indica el área donde se encuentra. Puede ser un número del 1 al 15, si el número es el 0 indica que el componente está en la línea de áreas.
- **Segundo número:** indica la línea donde se encuentra. Puede ser un número del 1 al 15, si el número es el 0 indica que el componente está en la línea principal.
- **Tercer número:** indica el número del componente. Puede ser un número del 1 al 255, si el número es el 0 indica que el componente al que se refiere es un acoplador de línea o de área.

De esta forma, puede distinguir entre una dirección física y una dirección de grupo, que utiliza una barra inclinada (/). Las direcciones físicas suelen limitarse a:

- 15 áreas (números 1–15)
- 12 líneas por área (números 1–12)
- 64 nodos por línea (63 sensores/actuadores con números del 1 al 63 y un acoplador de línea con el número de nodo 0)

Esto significa que un máximo de 63 x 12 x 15 = 11 340 sensores/actuadores, más 12 x 15 = 180 LC y 15 BC, dando un total de 11 535 nodos.
Por ejemplo: la dirección 1.2.2 se refiere al segundo nodo en la segunda línea de la primera área.

2.2.5.1.1 Direcciones físicas para acopladores y repetidores de línea

Las siguientes direcciones físicas están reservadas para acopladores de línea y backbone:

- A.L.0 para acopladores de línea (p. ej., 1.1.0, 1.2.0, …, 1.12.0, 2.1.0, 2.2.0, …, 15.12.0)
- A.0.0 para acopladores backbone (p. ej., 1.0.0, 2.0.0, …, 15.0.0)

A los repetidores de línea se les debe asignar un número de nodo mayor que cero, por ejemplo, 1.1.64.

2.2.5.1.2 Direcciones físicas de dispositivos conectados a una línea principal

Esto se debe a que el tráfico de datos resultante interferiría con el tráfico de datos a través de las líneas o áreas. Como resultado, la unidad de fuente de alimentación de una línea principal generalmente solo necesita suministrar energía a un acoplador de red troncal. Por este motivo, se pueden conectar un máximo de 63 sensores/actuadores a la línea principal. Se les asignan las direcciones físicas A.0.x, donde x puede variar de 1 a 255. La dirección A.0.0 se reserva para el acoplador backbone (Merz, 2019). Ejemplos de direcciones:

- 1.0.1–1.0.63.
- 2.0.100–2.0.162.
- 1.12.0 es un acoplador de línea que conecta la línea 12 en el área 1 a la línea principal del área 1.

Si el sistema KNX comprende solo un área y, por lo tanto, no necesita un acoplador de red troncal, entonces se pueden conectar un máximo de 64 sensores/actuadores a la línea principal

- 2.0.0 representa un acoplador troncal que conecta la línea principal de la segunda área con la línea troncal.

2.2.5.1.3 Direcciones físicas de los dispositivos conectados a una línea troncal

Al igual que con las líneas principales, los sensores y actuadores normalmente no están conectados a la línea troncal. Esto se debe a que el tráfico de datos resultante interferiría con el tráfico de datos entre áreas.

Como resultado, la fuente de alimentación de una línea troncal normalmente no tiene que suministrar energía a un dispositivo de bus. Por esta razón, se pueden conectar un máximo de 64 sensores/actuadores a la línea principal. Se les asignan las direcciones físicas 0.0.x, donde x puede variar de 1 a 255 (Merz, 2019).

Ejemplos de direcciones:

- 0.0.1–0.0.64
- 0.0.100–0.0.163

2.2.5.2 Direccionamiento Lógico

El direccionamiento lógico o direccionamiento de grupo, al poner en marcha un sistema KNX utilizando ETS, se deben direccionar o programar dispositivos específicos. Por esta razón, las tramas de datos se envían utilizando la dirección física única de un dispositivo de destino como dirección de destino. Durante el ciclo operativo normal de un sistema KNX, las tramas de datos se envían utilizando direcciones de grupo (Merz, 2019).

KNX distingue entre dos tipos de direcciones de grupo:

- **Direcciones de grupo:** con un grupo principal y un subgrupo (direccionamiento de dos niveles).

- **Direcciones de grupo:** con un grupo principal, un grupo intermedio y un subgrupo (direccionamiento de tres niveles).

Con ETS se puede seleccionar el tipo de direccionamiento deseado. Se reserva un campo de 16 bits en la trama de datos para la dirección de grupo, aunque solo se utilizan 15 bits.

2.2.5.2.1 Direccionamiento de Dos Niveles

Merz (2019), indica que, para el direccionamiento de dos niveles, los 15 bits disponibles se utilizan de la siguiente manera (Tabla 1).

Bytes Superiores								Bytes Inferiores							
D7	D6	D5	D4	D3	D2	D1	D0	D7	D6	D5	D4	D3	D2	D1	D0
0	M3	M2	M1	M0	S10	S9	S8	S7	S6	S5	S4	S3	S2	S1	S0
Grupo Principal					Subgrupo										

Tabla 1: Direccionamiento de dos niveles.

Fuente: (Merz, 2019)

Esto significa que:

- 24 = 16 grupos principales (números 0 - 15)
- 211 = 2048 subgrupos (números 0 - 2047)

La dirección de grupo para el direccionamiento de dos niveles se escribe como
Grupo principal/subgrupo.
Para poder identificar un determinado grupo, a estos grupos principales y subgrupos se les asignan nombres.
Ejemplos de direcciones de grupo:

- 0/1 iluminación central on/off
- 1/1 iluminación de la sala de estar on/off
- 1/2 iluminación de la oficina on/off
- 2/1 persianas on/off

2.2.5.2.2 Direccionamiento de Tres Niveles

Merz (2019), afirma que, para el direccionamiento de tres niveles, los 15 bits disponibles se utilizan de la siguiente manera (Tabla 2).

Bytes Superiores								Bytes Inferiores							
D7	D6	D5	D4	D3	D2	D1	D0	D7	D6	D5	D4	D3	D2	D1	D0
0	M3	M2	M1	M0	G2	G1	G0	S7	S6	S5	S4	S3	S2	S1	S0
Grupo Principal					Grupo Intermedio			Subgrupo							

Tabla 2: Direccionamiento de Tres Niveles.

Fuente: (Merz, 2019)

Esto significa que:

- 24 = 16 grupos principales (números 0–15)
- 23 = 8 grupos intermedios (números 0–7)
- 28 = 256 subgrupos (números 0–255)

La dirección de grupo para el direccionamiento de tres niveles se escribe como:
Grupo principal/grupo intermedio/subgrupo
Ejemplos de direcciones de grupo:

- 1/1/1 iluminación del techo de la sala de estar on/off
- 1/1/2 iluminación de la de la lámpara de pie de la sala de estar on/off
- 1/2/1 iluminación del techo de la oficina on/off
- 1/2/2 iluminación del escritorio de la oficina on/off

2.2.6 Telegrama KNX

Los dispositivos de bus KNX intercambian datos entre sí por telegrama. Un telegrama consta de caracteres de 8 bits, y un campo es una combinación de varios caracteres. Los medios de comunicación tienen diferentes estructuras de telegramas (Kortetjärvi y Khorami, 2021):

a) El telegrama de par trenzado KNX tiene cuatro campos:

- **Campo de control:** es el encargado de recibir una respuesta del receptor si la transmisión del telegrama fue exitosa o no.
- **Campo de dirección:** este campo contiene la dirección del remitente y del destinatario.
- **Campo de datos:** este campo contiene la carga útil del telegrama.
- **Checksum:** este campo es para controles de paridad. Por verificación de paridad significa que este campo se utiliza para detectar errores en el canal de comunicación.

b) Telegrama de protocolo de internet KNX:

- **Longitud del encabezado:** este campo es para identificar la estadística del telegrama.
- **Versión de protocolo:** este campo muestra qué versión de KNX IP se aplica.
- **Identificador de tipo de servicio IP KNX:** muestra la acción que se debe realizar.
- **Longitud total:** el objetivo de este campo es mostrar el tamaño del telegrama IP KNX.
- **Cuerpo IP KNX:** este campo contiene telegramas de carga útil.

2.2.7 KNX Virtual y su Protocolo KNXnet/IP

El KNX virtual es la forma virtual de un componente físico KNX. KNX virtual utiliza direcciones IP, puertos IP y TP para comunicarse intercambiando telegramas con controladores y otras aplicaciones. El controlador KNX usa la dirección física y KNXnet/IP

para comunicarse con otros dispositivos como KNX virtual. El protocolo KNX para estos métodos se llama KNXnet/IP.
Un sistema KNXnet/IP proporciona acceso de integración a diferentes redes KNX a través de un protocolo de Internet. La integración se realiza mediante un dispositivo específico llamado enrutador KNXnet/IP. La comunicación IP en KNX se puede explicar utilizando el modelo de referencia OSI (Kortetjärvi y Khorami, 2021):

- **Capa de aplicación:** la comunicación se realiza a través de esta capa que genera el telegrama KNXnet/IP.
- **Capa de Transporte:** donde ocurre el método de tunelización. La capa de transporte en el estándar KNX proporciona cuatro diferentes modos de comunicación:
    1. Sin conexión de multipunto a multipunto (multidifusión)
    2. Punto a todos los puntos sin conexión (difusión)
    3. Sin conexión punto a punto (unidifusión)
    4. Orientado a la conexión punto a punto
- **Capa de red:** en esta capa ocurre el protocolo de Internet.
- **Capa física y capa de enlace de datos:** Ethernet.

2.2.8 Seguridad en KNXnet/IP

Proteger el backbone contra interferencias maliciosas es un paso importante hacia una red KNX segura. Especialmente las redes backbone basadas en IP son propensas a los ataques. Esto se debe a dos razones: en primer lugar, debido al uso generalizado de redes IP, los protocolos basados en IP junto con sus defectos de diseño y vulnerabilidades de seguridad y, por lo tanto, en muchos protocolos basados en IP existen ataques de seguridad. En segundo lugar, el acceso físico a las redes troncales basadas en IP se puede obtener más fácilmente, ya que a menudo se comparten con la IP de la red LAN. Además, es común el acceso de administración remota (por ejemplo, desde Internet a través de una puerta de enlace web) que puede ser mal utilizado para obtener acceso al sistema.
Para proteger completamente la comunicación dentro de una red KNXnet/IP, se deben integrar diferentes mecanismos de seguridad en el protocolo KNXnet/IP. En cuanto a las demandas de una red KNXnet/IP segura, se pueden identificar los siguientes objetivos (Lechner et al., 2008):

- **Autenticación de entidad:** para evitar la suplantación de dispositivos KNXnet/IP legítimos, los servidores y clientes KNXnet/IP involucrados deben demostrar su identidad antes de que puedan comunicarse de forma segura entre sí.
- **Canal seguro:** para proteger los datos transmitidos que se intercambian entre los socios de comunicación autenticados, se debe proporcionar un canal seguro, tal canal utiliza técnicas físicas y/o criptográficas para garantizar distintos objetivos de seguridad. Dependiendo de los requisitos de seguridad de la aplicación, estos son la integridad de los datos, actualización y/o confidencialidad.
- **Compatibilidad con unidifusión y multidifusión:** KNXnet/IP especifica diferentes servicios de comunicación. El objetivo principal de una extensión de seguridad para

KNXnet/IP es admitir completamente todos estos servicios KNXnet/IP. Si bien la mayoría se basa en la comunicación de unidifusión, algunos servicios como el enrutamiento de KNXnet/IP y el servicio de detección de KNXnet/IP se basan en la multidifusión. Por lo tanto, se debe usar una extensión de seguridad que proporcione soporte para unidifusión y comunicación multidifusión.

- **Bajo poder de procesamiento y consumo de memoria:** Proporcionar seguridad mediante técnicas físicas (p. ej., empalmar los cables de red), en cuyo caso, se deben utilizar técnicas criptográficas. Por motivos de rentabilidad, los dispositivos integrados con capacidad de procesamiento y memoria limitadas se utilizan comúnmente en las instalaciones KNX.

2.2.9 Seguridad en EIB KONNEX con KNX Secure

2.2.9.1 KNX Secure

Topología con KNX Secure

Para KNX IP Secure, está la configuración de la línea backbone, que define el modo de seguridad deseado para el medio IP. El estado real final de la seguridad depende de varias condiciones de contorno. A continuación, se indican los modos posibles (Lourdas, 2020):

a) **Opción Desactivado:** la seguridad está deshabilitada o los dispositivos que se agregan no usan KNX IP Secure, incluso si lo admiten.
b) **Opción activada:** el estado de la seguridad está habilitado o los dispositivos que se agreguen deben ser compatibles con KNX IP Secure (no se pueden agregar otros dispositivos).

Seguridad KNX IP

Con KNX IP seguro, solo la comunicación KNX en el medio IP es segura; los telegramas en una línea principal o (sub) línea (que se muestra en la imagen aquí como una línea TP) siguen siendo simples o menos seguras, ver Figura 5.

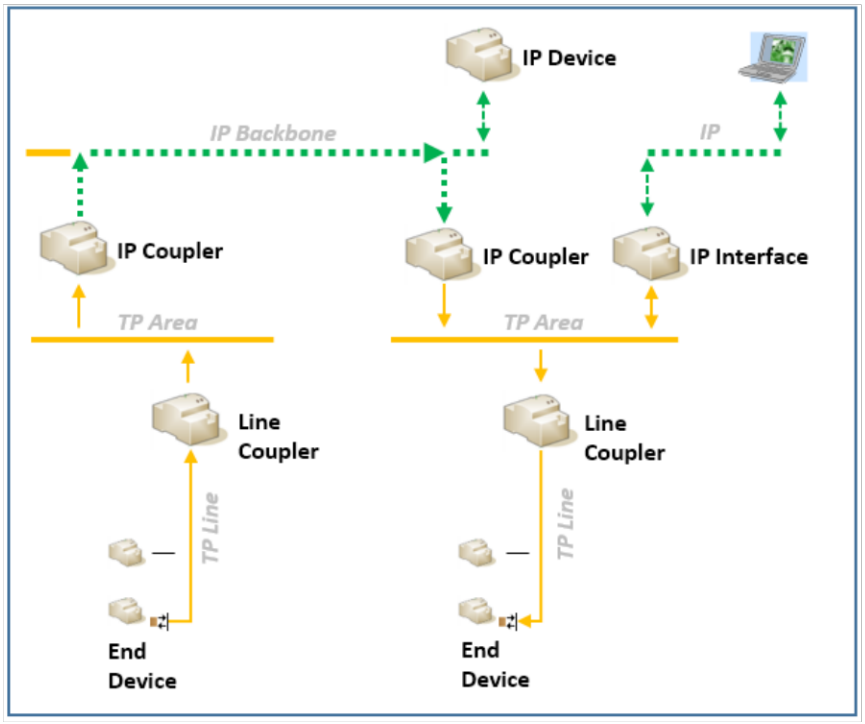


Figura 5: Seguridad IP KNX.
Fuente: (Lourdas, 2020)

Dispositivos seguros KNX

La diferencia entre los dispositivos KNX simples y los dispositivos seguros KNX es que los dispositivos seguros KNX pueden cifrar y descifrar telegramas. Esta tecnología añade un extra de seguridad a una instalación KNX, tanto durante la puesta en marcha de instalaciones KNX como para instalaciones KNX en tiempo de ejecución. Los telegramas KNX encriptados por dispositivos seguros KNX se denominan telegramas seguros KNX (Lourdas, 2020).

2.3 Software Herramienta de Ingeniería (ETS)

Engineering Tool Software (ETS) es un programa integrado para diseñar, planificar y poner en marcha sistemas KNX. El Software Herramienta de Ingeniería utilizada en esta investigación será la versión 5 o también conocido por sus siglas ETS 5.
La licencia utilizada será la demostración gratuita con un máximo de 5 dispositivos KNX por proyecto, sin exportar.

3. CAPÍTULO III: METODOLOGÍA.

González-Muñoz et al. (2018), el Delphi es una metodología estructurada para recolectar sistemáticamente juicios de expertos sobre un problema, procesar la información y a través de recursos estadísticos, construir un acuerdo general de grupo. Permite la transformación durante la investigación de las apreciaciones individuales de los expertos en un juicio colectivo superior.

3.1 TIPO DE ESTUDIO

3.1.1 INVESTIGACIÓN APLICADA.

El diseñar la red domótica para seguridad basada en la tecnología EIB KONNEX utilizando la norma ISO/IEC 14543, permitirá solucionar vulnerabilidades de seguridad del tercer piso del bloque A de la Facultad de Ingeniería.

3.1.2 INVESTIGACIÓN EXPLICATIVA.

Debido a que se describe la tecnología EIB KONNEX utilizando la norma ISO/IEC 14543 con el fin de tener información clara sobre la tecnología a utilizar, y detallar como va a estar el diseño de la red de domótica de seguridad.

3.2 HIPÓTESIS

El diseño de un sistema domótico basado en la tecnología EIB KONNEX mejorará la gestión de la seguridad del edificio de Ingeniería.

3.3 VARIABLES

3.3.1 Variable Independiente

Diseño de un sistema domótico con tecnología EIB KONNEX.

3.3.2 Variable Dependiente

Mejora de la Gestión de la seguridad del Edificio de Ingeniería de la Universidad Nacional de Chimborazo.

3.4 Operacionalización de variables

Tabla 3: Operacionalización de variables.

PREGUNTA DE INVESTIGACIÓN	TEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	CONCEPTUALIZACIÓN	DIMENSIÓN	INDICADORES
¿Cómo el diseño de un sistema domótico basado en la tecnología EIBKONNEX mejorará la gestión de la seguridad del edificio de Ingeniería de la Universidad Nacional de Chimborazo?	Diseño de un Sistema Domótico con Tecnología EIB KONNEX para gestionar la seguridad del edificio de Ingeniería de la UNACH.	**GENERAL** Diseñar un sistema domótico con tecnología EIB KONNEX para gestionar la seguridad del edificio de Ingeniería de la Universidad Nacional de Chimborazo. **ESPECÍFICOS** - Analizar las vulnerabilidades de seguridad dentro del tercer piso delbloque A de la Facultad de Ingeniería utilizando la tecnología EIB KONNEX. - Simular un sistema domótico para gestionar la seguridad en el	El diseño de un sistema domótico basado en la tecnología EIB KONNEX mejorará la gestión de la seguridad del edificio de Ingeniería.	**INDEPENDIENTE** Diseño de un sistema domótico con tecnología EIB KONNEX. **DEPENDIENTE** Mejora de la Gestión de la seguridad del Edificio de Ingeniería de la Universidad Nacional de Chimborazo.	Es un proceso sistemático basado en la norma ISO/IEC 14543, sustentado en la evaluación de la situación actual, para proceder a la selección de equipos, elaboración de diagramas y finalmente la puesta a prueba del sistema. Es un proceso diseñado para proteger personas, bienes, la red y los datos que fluyen en ella mediante controles tecnológicos.	Sistemas domóticos. EIB KONNEX Componentes domóticos. Control y servicios Aplicaciones Simulación	- Niveles de calidad de señal alámbrica e inalámbrica. - % de ahorro en el presupuesto de cables y equipos KNX. - Porcentaje de intrusión detectadas - Número de habitaciones con elementos de domótica implementados. - Número Incidentes detectados vs número deincidentes controlados por el sistema

		edificio de Ingeniería de la Universidad Nacional de Chimborazo. - Validar el sistema domótico a través de criterios de seguridad sobre un escenario simulado por medio de la norma KNX (ISO/IEC 14543).					- Nivel de confiabilidad del diseño, configuración y programación de equipos virtuales de la red de seguridad.

Fuente: El tesista

3.5 VALIDACIÓN DE LA HIPÓTESIS

La validación de la hipótesis se basa en el análisis de varianza de dos factores con una sola muestra por grupo, acomoda el modelo lineal en ANOVA bidireccional con diferentes sumas de cuadrados, grados de libertad, suma media de cuadrados, y la inferencia sobre el análisis; el procedimiento MS-EXCEL para cálculos de ANOVA bidireccional (Upendra et al., 2017).

Supuestos de ANOVA:

- Los errores experimentales de sus datos son normalmente distribuidos.
- Varianzas iguales entre tratamientos, es decir, homogeneidad de varianzas, e homocedasticidad.
- Independencia de las muestras, cada muestra es seleccionados en base a los indicadores.

ANOVA de dos vías:

Se utiliza el análisis de varianza de dos vías (ANOVA) para determinar si existen diferencias significativas entre las medias de tres o grupos más independientes (no relacionados).

La tabla 4 indica la distribución de datos para ANOVA de dos vías:

Filas	Columnas						Row total	Row mean
	1	2	---	j	----	c		
1	X_{11}	X_{12}	---	X_{1j}	----	X_{1c}	R_1	$\bar{R}_1$
2	X_{21}	X_{22}	---	X_{2j}	----	X_{2c}	R_2	$\bar{R}_2$
			---		----			
i	X_{i1}	X_{i2}	---	X_{ij}	----	X_{ic}	R_i	$\bar{R}$
			---		----			
r	X_{r1}	X_{r2}	---	X_{rj}	----	X_{rc}	R_r	$\bar{R}_r$
Column total	C_1	C_2	---	C_j	----	C_c	GT	
Column mean	$\bar{C}_1$	$\bar{C}_2$	---	$\bar{C}_j$	----	$\bar{C}_c$		

Tabla 4: Distribución de datos para ANOVA de dos vías.
Fuente: (Upendra, 2017)

Donde GT=Gran Total= $\sum_i \sum_j X_{ij}$; i =1, 2, , r, j=1, 2, -, c.

Donde X_{ij} = la observación en ith Fila y jth Columna
El modelo linear este dado por:

$X_{ij} = \mu + R_i + C_j + \varepsilon_{ij}$; i =1, 2,.. , r, j=1, 2, --, c.

μ = media

R_i = i^{th} efecto de fila

C_j = j^{th} efecto de columna

ε_{ij} = error aleatorio

3.6 POBLACIÓN

El proyecto de investigación de acuerdo a los márgenes de Delphi comprende a 10 expertos los cuales se dividirán en diferentes grupos dependiendo de las necesidades para validar el diseño a través la norma KNX.

Los expertos deberán tener un perfil de 4 nivel en el área de informática con experiencia en Domótica.

3.7 MUESTRA

Al tener una población menor a las 50 personas se debe tener en cuenta que la población pasa a ser la misma muestra. En nuestro caso sería 10 expertos.
La muestra corresponde al total de la población. En nuestro caso seria 10 expertos.

3.8 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.8.1 Técnicas

Observación: Se realizará la observación antes del diseño de la red domótica, con la finalidad de recabar información de la situación actual de la red del tercer piso del edificio de la Facultad de Ingeniería de la UNACH.
Encuesta: Se validará el diseño domótico de seguridad mediante encuestas dirigidas a grupos de expertos.

3.8.2 Instrumentos

Ficha de observación: Referente a documento sobre el que se recopilara toda la información utilizada con la técnica de la observación.
Encuesta: Diseñada mediante la escala de Likert, que permitirán valorar el diseño y simulación de la red domótica.

3.9 PROCEDIMIENTO

3.9.1 Análisis de las vulnerabilidades de seguridad

El análisis de las vulnerabilidades de seguridad dentro del tercer piso del bloque A de la Facultad de Ingeniería siguió el siguiente procedimiento:

1. **Elección de una herramienta open source para monitorear la red.**
   La elección del software de monitoreo de red dependió de los elementos de red a ser monitoreados y se seleccionaron mediante un ckecklist.
2. **Identificación de las posibles amenazas.**
   Recopilar información sobre los procesos tecnológicos y enumerar las principales amenazas que pueden poner en riesgo su sistema, tales como pérdida de datos, desastres naturales, software anticuado, fallas de sistema y error humano.
3. **Creación de una matriz para cada amenaza.**
   La matriz de riesgos está formada por dos componentes: probabilidad de ocurrencia del riesgo y el impacto que tendrá contra la amenaza. La probabilidad se divide en casi cierto, alta, media, baja y rara. El impacto puede ser gravísimo, grave, medio, leve y sin impacto. Cuanto mayor sea el riesgo y el nivel de impacto de la ocurrencia, más atención debe darse a la situación.
4. **Definir un ranking de importancia.**
   Después de colocar todos los elementos en la matriz de riesgo, es necesario crear un grado de importancia por orden de gravedad y urgencia de resolución. Es necesario separar lo que es relevante y lo que no tiene tanta importancia.
5. **Definir medidas de corrección.**
   Definir la estrategia de acción para cada amenaza. Aquí va a definir medidas preventivas y de actuación después de ocurrir el problema.

3.9.2 Diseñar el sistema domótico para gestionar la seguridad en el edificio de Ingeniería

1) Estudio de la tecnología EIB KONNEX

Consiste en el estudio de: Argumentos del sistema KNX, topología del par trenzado, comunicación, componentes de una red KNX y normativa.

2) Diseño del sistema domótico

El diseño del sistema domótico consiste en:

1. Selección de equipos y esquemas de conexión en el plano.
2. Elaboración del diagrama lógico.
3. Elaboración del diagrama funcional.

3.9.3 Implementar un escenario simulado

Para la simulación de la red se sigue el siguiente procedimiento:

1. Crear con el software ETS la estructura del edificio que consta de los espacios diseñados y los dispositivos insertados desde el catálogo de KNX.
2. Crear en ETS los grupos de direcciones basadas en el diseño para proceder a configurar, enlazar y programar cada dispositivo de KNX virtual.
3. Test para verificar el funcionamiento del diseño.

4. CAPÍTULO IV: ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD.

El análisis de las vulnerabilidades de seguridad dentro del tercer piso del bloque A de la Facultad de Ingeniería siguió el siguiente procedimiento:

4.1 Elección de una herramienta open source para monitorear la seguridad de la red

En la Tabla 5, se realiza un análisis comparativo de diferentes herramientas para detección y prevención de intrusiones, en la cual se resume cómo los rastreadores de paquetes se diferencian en las propiedades, como sus características para diferentes sistemas operativos, la identificación de protocolos, el uso del disco, etc.

Nombre de la herramienta	Proveedor	Tipo	Descripción	Plataforma
SNORT	Cisco system	NIDS, NIPS	Puede detector: Dos, CGI, Intrusion, Port Scans, SMB And Layer Attacks. SNORT Has The Ability To Make Concurrent Traffic Analysis And Packet Logging On Internet Protocol (IP) Networks	(Cross Platform) Linux, windows
SURICATA	Open security foundation	NMS, NIPS	Automatic Protocol Detection, File Matching Process And Compatible With SNORT	Linux, unix ,MAC,windows etc.,
Bro IDS	Vern Paxson	NIDS, AIDS	Empleado en combinación con Snort	Linux, MAC OS X, FreeBSD
OpenWIPS-ng	Aircrack-NG	NIPS	Openwips-Ng es un Open Source And Modular Wireless IPS (Intrusion Prevention System).	Linux
Security Onion	-	NMS	Contiene: Snort, Suricata, Sguil, Squert, Snorby, Bro, Networkminer, Xplico, And Many Other Security Tools	Linux
OSSEC	Daniel B. Cid	HIDS	Cuenta con un potente motor de correlación y análisis, integrando el análisis de registros	Cross-platform
NMAP	Gordon Lyon	GNU	Esta herramienta es usada para monitorear los problemas de seguridad en una red, enfocada en los puertos sus servicios y su topología.	Linux, Windows, MAC

Tabla 5: Comparaciones de diferentes herramientas para detección y prevención de intrusiones.

Fuente: Gandhi et al., 2014

La comparación propuesta en la Tabla 6, para los rastreadores de paquetes en parámetros cualitativos y cuantitativos muestra que ninguna de las herramientas lidera todos los parámetros. Por un lado, Colasoft Capsa es la herramienta con la que se podría medir la máxima seguridad de red.
En la tabla 6, se muestra las mejores herramientas a utilizar para detección y prevención de intrusiones.

No.	Caso	Mejor herramienta
1	Packets dropped	Wireshark
2	• Seguridad de la red: ARP attack • Worm activity • DoS attack • TCP port scanning • Suspicious conversation	Colasoft Capsa
3	Tiempo de respuesta	Wireshark
4	Alarmas de red	Colasoft Capsa
5	ps(Rendimiento)	Wireshark
6	Tamaño del paquete	Colasoft Capsa
7	PPS	Wireshark
8	Interface de usuario	Colasoft Capsa
9	Número de protocolos	Wireshark
10	Comunicación de red	Colasoft Capsa
11	Vulnerabilidades de puertos	NMAP

Tabla 6: Mejores herramientas a utilizar para detección y prevención de intrusiones.
Fuente: Gandhi et al., 2014

Una herramienta de monitoreo de red puede ser un dispositivo de hardware o un software libre o propietario que observa continuamente su red y los datos que fluyen a través de ella. Dependiendo de cómo la solución realmente monitorea una red, puede capturar datos directamente de la red a medida que pasa o recopilar datos almacenados por un nodo de red.

En Anexo 2, se hace una comparación de diferentes herramientas de monitoreo para redes con licencia General Public License (GPL) o libre con algunos softwares con licencia comercial con un periodo de prueba entre 14 días y 30 días gratis.

En la Tabla 7, se resumen algunas de las principales herramientas de monitoreo de redes del mercado, de las que destaca SolarWinds como una de las herramientas más completa del mercado, inclusive a nivel de publicaciones científicas basadas en esta herramienta existe una amplia aceptación. SolarWinds no tiene un único instalador, posee varios softwares para prueba entre 14 y 30 días. Específicamente para monitoreo de seguridad trabaja con la herramienta ManageEngine, la cual debe ser integrada a SolarWinds por usuarios avanzados. ManageEngine es una robusta herramienta para monitoreo de seguridad: seguridad organizacional, seguridad física, seguridad de infraestructura, seguridad de datos, identidad y control de acceso, seguridad operativa gestión de incidentes, divulgaciones responsables, gestión de proveedores, controles de clientes para seguridad.
Además, se tiene como una segunda opción de monitoreo de seguridad la herramienta Nagios, la cual tiene que ser instala en Windows usando una máquina virtual, ya que Nagios se ejecuta en Linux. Mientras que la herramienta de monitoreo de red Wireshark es una buena alternativa que no requiere una exhaustiva configuración en el servidor y es de fácil manejo.

Para el monitoreo de la seguridad de la red se seleccionó NMAP, por su fácil manejo. Este software es código abierto, se instaló en un computador ubicado en el cuarto de equipos y físicamente ubicado en el tercer piso de la Facultad de Ingeniería, el mismo que permite determinar las anomalías de seguridad de la red.

Software	Monitoreo de Seguridad en la red
Nagios	Seguridad incrementada Mayor conciencia de los problemas de infraestructura de red Mayor disponibilidad de servidores, servicios y aplicaciones Detección rápida de cortes de red y fallas de protocolo Detección rápida de procesos fallidos, servicios, trabajos cron y trabajos por lotes Cumplimiento de auditoría Cumplimiento normativo
Zabbix	Archivos de configuración, archivos de registro, Trampas SNMP, etc.
Zenoss	Cifrado de contraseña.
op5 Monitor	Ninguno
Network Performance Monitor	Ninguno
SolarWinds	Integrado con ManageEngine: seguridad organizacional, seguridad física, seguridad de infraestructura, seguridad de datos, identidad y control de acceso, seguridad operativa gestión de incidentes, divulgaciones responsables, gestión de proveedores, controles de clientes para seguridad.
Pandora FMS Community	Ninguna
Wormly	Web Server Security Scan
Cacti	Marco de gestión de fallas
OpenNMS	Vulnerabilidades de seguridad básicas
Pandora FMS Enterprise	Vulnerabilidades y exposiciones comunes

Tabla 7: Software para monitoreo de seguridad para redes.

Fuente: El tesista

5. CAPÍTULO V: SIMULACIÓN

La simulación del diseño domótico será realizada a través de un prototipo mediante el uso de los softwares ETS 5 y KNX Virtual 2.4.3, escenarios sobre los cuales se realiza las diferentes pruebas de funcionalidad de seguridad.

5.1 Elaboración de un proyecto con ETS 5

5.1.1 Localización del proyecto

Al instalar ETS 5, se crea automáticamente una carpeta de proyectos en la ubicación C:\Users\Public\Documents\KNX\Archive. Esta carpeta es la base de datos del proyecto o puede usarla como la base de datos central para todos los proyectos. Contiene no solo los datos del producto del fabricante, sino también los datos del proyecto proporcionados por el usuario.

Antes de seleccionar los dispositivos y configurar sus parámetros, primero se debe importar los datos del producto a la base de datos del proyecto, desde la base de datos del producto del fabricante (Catálogos/Importar...), tal como se muestra a continuación:

5.1.2 Diseño y configuración del proyecto

Una vez importado los datos del proyecto, se procede a diseñar y configurar el proyecto utilizando ETS 5. Esto implica convertir los requisitos cliente en especificaciones funcionales. En otras palabras, determinando el alcance del suministro y los servicios, definiendo el diseño y los tipos de dispositivos, y creando las conexiones lógicas (Merz, 2019).

1. El diseño y configuración de proyectos con ETS 5 podría seguir los siguientes pasos:
    a. Crear un nuevo proyecto: Esto abre la ventana de configuración de ETS 5, se pueden abrir ventanas adicionales utilizando el icono de menú respectivo.
    b. Ahora el proyecto se puede editar en la vista de construcción o en la vista de topología:
        i. En la vista de topología, el proyecto se puede ver como una topología de bus. Se debe hacer lo siguiente:
        ii. Crear áreas y líneas
        iii. Asignar dispositivos a líneas
        iv. Asignar direcciones físicas
        v. Editar parámetros del dispositivo
    c. En la vista de edificio, el proyecto se puede ver como una estructura de edificio. Se debe hacer lo siguiente:
        i. Crear edificios, partes de edificios, salas, armarios de control y sistemas
        ii. Asignar dispositivos a habitaciones, armarios de control o sistemas
        iii. Asignar direcciones físicas

iv. Editar parámetros del dispositivo

2. Luego al cambiar a la ventana de direcciones de grupo. Se debe hacer lo siguiente:
    a. Definir direcciones de grupo para asignar funciones
    b. Asigne objetos de comunicación a las direcciones de grupo. La asignación se puede ver en la ventana de direcciones de grupo y en la ventana de topología.
3. No es obligatorio seguir estos pasos en el orden indicado. Los pasos se pueden omitir o procesar en otro orden.

5.1.3 Puesta en marcha

Una vez que haya diseñado y configurado el proyecto, deberá cargar las direcciones físicas establecidas y el programa de aplicación (parámetros del dispositivo, objetos de comunicación asignados a las direcciones de grupo y la aplicación real) en cada dispositivo. Para hacerlo, se selecciona los dispositivos en la ventana de topología o en la ventana de construcción e inicie el proceso deseado haciendo clic con el botón derecho y seleccionando Descargar/...

Cuando se programa los dispositivos por primera vez, primero se debe cargar la dirección física en cada dispositivo (inicie el procedimiento de programación en ETS 5 y luego presione brevemente el botón de programación del dispositivo cuando se le solicite) y luego cargue el programa de aplicación para cada dispositivo (incluido los parámetros del dispositivo y las direcciones de grupo asignadas). También puede realizar ambos pasos al mismo tiempo.

Para que el acceso al bus funcione, la interfaz utilizada (serie PEI16-COM1, USB, si es necesario, puerta de enlace IP) debe seleccionarse y configurarse en la pestaña interfaces del elemento de menú ETS/Bus…

Posteriormente se deben programar las respectivas direcciones físicas. La interfaz seleccionada ahora se muestra en la parte inferior izquierda de ETS 5 y se puede editar allí.

Después de que la dirección física se haya programado una vez, solo necesita descargar el software de la aplicación si los parámetros del dispositivo cambian o para seleccionar otra aplicación para un dispositivo.

Una vez que haya cargado los programas de aplicación en los dispositivos, el sistema KNX estará listo para su uso y podrá probarse con las herramientas de diagnóstico de ETS 5, como el monitor de bus (elemento de menú: Bus/Monitor de bus). Este software le permite ver y analizar el tráfico en el autobús. Registra todas las tramas de datos enviadas en el bus.

5.2 Escenarios

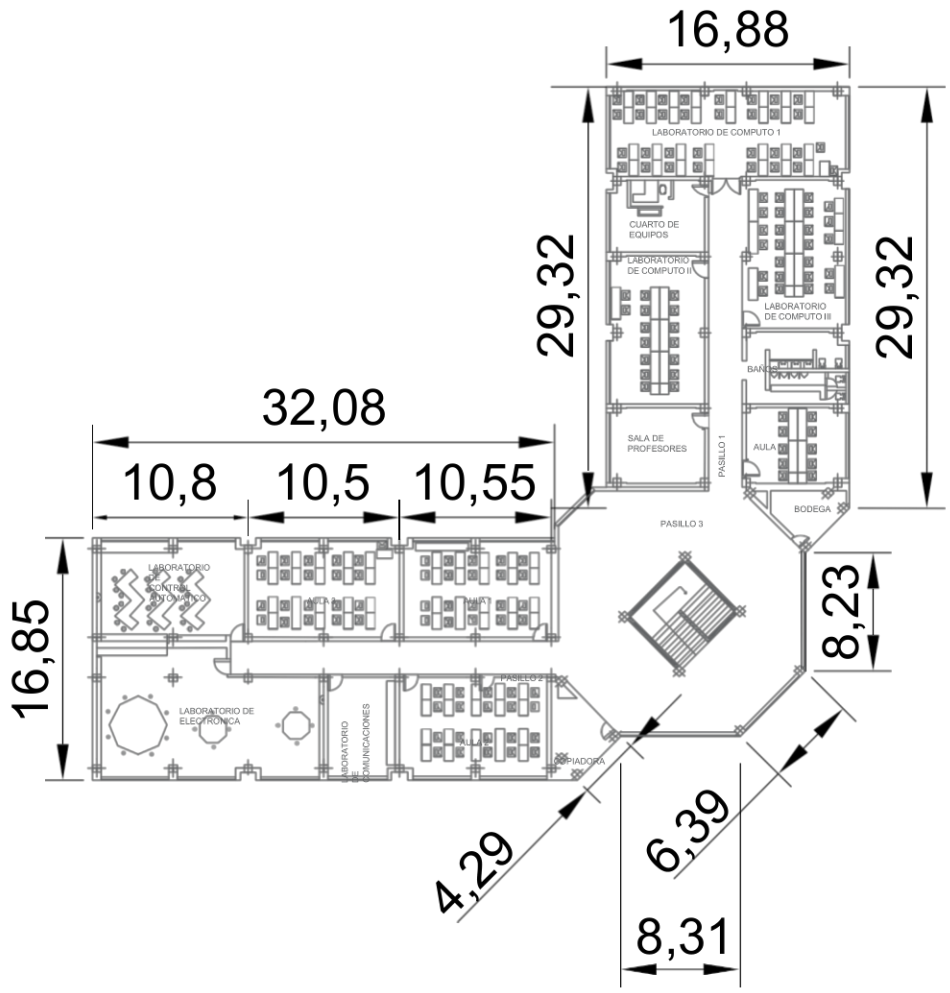
La simulación tendría 3 escenarios, tal y como se indica a en el Anexo 1.

6. CAPÍTULO VI. DISEÑO

Para el diseño del sistema domótico se considera la normativa KNX 14543, referente a la distancia máxima de los cables, distancia máxima entre dispositivos y el número máximo de dispositivos, que fue tratado en el capítulo II.

6.1 Esquema Arquitectónico

La Figura 6 muestra el diseño arquitectónico del tercer piso del bloque A, el mismo que está a escala 1: 100, donde se muestra el dibujo arquitectónico tanto de la infraestructura del tercer piso, como los muebles en cada espacio.



Plano del Tercer Piso
Escala 1: 100

Figura 6: Plano Arquitectónico del edificio de Ingeniería – tercer piso.
Fuente: El tesista

6.2 Seguridad de Acceso e Inundación

La Figura 7 muestra el esquema de conexión de acceso al tercer piso, donde la lampara se encenderá al existir una intrusión, el detector de presencia se activa y se enciende la lampara.

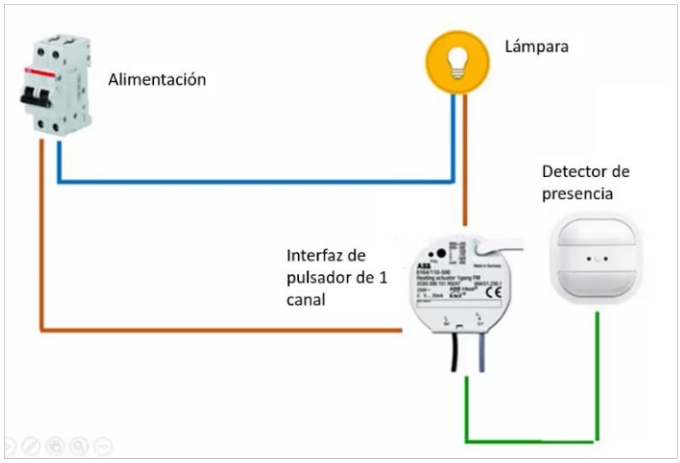


Figura 7: Esquema de conexión de Acceso.
Fuente: Paredes, (2016)

La figura 8 muestra el esquema de conexión para una sonda de inundación, donde el terminal de zona permitirá sectorizar la ubicación de las sondas, se deberá finalmente colocar una resistencia terminal antes de la sonda de inundación. El plano de diseño de Acceso e Inundación, se detalla en un anexo 1 entregado a las autoridades de la facultad. (El Anexo 3 se entrega a las autoridades por cuestiones de seguridad y confidencialidad)

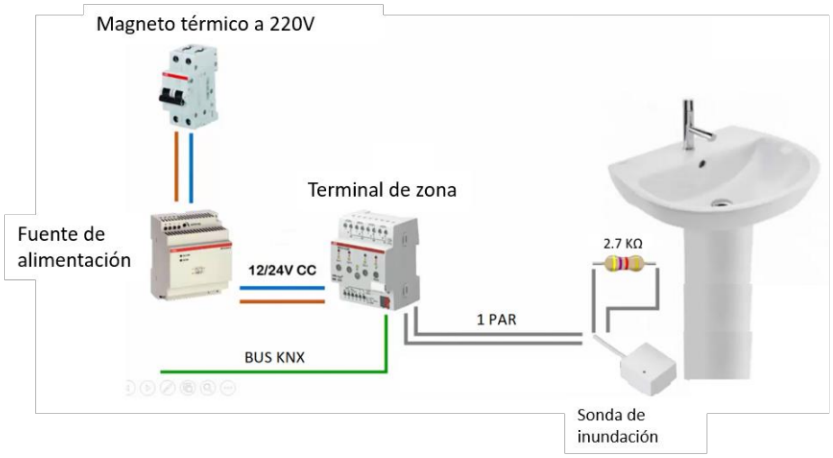


Figura 8: Esquema de conexión de Sonda de Inundación.
Fuente: Paredes, (2016)

6.3 Seguridad de Puertas y Ventanas

Para la seguridad de puertas y ventanas se utiliza contactos magnéticos colocados en puertas y ventanas, igualmente se deberá colocar al final una resistencia terminal. El terminal de zona dividirá en dos zonas los dispositivos: Sistemas y Computación y la de Electrónica y Telecomunicaciones. El momento de existir una intrusión se comunicará con la pantalla táctil, e enviará un sms a la persona responsable, como se indica en la figura 9.

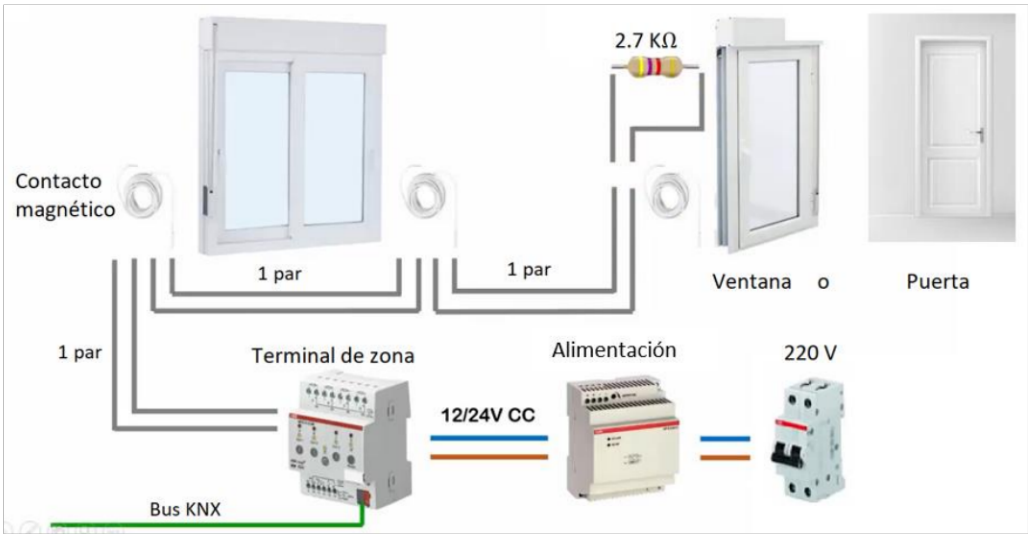


Figura 9: Esquema de conexión de puertas y ventanas.
Fuente: Paredes, (2016)

La tabla 8 indica el detalle del presupuesto acceso, inundación, puertas y ventanas.

PRESUPUESTO ACCESO, INUNDACION, PUERTAS Y VENTANAS			
Unidad	**Denominación**	**PVP/Unidad**	**Subtotal**
1	Detector de presencia de techo	138.39	138.39
3	Interface de pulsadores de 1 canal	62.02	186.06
1	Terminal de zona de 4 canales	300	300
2	Terminal de zona de 2 canales	181	181
4	Sonda de inundación	81	324
39	Contacto magnético	26.1	1017.9
1	Pantalla táctil con servidor web	490	490
4	Rollo 100 m cable Bus de 2 pares	151	604
1	Fuente de alimentación de 640 mA	410	410
		TOTAL 1	3651.35

Tabla 8: Presupuesto Acceso, Inundación, Puertas y Ventanas.
Fuente: El tesista

6.4 Sistema de Cámaras

La figura 10 muestra el esquema de conexión del sistema de cámaras, cada cámara ip con visión de 360 grados, se conecta al switch de 16 puertos mediante un cable POE (Power over Ethernet) que permite alimentar y enviar datos a la cámara. El switch se conecta a un rack y del rack se conecta al NVR (Network video recorder) que permite grabar lo capturado por las cámaras.

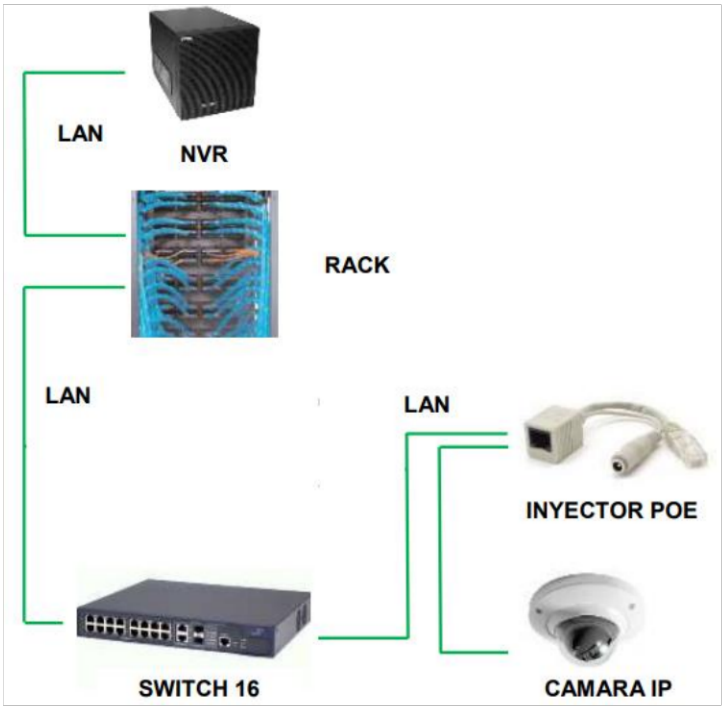


Figura 10: Esquema de conexión de Cámaras.
Fuente: Paredes, (2016)

La tabla 9 indica el detalle del presupuesto del sistema de cámaras.

PRESUPUESTO SISTEMA DE CAMARAS DE SEGURIDAD			
Unidad	**denominación**	**PVP/Unidad**	**Subtotal**
1	Video grabador digital	3539.49	3539.49
15	Cámara IP tipo Domo a 360 grados	200	3000
15	Passive power over ethernet inyector	20.6	309
1	Switch de borde 16 puertos POE	945.33	945.33
121	Cable UTP CAT 6	3.5	423.5
60	Canaleta lisa 20x12	4.5	270
		TOTAL 2	8487.32

Tabla 9: Presupuesto Sistema de cámaras.
Fuente: El tesista

6.5 Sistema Contra Incendios

La central de incendios direccionable, maneja datos digitales enviados desde los sensores de detección de humo y detección de gas; además permite ubicar en su panel direcciones Ip a los detectores en caso de que se active alguno de ellos; al mismo tiempo se activara la sirena-luz estroboscópica como señal audible/visible; la misma que puede ser localizada gracias a su módulo de control en el panel de la central de incendios, como se muestra en la figura 11.

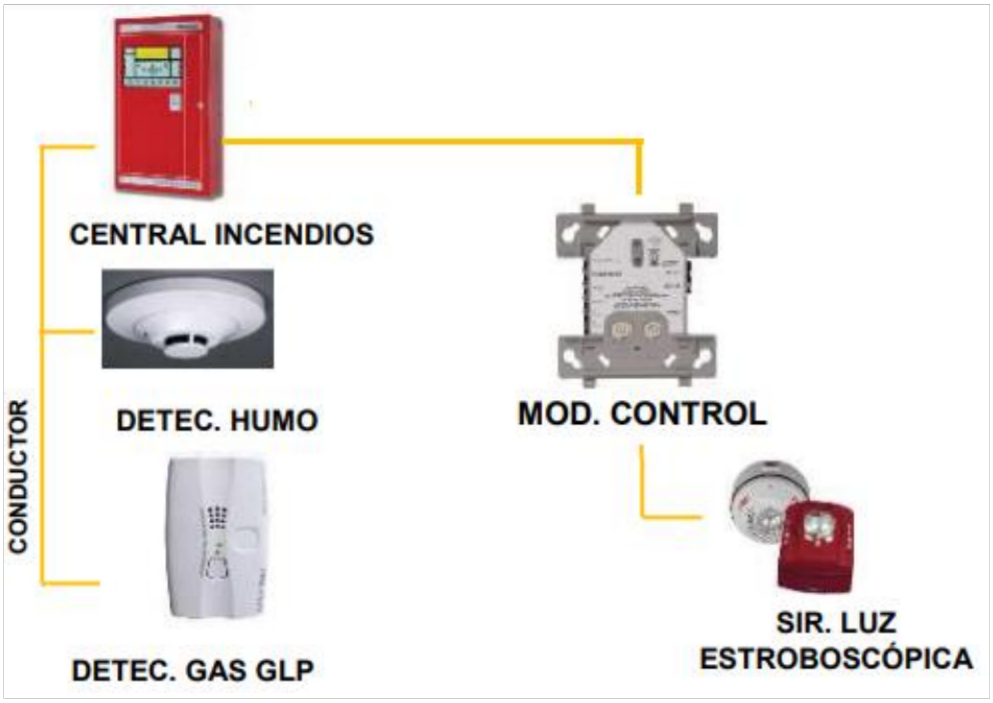


Figura 11: Esquema de conexión Sistema Contra Incendios.
Fuente: Paredes, (2016)

La tabla 10 indica el detalle del presupuesto del sistema contra incendio.

PRESUPUESTO SISTEMA CONTRA INCENDIO			
Unidad	**Denominación**	**PVP/Unidad**	**Subtotal**
1	Central de alarma de incendio direccionable	3000	3000
1	Módulo de control direccionable	125	125
17	Detector de humo fotoeléctrico	78	1326
1	Detector GPL	138	138
3	Sirena con luz estroboscópica	85	255
140	Cable 2x16 AWG Antiflama	2.31	323.4
71	Canaleta lisa 20x12	4.5	319.5
		TOTAL 3	5486.9

Tabla 10: Presupuesto Sistema Contra Incendio
Fuente: El tesista

6.6 Esquema Unifilar

La figura 12 muestra el esquema unifilar de los dispositivos conectados que pueden ser localizados en el panel táctil (1.1.11) mediante una dirección Ip. Es decir, el monitoreo del sistema se lo podrá realizar desde el cuarto de equipos o en remoto al conectarse mediante internet al panel táctil. Al activarse alguna alarma o sensor habrá una señal audible en el tercer piso, al mismo tiempo se notificará mediante SMS al responsable.

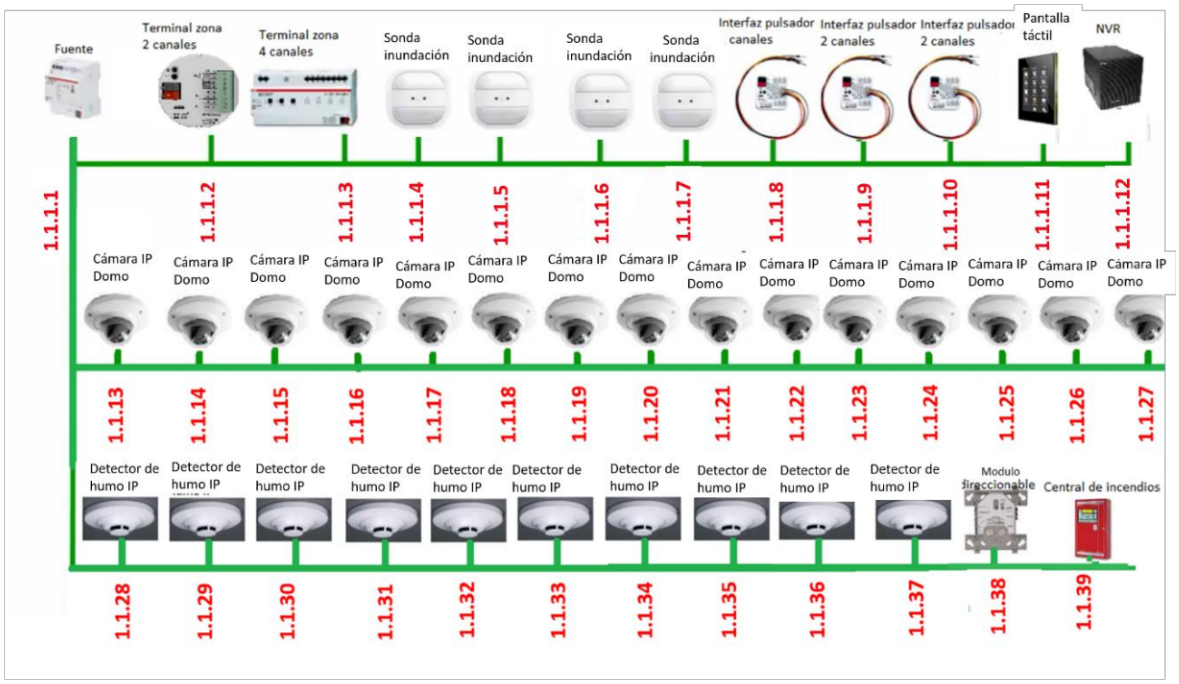


Figura 12: Esquema unifilar del tercer piso.
Fuente: El tesista

7. CAPÍTULO VII. RESULTADOS Y DISCUSIÓN

Para la primera parte la cual trata sobre el análisis de vulnerabilidades dentro del tercer piso del bloque A de la Facultad de Ingeniería se aplicó la técnica de observación con la finalidad de recabar información de la situación actual de la red, de igual manera se trabajó con la colaboración del Ingeniero Orlando Ortiz para una mejor comprensión del estado de cableado y cámaras.

De esta manera se obtuvo como resultado que el edificio en mención, incluido su tercer piso, actualmente dispone de un sistema de cámaras IP para intrusión y evidencia la falta de los siguientes sistemas:

- Falta de un sistema de alarma de intrusión para acceso no autorizado.
- Falta de un sistema de alarmas IP para puertas y ventanas.
- No existencia de un sistema contra incendios.
- Los baños y laboratorios que disponen de agua potable no disponen de un sistema contra inundaciones.

Adicionalmente, se evidencia que el edificio no dispone de un sistema de alarmas, en caso de robo; al existir solamente un sistema de cámaras de seguridad, en caso de ser este violentado, el edificio no dispone de ningún sistema de seguridad adicional, lo que posibilita que en cierta medida un riesgo para los bienes y personas que se encuentran resguardados en el edificio.

Posteriormente se procedió a realizar un monitoreo de la red con la ayuda de la herramienta NMAP, la cual se muestra a continuación.

7.1 RESULTADOS DEL MONITOREO DE LA RED

La siguiente captura de monitoreo intenso con NMAP desde el pc 172.30.3.170, fue ejecutado el comando "args="nmap -T4 -A -v 172.30.3.170". Se verifica 174 puertos abiertos que son vulnerables, los servicios vulnerables (tcpwrapped y msrpc):


```
<?xml version="1.0" encoding="iso-8859-1"?>
<?xml-stylesheet href="file:///C:/Program Files
(x86)/Nmap/nmap.xsl" type="text/xsl"?><nmaprun start="1659643403"
profile_name="Intense scan" xmloutputversion="1.04" scanner="nmap"
version="7.92" startstr="Thu Aug 4 15:03:23 2022" args="nmap -T4 -
A -v 172.30.3.170"><scaninfo services="1,3-4,6-7,9,13,17,19-
26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-
111,113,119,125,135,139,143-144,146,161,163,179,199,211-
212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-
417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-
545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-
668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,80
0-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-
```

993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-
1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-
1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-
1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-
1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-
1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-
1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1
687-1688,1700,1717-1721,1723,1755,1761,1782-
1783,1801,1805,1812,1839-1840,1862-
1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-
2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-
2049,2065,2068,2099-2100,2103,2105-
2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-
2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-
2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-
2608,2638,2701-2702,2710,2717-
2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-
2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-
3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-
3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-
3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-
3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-
3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3
986,3995,3998,4000-4006,4045,4111,4125-
4126,4129,4224,4242,4279,4321,4343,4443-
4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-
5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-
5102,5120,5190,5200,5214,5221-5222,5225-
5226,5269,5280,5298,5357,5405,5414,5431-
5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-
5679,5718,5730,5800-5802,5810-
5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-
5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-
6007,6009,6025,6059,6100-
6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-
6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-
6789,6792,6839,6881,6901,6969,7000-
7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-
7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-
7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-
8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-
8194,8200,8222,8254,8290-
8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-
8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-
9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-
9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-

9503,9535,9575,9593-9595,9618,9666,9876-
9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-
10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-
10617,10621,10626,10628-10629,10778,11110-
11111,11967,12000,12174,12265,12345,13456,13722,13782-
13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-
16001,16012,16016,16018,16080,16113,16992-
16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,
19801,19842,20000,20005,20031,20221-
20222,20828,21571,22939,23502,24444,24800,25734-
25735,26214,27000,27352-27353,27355-
27356,27715,28201,30000,30718,30951,31038,31337,32768-
32785,33354,33899,34571-
34573,35500,38292,40193,40911,41511,42510,44176,44442-
44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-
49176,49400,49999-
50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,
52848,52869,54045,54328,55055-55056,55555,55600,56737-
56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,
64680,65000,65129,65389" protocol="tcp" numservices="1000"
type="connect"></scaninfo><verbose level="1"></verbose><debugging
level="0"></debugging><output type="interactive">Starting Nmap 7.92
(https://nmap.org) at 2022-08-04 15:03 Hora est. PacÃfico,
SudamÃ©ricaWARNING: Could not import all necessary Npcap functions.
You may need to upgrade to the latest version from https://npcap.org.
Resorting to connect() mode -- Nmap may not function completelyNSE:
Loaded 155 scripts for scanning.NSE: Script Pre-scanning.Initiating
NSE at 15:03Completed NSE at 15:03, 0.01s elapsedInitiating NSE at
15:03Completed NSE at 15:03, 0.00s elapsedInitiating NSE at
15:03Completed NSE at 15:03, 0.00s elapsedInitiating Ping Scan at
15:03Scanning 172.30.3.170 [2 ports]Completed Ping Scan at 15:03,
0.00s elapsed (1 total hosts)Initiating Parallel DNS resolution of
1 host. at 15:03Completed Parallel DNS resolution of 1 host. at
15:03, 0.20s elapsedInitiating Connect Scan at 15:03Scanning
172.30.3.170 [1000 ports]Discovered open port 995/tcp on
172.30.3.170Discovered open port 445/tcp on 172.30.3.170Discovered
open port 139/tcp on 172.30.3.170Discovered open port 25/tcp on
172.30.3.170Discovered open port 993/tcp on . . . . . .

7.2 RESULTADOS DE LA SIMULACIÓN

A continuación, se muestran los resultados capturados del monitoreo del bus de datos para cada escenario de simulación, cada telegrama consta de los siguientes campos:

- #: número de telegrama
- Time: fecha y hora de la captura del telegrama en el bus

- Service: servicio tomado del bus de datos
- Flags: banderas; información de control; las banderas en el monitor de bus

  E: Formato de cuadro (Cuadro estándar)
  H: formato de trama (trama LTE-HEE)
  R: Repetición
  a: Confirmación esperada
  C: Indicador de confirmación, se establece si el reconocimiento es negativo
  F: Error de bit de parada de trama
  B: Error de bits de datos
  P: Error de bit de paridad
  O: Desbordamiento
  L: telegrama perdido
  S: contador de secuencia, x=0-7

- Prio: prioridad
- Source address: dirección del dispositivo KNX que hace el control
- Source name: nombre del dispositivo fuente (si el monitor está asignado a un proyecto)
- Destination: dirección de grupo que recibe el telegrama enviado

  Las siguientes variantes pueden ocurrir, dependiendo del "tipo" de telegrama:

  - Para comunicación P2P sin conexión/orientada a conexión > Visualización de la dirección individual
  - Para comunicación en grupo > Visualización de la Dirección del Grupo, siempre en la codificación respectiva de la estructura de la Dirección del Grupo
  - Para comunicación de difusión (sistema) > Visualización de la Dirección de grupo (con el valor 0), siempre en la codificación respectiva de la estructura de la Dirección de grupo (por ejemplo, 0/0/0)
  - Para comunicación de grupo LTE (etiqueta lógica ampliada) > Visualización de la información de las zonas LTE según la especificación KNX, p. ej., geográfica, específica de la aplicación, periférica general

- Destination name: nombre del destino
- Type: tipo de telegrama que ha sido enviado, puede ser de 3 tipos:

  - GroupValueWrite: cuando un valor es escrito al bus KNX
  - GroupValueRead: cuando un valor es leído desde bus KNX

- GroupValueResponse: Cuando hay una respuesta desde un dispositivo al bus KNX

- DPT: Tipo de telegrama que se envía al bus KNX.
- Info: Valor del telegrama que se ha enviado al bus KNX
- IACK (Reconocimiento inmediato):

Tiene los siguientes 3 formatos:

- Negative Acknowledgement: coding 0Ch (00001100b)
- Busy Acknowledgement: coding C0h (11000000b)
- Positive Acknowledgement: coding CCh (11001100b)

Los telegramas que se muestran de los 3 escenarios indican en todos los casos comunicación exitosa en el control de cada dispositivo, donde se muestra en detalle cada trama relacionada al ítem de cada escenario.

7.2.1 Resultados del Escenario 1: Conmutación

Resultados de las Funciones de construcción

1. D4.1 controla a D7.1 (sin realimentación)

#	Time	Service	Flags	Prio	Source A...	Source Name	Destinati...	Destination Name	Ho...	Type	DPT	Info	Iack
43	13/7/2022 4:34:1...	from bus		Low	1.1.1	KliX (D4)	1/1/1	New group address	6	GroupValu...	1.001 s...	$01 | On	LL_A...
44	13/7/2022 4:34:1...	from bus		Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...	$00 | Inactive	LL_A...
45	13/7/2022 4:34:1...	from bus		Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...	$00 | Inactive	LL_A...
46	13/7/2022 4:34:1...	from bus		Low	1.1.1	KliX (D4)	1/1/1	New group address	6	GroupValu...	1.001 s...	$00 | Off	LL_A...

Figura 13: Resultados monitoreo D4.1 control D7.1.
Fuente: El tesista

2. D10.1 controla a D7.1: detección de movimiento + detección de presencia

#	Time	Service	Flags	Prio	Source Add	Source Name	Destination	Destination Name
57	13/7/2022 4:34:34,480	from bus		Low	1.1.4	Movement/Presence Detector (D10)	1/1/1	New group address
65	13/7/2022 4:34:47,619	from bus		Low	1.1.4	Movement/Presence Detector (D10)	1/1/1	New group address
70	13/7/2022 4:34:51,540	from bus		Low	1.1.4	Movement/Presence Detector (D10)	1/1/1	New group address
173	13/7/2022 4:37:50,058	from bus		Low	1.1.4	Movement/Presence Detector (D10)	1/1/1	New group address
176	13/7/2022 4:37:55,121	from bus		Low	1.1.4	Movement/Presence Detector (D10)	1/1/1	New group address
270	13/7/2022 4:40:27,431	from bus		Low	1.1.4	Movement/Presence Detector (D10)	2/1/1	New group address
273	13/7/2022 4:40:32,436	from bus		Low	1.1.4	Movement/Presence Detector (D10)	2/1/1	New group address

#	Time	Service	Flags	Prio	Source A...	Source Name	Destinati...	Destination Name	Ho...	Type	DPT	Info	Iack
57	13/7/2022 4:34:3...	from bus		Low	1.1.4	Movement/Presence Detector (...	1/1/1	New group address	6	GroupValu...	1.001 s...	$01 | On	LL_...
70	13/7/2022 4:34:5...	from bus		Low	1.1.4	Movement/Presence Detector (...	1/1/1	New group address	6	GroupValu...	1.001 s...	$00 | Off	LL_...

Figura 14: Resultados monitoreo D10.1 controla a D7.1.
Fuente: El tesista

3. D9.1 controla a D7.1 – alarma de intrusión
   - D11.1 activa trigger (1) / remueve trigger para (0) D9.1 - alarma de intrusión
   - D11.2 activa trigger (1) D9.1 – reset de alarma de intrusión

#	Time	Service	Flags	Prio	Source A...	Source Name	Destinati...	Destination Name	Ho...	Type	DPT	Info	Iack
106	13/7/2022 4:35:5...	from bus		Low	1.1.5	Binary Input Module (D11)	1/1/4	New group address	6	GroupValu...	1.009 o...	$00 | Open	LL_...
107	13/7/2022 4:35:5...	from bus		Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...	$01 | Active	LL_...
108	13/7/2022 4:35:5...	from bus		Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...	$00 | Inactive	LL_...
109	13/7/2022 4:35:5...	from bus		Low	1.1.5	Binary Input Module (D11)	1/1/6	New group address	6	GroupValu...	1.015 r...	$01 | reset command (trigger)	LL_...
110	13/7/2022 4:36:0...	from bus		Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...	$00 | Inactive	LL_...

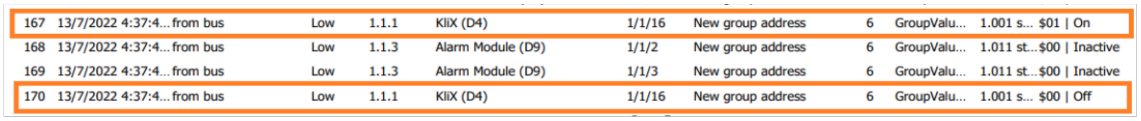
Figura 15: Resultados de monitoreo D9.1 control sobre D7.1.
Fuente: El tesista

4. D9.1 controla a D7.1 – alarma contra incendio
   - D11.3 activa trigger (1) / remueve trigger para (0) D9.1 - alarma contra incendio
   - D11.4 activa trigger (1) D9.1 - reset alarma contra incendio

151	13/7/2022 4:37:1...	from bus		Low	1.1.5	Binary Input Module (D11)	1/1/5	New group address	6	GroupValu...	1.009 o...	$00 | Open	LL_...
152	13/7/2022 4:37:1...	from bus		Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...	$00 | Inactive	LL_...
153	13/7/2022 4:37:1...	from bus		Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...	$01 | Active	LL_...
154	13/7/2022 4:37:1...	from bus		Low	1.1.5	Binary Input Module (D11)	1/1/7	New group address	6	GroupValu...	1.015 r...	$01 | reset command (trigger)	LL_...

Figura 16: Resultado de monitoreo de D9.1 controla a D7.1.
Fuente: El tesista

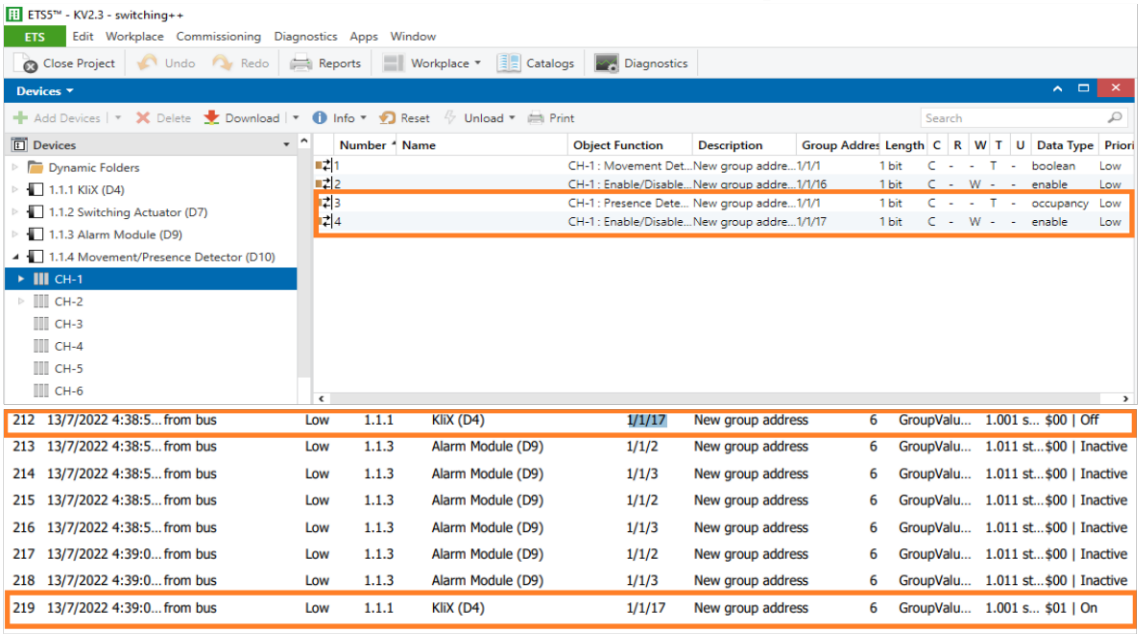
5. D4.2 deshabilita/habilita D10.1 (detección de movimiento)



167	13/7/2022 4:37:4...	from bus	Low	1.1.1	KliX (D4)	1/1/16	New group address	6	GroupValu...	1.001 s...	$01 | On
168	13/7/2022 4:37:4...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...	$00 | Inactive
169	13/7/2022 4:37:4...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...	$00 | Inactive
170	13/7/2022 4:37:4...	from bus	Low	1.1.1	KliX (D4)	1/1/16	New group address	6	GroupValu...	1.001 s...	$00 | Off

Figura 17: Resultado de monitoreo: D4.2 deshabilita/habilita D10.1.
Fuente: El tesista

6. D4.3 deshabilita/habilita D10.1 (detección de presencia)



212	13/7/2022 4:38:5...	from bus	Low	1.1.1	KliX (D4)	1/1/17	New group address	6	GroupValu...	1.001 s...	$00 | Off
213	13/7/2022 4:38:5...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...	$00 | Inactive
214	13/7/2022 4:38:5...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...	$00 | Inactive
215	13/7/2022 4:38:5...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...	$00 | Inactive
216	13/7/2022 4:38:5...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...	$00 | Inactive
217	13/7/2022 4:39:0...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...	$00 | Inactive
218	13/7/2022 4:39:0...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...	$00 | Inactive
219	13/7/2022 4:39:0...	from bus	Low	1.1.1	KliX (D4)	1/1/17	New group address	6	GroupValu...	1.001 s...	$01 | On

Figura 18: Resultado de monitoreo D4.3 deshabilita/habilita D10.1.
Fuente: El tesista

7. D4.4 deshabilita/habilita D11.1 y D11.2 (alarma de intrusión)

233	13/7/2022 4:39:2...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...$00 | Inactive
234	13/7/2022 4:39:3...	from bus	Low	1.1.1	KliX (D4)	1/1/40	New group address	6	GroupValu...	1.001 s... $00 | Off
235	13/7/2022 4:39:3...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...$00 | Inactive
236	13/7/2022 4:39:3...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...$00 | Inactive
237	13/7/2022 4:39:3...	from bus	Low	1.1.1	KliX (D4)	1/1/40	New group address	6	GroupValu...	1.001 s... $01 | On
238	13/7/2022 4:39:3...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...$00 | Inactive

Figura 19: Resultado de monitoreo D4.4 deshabilita/habilita D11.1 y D11.2.
Fuente: El tesista

8. D4.5 deshabilita/habilita D11.3 and D11.4 (alarma contra incendio)

243	13/7/2022 4:39:4...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...$00 | Inactive
244	13/7/2022 4:39:4...	from bus	Low	1.1.1	KliX (D4)	1/1/50	New group address	6	GroupValu...	1.001 s... $00 | Off
245	13/7/2022 4:39:4...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...$00 | Inactive
246	13/7/2022 4:39:4...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...$00 | Inactive
247	13/7/2022 4:39:5...	from bus	Low	1.1.1	KliX (D4)	1/1/50	New group address	6	GroupValu...	1.001 s... $01 | On
248	13/7/2022 4:39:5...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...$00 | Inactive

Figura 20: Resultado de monitoreo: D4.5 deshabilita/habilita D11.3 and D11.4.
Fuente: El tesista

9. D4.6 controla a D7.2

257	13/7/2022 4:40:0...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...$00 | Inactive
258	13/7/2022 4:40:0...	from bus	Low	1.1.1	KliX (D4)	2/1/1	New group address	6	GroupValu...	1.001 s... $01 | On
259	13/7/2022 4:40:0...	from bus	Low	1.1.1	KliX (D4)	2/1/1	New group address	6	GroupValu...	1.001 s... $00 | Off
260	13/7/2022 4:40:1...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...$00 | Inactive

Figura 21: Resultado de monitoreo: D4.6 controla a D7.2.
Fuente: El tesista

10. D10.2 controla a D7.2 - detección de movimiento

269	13/7/2022 4:40:2...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...$00 | Inactive
270	13/7/2022 4:40:2...	from bus	Low	1.1.4	Movement/Presence Detector (...	2/1/1	New group address	6	GroupValu...	1.001 s... $01 | On
271	13/7/2022 4:40:2...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...$00 | Inactive

Figura 22: Resultado de monitoreo: D10.2 controla a D7.2.
Fuente: El tesista

11. D4.7 deshabilita/habilita D10.2 (detección de movimiento)

291	13/7/2022 4:41:0...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...$00 | Inactive
292	13/7/2022 4:41:0...	from bus	Low	1.1.1	KliX (D4)	2/1/10	New group address	6	GroupValu...	1.001 s... $00 | Off
293	13/7/2022 4:41:0...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...$00 | Inactive
294	13/7/2022 4:41:0...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...$00 | Inactive
295	13/7/2022 4:41:1...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...$00 | Inactive
296	13/7/2022 4:41:1...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/3	New group address	6	GroupValu...	1.011 st...$00 | Inactive
297	13/7/2022 4:41:1...	from bus	Low	1.1.1	KliX (D4)	2/1/10	New group address	6	GroupValu...	1.001 s... $01 | On
298	13/7/2022 4:41:1...	from bus	Low	1.1.3	Alarm Module (D9)	1/1/2	New group address	6	GroupValu...	1.011 st...$00 | Inactive

Figura 23: Resultado de monitoreo: D4.7 deshabilita/habilita D10.2.
Fuente: El tesista

7.2.2 Resultados del escenario 2: Control de Persianas

1. D4.1 controla D2.1 (sin feedback)

#	Time	Service	Flags	Prio	Source A...	Source Name	Destinati...	Destination Name	Ho...	Type	DPT	Info
69	14/7/2022 8:28:1...	from bus		Low	1.1.1	KliX (D4)	1/1/1	New group address	6	GroupValue...	1.008 up/d...	$00 | Up
70	14/7/2022 8:28:1...	from bus		Low	1.1.1	KliX (D4)	1/1/2	New group address	6	GroupValue...	1.007 step	$00 | Decrease
71	14/7/2022 8:28:1...	from bus		Low	1.1.1	KliX (D4)	1/1/2	New group address	6	GroupValue...	1.007 step	$00 | Decrease

Figura 24: Resultado de monitoreo: D4.1 controla D2.1.
Fuente: El tesista

2. D4.2 controla D2.2 (sin feedback)

94	14/7/2022 8:28:2...	from bus		Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
95	14/7/2022 8:28:2...	from bus		Low	1.1.1	KliX (D4)	1/2/2	New group address	6	GroupValue...	1.007 step	$01 | Increase
96	14/7/2022 8:28:2...	from bus		Low	1.1.1	KliX (D4)	1/2/1	New group address	6	GroupValue...	1.008 up/d...	$01 | Down
97	14/7/2022 8:28:2...	from bus		Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm

Figura 25: Resultado de monitoreo: D4.2 controla D2.2.
Fuente: El tesista

3. D4.3 controla D2.3 (sin feedback)

141	14/7/2022 8:29:2...	from bus		Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
142	14/7/2022 8:29:2...	from bus		Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
143	14/7/2022 8:29:3...	from bus		Low	1.1.1	KliX (D4)	1/3/2	New group address	6	GroupValue...	1.007 step	$01 | Increase
144	14/7/2022 8:29:3...	from bus		Low	1.1.1	KliX (D4)	1/3/1	New group address	6	GroupValue...	1.008 up/d...	$01 | Down
145	14/7/2022 8:29:3...	from bus		Low	1.1.1	KliX (D4)	1/3/2	New group address	6	GroupValue...	1.007 step	$01 | Increase
146	14/7/2022 8:29:3...	from bus		Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm

Figura 26: Resultado de monitoreo: D4.3 controla D2.3.
Fuente: El tesista

4. D4.4 controla D2.4 (sin feedback)

191	14/7/2022 8:30:3...	from bus		Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
192	14/7/2022 8:30:3...	from bus		Low	1.1.1	KliX (D4)	1/4/2	New group address	6	GroupValue...	1.007 step	$01 | Increase
193	14/7/2022 8:30:3...	from bus		Low	1.1.1	KliX (D4)	1/4/1	New group address	6	GroupValue...	1.008 up/d...	$01 | Down
194	14/7/2022 8:30:3...	from bus		Low	1.1.1	KliX (D4)	1/4/2	New group address	6	GroupValue...	1.007 step	$01 | Increase
195	14/7/2022 8:30:3...	from bus		Low	1.1.1	KliX (D4)	1/4/2	New group address	6	GroupValue...	1.007 step	$01 | Increase

Figura 27: Resultado de monitoreo: D4.4 controla D2.4.
Fuente: El tesista

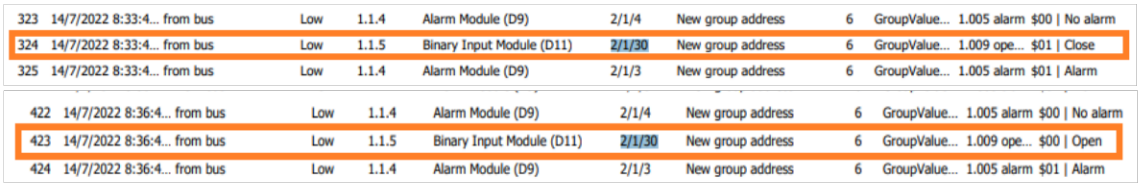
5. D4.5 controla D2.5 (sin feedback)

#	Time	Service	Flags	Prio	Source A...	Source Name	Destinati...	Destination Name	Ho...	Type	DPT	Info
307	14/7/2022 8:33:1...	from bus		Low	1.1.1	KliX (D4)	1/5/1	New group address	6	GroupValue...	1.008 up/d...	$00 | Up
308	14/7/2022 8:33:1...	from bus		Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm

Figura 28: Resultado de monitoreo: D4.5 controla D2.5.
Fuente: El tesista

6. D9.1 – control alarma de intrusión D2.4 y D2.5

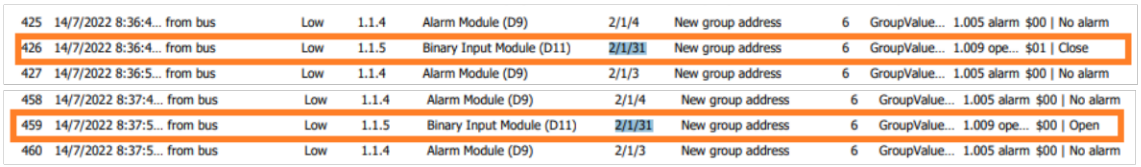
D11.1 configura la alarma de intrusión de D9.1, abre y cierra persianas



323	14/7/2022 8:33:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
324	14/7/2022 8:33:4...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/30	New group address	6	GroupValue...	1.009 ope... $01 | Close
325	14/7/2022 8:33:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $01 | Alarm
422	14/7/2022 8:36:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
423	14/7/2022 8:36:4...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/30	New group address	6	GroupValue...	1.009 ope... $00 | Open
424	14/7/2022 8:36:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $01 | Alarm

Figura 29: Resultado de monitoreo: D9.1 – control alarma de intrusión D2.4 y D2.5.
Fuente: El tesista

7. D11.2 reset de alarma de intrusión de D9.1

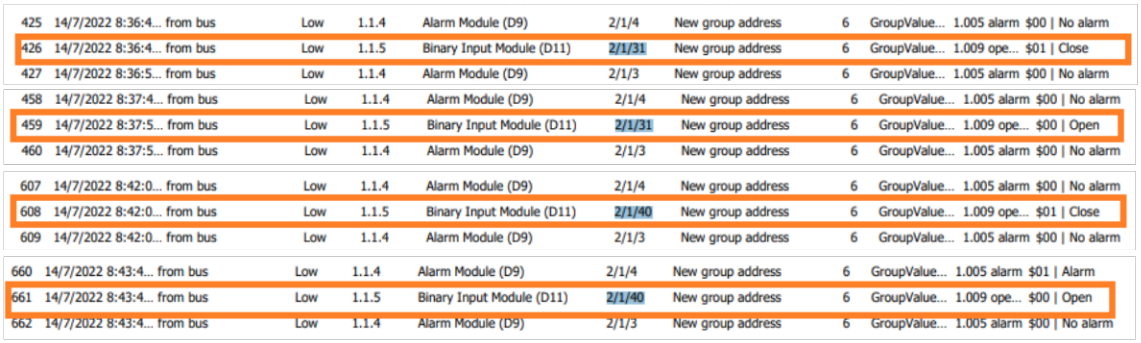


425	14/7/2022 8:36:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
426	14/7/2022 8:36:4...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/31	New group address	6	GroupValue...	1.009 ope... $01 | Close
427	14/7/2022 8:36:5...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
458	14/7/2022 8:37:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
459	14/7/2022 8:37:5...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/31	New group address	6	GroupValue...	1.009 ope... $00 | Open
460	14/7/2022 8:37:5...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $00 | No alarm

Figura 30: Resultado de monitoreo: D11.2 reset de alarma de intrusión de D9.1.
Fuente: El tesista

8. D11.3 – control de alarma de incendio D2.5

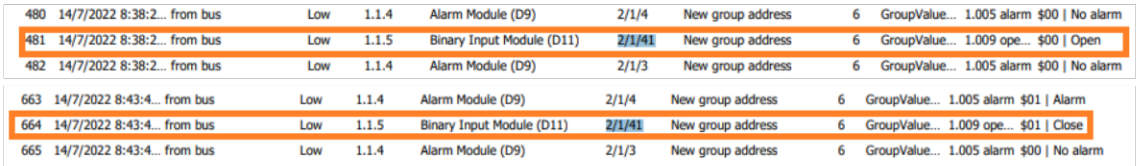
D11.3 configura la alarma de incendio de D9.1, y cierra persianas



425	14/7/2022 8:36:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
426	14/7/2022 8:36:4...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/31	New group address	6	GroupValue...	1.009 ope... $01 | Close
427	14/7/2022 8:36:5...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
458	14/7/2022 8:37:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
459	14/7/2022 8:37:5...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/31	New group address	6	GroupValue...	1.009 ope... $00 | Open
460	14/7/2022 8:37:5...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
607	14/7/2022 8:42:0...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
608	14/7/2022 8:42:0...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/40	New group address	6	GroupValue...	1.009 ope... $01 | Close
609	14/7/2022 8:42:0...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
660	14/7/2022 8:43:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $01 | Alarm
661	14/7/2022 8:43:4...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/40	New group address	6	GroupValue...	1.009 ope... $00 | Open
662	14/7/2022 8:43:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $00 | No alarm

Figura 31: Resultado de monitoreo: D11.3 – control de alarma de incendio D2.5.
Fuente: El tesista

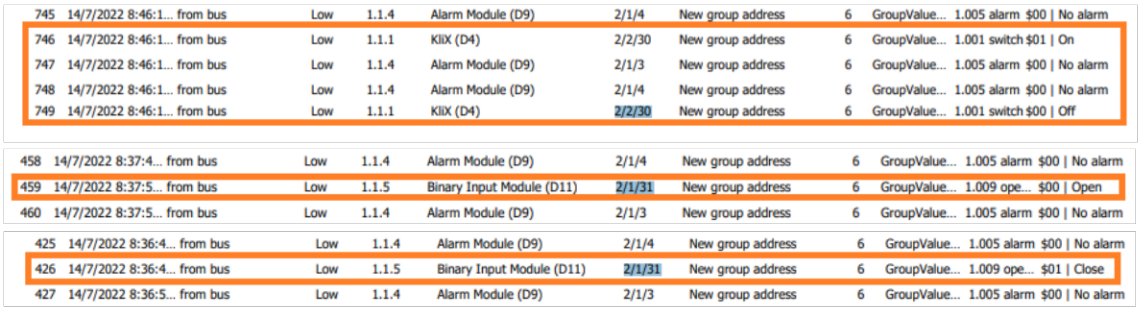
9. D11.4 resetea la alarma contra incendio de D9.1



480	14/7/2022 8:38:2...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
481	14/7/2022 8:38:2...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/41	New group address	6	GroupValue...	1.009 ope... $00 | Open
482	14/7/2022 8:38:2...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $00 | No alarm
663	14/7/2022 8:43:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm $01 | Alarm
664	14/7/2022 8:43:4...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/41	New group address	6	GroupValue...	1.009 ope... $01 | Close
665	14/7/2022 8:43:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm $00 | No alarm

Figura 32: Resultado de monitoreo: D11.4 resetea la alarma contra incendio de D9.1.
Fuente: El tesista

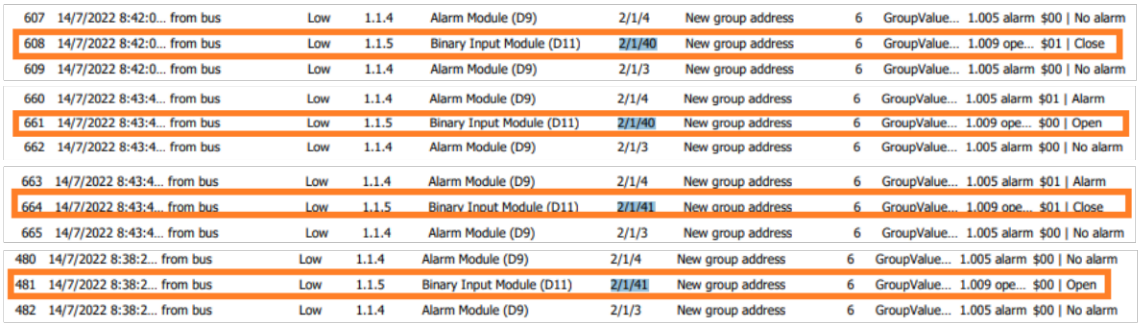
10. D4.6 habilita/deshabilita D11.1 y D11.2



745	14/7/2022 8:46:1...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
746	14/7/2022 8:46:1...	from bus	Low	1.1.1	KliX (D4)	2/2/30	New group address	6	GroupValue...	1.001 switch	$01 | On
747	14/7/2022 8:46:1...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
748	14/7/2022 8:46:1...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
749	14/7/2022 8:46:1...	from bus	Low	1.1.1	KliX (D4)	2/2/30	New group address	6	GroupValue...	1.001 switch	$00 | Off
458	14/7/2022 8:37:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
459	14/7/2022 8:37:5...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/31	New group address	6	GroupValue...	1.009 ope...	$00 | Open
460	14/7/2022 8:37:5...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
425	14/7/2022 8:36:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
426	14/7/2022 8:36:4...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/31	New group address	6	GroupValue...	1.009 ope...	$01 | Close
427	14/7/2022 8:36:5...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm

Figura 33: Resultado de monitoreo: D4.6 habilita/deshabilita D11.1 y D11.2.
Fuente: El tesista

11. D4.7 habilita/deshabilita D11.3 and D11.4

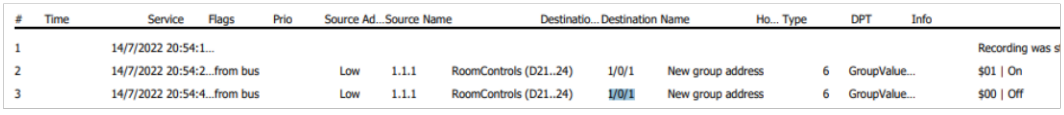


607	14/7/2022 8:42:0...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
608	14/7/2022 8:42:0...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/40	New group address	6	GroupValue...	1.009 ope...	$01 | Close
609	14/7/2022 8:42:0...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
660	14/7/2022 8:43:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$01 | Alarm
661	14/7/2022 8:43:4...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/40	New group address	6	GroupValue...	1.009 ope...	$00 | Open
662	14/7/2022 8:43:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
663	14/7/2022 8:43:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$01 | Alarm
664	14/7/2022 8:43:4...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/41	New group address	6	GroupValue...	1.009 ope...	$01 | Close
665	14/7/2022 8:43:4...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
480	14/7/2022 8:38:2...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/4	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm
481	14/7/2022 8:38:2...	from bus	Low	1.1.5	Binary Input Module (D11)	2/1/41	New group address	6	GroupValue...	1.009 ope...	$00 | Open
482	14/7/2022 8:38:2...	from bus	Low	1.1.4	Alarm Module (D9)	2/1/3	New group address	6	GroupValue...	1.005 alarm	$00 | No alarm

Figura 34: Resultado de monitoreo: D4.7 habilita/deshabilita D11.3 and D11.4.
Fuente: El tesista

7.2.3 Resultados del escenario 3: Control en 2 habitaciones

1. **Room21**
    1. **D21.1 controla D7.1**



#	Time	Service	Flags	Prio	Source Ad...	Source Name	Destinatio...	Destination Name	Ho...	Type	DPT	Info
1		14/7/2022 20:54:1...										Recording was s
2		14/7/2022 20:54:2...	from bus	Low	1.1.1	RoomControls (D21..24)	1/0/1	New group address	6	GroupValue...		$01 | On
3		14/7/2022 20:54:4...	from bus	Low	1.1.1	RoomControls (D21..24)	1/0/1	New group address	6	GroupValue...		$00 | Off

Figura 35: Resultado de monitoreo: D21.1 controla D7.1.
Fuente: El tesista

2. D21.2 controla D7.2

4		14/7/2022 20:54:5...	from bus	Low	1.1.1	RoomControls (D21..24)	1/0/2	New group address	6	GroupValue...	$01 | On
5		14/7/2022 20:55:0...	from bus	Low	1.1.1	RoomControls (D21..24)	1/0/2	New group address	6	GroupValue...	$00 | Off

Figura 36: Resultado de monitoreo: D21.2 controla D7.2.
Fuente: El tesista

3. D21.5 controla D2.1

6	14/7/2022 20:55:1...from bus	Low	1.1.1	RoomControls (D21..24)	4/1/1	New group address	6	GroupValue...	$01 | Down
7	14/7/2022 20:55:1...from bus	Low	1.1.1	RoomControls (D21..24)	4/1/2	New group address	6	GroupValue...	$01 | Increase
8	14/7/2022 20:55:1...from bus	Low	1.1.1	RoomControls (D21..24)	4/1/1	New group address	6	GroupValue...	$01 | Down
9	14/7/2022 20:55:3...from bus	Low	1.1.1	RoomControls (D21..24)	4/1/1	New group address	6	GroupValue...	$00 | Up

Figura 37: Resultado de monitoreo: D21.5 controla D2.1.
Fuente: El tesista

4. D10.1 controla D7.1 – detección de presencia

10	14/7/2022 20:56:0...from bus	Low	1.1.9	Movement/Presence Detecto...	1/0/1	New group address	6	GroupValue...	$01 | On
11	14/7/2022 20:56:2...from bus	Low	1.1.9	Movement/Presence Detecto...	1/0/1	New group address	6	GroupValue...	$00 | Off

Figura 38: Resultado de monitoreo: D10.1 controla D7.1.
Fuente: El tesista

2. Room22

1. D22.1 controla D7.3

12	14/7/2022 20:56:3...from bus	Low	1.1.2	RoomControls (D21..24)	1/0/3	New group address	6	GroupValue...	$01 | On
13	14/7/2022 20:56:4...from bus	Low	1.1.2	RoomControls (D21..24)	1/0/3	New group address	6	GroupValue...	$00 | Off

Figura 39: Resultado de monitoreo: D22.1 controla D7.3.
Fuente: El tesista

2. D22.2 controla D7.4

14	14/7/2022 20:56:4...from bus	Low	1.1.2	RoomControls (D21..24)	1/0/4	New group address	6	GroupValue...	$01 | On
15	14/7/2022 20:57:0...from bus	Low	1.1.2	RoomControls (D21..24)	1/0/4	New group address	6	GroupValue...	$00 | Off

Figura 40: Resultado de monitoreo: D22.2 controla D7.4.
Fuente: El tesista

3. D22.5 controla D2.2

18	14/7/2022 20:57:1...from bus	Low	1.1.2	RoomControls (D21..24)	4/2/1	New group address	6	GroupValue...	$01 | Down
19	14/7/2022 20:57:1...from bus	Low	1.1.2	RoomControls (D21..24)	4/2/1	New group address	6	GroupValue...	$01 | Down
20	14/7/2022 20:57:4...from bus	Low	1.1.2	RoomControls (D21..24)	4/2/1	New group address	6	GroupValue...	$00 | Up

Figura 41: Resultado de monitoreo: D22.5 controla D2.2.
Fuente: El tesista

4. D10.2 controla a D7.2 – detección de presencia

4	14/7/2022 20:54:5...from bus	Low	1.1.1	RoomControls (D21..24)	1/0/2	New group address	6	GroupValue...	$01 | On
5	14/7/2022 20:55:0...from bus	Low	1.1.1	RoomControls (D21..24)	1/0/2	New group address	6	GroupValue...	$00 | Off
6	14/7/2022 20:55:1...from bus	Low	1.1.1	RoomControls (D21..24)	4/1/1	New group address	6	GroupValue...	$01 | Down
7	14/7/2022 20:55:1...from bus	Low	1.1.1	RoomControls (D21..24)	4/1/2	New group address	6	GroupValue...	$01 | Increase
8	14/7/2022 20:55:1...from bus	Low	1.1.1	RoomControls (D21..24)	4/1/1	New group address	6	GroupValue...	$01 | Down
9	14/7/2022 20:55:3...from bus	Low	1.1.1	RoomControls (D21..24)	4/1/1	New group address	6	GroupValue...	$00 | Up
10	14/7/2022 20:56:0...from bus	Low	1.1.9	Movement/Presence Detecto...	1/0/1	New group address	6	GroupValue...	$01 | On
11	14/7/2022 20:56:2...from bus	Low	1.1.9	Movement/Presence Detecto...	1/0/1	New group address	6	GroupValue...	$00 | Off
12	14/7/2022 20:56:3...from bus	Low	1.1.2	RoomControls (D21..24)	1/0/3	New group address	6	GroupValue...	$01 | On
13	14/7/2022 20:56:4...from bus	Low	1.1.2	RoomControls (D21..24)	1/0/3	New group address	6	GroupValue...	$00 | Off
14	14/7/2022 20:56:4...from bus	Low	1.1.2	RoomControls (D21..24)	1/0/4	New group address	6	GroupValue...	$01 | On
15	14/7/2022 20:57:0...from bus	Low	1.1.2	RoomControls (D21..24)	1/0/4	New group address	6	GroupValue...	$00 | Off
16	14/7/2022 20:57:1...from bus	Low	1.1.2	RoomControls (D21..24)	4/2/2	New group address	6	GroupValue...	$01 | Increase
17	14/7/2022 20:57:1...from bus	Low	1.1.2	RoomControls (D21..24)	4/2/2	New group address	6	GroupValue...	$01 | Increase
18	14/7/2022 20:57:1...from bus	Low	1.1.2	RoomControls (D21..24)	4/2/1	New group address	6	GroupValue...	$01 | Down
19	14/7/2022 20:57:1...from bus	Low	1.1.2	RoomControls (D21..24)	4/2/1	New group address	6	GroupValue...	$01 | Down
20	14/7/2022 20:57:4...from bus	Low	1.1.2	RoomControls (D21..24)	4/2/1	New group address	6	GroupValue...	$00 | Up
21	14/7/2022 20:57:5...from bus	Low	1.1.9	Movement/Presence Detecto...	1/0/3	New group address	6	GroupValue...	$01 | On
22	14/7/2022 20:58:3...								Recording was stopped

Figura 42: Resultado de monitoreo: D10.2 controla a D7.2.
Fuente: El tesista

7.3 RESULTADOS DE LA ENCUESTA

En Anexo 4 se explica la tabulación de datos por cada pregunta, y en Anexo 5 la encuesta. La Figura 43 muestra los resultados de la encuesta en base a 10 preguntas realizada a 8 expertos, con el 27% está totalmente satisfecho, 61% de encuestados están muy satisfechos con el trabajo investigativo, el 10% está parcialmente satisfecho y el 1% está poco satisfecho y el 1% insatisfecho.

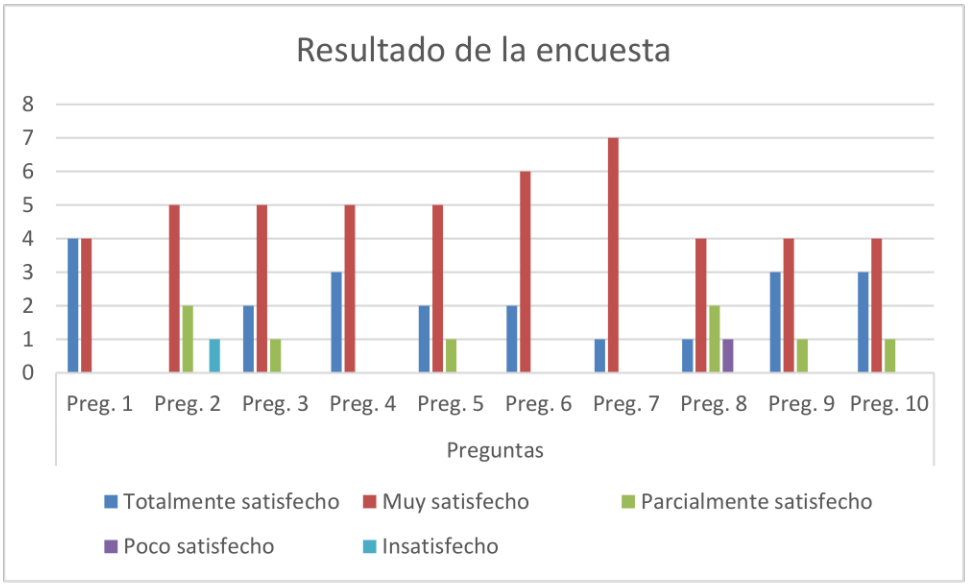


Figura 43: Resultados de la encuesta.
Fuente: El tesista

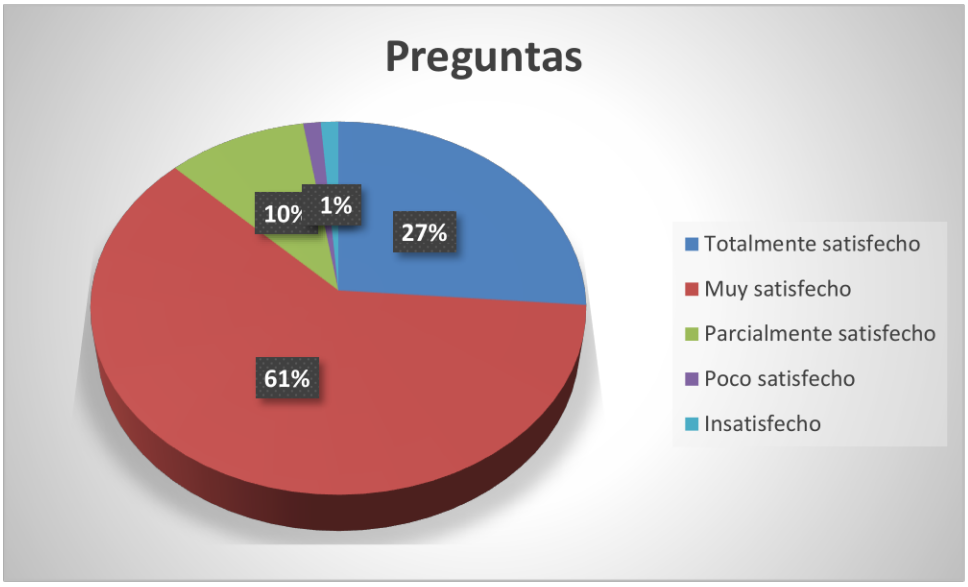


Figura 44: Resultados de la encuesta.
Fuente: El tesista

A continuación, se muestran los resultados de la encuesta basada en 10 preguntas, realizada a 8 expertos, que se encuentra adjunta en Anexo 1.

7.4 COMPROBACIÓN DE HIPÓTESIS

La hipótesis será comprobada de acuerdo a los resultados de la encuesta realizada a los 8 expertos utilizando el método ANOVA. los indicadores antes y después de la implementación del sistema domótico, con una ponderación:

- Totalmente satisfecho: 0.5
- Muy satisfecho: 0.4
- Parcialmente satisfecho: 0.3
- Poco satisfecho: 0.2
- Insatisfecho: 0.1

7.4.1 Indicador 1: Niveles de calidad de señal alámbrica e inalámbrica.

Valoración antes de propuesta: 3.2

Este indicador se considera con un valor de 3.2 antes de la propuesta, ya que la señal alámbrica e inalámbrica en el tercer piso es totalmente funcional.

Valoración aplicando la propuesta: 3.3

Este indicador se considera con un valor de 3.3 luego de aplicada la propuesta, como resultado de la encuesta a expertos.

7.4.2 Indicador 2: % de ahorro en el presupuesto de cables y equipos KNX.

Valoración antes de propuesta: 4

Este indicador se considera con un valor de 4 antes de la propuesta, ya que el presupuesto de cables y equipos es menor al utilizado con la implementación de KNX.

Valoración aplicando la propuesta: 3.4

Este indicador se considera con un valor de 3.4 luego de aplicada la propuesta, como resultado de la encuesta a expertos.

7.4.3 Indicador 3: % de intrusiones detectadas por el sistema.

Valoración antes de propuesta: 3

Este indicador se considera con un valor de 3 antes de la propuesta, ya que dispone de un sistema de control de intrusión a nivel del campus donde se encuentra el edificio de ingeniería, mas no en el tercer piso del edificio.

Valoración aplicando la propuesta: 3.3

Este indicador se considera con un valor de 3.3 luego de aplicada la propuesta, como resultado de la encuesta a expertos.

7.4.4 Indicador 4: Número de habitaciones con elementos de domótica implementados.

Valoración antes de propuesta: 2.6

Este indicador se considera con un valor de 2.6 antes de la propuesta, ya que se reutilizarán los equipos actuales para migrar a un sistema KNX.

Valoración aplicando la propuesta: 2.9

Este indicador se considera con un valor de 3.3 luego de aplicada la propuesta, como resultado de la encuesta a expertos.

7.4.5 Indicador 5: Número Incidentes detectados vs número de incidentes controlados por el sistema.

Valoración antes de propuesta: 3

Este indicador se considera con un valor de 0 antes de la propuesta, ya que al existir incidentes en la red no fueron detectados estos.

Valoración aplicando la propuesta: 3.4

Este indicador se considera con un valor de 3.3 luego de aplicada la propuesta, como resultado de la encuesta a expertos.

7.4.6 Indicador 6: Nivel de confiabilidad del diseño, configuración y programación de equipos virtuales de la red de seguridad.

Valoración antes de propuesta: 3

Este indicador se considera con un valor de 3 antes de la propuesta, ya que se considera confiable el funcionamiento de la red actual.

Valoración aplicando la propuesta: 3.4

Este indicador se considera con un valor de 3.4 luego de aplicada la propuesta, como resultado de la encuesta a expertos.

7.4.7 Tratamiento estadístico ANOVA y Dictamen

La Tabla 11, muestra los indicadores antes y después de la implementación del sistema domótico, con una ponderación:

- Totalmente satisfecho: 0.5
- Muy satisfecho: 0.4
- Parcialmente satisfecho: 0.3
- Poco satisfecho: 0.2
- Insatisfecho: 0.1

La Tabla 12 indica el análisis de varianza de dos factores con una sola muestra por grupo para cada indicador de la Tabla 13 y Figura 146 se evidencia el valor de F (5.06) es menor al valor critico de F (5,11) lo que **VALIDA LA HIPÓTESIS** *"El diseño de un sistema domótico basado en la tecnología EIB KONNEX mejorará la gestión de la seguridad del edificio de Ingeniería".*

MUESTRAS	*Pregunta 1*	*Pregunta 2*	*Pregunta 3*	*Pregunta 4*	*Pregunta 5*	*Pregunta 6*	*Pregunta 7*	*Pregunta 8*	*Pregunta 9*	*Pregunta 10*
Antes de aplicar la solución	2.5	2	2	3.2	3.2	4	3	2.6	3	0
Luego de implementar	3.6	3.1	3.3	3.5	3.3	3.4	3.3	2.9	3.4	3.4

Tabla 11: Tabla de muestras de indicadores antes y después de la implementación.
Fuente: El tesista

RESUMEN	*Cuenta*	*Suma*	*Promedio*	*Varianza*
Antes de aplicar la solución	10	25.5	2.55	1.16277778
Luego de implementar	10	33.2	3.32	0.03955556
Pregunta 1	2	6.1	3.05	0.605
Pregunta 2	2	5.1	2.55	0.605
Pregunta 3	2	5.3	2.65	0.845
Pregunta 4	2	6.7	3.35	0.045
Pregunta 5	2	6.5	3.25	0.005
Pregunta 6	2	7.4	3.7	0.18
Pregunta 7	2	6.3	3.15	0.045
Pregunta 8	2	5.5	2.75	0.045
Pregunta 9	2	6.4	3.2	0.08
Pregunta 10	2	3.4	1.7	5.78

Tabla 12: Análisis de varianza de dos factores con una sola muestra por grupo.
Fuente: El tesista

ANÁLISIS DE VARIANZA

Origen de las variaciones	*Suma de cuadrados*	*Grados de libertad*	*Promedio de los cuadrados*	*F*	*Probabilidad*	*Valor crítico para F*
Filas	2.9645	1	2.9645	5.06223318	0.0510082	5.11735503
Columnas	5.5505	9	0.61672222	1.05312589	0.4699016	3.1788931
Error	5.2705	9	0.58561111			
Total	13.7855	19				

Tabla 13: Análisis de varianza.
Fuente: El tesista

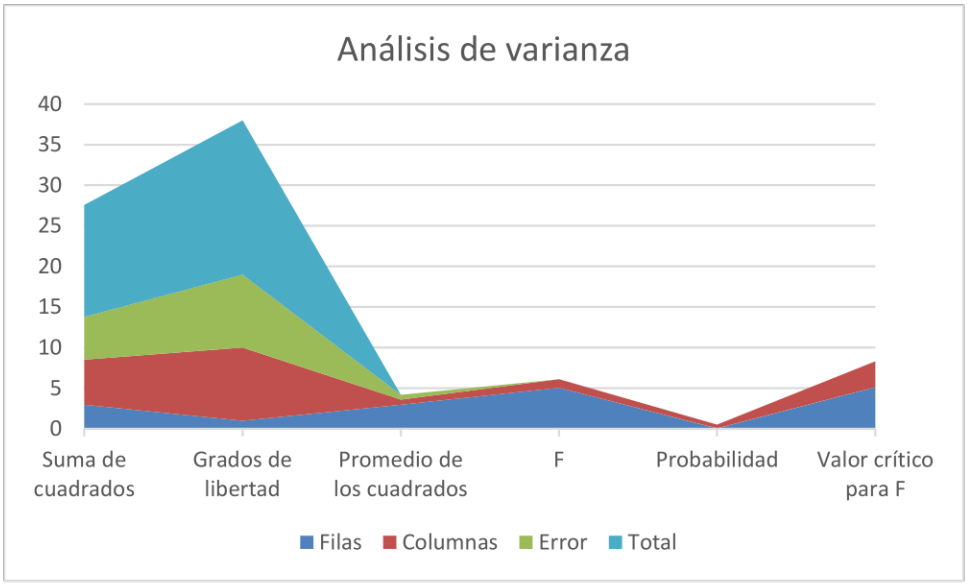


Figura 45: Análisis de varianza.
Fuente: El tesista

8. CAPÍTULO VIII. CONCLUSIONES Y RECOMENDACIONES

8.1 CONCLUSIONES

El fundamento teórico sobre la Tecnología EIB KONNEX permitió conocer las bases teóricas sobre esta tecnología previo al diseño y simulación de la red domótica.

Para la simulación se basó en tres escenarios, el primer escenario de conmutación demostró el uso de pulsadores, actuadores de conmutación, módulos de alarma, detector de movimiento y entrada binaria; este escenario permito el control de iluminación sin retroalimentación, detección de movimiento + detección de presencia, alarma de intrusión, alarma contra incendio. El segundo escenario referente al control de persianas utilizo un actuador de persianas, pulsador, módulo de alarma y entrada binaria: este escenario permitió el control de alarma de intrusión, alarma contra incendio, apertura y cierre de persianas. El tercer escenario el control de dos habitaciones utilizo actuadores de persianas, actuadores de conmutación, detector de movimiento y presencia, y pulsadores; para control de iluminación, control de persianas y presencia.

El capítulo de resultados de simulación, indica las tramas capturadas en el bus de datos, en todos los casos la comunicación fue exitosa, ya que no existen banderas (flags) que indiquen error de transmisión o error de trama.

Para el diseño de la red domótica se realizó un diagnóstico de la situación actual de red del tercer piso de la Facultad de Ingeniería de la UNACH, en base a ello se procedió a evaluar la topología de la red. El diseño de la red domótica se basó en las normas en el cumplimiento de la norma ISO/IEC 14543, lo que permitirá una recuperación de la inversión en relación al presupuesto inicial de cables y equipos. El diseño permitirá un adecuado control del tercer piso en lo relacionado a los diferentes sistemas de seguridad, para lo cual se ha diseñado en base a zonas, para un adecuado monitoreo.
Existen 174 puertos vulnerables no detectados en la red implementada, usando el protocolo tcp, con los servicios tcpwrapped y msrpc. Tcpwrapped protege a los programas no a los puertos, indicando que un servicio de red disponible pero no está en la lista de host autorizados para comunicarse. Msrpc representa el servicio de la conexión remota al escritorio del pc que se está realizando el monitoreo.

En el capítulo de resultados, de acuerdo a la tabulación del juicio de expertos, se concluye que el sistema simulado y diseñado, basado en tecnología KNX es *muy satisfactorio*, y que en un futuro se podría dotar de seguridad de acceso-intrusión e inundación, sistema de cámaras, sistema contra incendios; los mismos que podrá ser monitoreados desde el cuarto de equipos o de forma remota. Por otro lado, basado en el juicio de expertos se demuestra que la hipótesis es verdadera utilizando el método estadístico ANOVA, confirmando que el trabajo de investigación propuesto como valido.

8.2 RECOMENDACIONES

Se recomienda usar la versión no demo del software KNX Virtual, para aprovechar todas las funcionalidades y poder simular todo el diseño, con la finalidad de verificar la validez del diseño antes de implementarlo.

Se sugiere reestructurar la red e incluir algún servidor para monitorear la red, e instalar algún software para monitoreo; además se sugiere realizar un bosquejo de la topología de la red, y una lista de los equipos de la red. Como también implementar los sistemas de seguridad de presencia, intrusión, incendio e inundación.

En lo relacionado al diseño de la red domótica, se recomienda verificar la arquitectura de cada sistema de seguridad antes de proceder con el diseño, ya que, dependiendo de la arquitectura de cada sistema, podría abaratar o incrementar los costos. En este sentido se recomienda que los dispositivos del sistema de seguridad sean direccionables, es decir, dispongan de una dirección IP para su respectivo monitoreo.

Se recomienda tomar este estudio como punto de partida para la implementación de un sistema automatizado para el edificio de ingeniería basado en KNX, para lo cual se entregará los diseños previos a las autoridades de la facultad para su consideración.

BIBLIOGRAFIA

Aguilar, A., Tuch, S., Bello, M., Reyes, J., & Ramirez, L. (2018). Interpretation and Emulation for Telegrams of the KNX Standard on MATLAB Simulink. International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE). 129-133.

Baldeón D., & Congacha, M. (2014). Estudio y diseño de un sistema domótico aplicado en el edificio de laboratorios para la facultad de Mecánica (Tesis de grado).

Cash, M., Morales, C., Wang, S., Jin, X., Parlato, A., Sun, Q. Z., & Fu, X. (2022). On False Data Injection Attack against Building Automation Systems. arXiv preprint arXiv:2208.02733.

Ciholas, P., Lennie, A., Sadigova, P., & Such, J. (2019). The security of smart buildings: a systematic literature review. arXiv preprint arXiv:1901.05837.

Dweik, W., Abdalla, M., AlHroob, Y., AlMajali, A., Mustafa, S. A., & Abdel-Majeed, M. (2022). Skeleton of Implementing Voice Control for Building Automation Systems. Scientific Programming.

Gandhi, C., Suri, G., Golyan, R. P., Saxena, P., & Saxena, B. K. (2014). Packet sniffer–a comparative study. International Journal of Computer Networks and Communications Security, 2(5), 179-187.

Garlik, B. (2022). Energy Centers in a Smart City as a Platform for the Application of Artificial Intelligence and the Internet of Things. Applied Sciences, 12(7), 3386.

Goltz, J. (2020). Investigating the Filter Capacity of Line couplers in KNX regarding network security. IEEE. 426-432.

Goltz, J. (2021). Securing Building Automation Systems. 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS). 1-7. doi: 10.1109/NTMS49979.2021.9432650.

Goltz, J. (2020). Investigating the Filter Capacity of Line couplers in KNX regarding network security. International Wireless Communications and Mobile Computing (IWCMC). 426-432.

Graveto, V., Cruz, T., & Simöes, P. (2022). Security of Building Automation and Control Systems: Survey and future research directions, Computers & Security, Vol 112, 102527.

González-Muñoz, Y., Palomino-Camargo, C., Pérez-Sira, E., & Aguilar, V. H. (2018). Aplicaciones Y Tendencias Futuras De La Consulta De Expertos En El Sector De Los Alimentos: Generalidades De La Metodología Delphi Applications And Future Trends Of The Consultation Of Experts In The Food Sector. Actualización en nutrición, 19(2), 55-68.

Himeur, Y., Elnour, M., Fadli, F., Meskin, N., Petri, I., Rezgui, Y., ... & Amira, A. (2022). AI-big data analytics for building automation and management systems: a survey, actual challenges and future perspectives. Artificial Intelligence Review, 1-93.

Ivanov, H., Bekhrad, P., & Leitgeb, E. (2022). Power Line Communication for Building Automation Using Visible Light Sensing Systems. In 2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP). 1-4.

Kortetjärvi, F., & Khorami, R. (2021). Software development of visualization system (Tesis de grado).

Lechner, D., Granzer, W., & Kastner, W. (2008). Security for knxnet/IP. In Konnex Scientific Conference.

Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., ... & O'Neill, Z. (2022). A critical review of cyber-physical security for building automation systems. arXiv preprint arXiv:2210.11726.

Lourdas, V. (Mayo 2020). KNX IP Secure - KNX Association. Obtenido: junio 24 2022, https://support.knx.org/hc/en-us/articles/360012666599-KNX-IP-Secure

Majdi, A., Alrubaie, A. J., Al-Wardy, A. H., Baili, J., & Panchal, H. (2022). A novel method for Indoor Air Quality Control of Smart Homes using a Machine learning model. Advances in Engineering Software, 173, 103253.

Mori Rojas, A. (2022). Sistema de monitoreo de infraestructura de TI y su influencia en la gestión de incidencias en la red LAN de la empresa Electro Oriente SA–Unidad de Negocios Bellavista (Tesis de Grado).

Merz, H., Hansemann, T., & Hübner, C. (2019). Building Automation: Communication Systems with EIB/KNX, LON and BACnet. SPRINGER

Mundt, T., Wiedenmann, S., Goltz, J., Bauer, J., & Jung, M. (2019). Detecting Intrusive Behaviour of People in a Building through Data Analysis and Anomaly Detection in Home Automation Systems. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security.

Paredes Burnham, D. (2016). Diseño de la red inmótica del nuevo edificio de la Facultad de Ciencias de la Educación de la Universidad Nacional de Chimborazo (UNACH).

Ruta, M., Scioscia, F., Loseto, G., & Di Sciascio, E. (2017). KNX: A Worldwide Standard Protocol for Home and Building Automation: State of the Art and Perspectives. Industrial Communication Technology Handbook, 58-1.

Shehata, M., Eberlein, A., & Fapojuwo, A. (2007, July). Managing policy interactions in KNX-based smart homes. In 31st Annual International Computer Software and Applications Conference (COMPSAC 2007) (Vol. 2, pp. 367-378). IEEE.

Thirupathi, L., Rajesh, A., Sandeep, R. (2023). Internet of Lighting for Smart Cities. OWT 2021. Lecture Notes in Electrical Engineering, vol 892. Springer, Singapore.

Upendra, S., Mahendra, S., & Rao, P. S. (2017). Two-way ANOVA calculations using MS-Excel. Research Journal of Science and Technology, 9(4), 532-536.

Vacherot, C. (2020). Sneak into buildings with KNXnet/IP. In Sneak into buildings with KNXnet/IP.

Vanus, J., Martinek, R., Danys, L., Nedoma, J., & Bilik, P. (2022). Occupancy Detection in Smart Home Space Using Interoperable Building Automation Technologies. Human-Centric Computing And Information Sciences, 12.

Zdziarstek, A., Brekenfelder, W., Eibisch, F. (2020). Using the Physical Layer to Detect Attacks on Building Automation Networks. Security and Privacy in Communication Networks. Secure Comm 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 336. Springer.

9. ANEXOS

9.1 ANEXO 1

Escenario 1: Conmutación

Dispositivos requeridos:

D4: pulsador
D7: actuador de conmutación
D9: módulo de alarma
D10: detector de movimiento y presencia
D11: Entrada binaria

Funciones de construcción:

1. D4.1 controla a D7.1 (sin realimentación)
2. D10.1 controla a D7.1: detección de movimiento + detección de presencia
3. D9.1 controla a D7.1 – alarma de intrusión
   - D11.1 activa trigger (1) / remueve trigger para (0) D9.1 - alarma de intrusión
   - D11.2 activa trigger (1) D9.1 – reset de alarma de intrusión
4. D9.1 controla a D7.1 – alarma contra incendio
   - D11.3 activa trigger (1) / remueve trigger para (0) D9.1 - alarma contra incendio
   - D11.4 activa trigger (1) D9.1 - reset alarma contra incendio
5. D4.2 deshabilita/habilita D10.1 (detección de movimiento)
6. D4.3 deshabilita/habilita D10.1 (detección de presencia)
7. D4.4 deshabilita/habilita D11.1 and D11.2 (alarma de intrusión)
8. D4.5 deshabilita/habilita D11.3 and D11.4 (alarma contra incendio)
9. D4.6 controla a D7.2
10. D10.2 controla a D7.2 - detección de movimiento
11. D4.7 deshabilita /habilita D10.2 (detección de movimiento)

La Figura 46 muestra el panel de ETS 5 al finalizar la programación del escenario de conmutación y empezar el monitoreo de la simulación, mientras que la Figura 47 muestra los dispositivos de conmutación simulados que son monitoreados en la Figura 46.

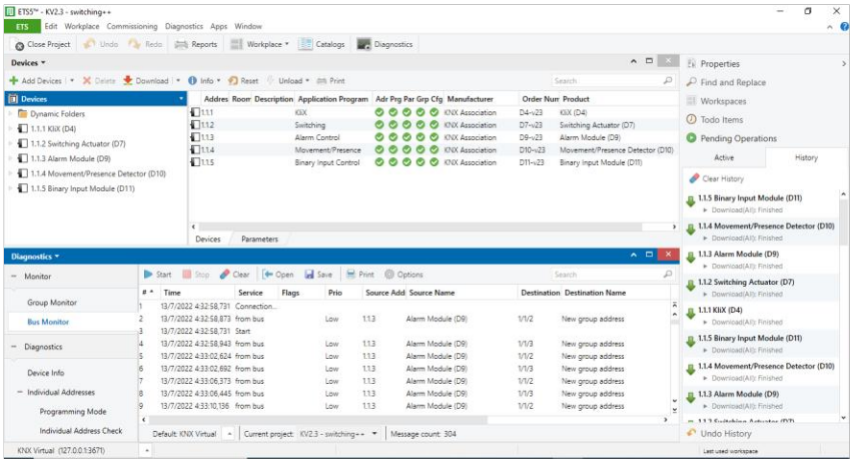


Figura 46: Panel de ETS 5.
Fuente: El tesista

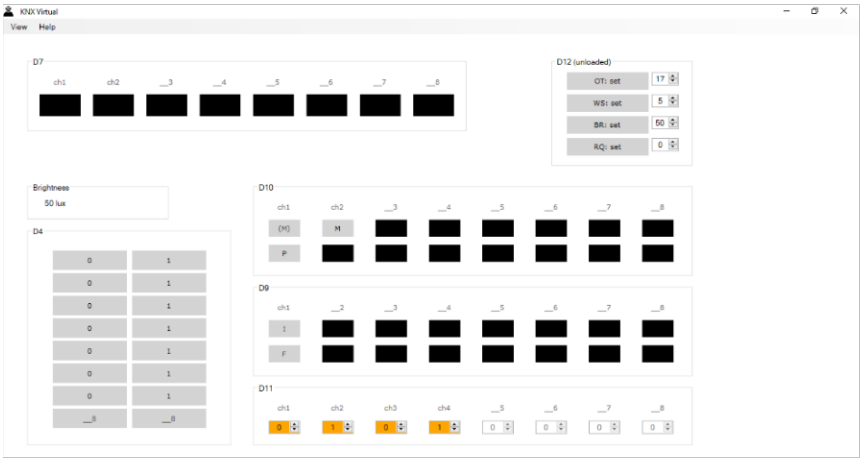


Figura 47: KNX Virtual – Escenario de conmutación.
Fuente: El tesista

Monitoreo

La Figura 48 muestra el control de la lampara D7.1 sin retroalimentación por medio del interruptor pulsador D4.1, ch1 está en ON.

1. **D4.1 controla a D7.1 (sin realimentación)**

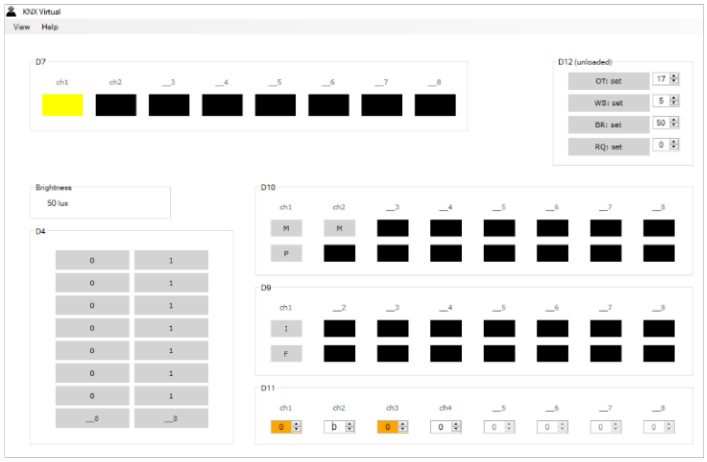


Figura 48: KNX Virtual – D4.1 controla a D7.1.
Fuente: El tesista

2. **D10.1 controla a D7.1: detección de movimiento**

La Figura 49 muestra el control de detección de movimiento (D10.1 - ch1 está en ON), donde la lampara D7.1 se activa (ch1 está en ON) por medio del interruptor pulsador D10.1.

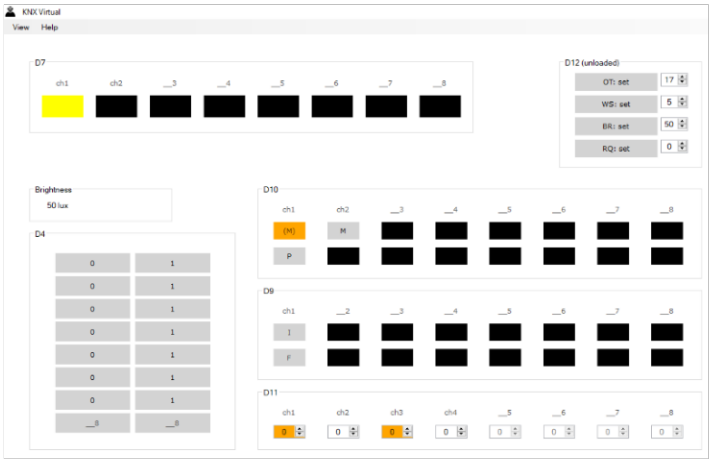


Figura 49: KNX Virtual – Escenario de conmutación.
Fuente: El tesista

3. D9.1 controla a D7.1 – alarma de intrusión

La Figura 50 muestra el control de detección de intrusión del escenario de conmutación con KNX Virtual (Figura 51), donde (D9.1 - ch1 está en ON), donde la lampara D7.1 se activa (ch1 está en ON):

D11.1 activa trigger (1) para activar D9.1 - alarma de intrusión.

D11.2 activa trigger (1) D9.1 para reset de alarma de intrusión

La Figura 52 muestra el resultado del monitoreo del Modulo D11 con sus canales activos: 1, 2, 3, y 4.

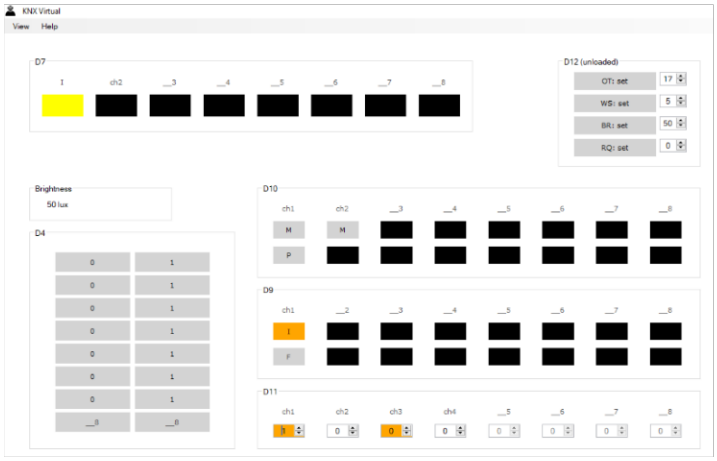


Figura 50: KNX Virtual – D9.1 controla a D7.1.
Fuente: El tesista

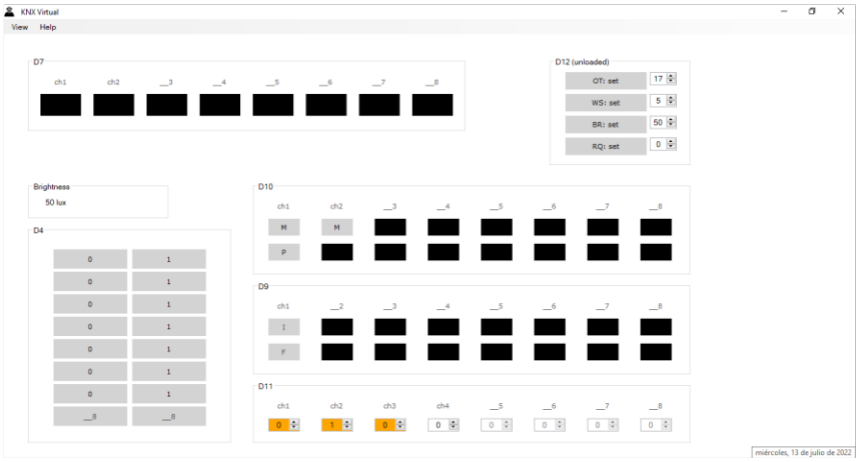


Figura 51: KNX Virtual – Escenario de conmutación.
Fuente: El tesista

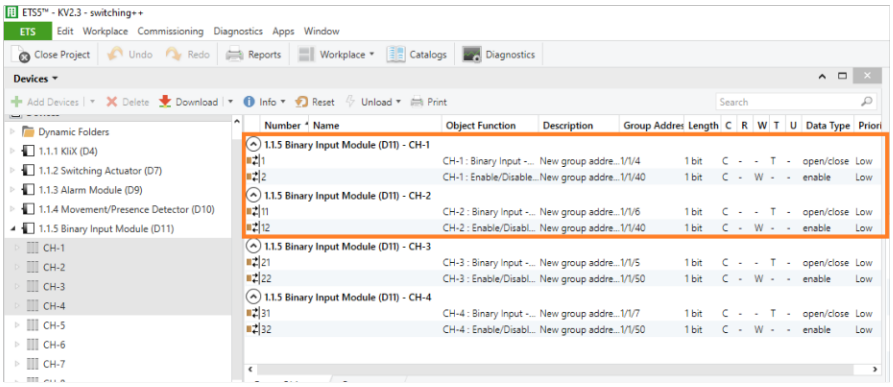


Figura 52: Modulo D11 – Canales activos: 1, 2, 3, y 4.
Fuente: El tesista

4. D9.1 controla a D7.1 – alarma contra incendio

La Figura 53 muestra el control de detección de intrusión del escenario de conmutación con KNX Virtual (Figura 54), donde (D9.1 - ch1 está en ON), donde la lampara D7.1 se activa (ch1 está en ON):

- D11.3 activa trigger (1) y D9.1 activa alarma contra incendio
- D11.4 activa trigger (1) D9.1 - reset alarma contra incendio

La Figura 55 muestra el resultado del monitoreo del Modulo D11 con sus canales activos: 1, 2, 3, y 4.

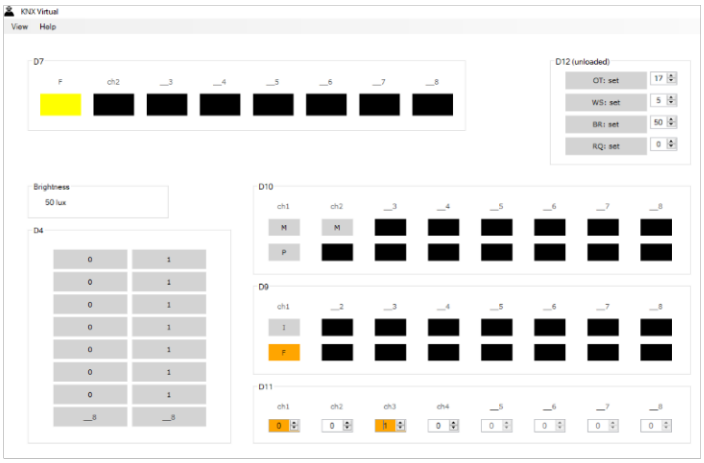


Figura 53: KNX Virtual – Escenario de conmutación.
Fuente: El tesista

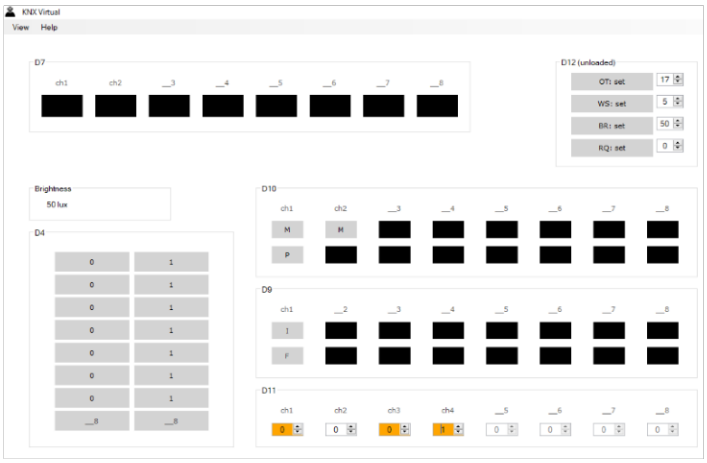


Figura 54: KNX Virtual – Escenario de conmutación.
Fuente: El tesista

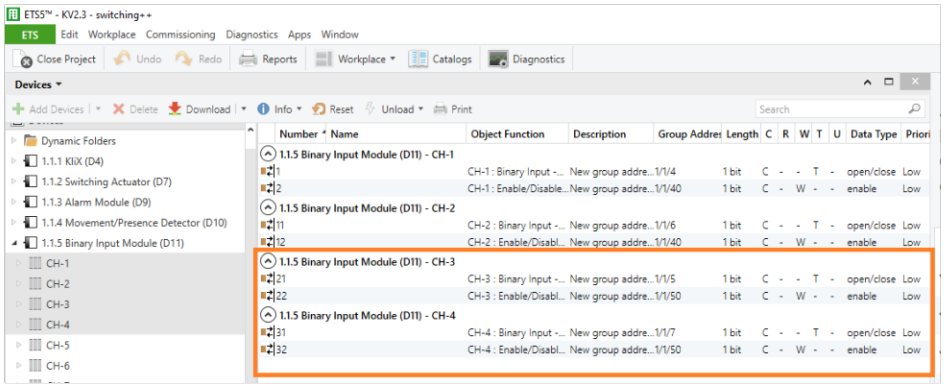


Figura 55: D11 – Canales activos: 1, 2, 3 y 4.
Fuente: El tesista

Escenario 2: Control de Persianas

Dispositivos requeridos:

D2: Actuador de persianas
D4: Pulsador
D9: Modulo de alarma
D11: Entrada binaria

Funciones de control

1. **D4.1 controla D2.1**

La Figura 56 muestra la configuración del pulsador para control de persianas D4, mientras que la Figura 57 muestra la configuración de la persiana D2, sin retroalimentación. Mientras que la Figura 58 muestra el escenario de control de persianas utilizando KNX Virtual donde el interruptor pulsador D4.1 controla la persiana D2.1.

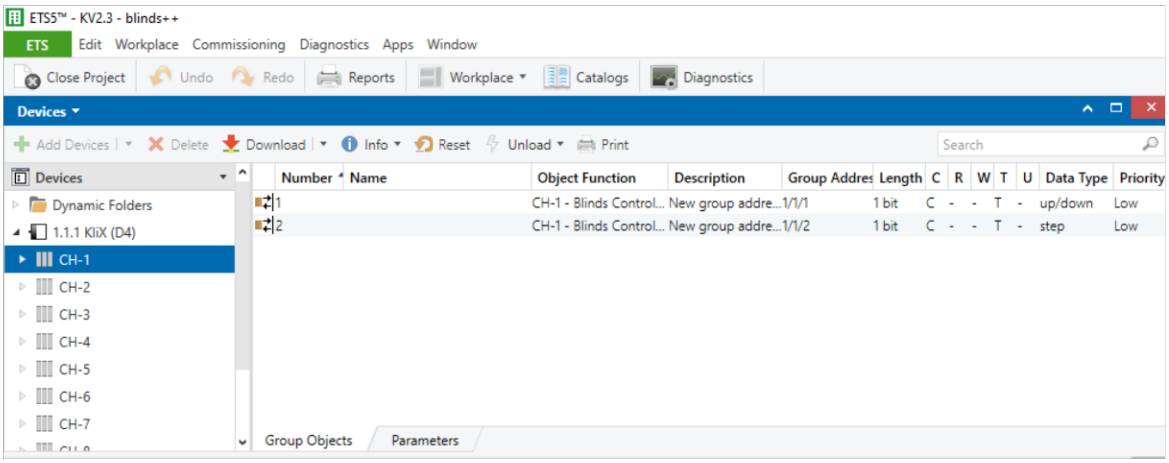


Figura 56: D4 – Canal activo CH-1.
Fuente: El tesista

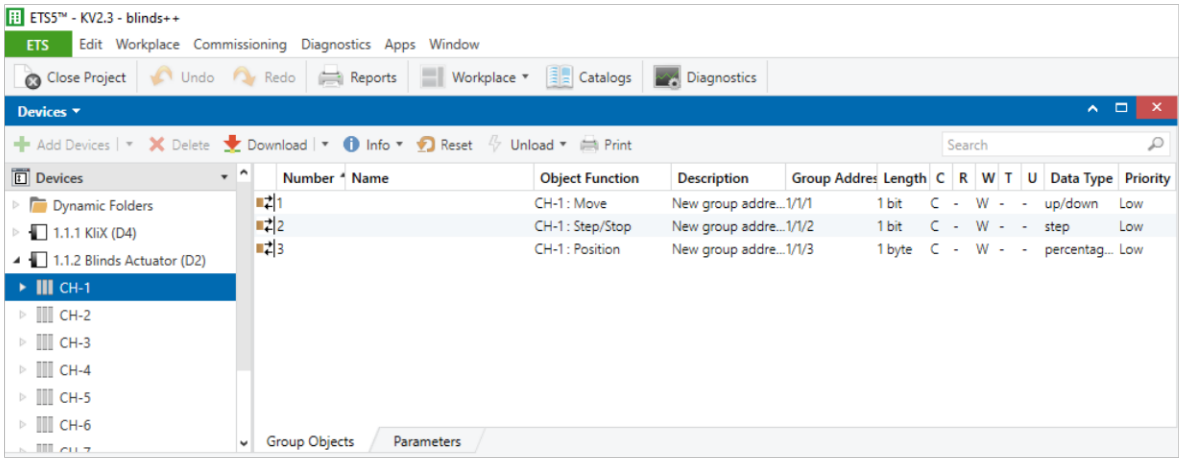


Figura 57: D2 – Canal activo CH-1.
Fuente: El tesista

Figura 58: KNX Virtual – Escenario de control de persianas.
Fuente: El tesista

2. D9.1 – control alarma de intrusión D2.4 y D2.5

La Figura 59 muestra la configuración del módulo de alarma D9 canal 1, para abrir y cerrar persianas. La Figura 60 indica la configuración del actuador de persianas D2 en sus canales CH-4 y CH-5. La Figura 61 muestra la configuración del módulo de entrada binario D11 en su canal CH-1. Mientras que la Figura 62 indica el escenario de control de persianas con KNX Virtual, al cambiar D11 CH-1 en ON detecta intrusión en D9 CH-1 y se accionan las persianas D2 CH-4 y D2 CH-5.

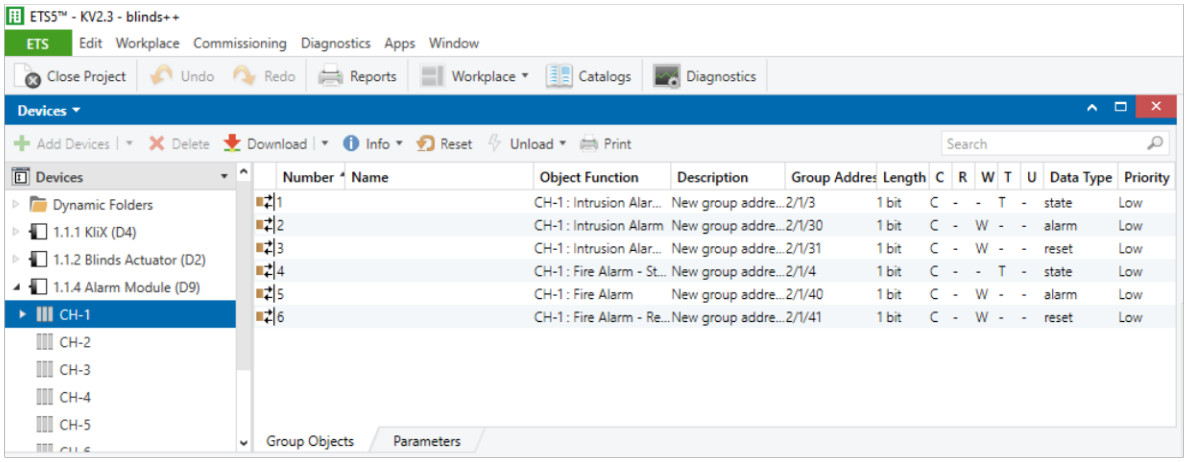


Figura 59: D9 – CH-1 Activo.
Fuente: El tesista

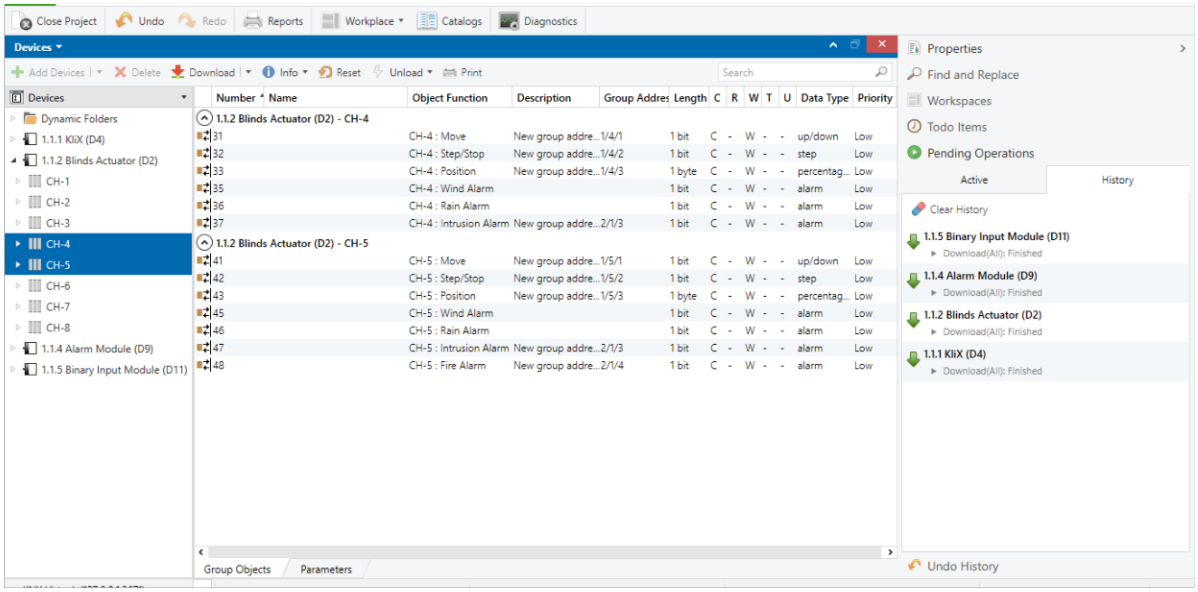


Figura 60: D2- CH-4 y CH-5 Activos.
Fuente: El tesista

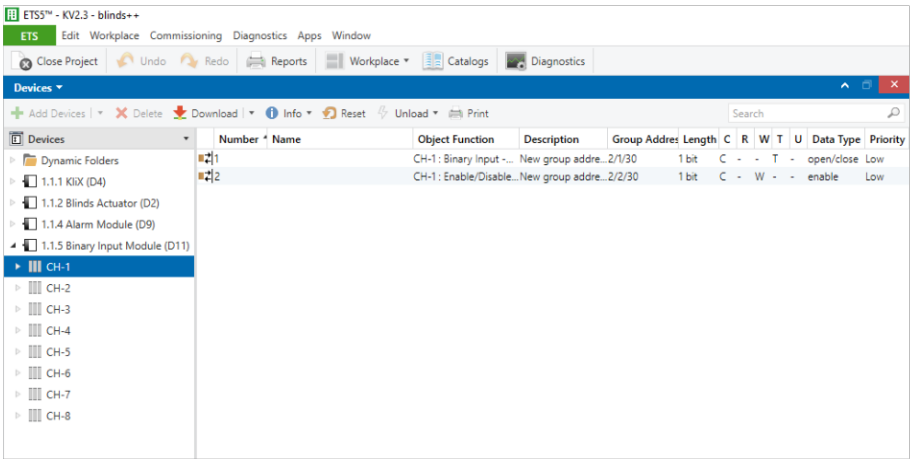


Figura 61: D11- CH-1 Activo.
Fuente: El tesista

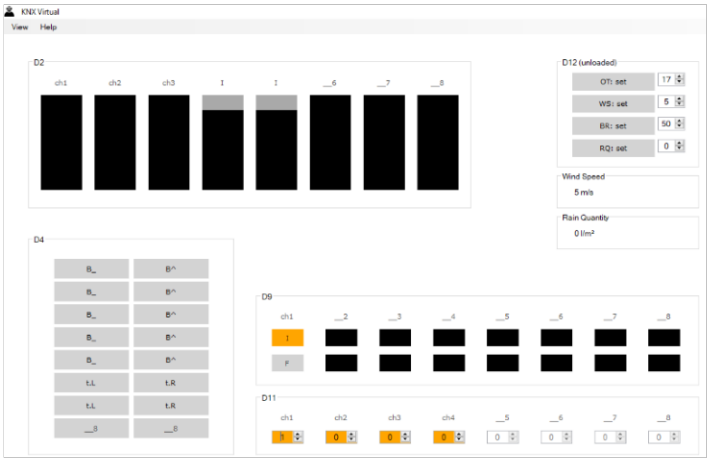


Figura 62: KNX Virtual – Escenario de control de persianas.
Fuente: El tesista

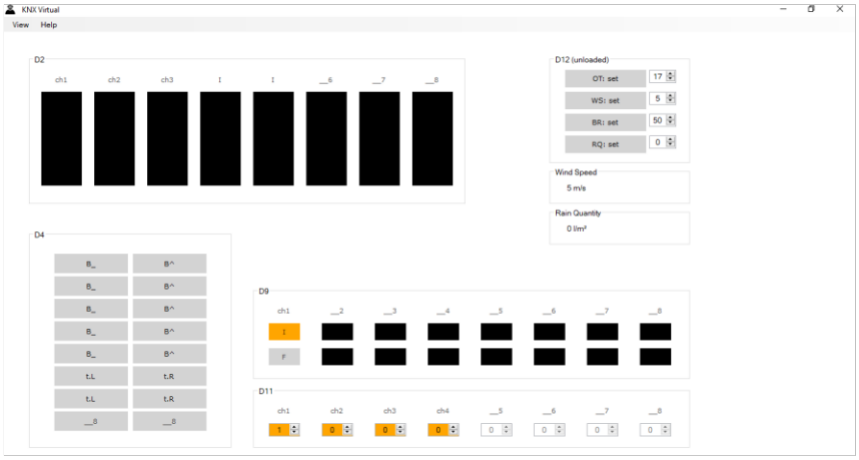


Figura 63: KNX Virtual – Escenario de control de persianas.
Fuente: El tesista

El reset de la alarma de intrusión se indica en la Figura 64 y Figura 65, la configuración de los dispositivos D11 y D9 respectivamente con ETS. La Figura 66 muestra que al poner D11 CH-2 en OFF se desactiva la alarma de intrusión D9 CH-1 está en OFF (se pone de color gris) y finalmente se cierran las persianas D2 CH-4 y D2 CH-5.

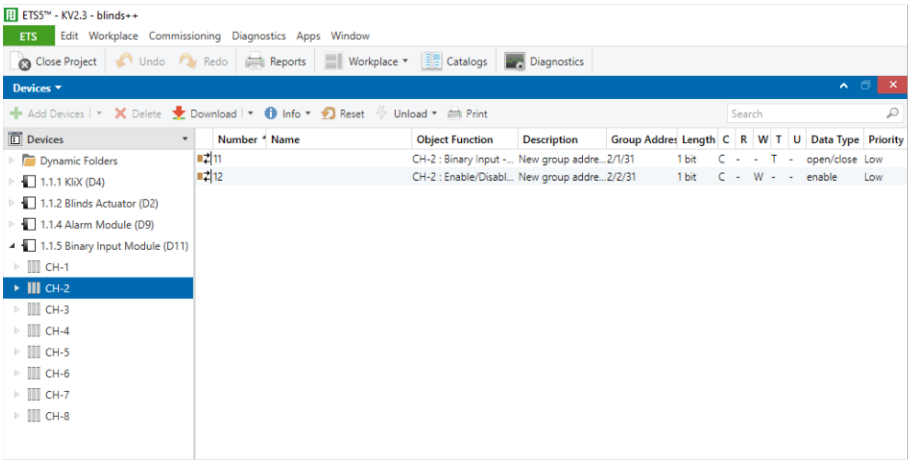


Figura 64: D11 – CH-2 Activo.
Fuente: El tesista

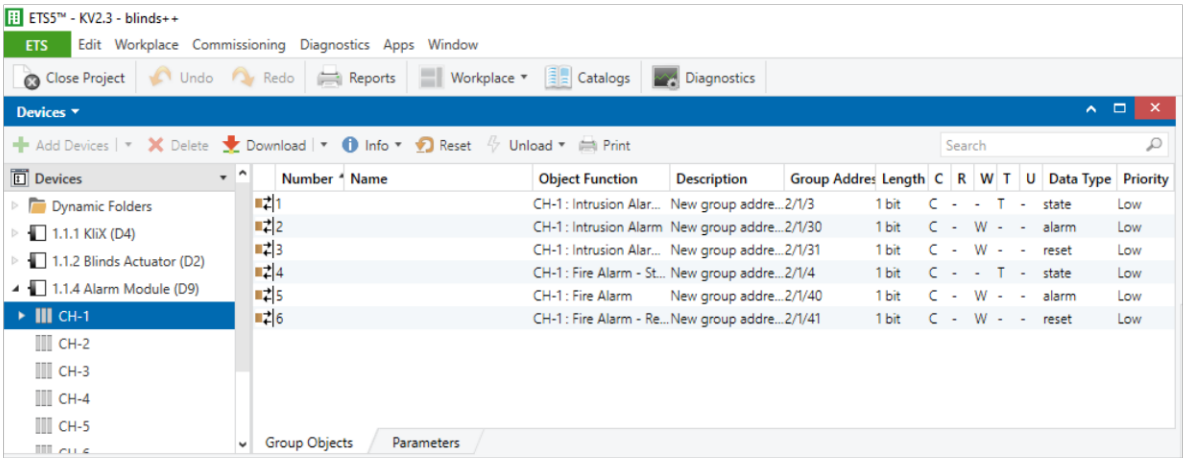


Figura 65: D9 – CH-1 Activo.
Fuente: El tesista

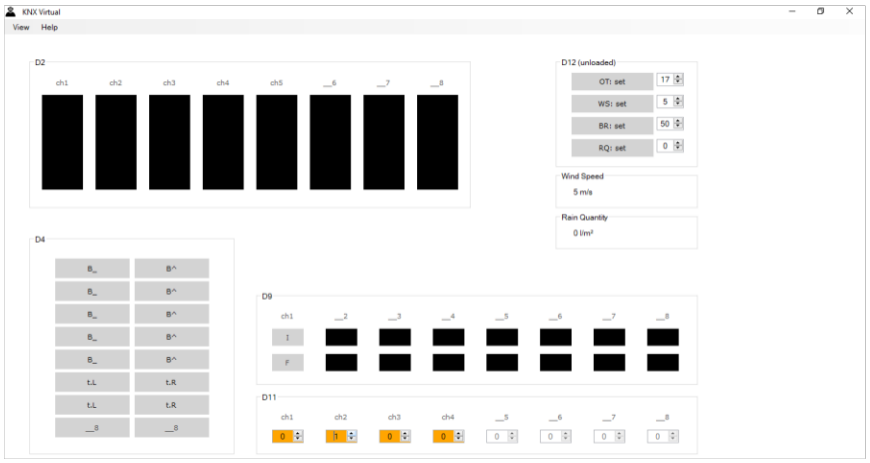


Figura 66: KNX Virtual – Escenario de control de persianas.
Fuente: El tesista

3. D11.3 – control de alarma de incendio D2.5

La Figura 67 muestra la configuración del módulo de alarma contra incendio D9 canal 1. La Figura 68 indica la configuración del actuador de persianas D2 en su canal CH-5. La Figura 69 muestra la configuración del módulo de entrada binario D11 en su canal CH-3. Mientras que la Figura 70 indica el escenario de control de persianas con KNX Virtual, al cambiar D11 CH-3 en ON detecta una alarma en D9 CH-1 y se accionan las persianas D2 CH-5.

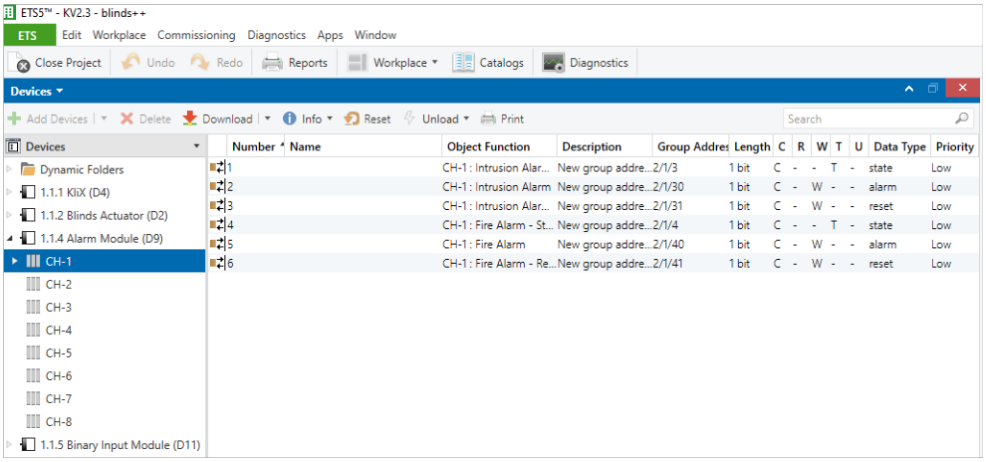


Figura 67: D9 – CH-1 Activo.
Fuente: El tesista

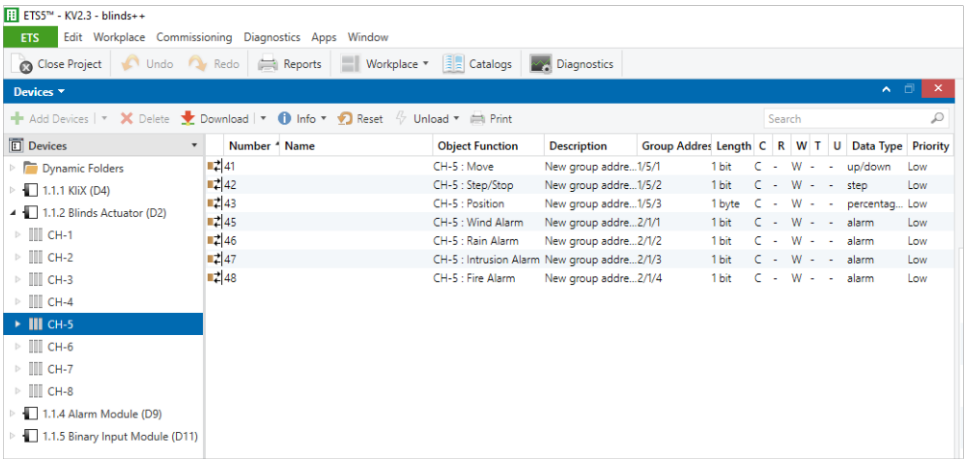


Figura 68: D2 – CH-5 Activo.
Fuente: El tesista

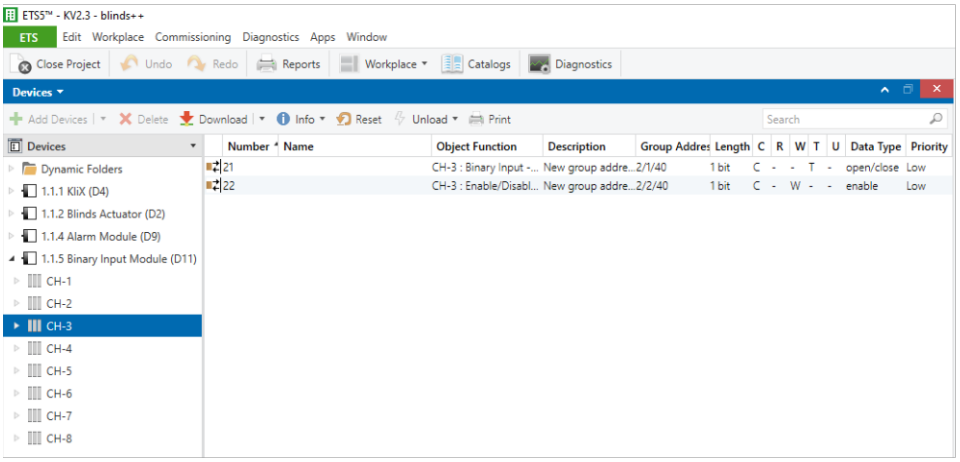


Figura 69: D11- CH-3 Activo.
Fuente: El tesista

Figura 70: KNX Virtual – Escenario de control de persianas.
Fuente: El tesista

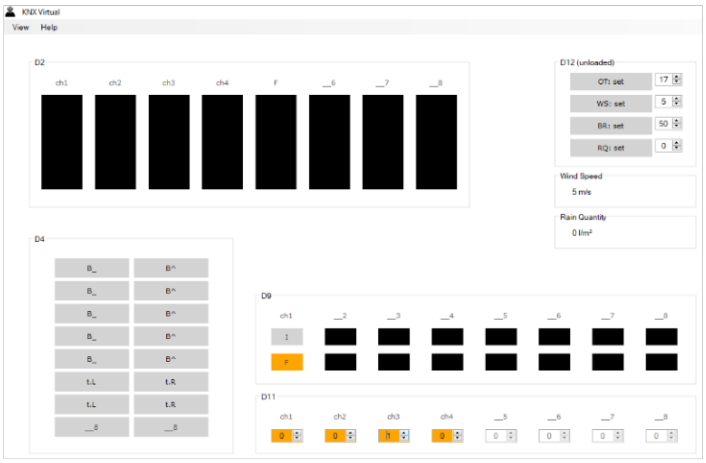


Figura 71: KNX Virtual – Escenario de control de persianas.
Fuente: El tesista

El reset de la alarma contra incendios se indica en la Figura 72 y Figura 73, la configuración de los dispositivos D9 y D11 respectivamente con ETS. La Figura 74 muestra que al poner D11 CH-4 en OFF se desactiva la alarma contra incendios D9 CH-1 está en OFF (se pone de color gris) y finalmente se cierran la persiana D2 CH-5.

4. D11.4 reinicia la alarma contra incendio de D9.1

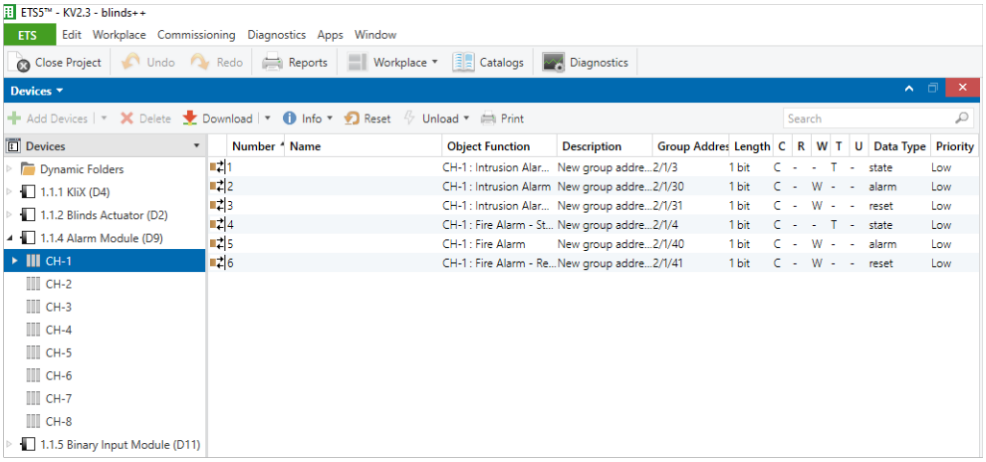


Figura 72: D9 – CH-1 Activo.
Fuente: El tesista

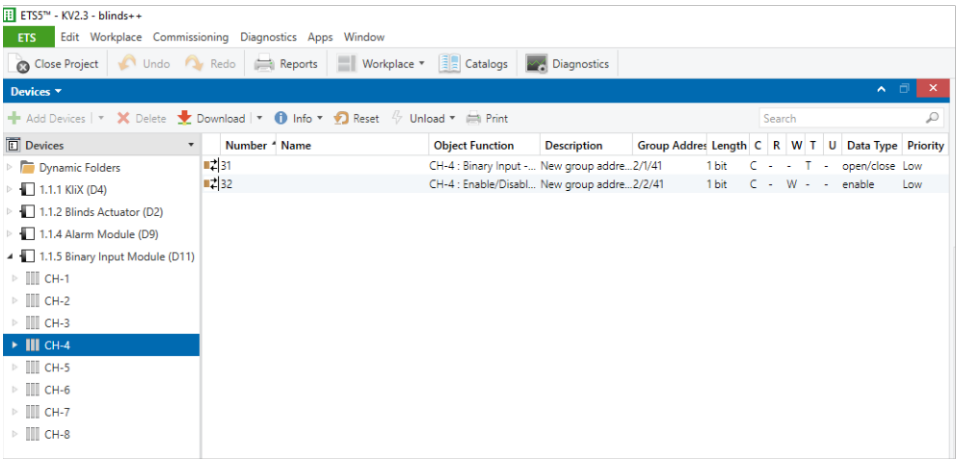


Figura 73: D11 – CH-4 Activo.
Fuente: El tesista

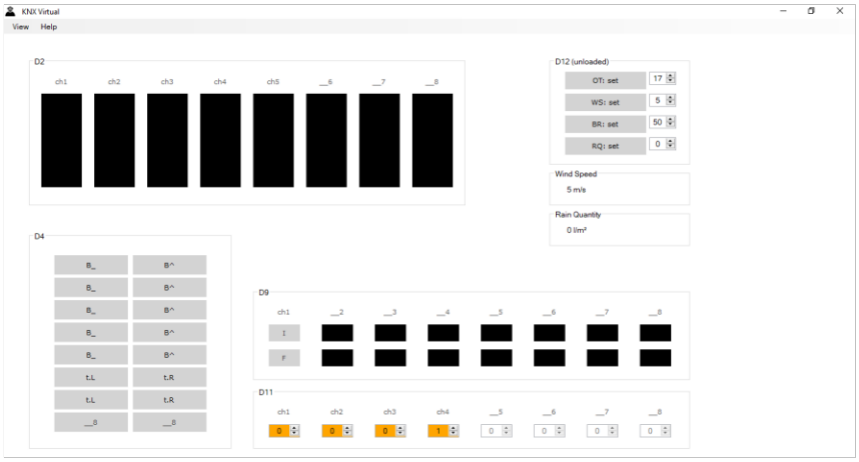


Figura 74: KNX Virtual – Escenario de control de persianas.
Fuente: El tesista

Escenario 3: Control en 2 habitaciones

Dispositivos Requeridos:

D2: Actuador de persianas
D7: Actuador de conmutación
D10: Detector de movimiento y presencia
D21: Pulsador cuarto 21
D22: Pulsador cuarto 22

Room21

La Figura 75 muestra la configuración del control del cuarto 21 en CH-1 para encendido de una lampara con su configuración que se muestra en la Figura 76 la configuración del dispositivo D7 CH-1 referente a una lampara. La Figura 77 muestra en KNX Virtual el escenario de control de la habitación 21.

1. D21.1 controla D7.1

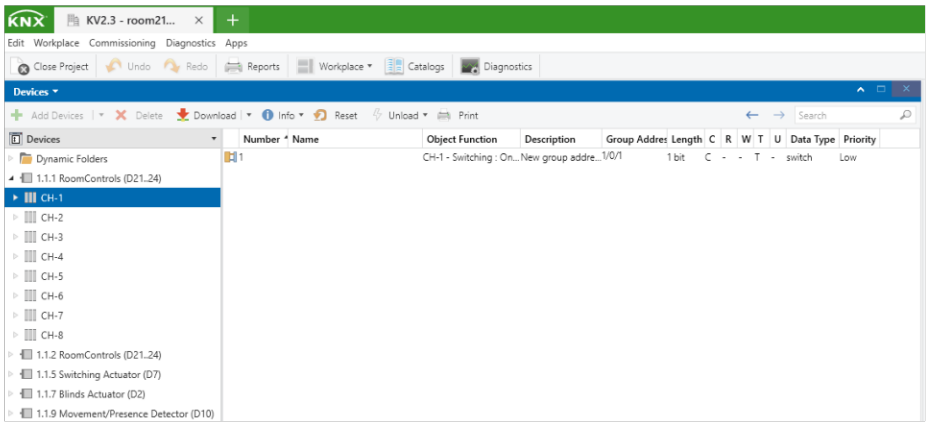


Figura 75: D21 – CH-1 Activo.
Fuente: El tesista

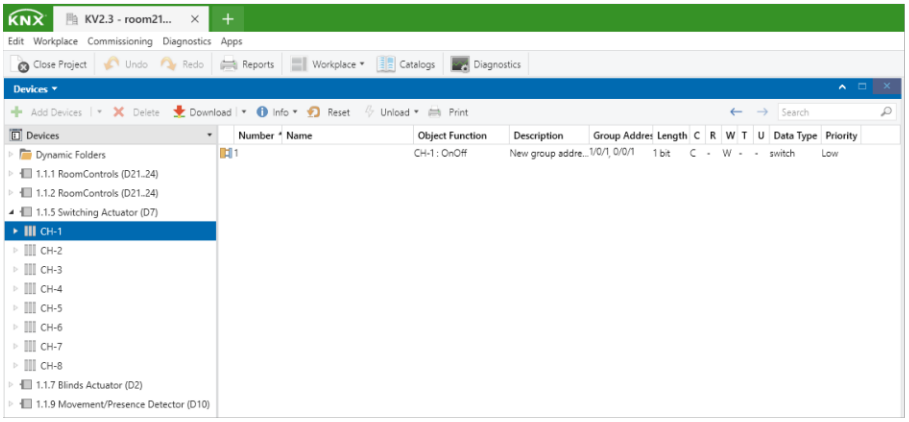


Figura 76: D7 – CH-1 Activo.
Fuente: El tesista

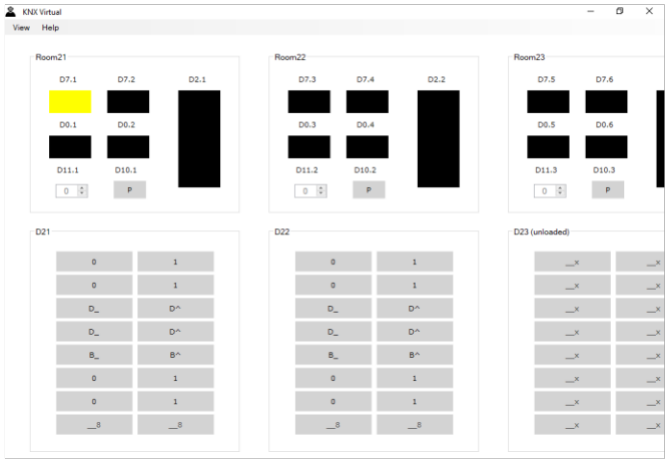


Figura 77: KNX Virtual – Escenario de control de 2 habitaciones.
Fuente: El tesista

2. D21.5 controla D2.1

La Figura 81 muestra la configuración del control del cuarto 21 en CH-5 para abrir persianas con su configuración que se muestra en la Figura 82 la configuración del dispositivo D2 CH-1 referente a una persiana. La Figura 83 muestra en KNX Virtual el escenario de control de la habitación 21.

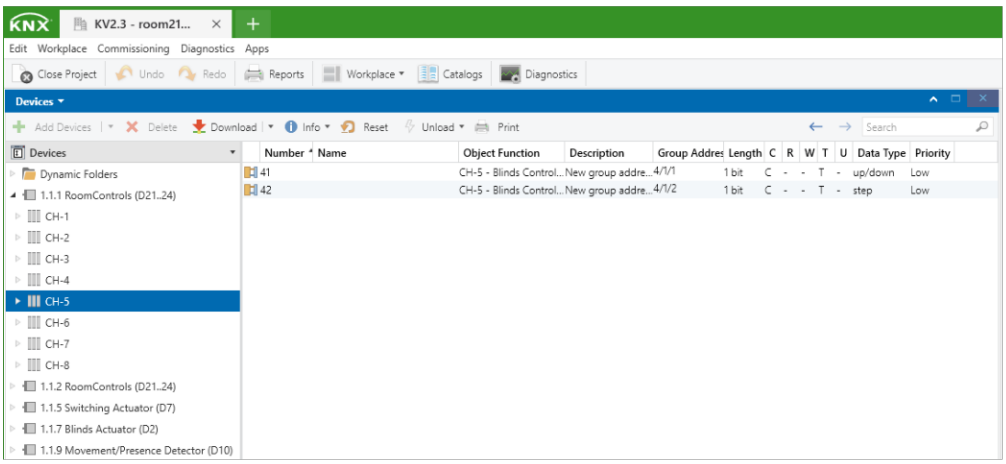


Figura 78: D21 – CH-5 Activo.
Fuente: El tesista

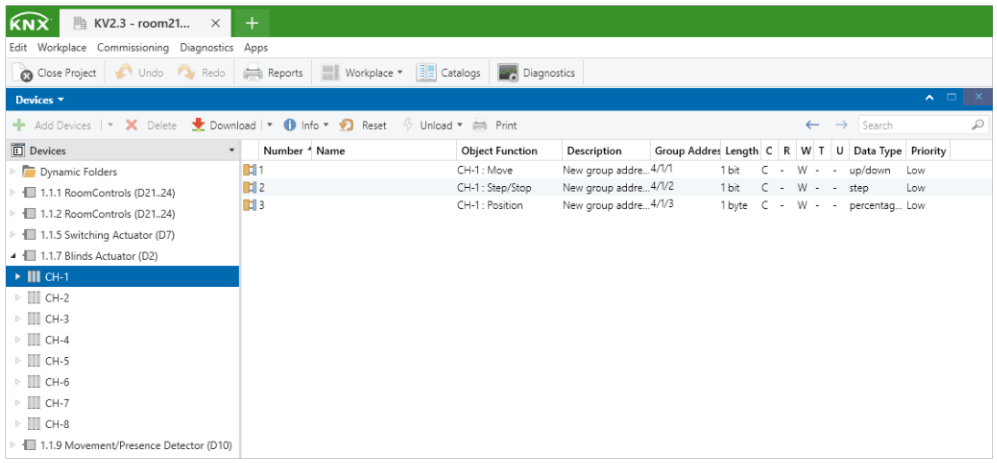


Figura 79: D2 – CH-1 Activo.
Fuente: El tesista

Figura 80: KNX Virtual – Escenario de control de 2 habitaciones.
Fuente: El tesista

3. D10.1 controla D7.1 – detección de presencia

La Figura 84 muestra la configuración del control del cuarto 21 en CH-1 para activar un actuador para una lámpara, su configuración que se muestra la Figura 85 la configuración del dispositivo D7 CH-1 referente a un actuador. La Figura 86 muestra en KNX Virtual el escenario de control de la habitación 21.

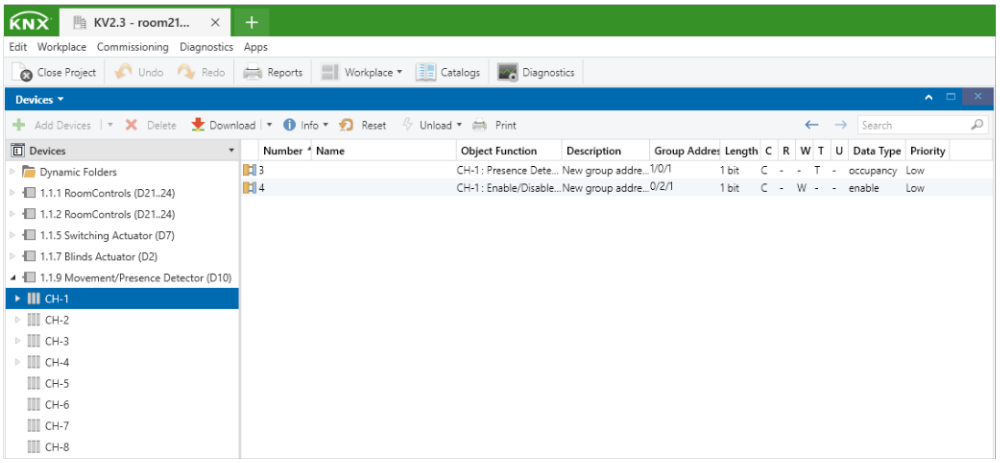


Figura 81: D10 – CH-1 Activo.
Fuente: El tesista

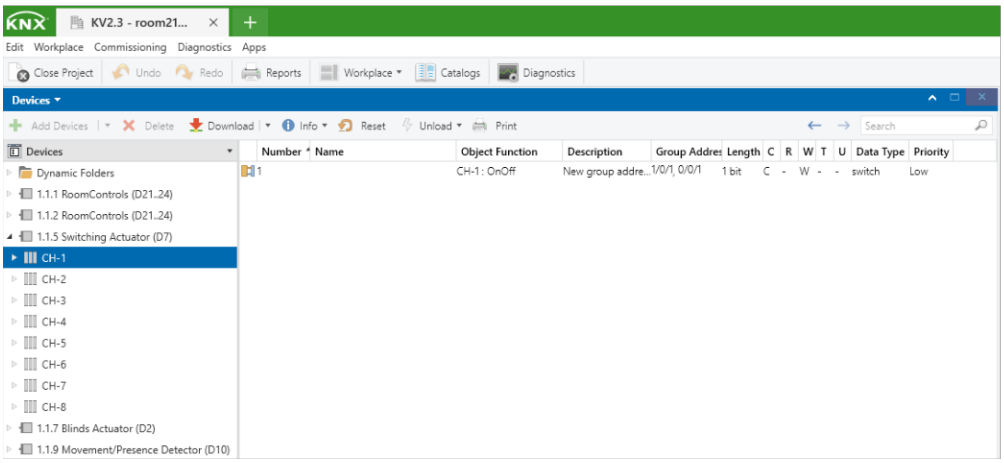


Figura 82: D7 – CH-1 Activo.
Fuente: El tesista

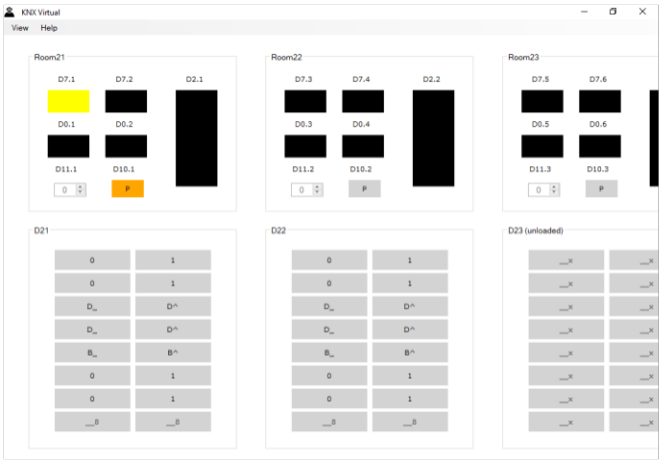


Figura 83: KNX Virtual – Escenario de control de 2 habitaciones.
Fuente: El tesista

Room22

1. **D22.1 controla D7.3**

La Figura 87 muestra la configuración del control del cuarto 22 en CH-1 para encendido de una lampara con su configuración que se muestra en la Figura 88 la configuración del dispositivo D7 CH-3 referente a una lampara. La Figura 89 muestra en KNX Virtual el escenario de control de la habitación 22.

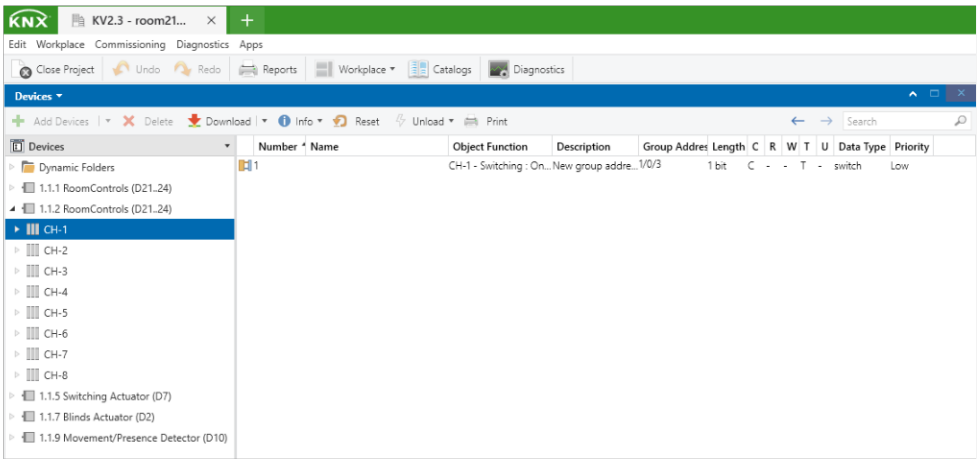


Figura 84: D22 – CH-1 Activo.
Fuente: El tesista

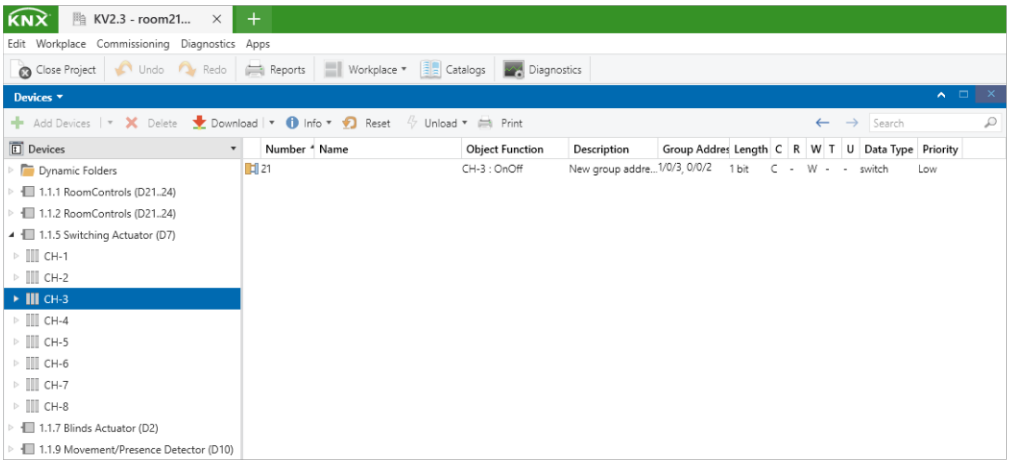


Figura 85: D7- CH-3 Activo.
Fuente: El tesista

Figura 86: KNX Virtual – Escenario de control de 2 habitaciones.
Fuente: El tesista

2. D22.2 controla D7.4

La Figura 90 muestra la configuración del control del cuarto 22 en CH-2 para activar un actuador para una lámpara, su configuración que se muestra la Figura 91 la configuración del dispositivo D7 CH-4 referente a un actuador. La Figura 92 muestra en KNX Virtual el escenario de control de la habitación 21.

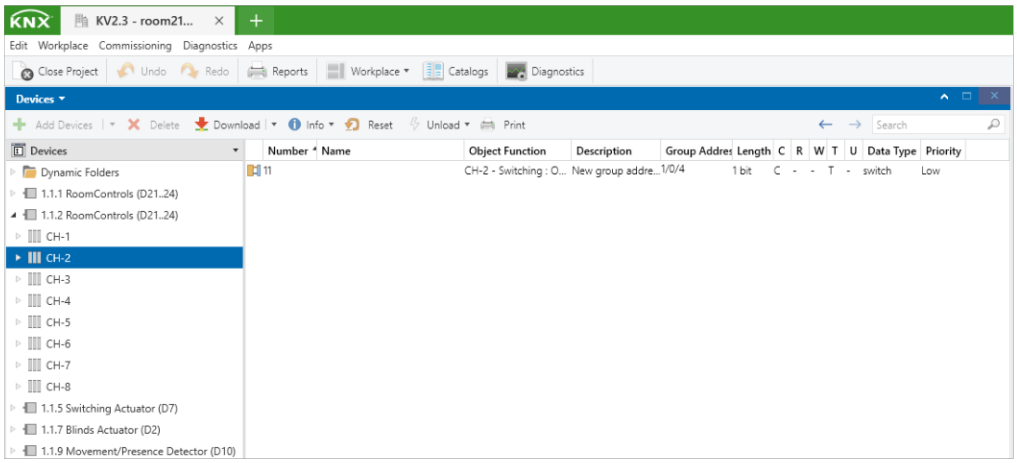


Figura 87: D21 – CH-2 Activo.
Fuente: El tesista

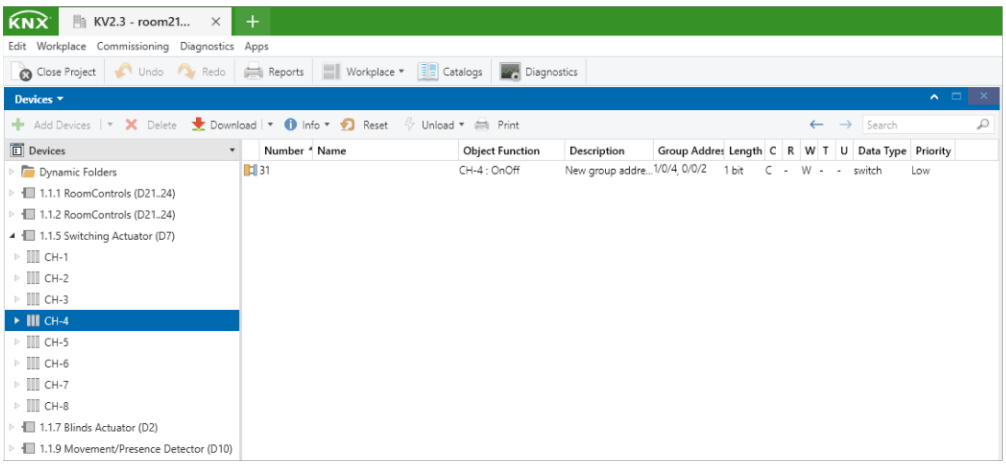


Figura 88: D7 – CH-4 Activo.
Fuente: El tesista

Figura 89: KNX Virtual – Escenario de control de 2 habitaciones.
Fuente: El tesista

3. D22.5 controla D2.2

La Figura 93 muestra la configuración del control del cuarto 22 en CH-5 para abrir persianas con su configuración que se muestra en la Figura 94, la configuración del dispositivo D2 CH-2 referente a una persiana. La Figura 95 muestra en KNX Virtual el escenario de control de la habitación 22.

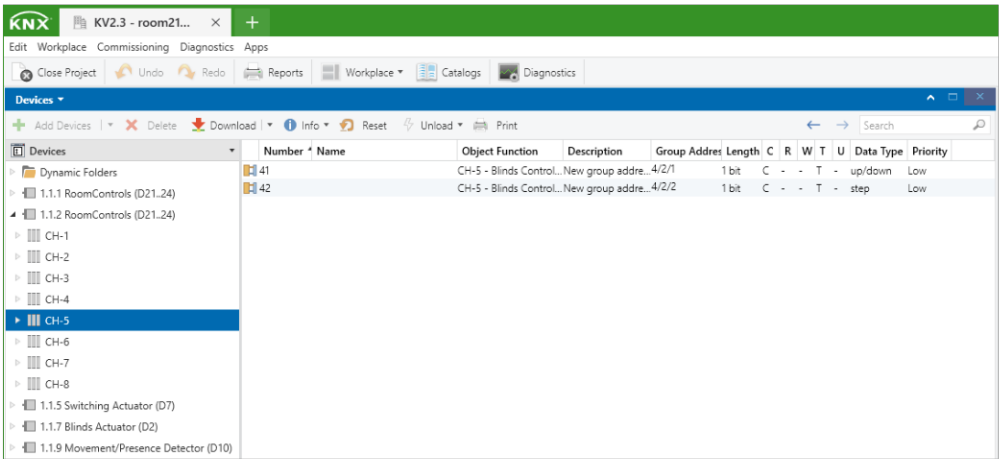


Figura 90: D22 – CH-5 Activo.
Fuente: El tesista

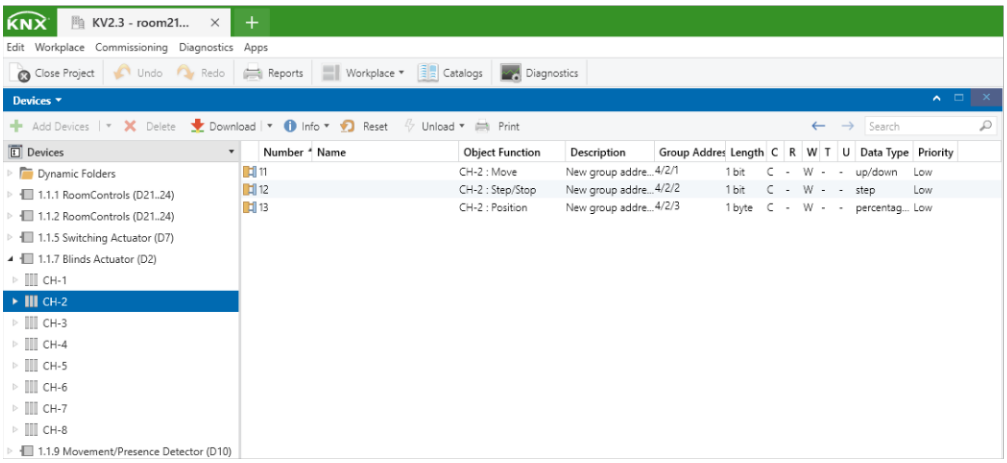


Figura 91: D2 – CH-2 Activo.
Fuente: El tesista

Figura 92: KNX Virtual – Escenario de control de 2 habitaciones.
Fuente: El tesista

4. D10.2 controla a D7.2 – detección de presencia

La Figura 96 muestra la configuración del control del cuarto 22 en CH-2 para activar un actuador para una lámpara, su configuración que se muestra la Figura 97 la configuración del dispositivo D7 CH-2 referente a un actuador. La Figura 98 muestra en KNX Virtual el escenario de control de la habitación 22.

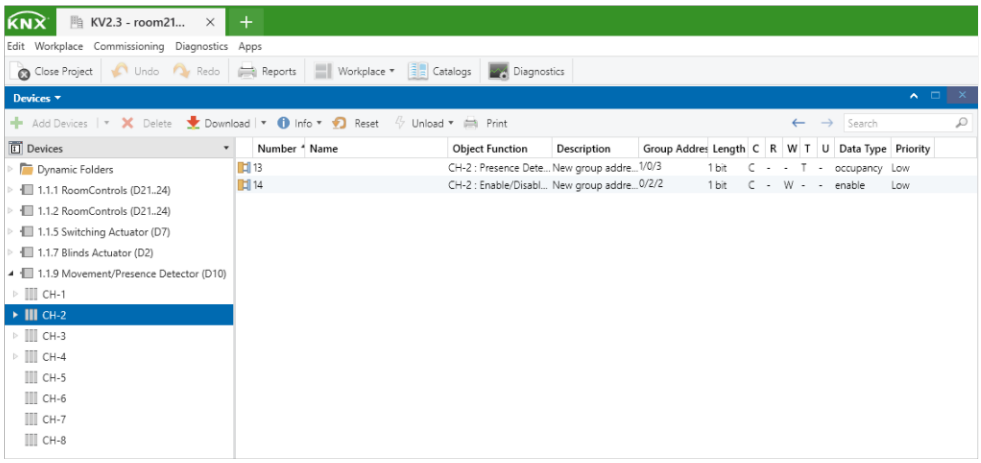


Figura 93: D0 – CH-2 Activo.
Fuente: El tesista

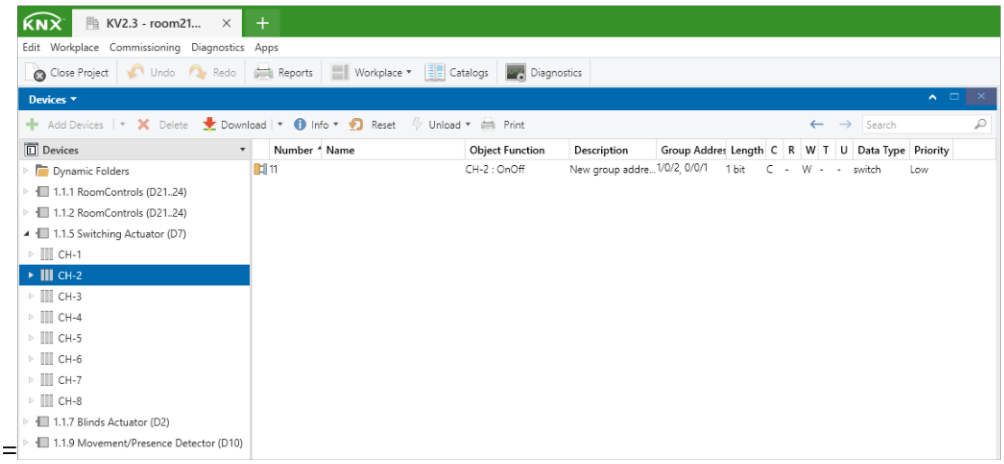


Figura 94: D7 – CH-2 Activo.
Fuente: El tesista

Figura 95: KNX Virtual – Escenario de control de 2 habitaciones.
Fuente: El tesista

9.2 ANEXO 2

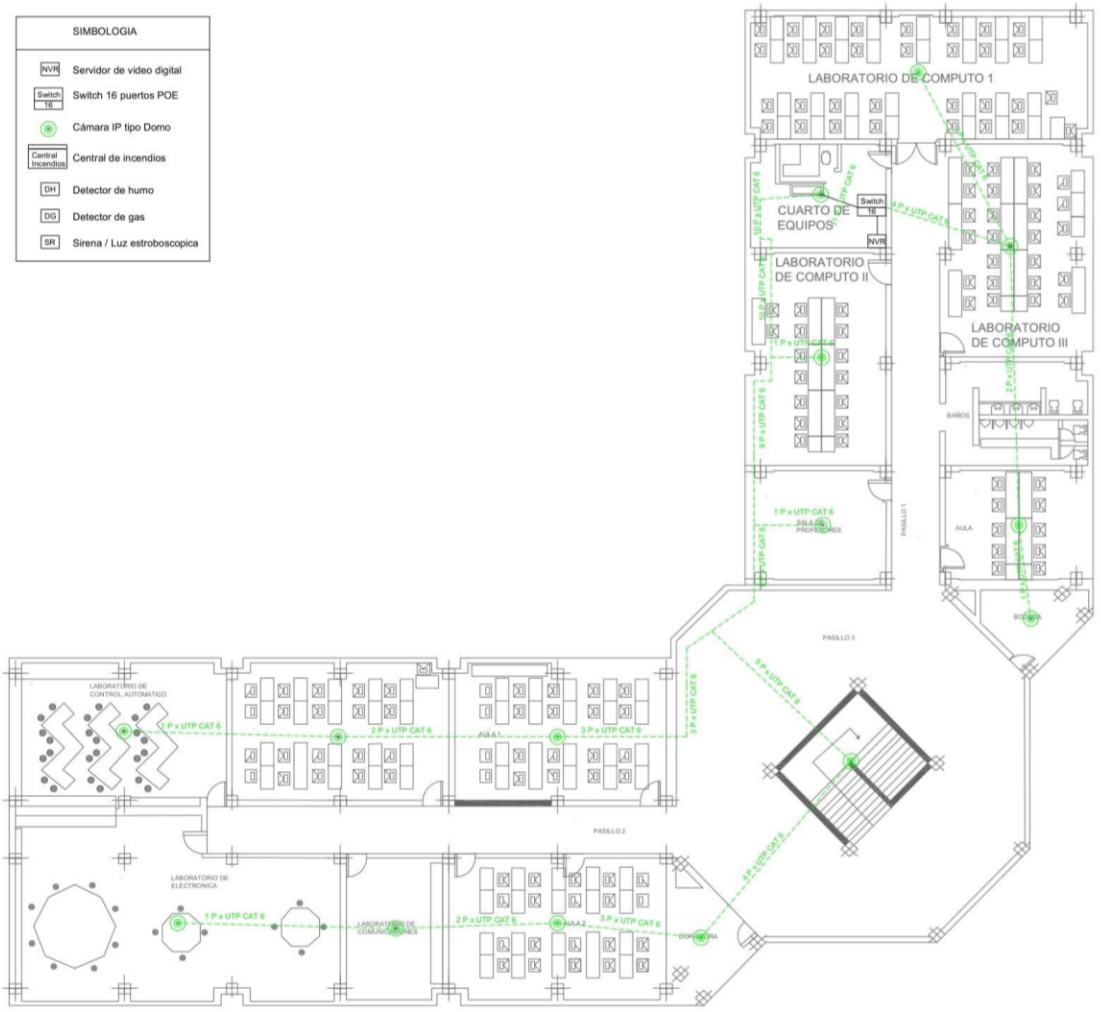
Nombre	Gráficas	Informes	Grupos Lógicos	Auto Descubrimiento	Agentes	SNMP	Plugins	Aplicación Web	Alertas	Monitoreo Distribuido	Base De Datos	Licencia
Nagios	Sí	Sí	Sí	Sí	Sí	Uso de plugins	Sí	Sólo Visualización	Sí	Sí	SQL	Comercial 30 días free
Zabbix	Sí	Sí	No	Sí	Sí	Sí	Sí	Control Total	Sí	Sí	SQL	GPL
Zenoss	Sí	No	Sí	Sí	SNMP, WMI, JMX, etc.	Sí	Sí	Control Total	Sí	Sí	RRDtool y MySQL	GPL
Network Performance Monitor	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Control Total	Sí	Sí	SQL	Comercial 30 días free
SolarWinds	Sí	Sí	Sí	Sí	SNMP, WMI	Sí	Sí	Control Total	Sí	Sí	Archivos Planos	Comercial 14-30 días free
Pandora FMS Community	Sí	En tiempo real o programados	Sí	Sí	Con agente y sin agente	Sí	Sí	Control Total	Sí	Sí	MySQL y Oracle	GPL
Wormly	Sí	Desconocido	No	No	Windows, Linux	No	No	Control Total	Sí	Sí	Desconocido	Comercia 30 días free

Cacti	Sí	Sí	Sí	A través de plugins	Sí	Sí	Sí	Control Total	Sí	No	RRDtool y MySQL	GPL
OpenNMS	Sí	Sí	No	Sí	SNMP, WMI, JMX, usando	Sí	Sí	Control Total	Enrutamiento, escalas y horarios	cliente mínimo o snmp	jrobin, RRDtool y PostgreSQL	GPL
Pandora FMS Enterprise	Sí	En tiempo real o programados	Sí	Sí	Con agente y sin	Sí	Sí	Control Total	Sí	Sí	MySQL y Oracle	Comercial 30 días free

Tabla 14: Comparación de Herramientas para Monitoreo de Redes.
Fuente: Mori Rojas, A. (2022).

9.3 ANEXO 3


SIMBOLOGIA
SI Sonda de inundacion
DP Detector de Presencia
LDP Lampara para Detector de Presencia
FA Fuente de alimentacion
IP Interfaz de pulsador
TZ Terminal de zona de 2 canales
TZ Terminal de zona de 4 canales
CM Contacto magnetico
LABORATORIO DE COMPUTO 1
CUARTO DE EQUIPOS
LABORATORIO DE COMPUTO II
LABORATORIO DE COMPUTO III
BAÑOS
SALA DE PROFESORES
PASILLO 1
AULA
BODEGA
PASILLO 3
LABORATORIO DE CONTROL AUTOMATICO
AULA 3
AULA 1
PASILLO 2
LABORATORIO DE ELECTRONICA
LABORATORIO DE COMUNICACIONES
AULA 2
COPIADORA
Seguridad de Puertas y Ventanas
Escala 1: 100

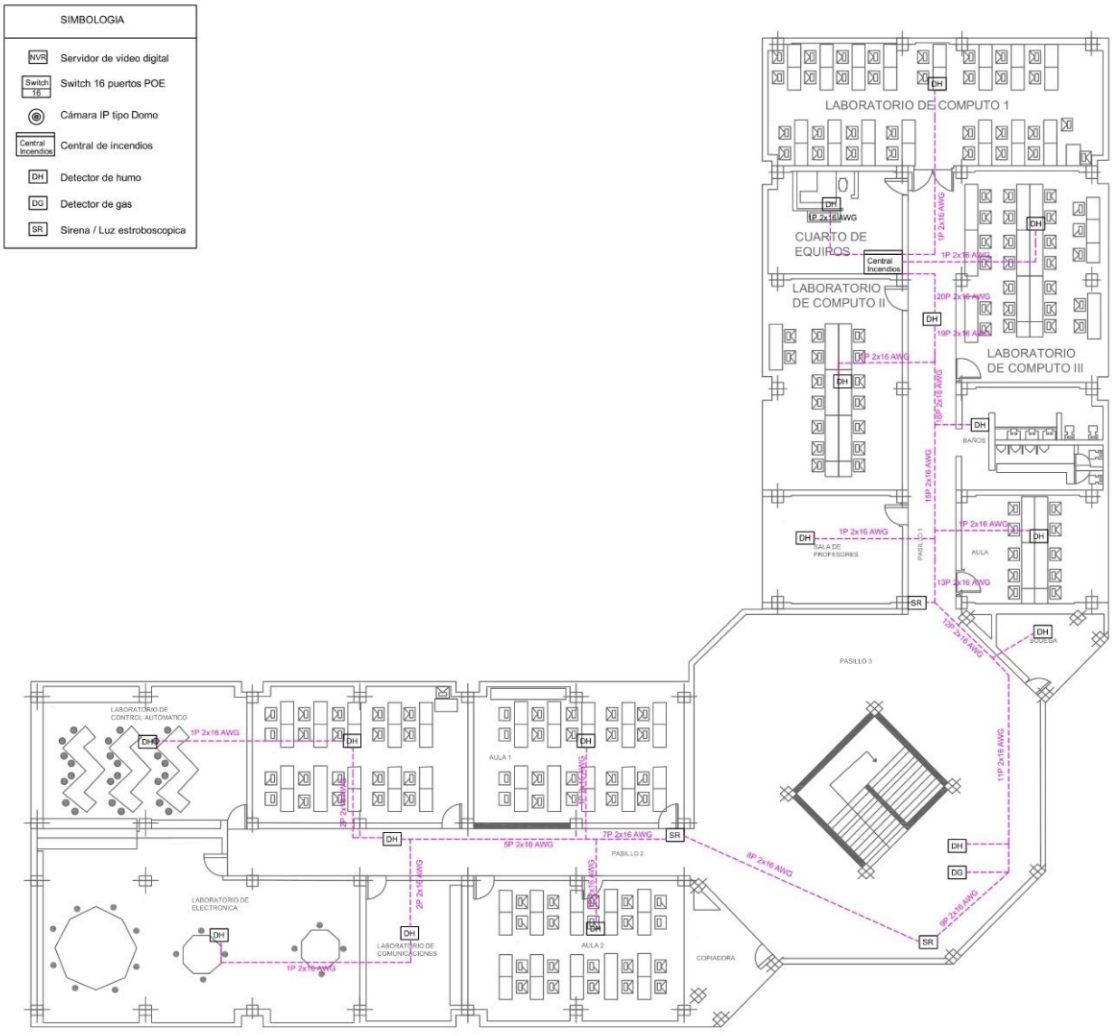


Sistema de cámaras de seguridad

Escala 1: 100

Seguridad de Acceso e Inundación

Escala 1: 100



Sistema contra incendio

Escala 1: 100

9.4 ANEXO 4

Pregunta 1

¿Considera usted que el sistema domótico propuesto, es el adecuado y mejoraría la seguridad del tercer piso del edificio?

La Figura 96 muestra el resultado de la tabulación de la Pregunta 1, que indica que el 50% de los expertos está muy satisfecho con los resultados, mientras que el otro 50% está totalmente satisfecho.

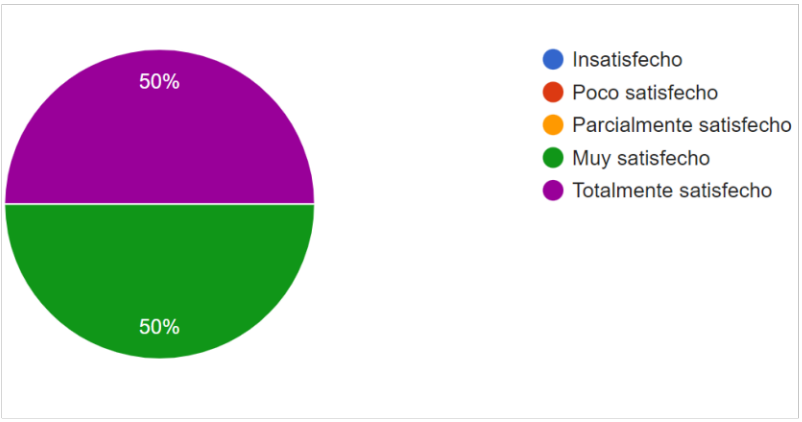


Figura 96: Resultado de la tabulación de la Pregunta 1.
Fuente: El tesista

Pregunta 2

¿Piensa que el proceso adoptado para el planteamiento del sistema domótico, es el apropiado?

La Figura 97 muestra el resultado de la tabulación de la Pregunta 2, que indica que 12.5% está totalmente satisfecho, el 62.5% de los expertos está muy satisfecho con los resultados, mientras que el 25% está parcialmente satisfecho.

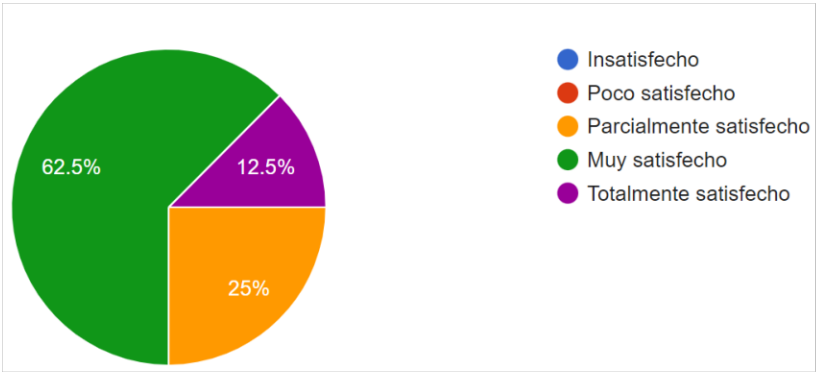


Figura 97: Resultado de la tabulación de la Pregunta 2.
Fuente: El tesista

Pregunta 3

¿Considera que el sistema domótico planteado cumple con la normativa KNX?

La Figura 98 muestra el resultado de la tabulación de la Pregunta 3, que indica que 25% está totalmente satisfecho, el 62.5% de los expertos está muy satisfecho con los resultados, mientras que el 12.5% está parcialmente satisfecho.

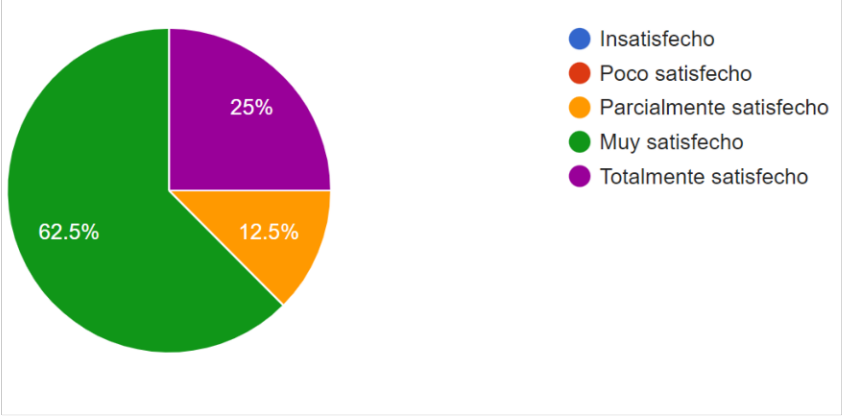


Figura 98: Resultado de la tabulación de la Pregunta 3.
Fuente: El tesista

Pregunta 4

¿Considera que una posterior implementación del sistema domótico planteado, mejoraría la seguridad y gestión del tercer piso?

La Figura 99 muestra el resultado de la tabulación de la Pregunta 4, que indica que el 62.5% de los expertos está muy satisfecho con los resultados, mientras que el 37.5% está totalmente satisfecho.

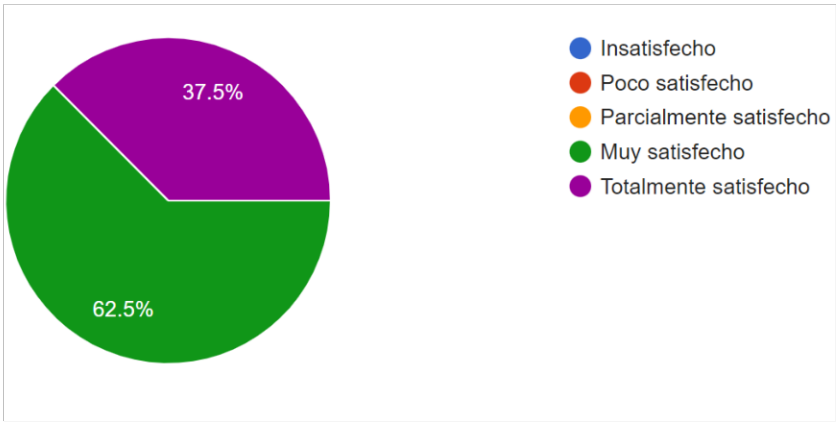


Figura 99: Resultado de la tabulación de la Pregunta 4.
Fuente: El tesista

Pregunta 5

¿Los niveles de calidad de señal alámbrica e inalámbrica mejorarían con la implementación de la propuesta?

La Figura 100 muestra el resultado de la tabulación de la Pregunta 5, que indica que el 62.5% de los expertos está muy satisfecho con los resultados, mientras que el 25% está totalmente satisfecho y el 12.5% está parcialmente satisfecho.

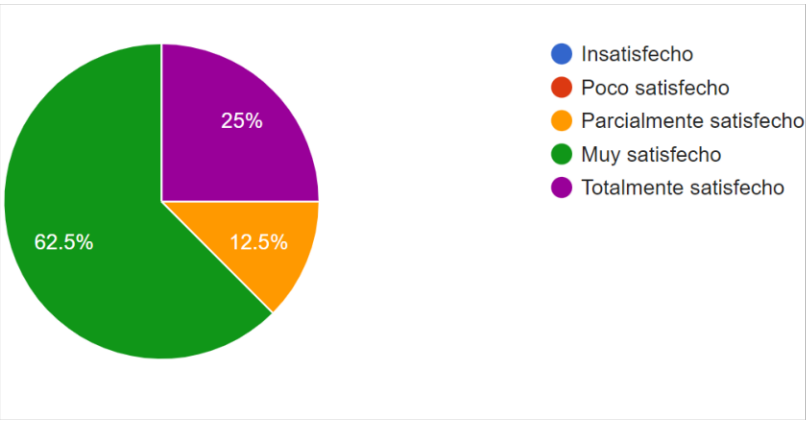


Figura 100: Resultado de la tabulación de la Pregunta 5.
Fuente: El tesista

Pregunta 6

¿Habría un ahorro en el presupuesto de cables y equipos KNX con la implementación de la propuesta?

La Figura 101 muestra el resultado de la tabulación de la Pregunta 6, que indica que el 75% de los expertos está muy satisfecho con los resultados, mientras que el 25% está totalmente satisfecho.

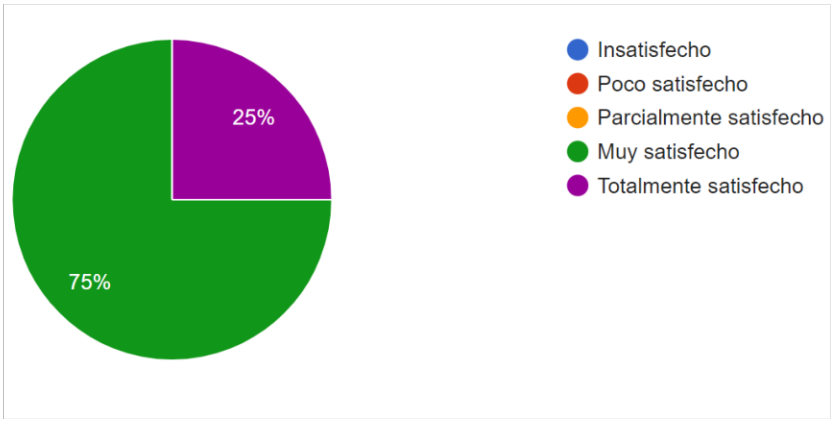


Figura 101: Resultado de la tabulación de la Pregunta 6.
Fuente: El tesista

Pregunta 7

¿Con la nueva propuesta la seguridad de la red mejoraría frente al porcentaje de intrusión detectada?

La Figura 102 muestra el resultado de la tabulación de la Pregunta 7, que indica que el 87.5% de los expertos está muy satisfecho con los resultados, mientras que el 12.5% está totalmente satisfecho.

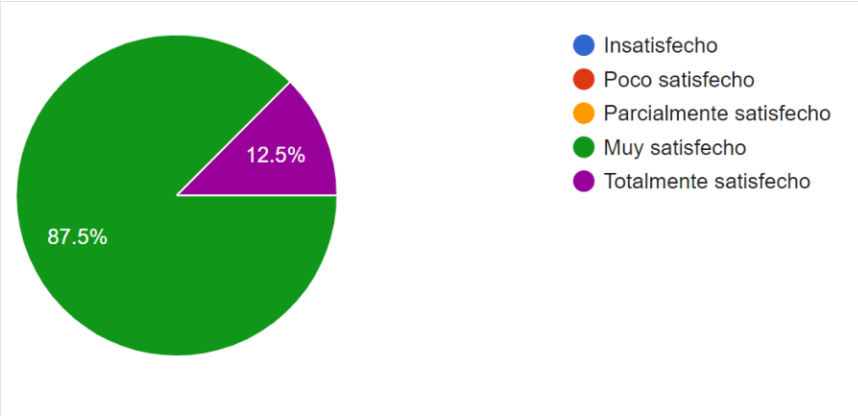


Figura 102: Resultado de la tabulación de la Pregunta 7.
Fuente: El tesista

Pregunta 8

¿Considera que todas las habitaciones están con elementos de domótica implementados?

La Figura 103 muestra el resultado de la tabulación de la Pregunta 8, que indica que el 50% de los expertos está muy satisfecho con los resultados, mientras que el 12.5% está totalmente satisfecho, el 12.5% está poco satisfecho y el 25% está parcialmente satisfecho.

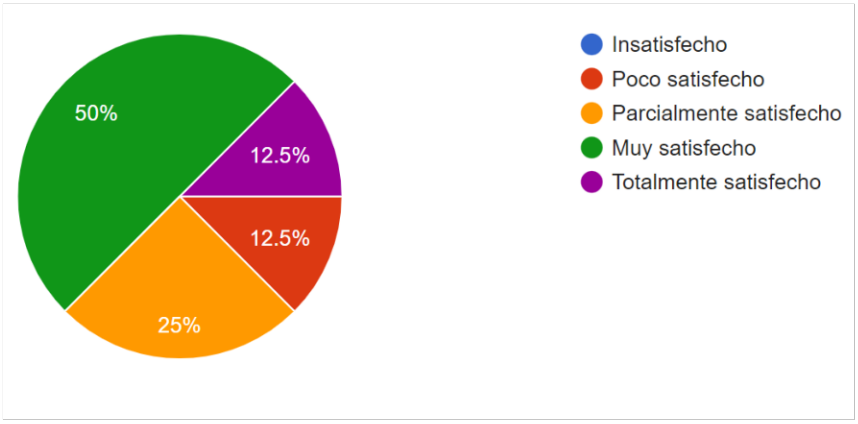


Figura 103: Resultado de la tabulación de la Pregunta 8.
Fuente: El tesista

Pregunta 9

¿Basándose en la propuesta, piensa que optimizara el número incidentes detectados vs número de incidentes controlados por el sistema?

La Figura 104 muestra el resultado de la tabulación de la Pregunta 9, que indica que el 50% de los expertos está muy satisfecho con los resultados, mientras que el 37.5% está parcialmente satisfecho, y el 12.5% está parcialmente satisfecho.

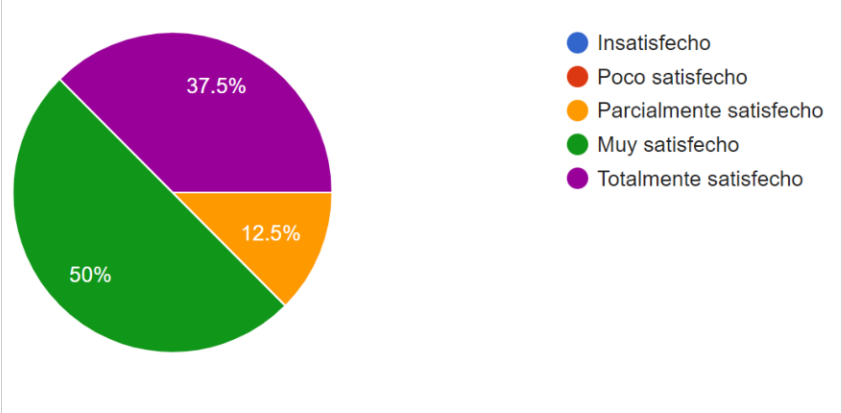


Figura 104: Resultado de la tabulación de la Pregunta 9.
Fuente: El tesista

Pregunta 10

¿Basándose en la propuesta, piensa que se optimizara el nivel de confiabilidad del diseño, configuración y programación de equipos virtuales de la red de seguridad?

La Figura 105 muestra el resultado de la tabulación de la Pregunta 10, que indica que el 50% de los expertos está muy satisfecho con los resultados, mientras que el 37.5% está parcialmente satisfecho, y el 12.5% está parcialmente satisfecho.

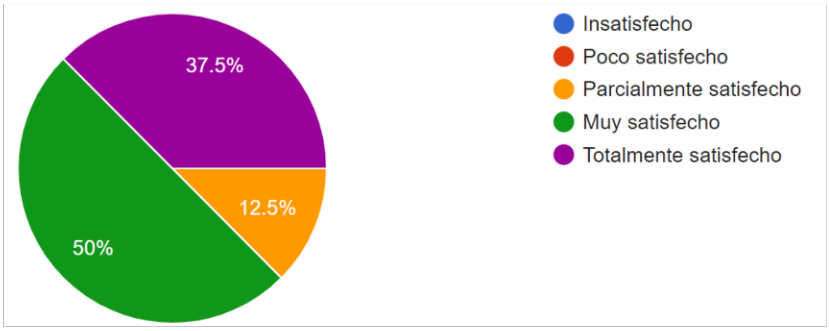


Figura 105: Resultado de la tabulación de la Pregunta 10.
Fuente: El tesista

9.5 ANEXO 5

ENCUESTA

Indicaciones

La encuesta es de carácter anónimo, que permitirá conocer si la propuesta que se adjunta está adecuadamente planteada y los resultados de la misma serán usados estrictamente para el desarrollo de una tesis de grado.

1. ¿Considera usted que el sistema domótico propuesto, es el adecuado y mejoraría la seguridad del tercer piso del edificio?

   - ☐ Insatisfecho
   - ☐ Poco satisfecho
   - ☐ Parcialmente satisfecho
   - ☐ Muy satisfecho
   - ☐ Totalmente satisfecho

2. ¿Piensa que el proceso adoptado para el planteamiento del sistema domótico, es el apropiado?

   - ☐ Insatisfecho
   - ☐ Poco satisfecho
   - ☐ Parcialmente satisfecho
   - ☐ Muy satisfecho
   - ☐ Totalmente satisfecho

3. ¿Considera que el sistema domótico planteado cumple con la normativa KNX?

   - ☐ Insatisfecho
   - ☐ Poco satisfecho
   - ☐ Parcialmente satisfecho
   - ☐ Muy satisfecho
   - ☐ Totalmente satisfecho

4. ¿Considera que una posterior implementación del sistema domótico planteado, mejoraría la seguridad y gestión del tercer piso?

   - ☐ Insatisfecho
   - ☐ Poco satisfecho
   - ☐ Parcialmente satisfecho
   - ☐ Muy satisfecho
   - ☐ Totalmente satisfecho

5. ¿Los niveles de calidad de señal alámbrica e inalámbrica mejorarían con la implementación de la propuesta?

   - ☐ Insatisfecho
   - ☐ Poco satisfecho
   - ☐ Parcialmente satisfecho
   - ☐ Muy satisfecho
   - ☐ Totalmente satisfecho

6. ¿Habría un ahorro en el presupuesto de cables y equipos KNX con la implementación de la propuesta?

   - ☐ Insatisfecho
   - ☐ Poco satisfecho
   - ☐ Parcialmente satisfecho
   - ☐ Muy satisfecho
   - ☐ Totalmente satisfecho

7. ¿Con la nueva propuesta la seguridad de la red mejoraría frente al porcentaje de intrusión detectada?

   - ☐ Insatisfecho
   - ☐ Poco satisfecho
   - ☐ Parcialmente satisfecho
   - ☐ Muy satisfecho
   - ☐ Totalmente satisfecho

8. ¿Considera que todas las habitaciones están con elementos de domótica implementados?

Insatisfecho	☐
Poco satisfecho	☐
Parcialmente satisfecho	☐
Muy satisfecho	☐
Totalmente satisfecho	☐

9. ¿Basándose en la propuesta, piensa que optimizara el número incidentes detectados vs número de incidentes controlados por el sistema?

Insatisfecho	☐
Poco satisfecho	☐
Parcialmente satisfecho	☐
Muy satisfecho	☐
Totalmente satisfecho	☐

10. ¿Basándose en la propuesta, piensa que se optimizara el nivel de confiabilidad del diseño, configuración y programación de equipos virtuales de la red de seguridad?

Insatisfecho	☐
Poco satisfecho	☐
Parcialmente satisfecho	☐
Muy satisfecho	☐
Totalmente satisfecho	☐