KNX NATIONAL ESPAÑA

Soluciones inteligentes para viviendas y edificios.
Global. Seguro. Conectado.

Únase a **nosotros**
www.knx.es

KNX SECURE

Ciberseguridad para sistemas de control y automatización en viviendas y edificios

ÍNDICE

Seguridad en instalaciones domóticas / inmóticas

¿Por qué es tan importante hablar de seguridad en instalaciones domóticas o inmóticas?

- La demanda de soluciones *"Smart Home / Smart Building"* está en auge a un ritmo vertiginoso.

- Cada vez más se añaden aplicaciones que manejan información crítica:

  Códigos de acceso
  Parámetros de alarmas
  Videoporteros
  Estado contactos puertas / ventanas
  Consumos de energía, agua, …
  Otros códigos o passwords personales

- Cada vez más se añaden aplicaciones que requieren un acceso remoto, que representa el punto más vulnerable de una instalación:

  Control simultáneo de varios edificios
  Conexión a BMS
  Control vía Smartphone
  Mantenimiento a distancia
  Internet of Things

- Cualquier tecnología de comunicación puede ser hackeada, y por lo tanto también los sistemas de control y automatización de viviendas y edificios.

Seguridad en instalaciones domóticas / inmóticas

Noticias aparecidas en diversos medios de comunicación

KIM ZETTER SECURITY 07.17.14 6:30 AM

HERE'S HOW EASY IT COULD BE FOR HACKERS TO CONTROL YOUR HOTEL ROOM

BUSINESS INSIDER UK — TECH

Smart home devices could put you in danger

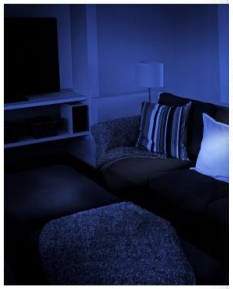
Cadie Thompson
Jul. 15, 2015, 11:39 PM 289

FACEBOOK LINKEDIN TWITTER EMAIL

Smart home products are supposed to help keep you safe, but some of these connected devices could put you in danger.

As home automation products flood the market, there's growing concern that these internet connected devices — like smart cameras and thermostats — are an easy target for hackers because they lack basic security measures.

"Really, the state of security on these things right now is pretty atrocious," Colby Moore, a security research engineer at the cybersecurity firm Synack, told Business Insider.



Poor security on smart home devices can enable aren't at home.

Home > Security

Smart home hacking is easier than you think

RELATED

How to keep your connected home safe: 7 steps you can take to boost home...

What can I do with home

INTERNET

Un 'hacker' español piratea un hotel de lujo en China

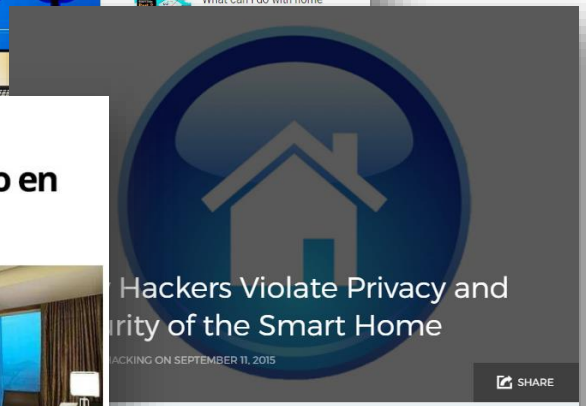
Jesús Molina, que trabaja como asesor independiente en San Francisco, asegura que pudo hacerlo porque el estándar de domótica que utilizaba el establecimiento fue diseñado en los 90

MICHAEL MCLOUGHLIN | MADRID
@MICHAELMCSAEZ
3 agosto 2014 16:05

El hotel 'hackeado', St. regis en Shezhen, en Hong Kong. / Hotel St Regis

Que si un agujero en Whatsapp, que si una brecha en los sistemas de Facebook, que si han conseguido eludir los sistemas de bloqueo del iPhone... Cada cierto tiempo, salta la noticia de que algún experto informático ha sacado los colores a los responsables de seguridad de alguna que otra empresa de internet tras andar escrutando las entrañas de su código fuente.

Unas de las últimas muescas que se han grabado en este palmarés de 'hackers' es la de un analista español de 37 años natural de Ciudad Real. Jesús Molina, que reside en Estados Unidos desde hace una década, ha conseguido piratear el sistema por el que se controlan las habitaciones de un hotel chino. Y no en cualquier local, si no en un cinco estrellas como St. Regis de Shénzhen, una urbe cercana a la cosmopolita Hong-Kong.



Hackers Violate Privacy and rity of the Smart Home

ACKING ON SEPTEMBER 11, 2015

SHARE

chnology Invades Our Living Room

rowth of the paradigm of the Internet of Things is influencing in a way our concept of "house." Modern homes are full of smart devices and a ation of smart appliances promises to make our life easier and more e, but we cannot underestimate that risk of cyber attacks.

ns for home automation are flooding the market, but these devices in the majority of cases lack security; security experts are aware that smart cameras and meters are an easy target for hackers.

Seguridad en instalaciones domóticas / inmóticas

Teoría vs. Práctica

- En la teoría:
  Todos los sistemas basados en tecnologías de comunicación son susceptibles a ser pirateados (y muchos ya lo han sido):

  Bancos
  Google
  WhatsApp
  NASA
  Visa, Mastercard, …
  Apple
  Facebook
  y un largo etc.

- En la práctica:
  ¿Cuál es el riesgo de pirateo informático en una instalación residencial (domótica)?

  Probabilidad baja, a no ser que exista una conexión a internet o existan dispositivos instalados en el exterior con fácil acceso.

  ¿Cuál es el riesgo de pirateo informático en una instalación terciaria (inmótica)?

  Probabilidad media, sobre todo si existe una conexión a internet o en instalaciones con afluencia fluctuante de personas (p.ej. hoteles).

Seguridad en instalaciones domóticas / inmóticas

Teoría vs. Práctica

- Conclusión:
  Estudiar en cada caso qué tipos de medidas son realmente necesarios para impedir el pirateo informático

- Desde KNX se recomiendan tres tipos de medidas:

  Impedir el acceso físico al bus de comunicación
  Se debería aplicar en prácticamente todas las instalaciones, independiente si es KNX o no.

  Usar las herramientas KNX de programación y configuración
  Aplicar en instalaciones con un riesgo medio.

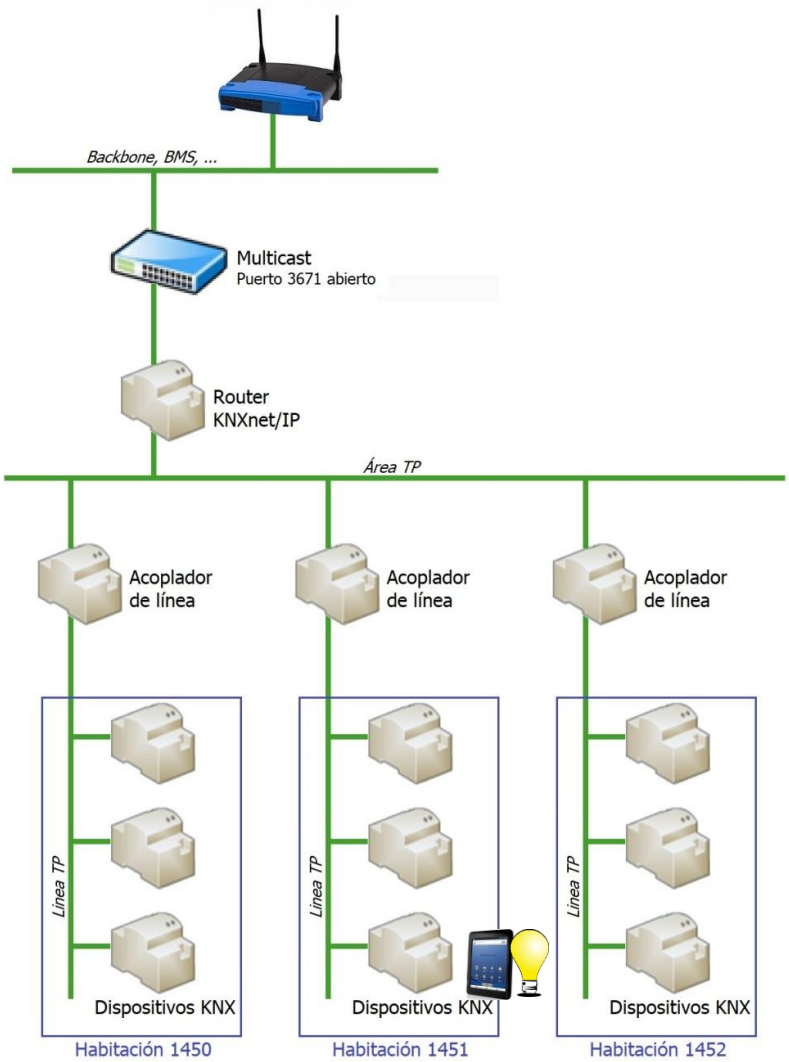
  Nuevo: KNX Data Secure / KNX IP Secure
  Aplicar en instalaciones con un riesgo alto.

- Antes de entrar en detalle:
  Veamos unos casos reales de pirateo informático

ÍNDICE

Escenarios reales de pirateo

Escenario 1



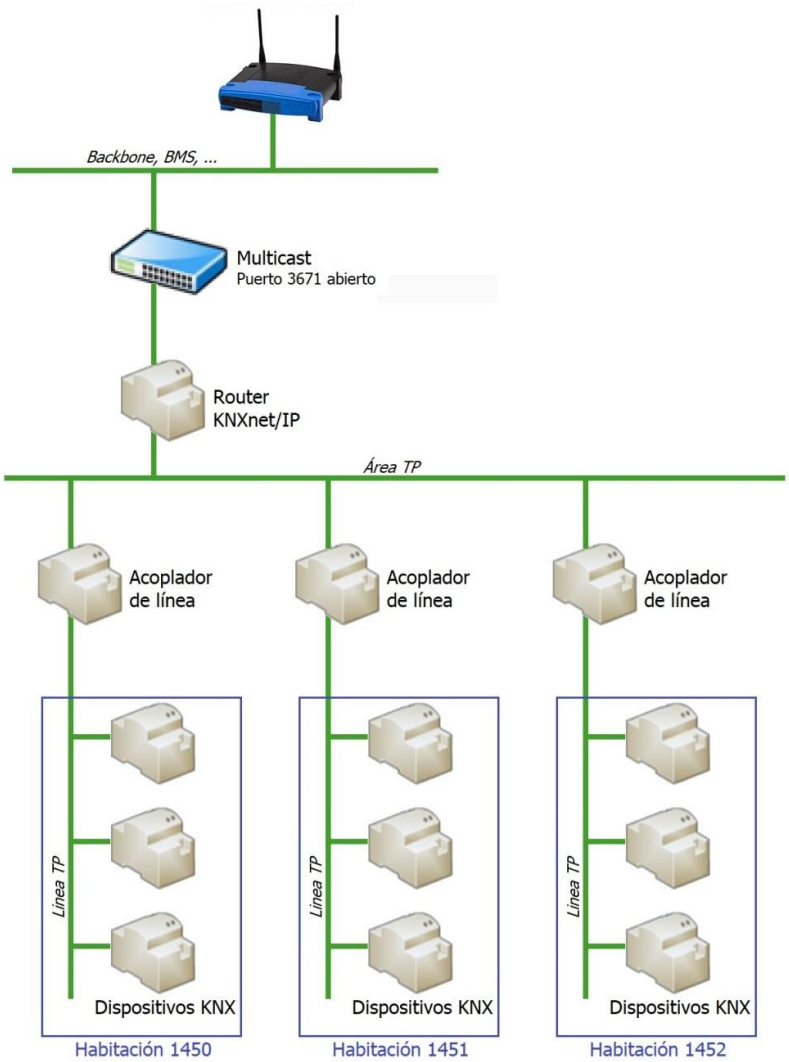
Situación:

- Dispositivos KNX controlan varias funciones (iluminación, climatización, persianas, etc.) en cada habitación de un hotel. A través de una línea principal (p.ej. BMS) se controlan todas las habitaciones.
- El cliente recibe una tablet para controlar las funciones dentro de su habitación ("Butler-App").
  Ejemplo: el cliente ocupa la habitación 1451, y desde su tablet enciende la luz
- El cliente recibe también una contraseña WiFi para acceder con su portátil a internet.

- Hasta ahí – todo bien.

Escenarios reales de pirateo

Escenario 1

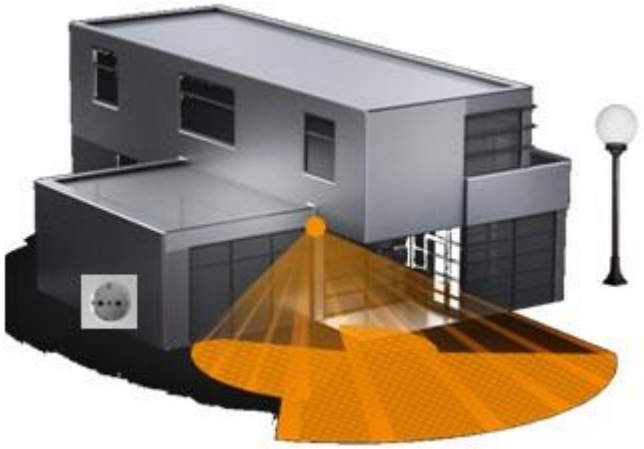


Pirateo informático:

- Es evidente que la tablet de su habitación usa una conexión WiFi para controlar las funciones
- El hacker tiene amplios conocimientos informáticos, y también conoce en detalle el sistema KNX. Con su portátil detecta que se ha usado el puerto 3671, que es un puerto abierto para comunicaciones multicast.
- El hacker pide una nueva habitación, y desde ahí puede controlar las funciones de la habitación anterior usando la contraseña de esa habitación.
  Ejemplo: desde su nueva habitación 1452 enciende la luz de la habitación 1451.

Escenarios reales de pirateo

Escenario 2

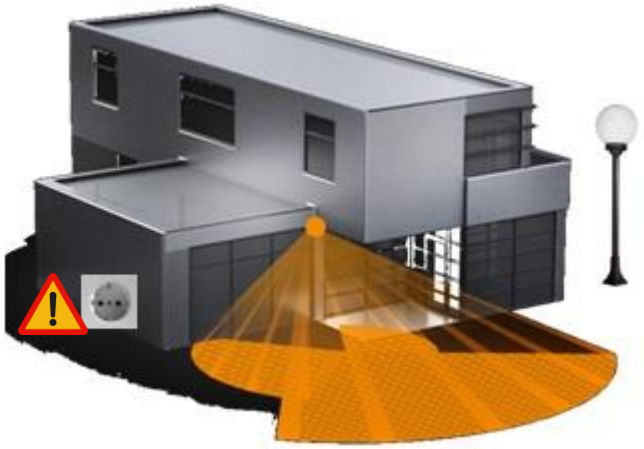


Situación:

- En una vivienda unifamiliar, KNX controla prácticamente todas las funciones dentro de la vivienda.
- KNX controla también algunas aplicaciones en el exterior, como por ejemplo el alumbrado, un detector de movimiento, así como una toma de corriente.
- Hasta ahí – todo bien.

Escenarios reales de pirateo

Escenario 2



Pirateo informático:

- Los dispositivos KNX exteriores no se han protegido adecuadamente para impedir el acceso físico al bus KNX.
- El hacker desmonta la toma de corriente y tiene acceso al bus KNX.
- Con las herramientas y conocimientos adecuados puede tomar el control sobre toda la instalación, modificar parámetros, leer datos, etc.

Escenarios reales de pirateo

¿Se podrían haber evitado estos casos?

¡Por supuesto que sí!

Sobre todo si se tienen en cuenta las medidas que recomienda y ofrece KNX para proteger su instalación.

ÍNDICE

Medidas de seguridad

Medidas simples para impedir el acceso al bus

En el caso de usar el Par Trenzado (Twisted Pair TP) como medio de comunicación, los finales del cable bus nunca deben ser visibles.

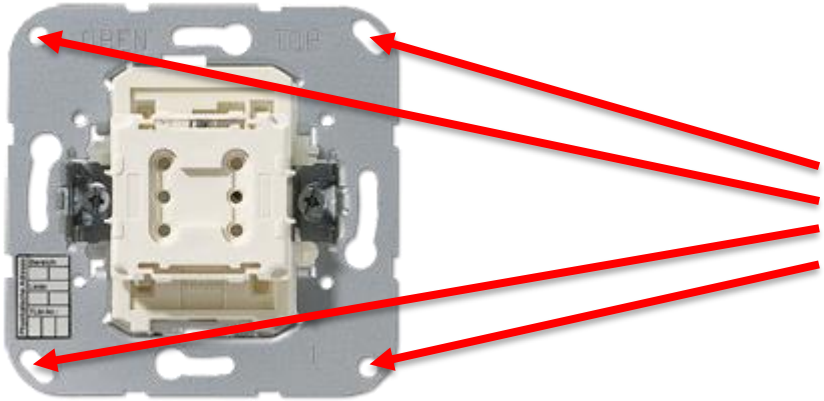
Cables sueltos son una puerta de entrada para hackers

Los cables instalados en el exterior deben ser especialmente protegidos para impedir cualquier tipo de acceso

Medidas de seguridad

Medidas simples para impedir el acceso al bus

Los dispositivos deben ser fijados adecuadamente para evitar que se puedan desmontar de forma fácil.



Atornille todos los dispositivos de forma segura, usando por ejemplo tornillos antirrobo.

Medidas de seguridad

Medidas simples para impedir el acceso al bus

Hay una gran variedad de accesorios que evitan que se pueda desmontar un dispositivo.

Use tornillos y tuercas antirrobo que no pueden ser removidos, o sólo con herramientas especiales

Medidas de seguridad

Medidas simples para impedir el acceso al bus

Los cuadros eléctricos equipados con dispositivos KNX deben estar cerrados con llave, y/o ubicados en espacios con acceso restringido.

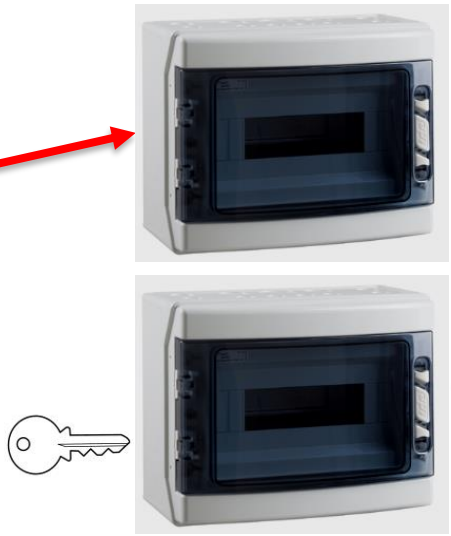
Instale el cuadro eléctrico en sitios con acceso sólo para personas autorizadas

Siempre que sea posible, cierre y bloquee con llave la puerta del cuadro eléctrico

Medidas de seguridad

Medidas simples para impedir el acceso al bus

Si no puede ubicar los cuadros eléctricos en espacios con acceso restringido, use dos cuadros independientes.



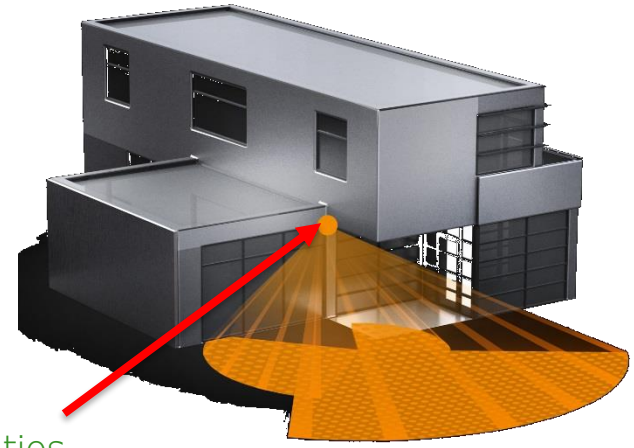
Cuadro eléctrico con elementos accesibles a todo el público, por ejemplo magneto-térmicos

Cuadro eléctrico con dispositivos KNX y otros elementos de seguridad, cerrado con llave

Medidas de seguridad

Medidas simples para impedir el acceso al bus

Los dispositivos instalados en el exterior (sensores de movimiento, estaciones meteorológicas, cámaras de video-vigilancia, alumbrado, interruptores, tomas de corriente, etc.) son una puerta de entrada preferida para hackers.

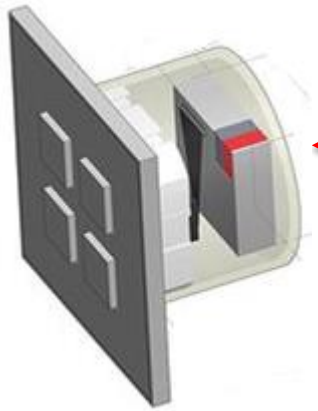


Ubique los dispositivos en sitios de difícil acceso (p.ej. a gran altura), y/o protéjalos adecuadamente

Medidas de seguridad

Medidas simples para impedir el acceso al bus

En caso necesario, como alternativa a los dispositivos con BCU incorporada, puede usar dispositivos convencionales conectados a entradas binarias instaladas en espacios de difícil acceso.



Dispositivos con la BCU incorporada permiten un acceso directo al bus KNX, si ese dispositivo se puede desmontar con facilidad

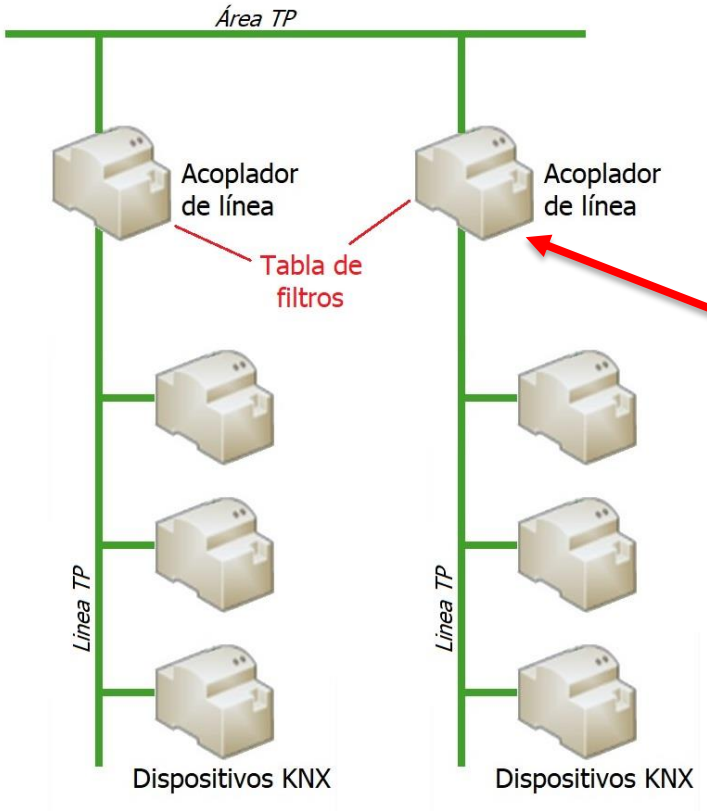
Entradas binarias permiten el uso de dispositivos convencionales y evitan el acceso al bus

ÍNDICE

Medidas de seguridad

Medidas mediante configuración / programación

Par Trenzado *(Twisted Pair TP)*:
Para dispositivos instalados en áreas de poca vigilancia (exterior, parkings, lavabos, almacén, etc.) se puede prever una línea independiente.



Las tablas de filtro en los acopladores de línea evitan que un hacker tenga acceso a toda la instalación

Medidas de seguridad

Medidas mediante configuración / programación

Línea de fuerza *(Power Line PL)*:
Se recomienda el uso de filtros electrónicos para filtrar las señales entrantes y salientes.

Con el uso de filtros electrónicos, los telegramas se limitan a una única línea

Medidas de seguridad

Medidas mediante configuración / programación

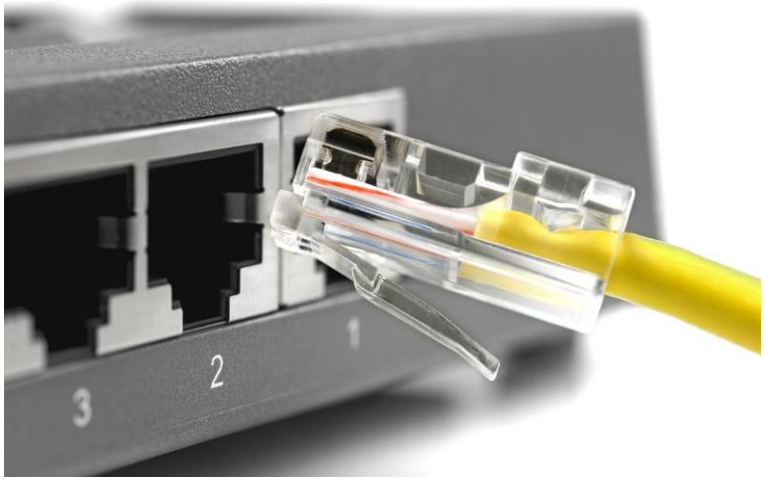
Radiofrecuencia *(Radio Frequency RF)*:
Dado que la transmisión inalámbrica por radiofrecuencia es un medio abierto, no hay medidas de protección físicas para aumentar la seguridad.

Ver las medidas que se mencionan más adelante

Medidas de seguridad

Medidas mediante configuración / programación

Comunicación IP a través de Ethernet:
Sistemas de automatización de edificios deberían usar una red LAN o WLAN independiente con su propio hardware (acopladores, enrutadores, …).



Use los mecanismos de protección conocidos para redes IP:

- Filtros MAC
- Encriptación del WLAN (WPA2)
- Cambiar y ocultar SSID

Medidas de seguridad

Medidas mediante configuración / programación

Comunicación IP a través de Internet:

KNXnet/IP no se ha concebido para la comunicación masiva a través de internet:
→ No es aconsejable abrir puertos de enrutadores hacia internet.

La instalación LAN o WLAN debería estar protegida mediante firewalls.

En caso de que no sea necesario un acceso externo a la instalación, la puerta de enlace predeterminada se puede establecer en 0, bloqueando así cualquier comunicación a internet.

Medidas de seguridad

Medidas mediante configuración / programación

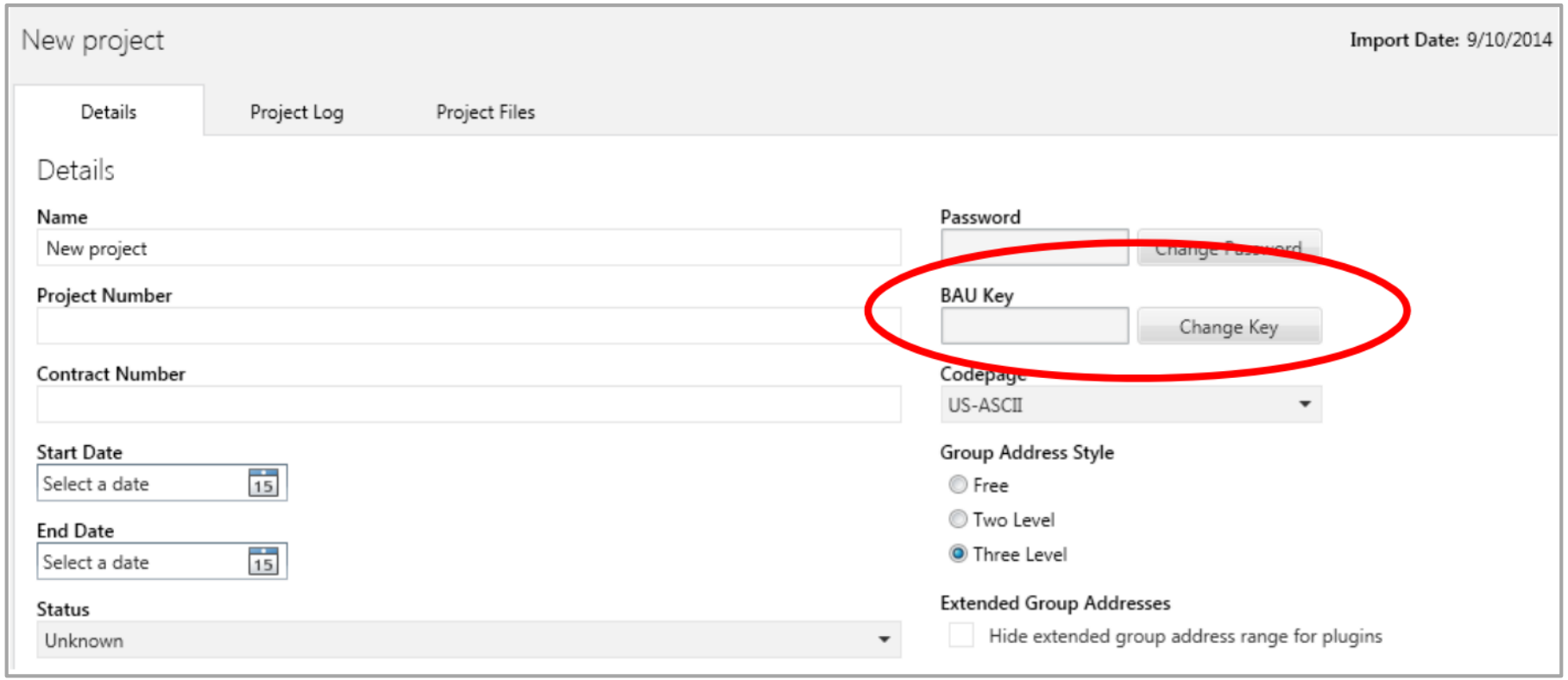
Comunicación IP a través de Internet:

Si, no obstante, es necesario acceder a la instalación a través de internet (por ejemplo, configuración remota), tenga en cuenta:

Asegure que el acceso a la instalación KNX sea a través de conexiones VPN (requiere enrutador o servidor con funcionalidad VPN).

Use soluciones dedicadas de fabricantes específicos (por ejemplo, aquellos que permiten un acceso https).

Protección mediante configuración ETS



ETS permite definir una contraseña de bloqueo específica para cada proyecto.
Esta configuración no puede ser leída / modificada por personas no autorizadas

Medidas de seguridad

Medidas mediante configuración / programación

¡¡¡No invente la rueda!!!

Para proyectos de gran envergadura, no dude en involucrar especialistas en integración de tecnologías IT, para medidas de seguridad adicionales.

ÍNDICE

Medidas de seguridad

KNX Secure

Antes de conocer los detalles…….. ¿qué es AES?

Advanced Encryption Standard (AES):

Se trata de un estándar internacional que describe un algoritmo de encriptación (ISO/IEC 18033-3)

Longitud de la clave: 128 bit

Métodos de encriptación:

- Sustitución de bytes
- Cambio de filas
- Mezcla de columnas
- AddRoundKey

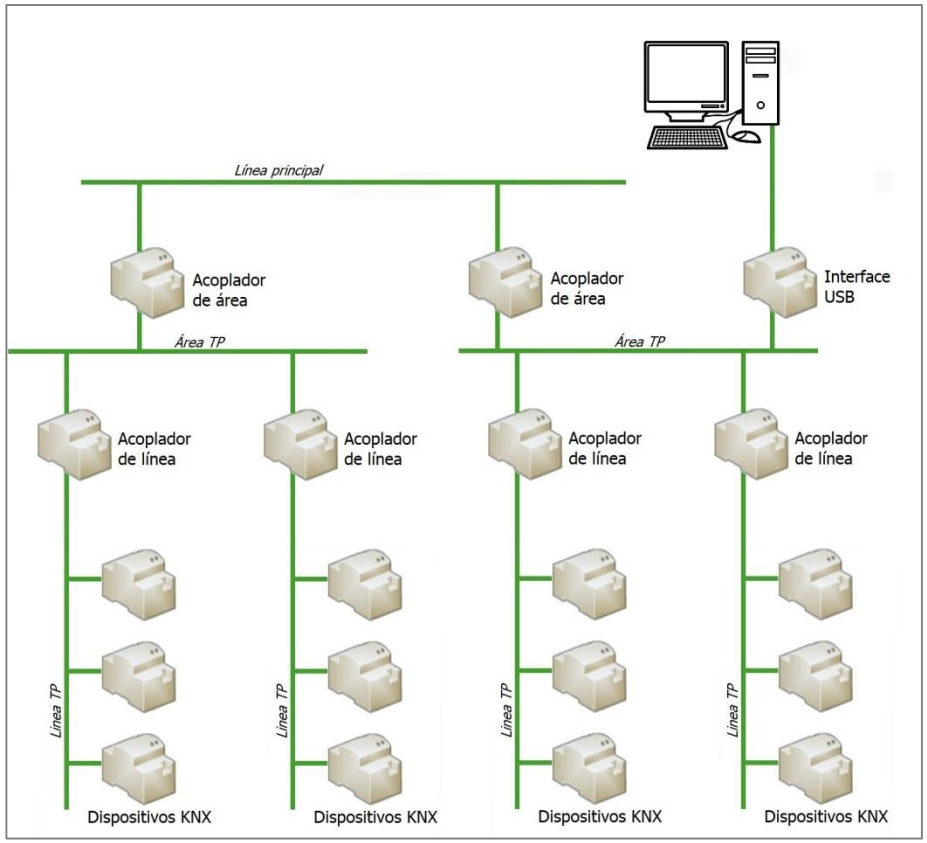
Medidas de seguridad

KNX Secure

KNX ha desarrollado un doble concepto de protección:

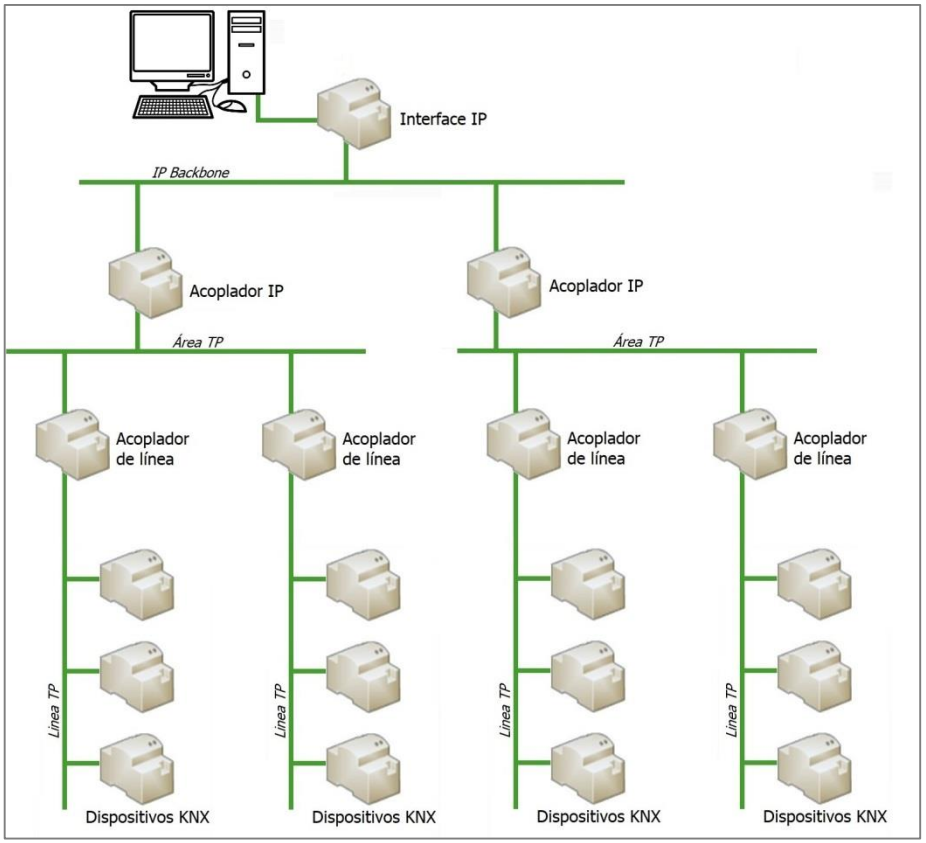
KNX Data Secure

Para instalaciones KNX sin comunicación IP



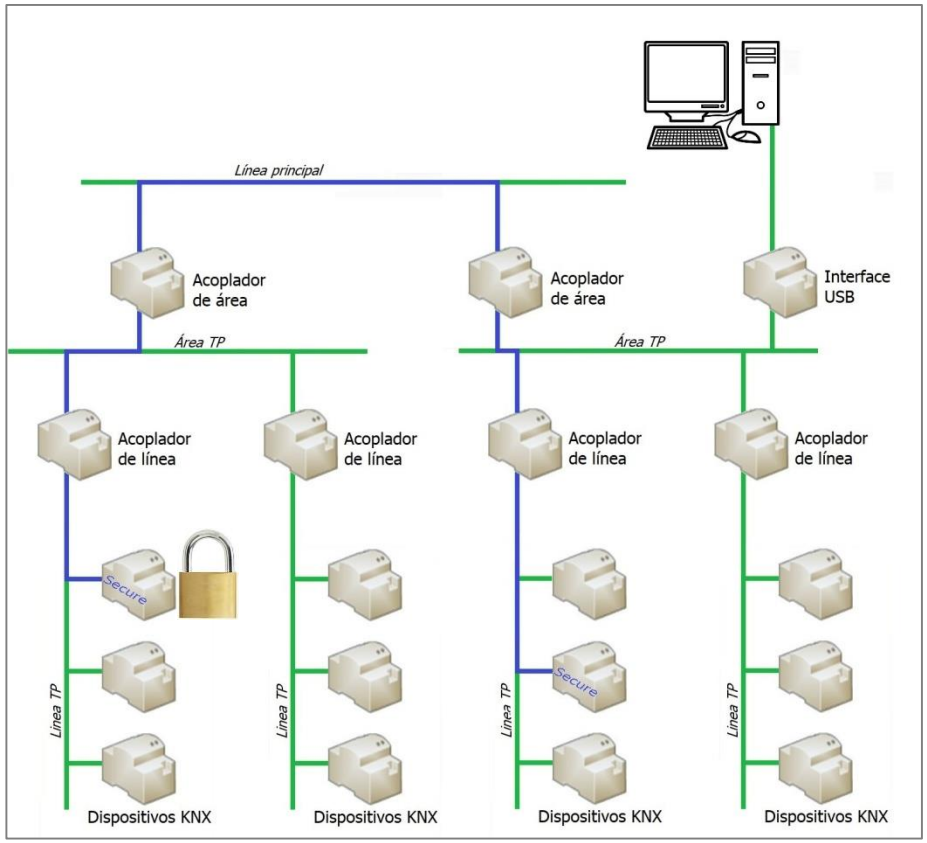
KNX IP Secure

Para instalaciones KNX con comunicación IP



KNX Data Secure

Para instalaciones KNX sin comunicación IP



KNX Data Secure asegura la comunicación dentro de una instalación KNX.

Ejemplo:

Un dispositivo debe enviar un telegrama protegido a otro dispositivo, aunque esté en una línea o incluso área diferente.

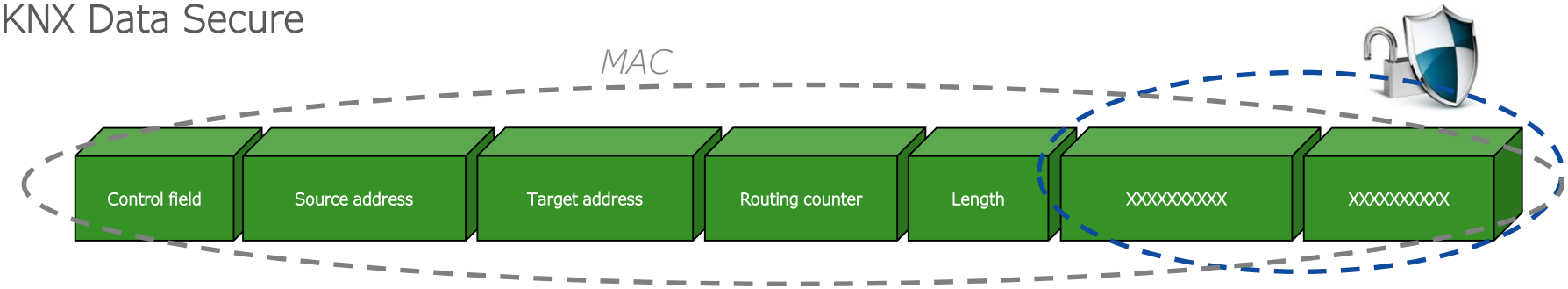
Solución:

En este caso, ambos dispositivos deben ser sustituidos por dispositivos con funcionalidad KNX Data Secure. Dispositivos KNX con y sin funcionalidad KNX Data Secure pueden convivir en una misma instalación.

Medidas de seguridad

KNX Secure

KNX Data Secure



Se encriptan los datos 'útiles' del telegrama KNX, p.ej. una orden de actuación (encender, apagar, subir, bajar, …), o un valor (lectura temperatura), etc.

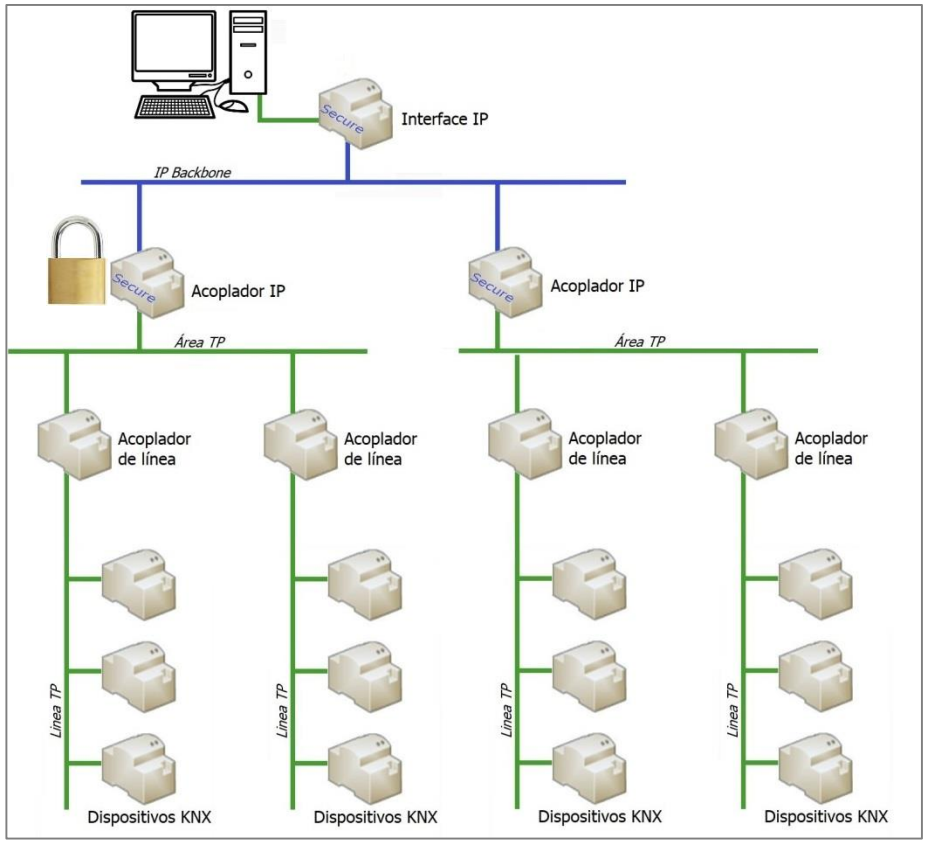
La encriptación es realizada por el dispositivo emisor, y la desencriptación por el dispositivo receptor. Ambos requieren de la funcionalidad KNX Data Secure.

El resto del telegrama no es encriptado, pero asegurado por AES128:

- El telegrama es ampliado por el *Message Authentification Code (MAC)*
- Cualquier manipulación del telegrama provoca una incompatibilidad con el MAC:
  → el telegrama sería inválido

KNX IP Secure

Para instalaciones KNX con comunicación IP



KNX IP Secure asegura la comunicación a través de internet.

Ejemplo:

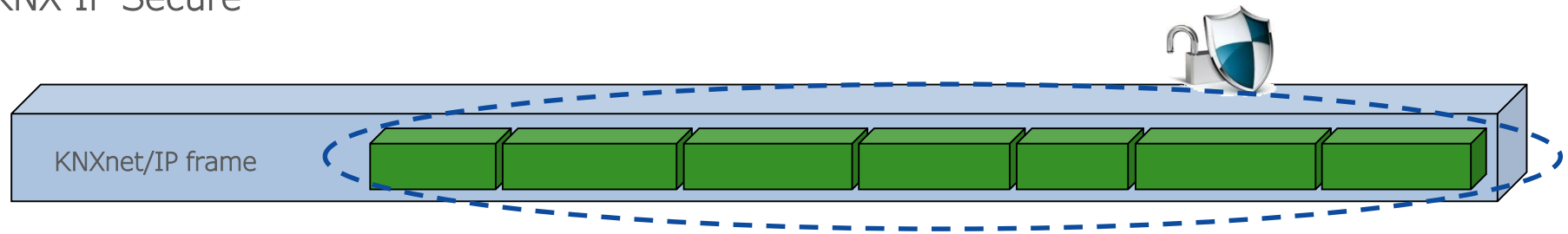
Dos instalaciones KNX están conectadas entre sí mediante comunicación IP. Se requiere una transmisión segura de los telegramas.

Solución:
En este caso, todos los acopladores conectados al IP backbone deben tener la funcionalidad KNX IP Secure.

Medidas de seguridad

KNX Secure

KNX IP Secure



Se encripta el telegrama KNX completo.

El telegrama es encriptado por el enrutador emisor, y desencriptado por el(los) enrutadores receptores. Todos requieren de la funcionalidad KNX IP Secure.

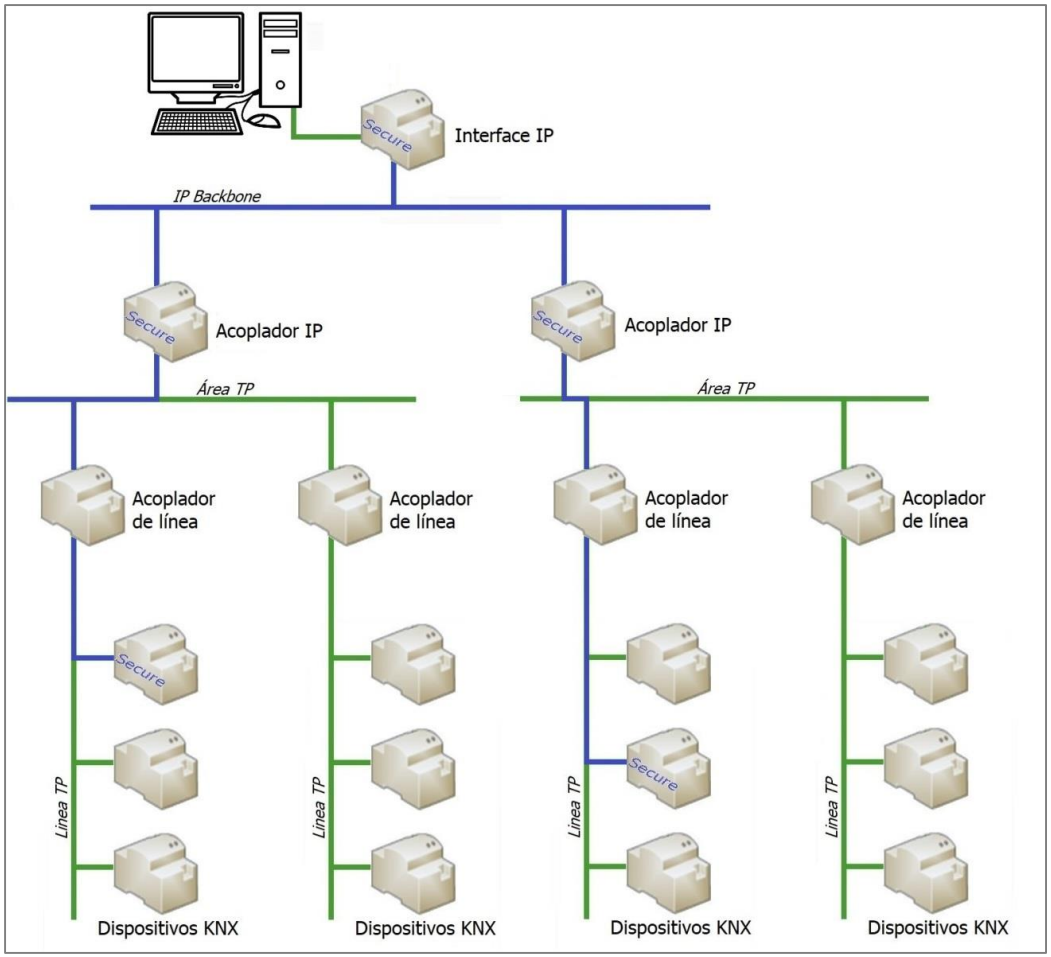
Ninguna persona no autorizada (es decir, sin la clave AES128) puede leer la información cuando se transmite por internet.

Si alguien “inyecta” un telegrama malintencionado no es reconocido por los enrutadores conectados al backbone.

Medidas de seguridad

KNX Secure

KNX Data Secure + IP Secure



KNX Data Secure y KNX IP Secure pueden usarse simultáneamente en una misma instalación KNX.

ÍNDICE

Resumen

Lo más destacado de esta ponencia:

- Cualquier tecnología basada en una comunicación abierta es vulnerable a ser hackeada.
- Existen varios tipos de medidas para proteger una instalación. Hay que analizar proyecto por proyecto qué medidas son las más adecuadas y si son realmente necesarias.
- KNX ofrece varios métodos para aumentar la seguridad de una instalación:
  - Configuración y programación en ETS
  - KNX Data Secure y KNX IP Secure
- Dispositivos con y sin KNX Data Secure pueden convivir en una misma instalación. KNX Data Secure y KNX IP Secure pueden convivir en una misma instalación.
- Ambos sistemas aseguran una comunicación segura entre dispositivos KNX, estén en una misma instalación, o a distancia conectados a través de internet:
  - Se impide que personas no autorizadas puedan leer el contenido de los telegramas KNX.
  - Se impide la infiltración de telegramas manipulados que pretenden obtener el control de la instalación.

Resumen

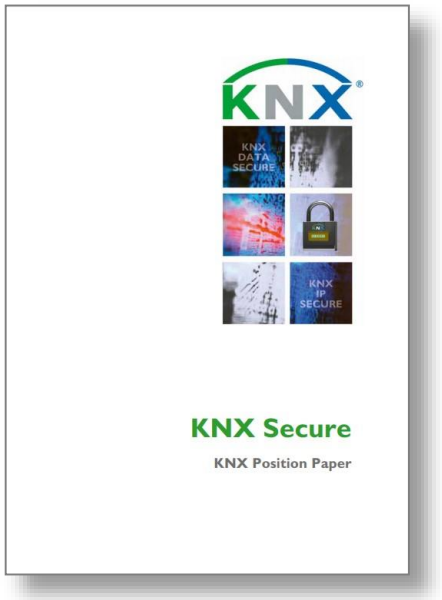
Visite la web de KNX:

https://www.knx.org/knx-es/para-profesionales/beneficios/knx-secure/index.php

Resumen

Descargue gratuitamente más información:

https://www.knx.org/knx-es/para-profesionales/descargas/index.php



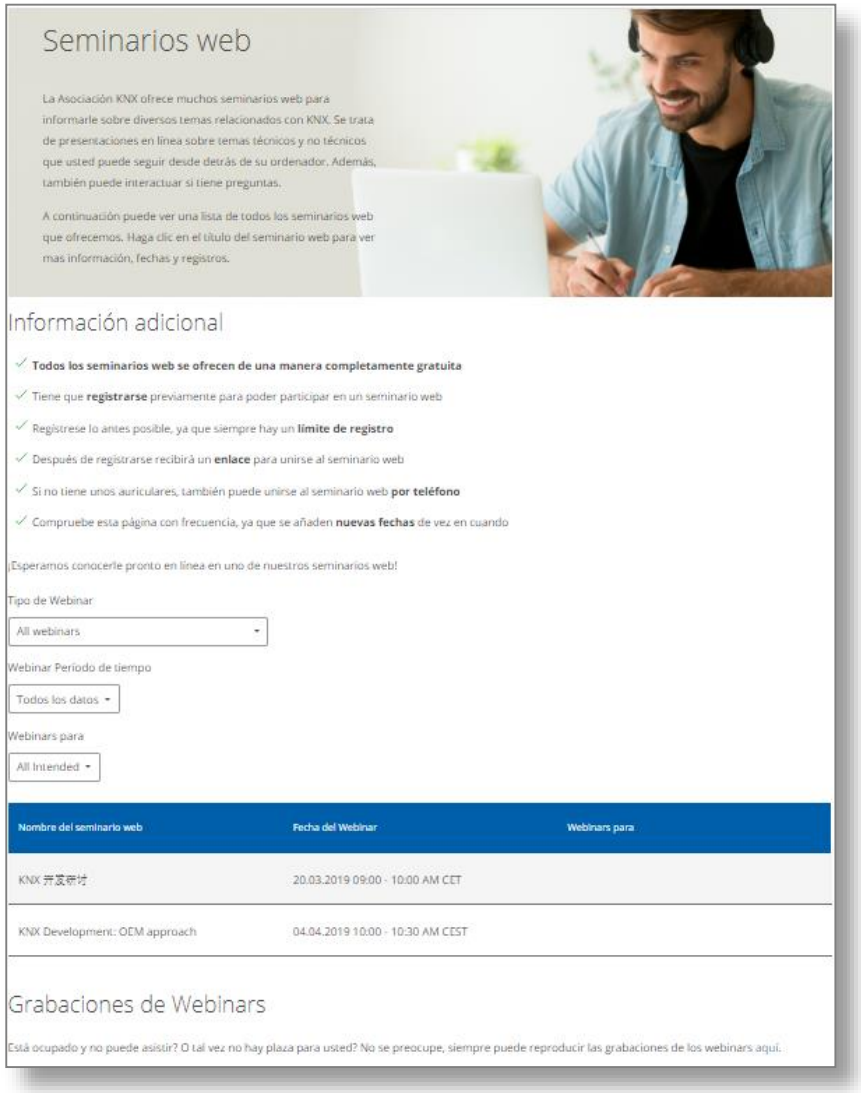
Resumen

¿Desea estar siempre actualizado?

Participe en los webinars gratuitos ofrecidos por KNX Association.

Visite la página con frecuencia, dado que constantemente se van añadiendo nuevos webinars con diferentes temarios y en diferentes fechas.

https://www.knx.org/knx-es/para-profesionales/training/knx-eacademy/webinars/index.php



KNX NATIONAL ESPAÑA

Soluciones inteligentes para viviendas y edificios.
Global. Seguro. Conectado.

Únase a **nosotros**
www.knx.es

¡Muchas gracias por su atención!

Michael Sartor

Secretario Técnico – Asociación KNX España

(+34) 934 050 725

info@knx.es

www.knx.es