KNX NATIONAL ESPAÑA

Soluciones inteligentes para viviendas y edificios.
Globales. Seguros. Conectados.

KNX SECURE

Ciberseguridad en instalaciones de control y automatización de viviendas y edificios

Únase a **nosotros**
www.knx.es

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
  - Estado contactos puertas / ventanas
  - Parámetros de alarmas
  - Consumos de energía, agua, …
  - Videoporteros
  - Contraseñas

- Cada vez más se añaden aplicaciones que requieren un acceso remoto, que representa el punto más vulnerable de una instalación:
  - Control vía Smartphone
  - Control simultáneo de varios edificios
  - Conexión a BMS
  - Mantenimiento a distancia
  - Internet of Things

- Teóricamente, 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

Teoría vs. Práctica

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

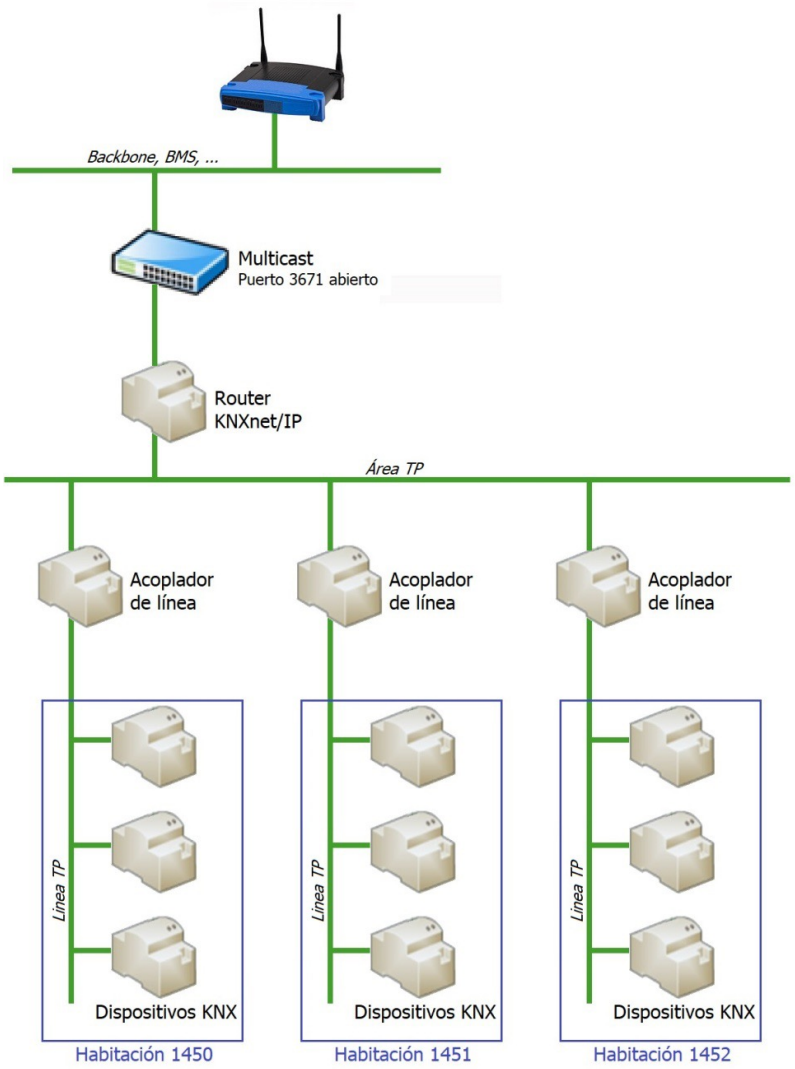
- Desde KNX se recomiendan tres tipos de soluciones:
  - Impedir/dificultar el acceso físico al bus de comunicación:
    → Se deberían aplicar en la mayoría de instalaciones
  - Usar las herramientas KNX de programación y/o configuración:
    → Aplicar en instalaciones con un nivel medio de riesgo
  - KNX Data Secure / KNX IP Secure
    → Aplicar en instalaciones con un nivel alto de riesgo

➢ **Pero antes, veamos unos casos reales …**

Índice

Escenarios reales de pirateo informático

Caso 1



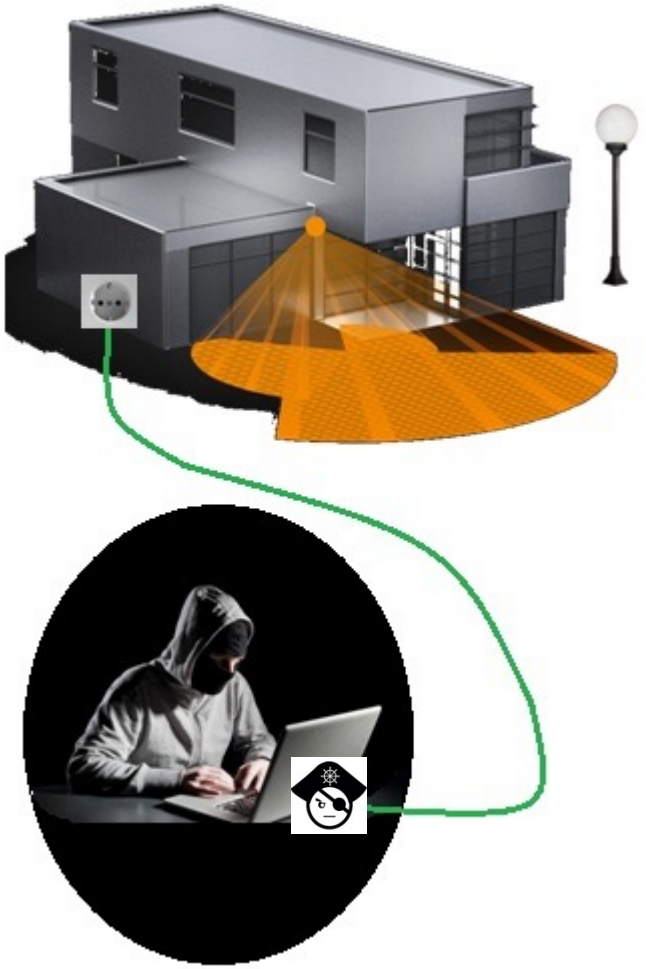
Pirateo Informático:

- Es evidente que la tablet de su habitación usa una conexión WiFi para controlar las funciones.
- El hacker observa que para la conexión Wifi se ha usado el puerto 3671 abierto.
- 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 informático

Caso 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 informático

¿Se podrían haber evitado estos casos?

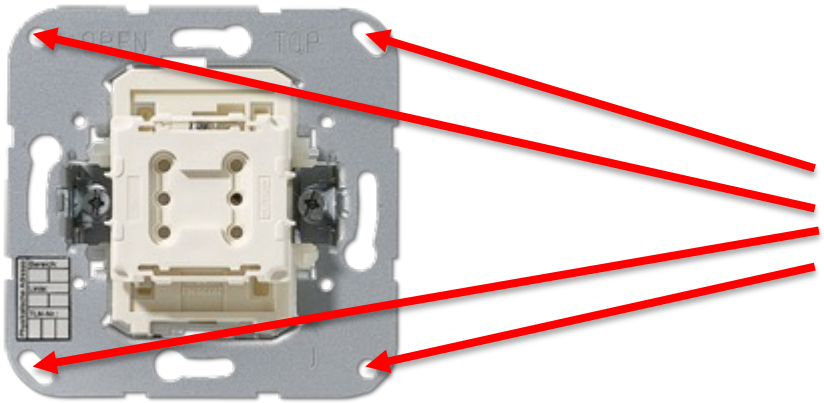
¡¡¡Por supuesto que sí!!!

Teniendo en cuenta los tres tipos de soluciones para proteger su instalación.

Índice

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 simples para impedir el acceso al bus

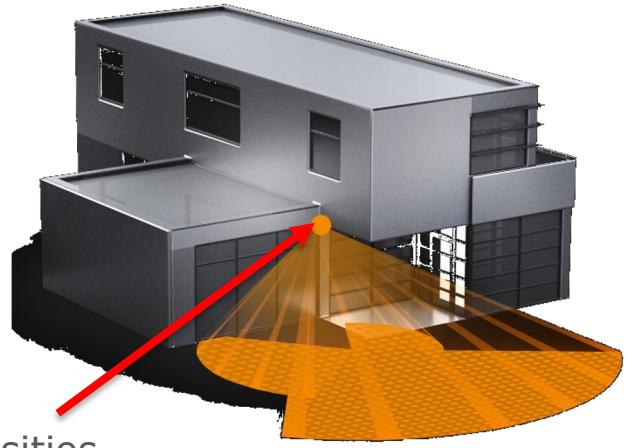
Los cuadros eléctricos equipados con dispositivos de control deben estar cerrados con llave, y/o ubicados en espacios con acceso restringido.

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

Cierre y bloquee con llave la puerta del cuadro eléctrico

Medidas simples para impedir el acceso al bus

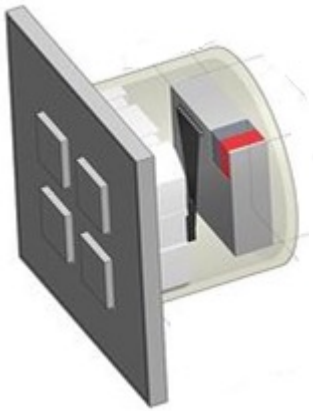
Los dispositivos instalados en el exterior (sensores de movimiento, estaciones meteorológicas, cámaras de video-vigilancia, etc.) son una puerta de entrada preferida para hackers.



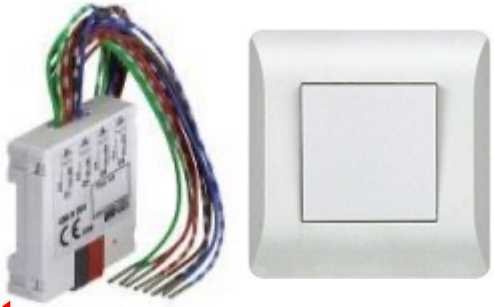
Ubique los dispositivos en sitios de difícil acceso (p.ej. a gran altura), y/o protéjalos adecuadamente

Medidas 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

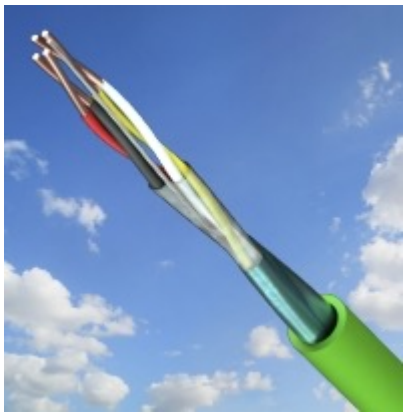


Entradas binarias permiten el uso de dispositivos convencionales y evitan el acceso al bus

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 muy fácil para hackers



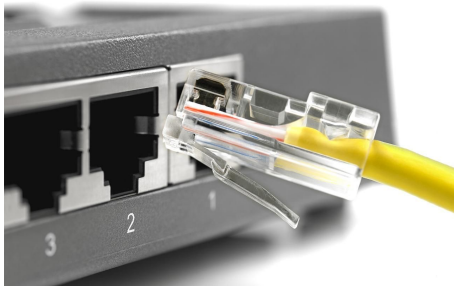
Los cables instalados en el exterior deben ser especialmente protegidos para impedir cualquier tipo de acceso

Índice

Medidas mediante configuración / programación

Comunicación IP a través de Ethernet/Internet:

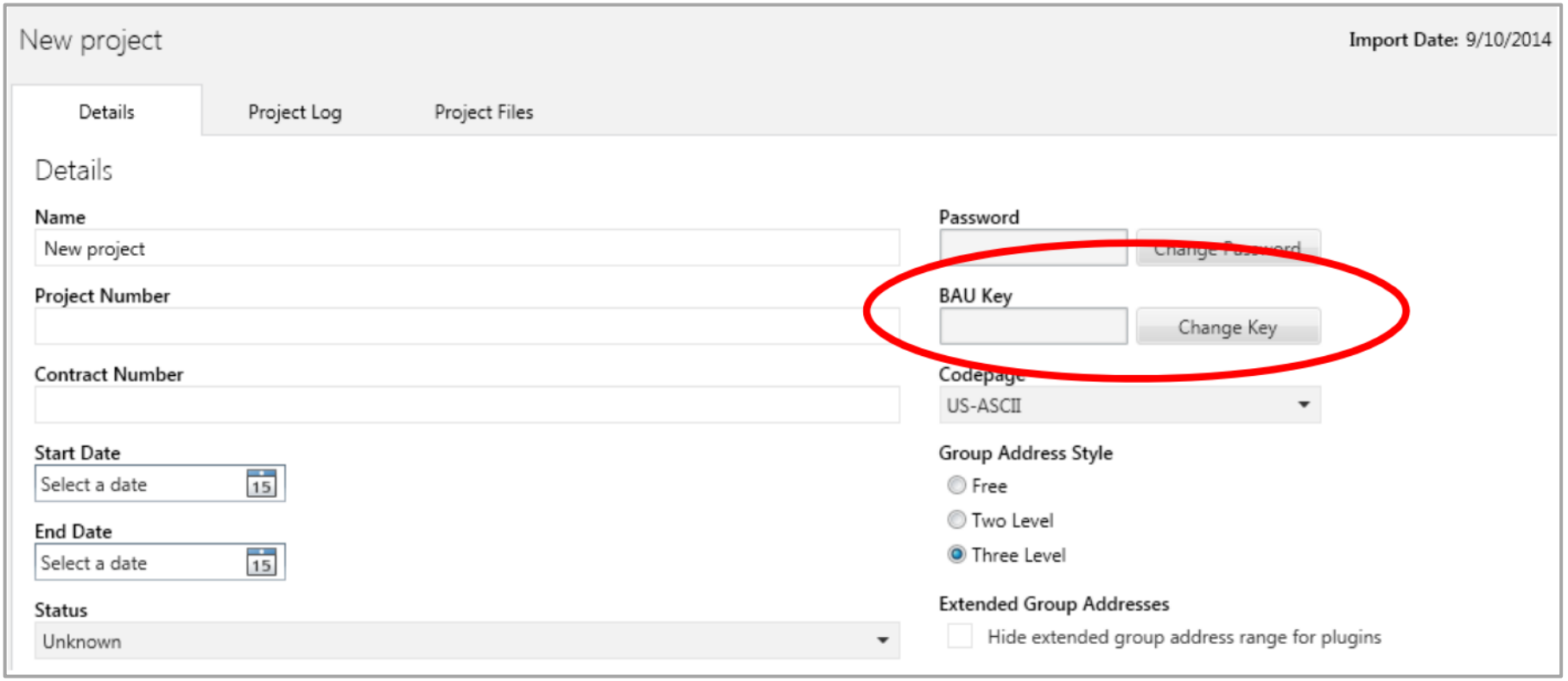
Use una red LAN o WLAN independiente con su propio hardware (acopladores, enrutadores, firewalls, …).



- Use los mecanismos de protección conocidos para redes IP:
  - Filtros MAC
  - Encriptación del WLAN (WPA2)
  - Cambiar y ocultar SSID
- 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.
- Asegure que el acceso a la instalación KNX sea a través de conexiones VPN (requiere enrutador o servidor con funcionalidad VPN).

Medidas mediante configuración / programación

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

Índice

KNX Data Secure / KNX IP 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

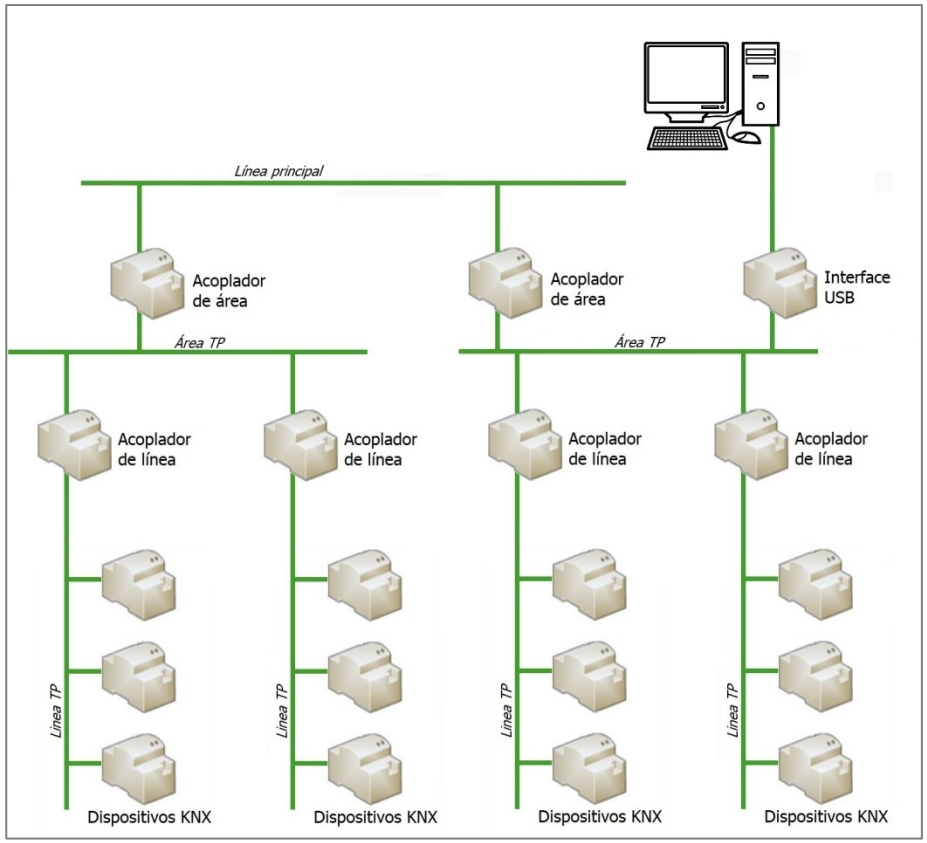
Métodos de encriptación:

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

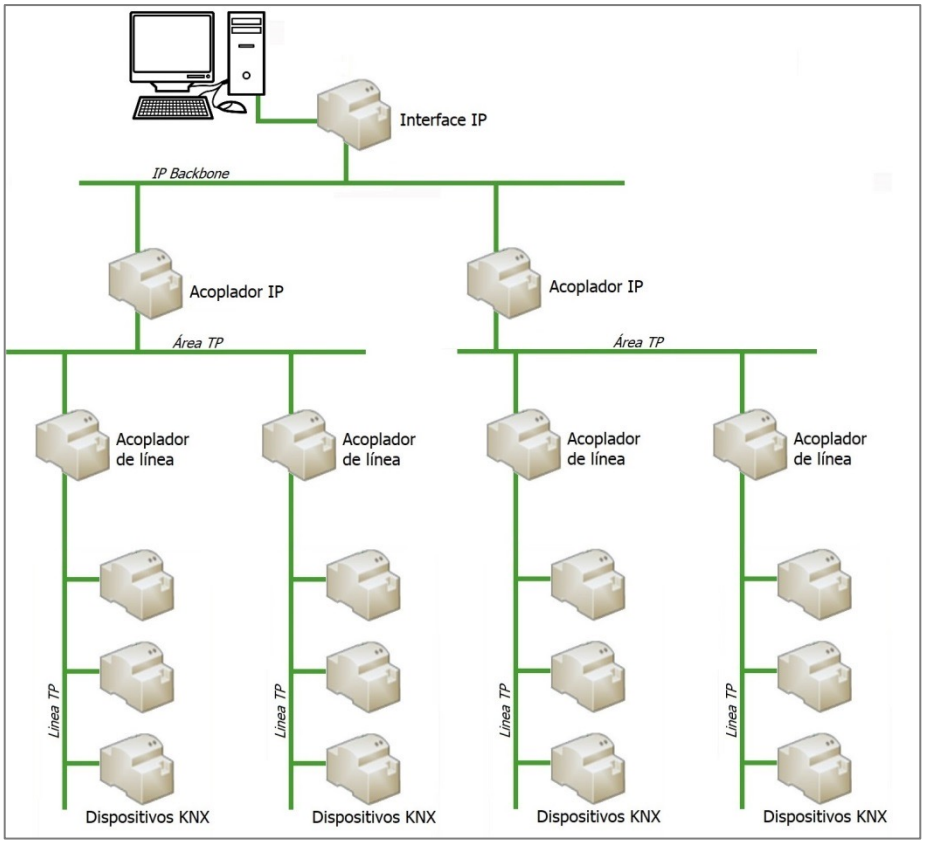
KNX Data Secure / KNX IP Secure

KNX ha desarrollado un doble concepto de protección:

KNX Data Secure, para la comunicación dentro de una instalación KNX



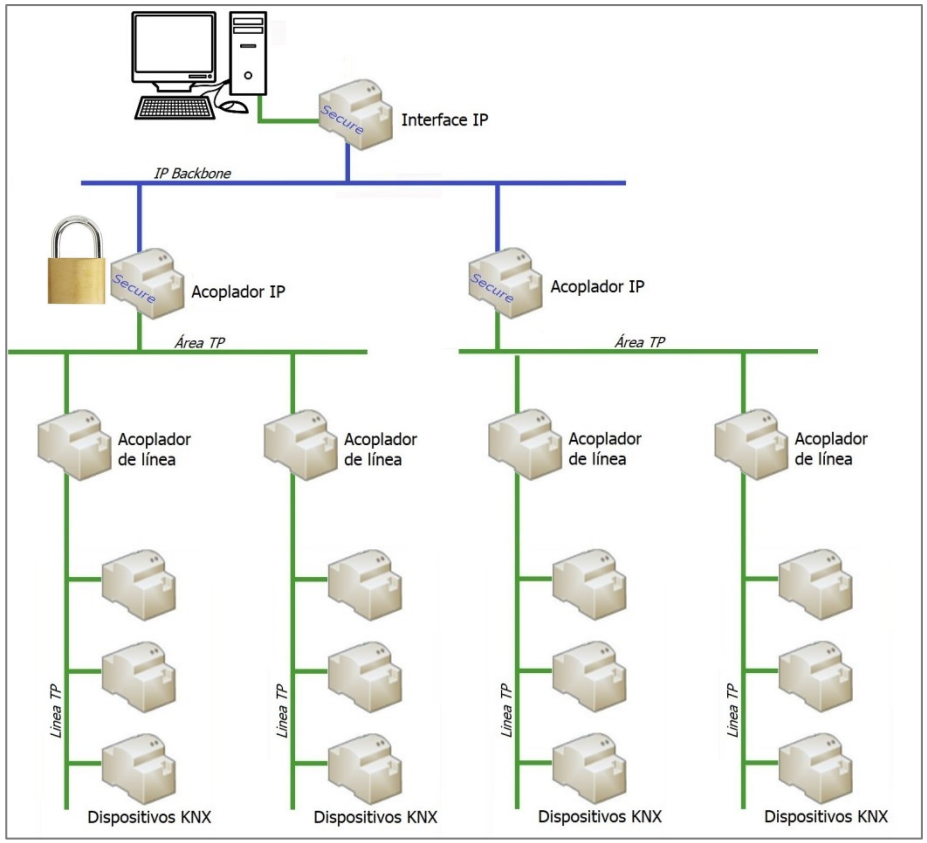
KNX IP Secure, para la comunicación vía IP



KNX Data Secure / KNX IP Secure

KNX IP Secure:

Para la comunicación vía IP

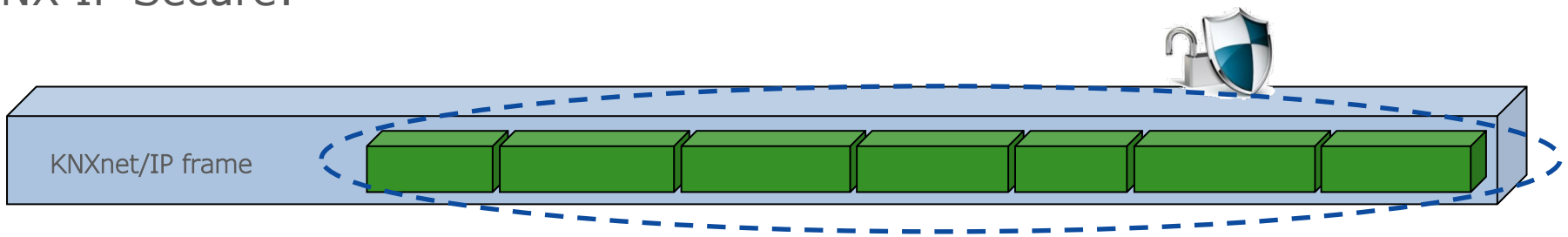


Ejemplo:
Dos instalaciones KNX están conectadas entre sí mediante comunicación IP. Se requiere una transmisión segura de los telegramas.

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

KNX Data Secure / KNX IP Secure

KNX IP Secure:



Se encripta el telegrama KNX completo.

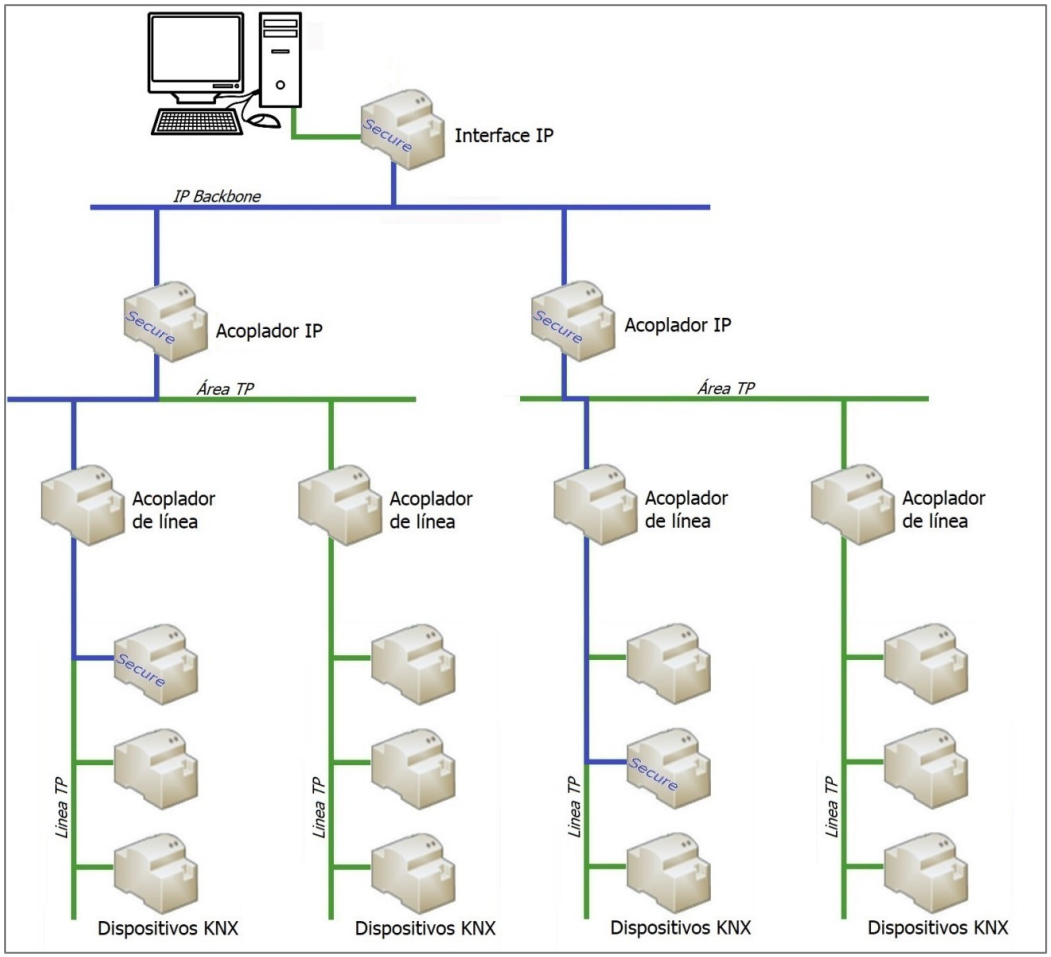
El telegrama es encriptado por el enrutador emisor, y desencriptado por el(los) enrutadores receptores. Todos requieren de la funcionalidad KNX IP Secure.

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.

KNX Data Secure / KNX IP Secure

KNX Data Secure + KNX 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

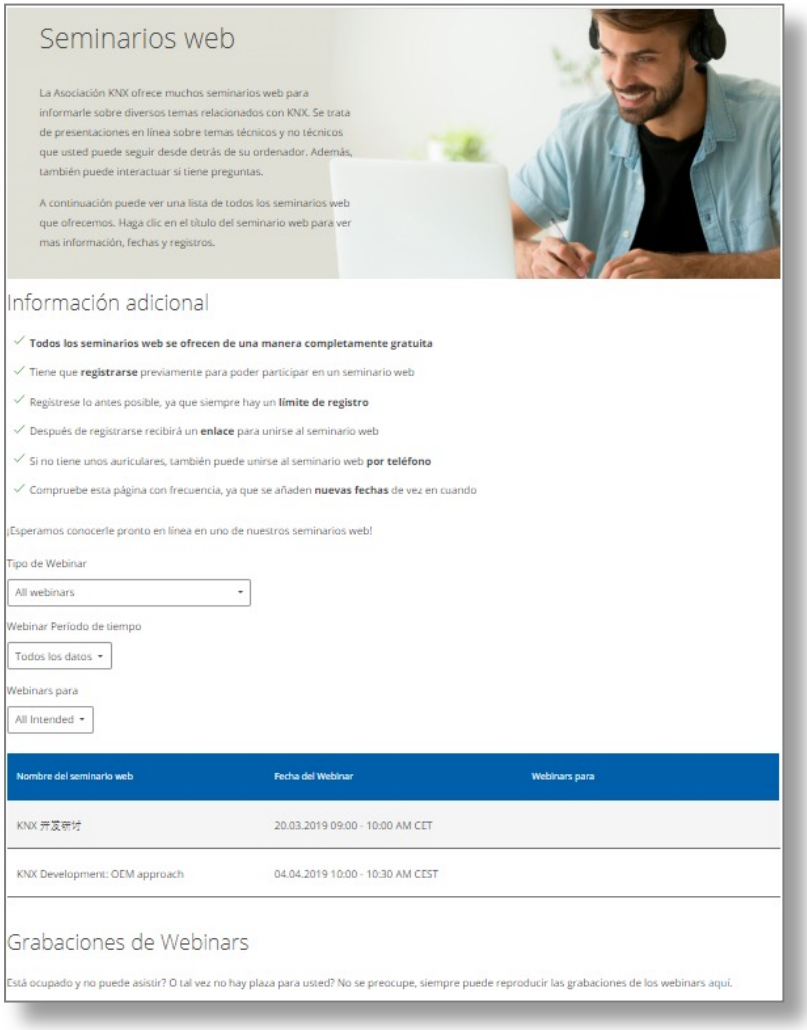
Resumen

¿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.
Globales. Seguros. Conectados.

¡Gracias por su atención!

Antonio -Moreno
Presidente KNX España

info@knx.es