Por **Antonio Moreno**
Presidente de la **Asociación KNX**

RECOMENDACIONES Y PROTOCOLOS DE CIBERSEGURIDAD

Durante las últimas décadas hemos asistido a una rápida evolución social, económica, política y también tecnológica. Lo que era impensable hace pocos años se ha transformado en algo habitual, y eso parece ser la regla que tenemos por delante para un futuro. La tecnología está cambiando muchos aspectos de nuestras vidas, generalmente a mejor, y esa evolución sigue de forma imparable. Cada avance tecnológico sirve de base para el siguiente, y así sucesivamente. Así las cosas, la tecnología no avanza de forma lineal sino exponencial.

Con el foco puesto en la conectividad

Dentro de la tecnología debemos poner el foco en las comunicaciones y, por tanto, en la conectividad. Casi nadie sale a la calle sin un smart phone en el bolsillo, básicamente porque necesitamos estar conectados. Ya no es una opción. Incluso hemos sustituido elementos tradicionales como el monedero y la cartera porque ya no necesitamos llevar encima un calendario, un título de transporte ni el dinero. Todo eso nos lo proporciona el móvil, igual que la hora.

Y este avance tiene aspecto de cobrar nuevos impulsos que le hagan evolucionar más rápido. La propia Unión Europea está poniendo en marcha el "Mecanismo de recuperación y resiliencia", que tiene como objetivo ayudar a superar la actual crisis económica creada por la pandemia dentro de los estados miembros. Del cumplimiento de ese mecanismo va a depender que los estados reciban las abultadas ayudas económicas que van a necesitar para salir de esta situación. Pues bien, uno de los cuatro ejes fundamentales de ese mecanismo de recuperación es precisamente la digitalización, que obviamente se fundamenta en la conectividad.

La domótica y la inmótica en general no son en absoluto ajenas a este contexto, puesto que juegan un papel fundamental en la digitalización de los edificios y viviendas y marcan una clara tendencia de hacia dónde caminan las instalaciones eléctricas. En ese sentido, la tecnología KNX evoluciona de forma constante y los fabricantes que la sustentan trabajan cada día para ofrecer mejores soluciones al mercado; más potentes,

competitivas y en línea con el progreso tecnológico que nos envuelven.

La conectividad ha sido uno de los grandes caballos de batalla en los últimos años, dando como resultado la integración del medio básico de transmisión por par trenzado con otros medios, especialmente con la tecnología IP. Hoy en día ya existen muchas soluciones ioT que se integran dentro del mundo de KNX. Desde el control de iluminación, persianas o clima en remoto hasta envío de alarmas, pasando por el más puro concepto ioT que representa la integración entre varias tecnologías. La más conocida de las cuales pueden ser los asistentes de voz. El hecho de encender una luz con la voz es uno de los mejores ejemplos de conectividad que se pueden dar dentro del ámbito de la domótica.

Incógnitas e incertidumbres

Hoy en día, la conectividad ya es para la domótica una razón de ser en sí misma. Pero también plantea una serie de incógnitas e incertidumbre en el plano de la ciberseguridad que a veces impiden a los usuarios decidirse por la implantación de estas tecnologías. Si ni la instalación ni su conectividad son seguras, entonces podemos temer que cualquiera pueda "colarse" dentro de ella para realizar funciones no autorizadas, e incluso invadir nuestra privacidad. No son temores infundados, si bien es cierto que al menos quien les habla no conoce ningún caso de una instalación domótica que haya sido víctima de un ciberataque. Esa es la realidad.

Entrando ya en ese campo de la ciberseguridad, lo mejor es aplicar de entrada el sentido común. Si tenemos componentes domóticos en un exterior de manera que sean fácilmente manipulables, estaremos dando facilidades para que la instalación sufra ataques o sabotajes. Lo mismo se puede decir en componentes interiores en lugares de pública concurrencia que estén lo suficientemente expuestos y poco protegidos como para que cualquiera los pueda desmontar y actuar. Finalmente, está el tema de las redes WiFi, que sí representan realmente un peligro por la facilidad con que alguien puede llegar a acceder a aparatos no autorizados. En resumen, hay dos cosas que proteger: el medio físico y la red IP.

LA CONECTIVIDAD: UNA OPORTUNIDAD PARA QUE LAS NUEVAS TECNOLOGÍAS HAGAN LA VIDA MÁS FÁCIL, EFICIENTE Y SEGURA

Nace el concepto "KNX Secure"

La organización KNX abordó este tema hace ya años y se puso manos a la obra haciendo, en primera instancia una guía de recomendaciones a seguir para evitar ciberataques, algunas de las cuales ya he mencionado en este artículo. Lo siguiente fue reescribir su protocolo para permitir a los fabricantes crear componentes seguros, capaces de comunicarse entre ellos mediante mensajes encriptados de muy difícil manipulación. Había nacido el concepto "KNX Secure", que hoy ya es una realidad con la salida al mercado de los primeros aparatos que cumplen con ese estándar seguro. Se ha desarrollado a dos niveles. Por un lado, tenemos la vertiente "IP Secure" que encripta la comunicación IP dentro de KNX, incluso si el dispositivo emisor está a mucha distancia del dispositivo receptor y comunicados a través de (por ejemplo) internet. Eso afecta a la comunicación con el sistema desde, por ejemplo, el software de configuración KNX o las visualizaciones. Es decir, estamos evitando la posibilidad de una intervención por parte de un no autorizado que se cuele en la red local.

Por otro lado, está el concepto "Data Secure" que encripta los telegramas que circulan por el propio bus de datos, haciendo así imposible un ciberataque incluso si alguien tiene acceso físicamente al bus y las herramientas de software adecuadas. Si no dispone del proyecto ETS y el password adecuado no podrá interactuar con la instalación de KNX. Así hemos dado respuesta a cualquier temor que pueda haber por parte de un proyectista o usuario final. Se lo hemos puesto muy difícil a los "hackers" y ya podemos afirmar que las instalaciones de domótica son seguras, incluso si están conectadas a internet. No olvidamos a nuestros antiguos usuarios. El KNX Secure es totalmente compatible con las instalaciones existentes puesto que podemos inhabilitar la seguridad de ciertos objetos que deban interactuar con aparatos que no disponen de esta comunicación segura.

Constante evolución

Tal como comenté más arriba, la tecnología KNX evoluciona constantemente. Desde hace muchos años, KNX ofrece una conectividad a internet, a través de interfaces KNXnet/IP. No obstante, lo que se transmite son telegramas del "lenguaje" KNX. Ahora, KNX ha ampliado el estándar para que los fabricantes puedan desarrollar servidores IoT que permiten conectar una instalación KNX con el mundo IT, pero transmitiendo en lenguaje IT. Dicho de otra forma, los expertos IT pueden acceder a la información de una instalación KNX sin necesidad de conocer el protocolo KNX. En una segunda fase, esa conectividad IoT no se limitará a un servidor (y en consecuencia a una instalación KNX completa), sino será posible integrarla a los dispositivos KNX individuales.

"KNX HA AMPLIADO EL ESTÁNDAR PARA QUE LOS FABRICANTES PUEDAN DESARROLLAR SERVIDORES IOT QUE PERMITEN CONECTAR UNA INSTALACIÓN KNX CON EL MUNDO IT"

Otro aspecto muy importante en este contexto es la semántica: Se está regulando para que todos los profesionales involucrados en la comunicación, sean del sector que sean, puedan entenderse entre sí. Para ello, KNX está colaborando con varios consorcios internacionales que trabajan para conseguir un lenguaje IoT común.

En definitiva, bajo el punto de vista de la domótica en general y del KNX en particular, la conectividad es y debe ser considerada como la gran oportunidad que tenemos para que nuestras tecnologías entren dentro del día a día de los consumidores y les hagan la vida más fácil, eficiente y segura.