

soluções em domótica na segurança residencial

Alberto Rufino e Mário Silva
ATEC - Academia de Formação

Nos últimos anos, o mercado tem assistido a um aumento significativo de soluções para tornar os edifícios inteligentes e conectáveis (*routers* de Internet, protocolo IP, servidores, *tablets*, *smartphones* e componentes IoT), muitas vezes instalados numa ótica *Do It Yourself* (DIY).

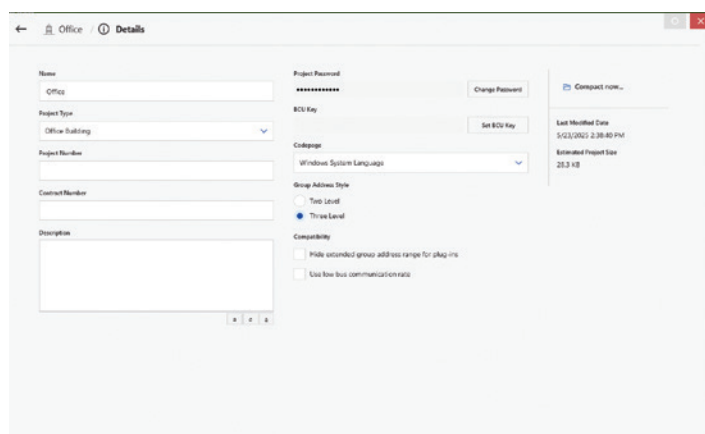


Figura 1. Definição de password de dispositivo.

A debilidade técnica de alguns destes sistemas, aliada ao desconhecimento e/ou desvalorização da segurança de dados, facilitam acessos externos indevidos às instalações, colocando em risco pessoas e bens. Os *hackers* podem aceder a dados não protegidos e sensíveis dos edifícios (consumos energéticos, hábitos de saída/entrada no edifício, programas de supervisão, entre outros), e causar todo o tipo de danos.

SOLUÇÕES EM DOMÓTICA KNX PARA A SEGURANÇA RESIDENCIAL

Criado em 1990, o sistema KNX é um protocolo aberto, standard, que obedece às mais variadas normas internacionais para automação de edifícios, permitindo a interoperabilidade entre mais de 500 fabricantes. Trata-se de um sistema descentralizado, onde os dispositivos da rede (sensores e atuadores) são dotados de microcontroladores que lhes permitem ter autonomia nas tomadas de decisão e de comunicação (não recorre a unidades controladores centrais). As comunicações consistem em telegramas *standards*, o que permite a interoperabilidade entre os dispositivos, independentemente do fabricante.

As instalações KNX devem ser planeadas e executadas por profissionais certificados. As instalações obedecem a medidas de proteção contra acessos não autorizados à rede do edifício, sendo o seu funcionamento alvo de posterior supervisão. Uma instalação KNX é por norma segura. Isto, no entanto, não significa que uma instalação KNX não tenha de seguir um conjunto de regras de segurança, com o objetivo de impedir o acesso não autorizado à sua instalação KNX.

Entre o projeto e a instalação, devem ser observados os seguintes passos:

- Garantir o isolamento dos dispositivos físicos contra acessos diretos indevidos;
- Configurar os acopladores para bloquear a transmissão de telegramas exteriores às linhas da instalação;
- Utilizar o ETS para definir uma palavra-passe para proteção de alterações não autorizadas de parâmetros dos BCU;
- Recorrer a ligações por VPN sempre que se pretenda aceder remotamente à instalação KNX.

Além destas recomendações, e em resposta às necessidades atuais e futuras, surge a extensão KNX Secure, alicerçada nos padrões de proteção assentes em algoritmos de segurança normalizados internacionalmente de acordo com a norma ISO 18033-3 e utilizam encriptação reconhecida de acordo com o padrão AES 128 CCM. O KNX Secure também respeita as normas EN 50090 (parte 3-4) e EN ISO 22510. Estas certificações fazem do KNX o primeiro sistema de *bus* de campo para edifícios a oferecer um conceito de segurança independente do fabricante.

Os dispositivos KNX Secure surgem identificados com a letra "X" impressa na etiqueta. Para obter elevados níveis de segurança, o KNX Secure recorre a técnicas de autenticação e encriptação da comunicação.

No que concerne à autenticação, os telegramas são autenticados de forma que os destinatários possam reconhecê-los como provenientes de um remetente de confiança. Para tal, é inserido um código de autenticação no telegrama que comprova o dispositivo fonte do telegrama. Caso o telegrama seja adulterado, o dispositivo de destino irá fazer a sua rejeição.

Adicionalmente, pode ser acrescentada a encriptação com o objetivo de tornar os dados do utilizador indecifráveis e impossíveis de alterar. Os telegramas também podem ser apenas autenticados, permitindo que o conteúdo dos dados permaneça apenas visível (por exemplo, para *software* de visualização), mas sem hipótese de serem copiados ou manipulados.

Para impedir que sejam copiados e reinseridos nas comunicações, os telegramas transportam um número de série. Os dispositivos KNX Secure mantêm, para todos os seus parceiros de comunicação (através do endereço individual), um registo com o último número de sequência recebido de cada parceiro. Consequentemente, sempre que um dispositivo leia uma mensagem com um número de sequência conhecido, o dispositivo deve descartar a mensagem.

O KNX Secure apresenta dois mecanismos de segurança, que podem ser operados em paralelo. Por um lado, o KNX IP Secure tem como objetivo proteger as comunicações IP do KNX. Para o efeito, recorre a roteadores KNX IP Secure em substituição dos modelos convencionais. Uma vez que estes estendem o protocolo KNX IP com autenticação e criptografia, o telegrama IP é protegido (os telegramas KNX IP Secure são rejeitados por Roteadores IP convencionais). Por outro lado, o KNX Data Secure protege a comunicação em tempo de execução (por exemplo, telegramas de grupo). Quando todos os dispositivos são KNX Data Secure, os telegramas trocados são criptografados e autenticados. Caso o dispositivo KNX não suporte KNX Data Secure, então o telegrama será descartado. Por sua vez, o ETS apenas permite que objetos de grupo KNX Data Secure sejam associados a endereços de grupo seguros.

Com KNX Data Secure é possível conceber soluções de proteção completa de áreas e linhas KNX, bem como soluções flexíveis onde o