KNX NATIONAL SWISS

# SISTEMI INFORMATICI E DI TECNICA DEGLI EDIFICI SICURI

**Guida KNX SWISS** alla sicurezza dei sistemi di automazione degli edifici e degli ambienti con KNX e reti IP

**Note**

Informazioni tecniche
Le informazioni e le indicazioni pubblicate nel presente opuscolo sono state formulate secondo scienza e coscienza. Salvo errori e modifiche tecniche.

Esclusione della responsabilità
KNX Swiss non risponde per eventuali danni derivanti dall'applicazione dei contenuti della presente pubblicazione. Viene esclusa qualunque responsabilità per danni direttamente o indirettamente derivanti dall'utilizzo delle informazioni contenute nel presente documento.



Il documento è disponibile in formato PDF al seguente indirizzo:
www.knx.ch/secure

# Indice



Versione 1.1 | 01/2023

# 1 Finalità del documento

## 1.1 Situazione iniziale

Gli edifici intelligenti che regolano autonomamente la loro energia sono integrati in un sistema energetico più ampio, sono in grado di comunicare con l'utenza attraverso lo smartphone – o persino di scambiare dati con altri edifici – sono la chiave per un futuro più intelligente del parco edifici in Svizzera nonché una piattaforma verso una progressiva digitalizzazione e una condizione di sostenibilità dell'economia e della società.

La digitalizzazione e il networking costituiscono i presupposti dell'automazione. Le nuove possibilità che ne derivano, i nuovi accessi da e verso l'esterno e l'impiego dell'intelligenza artificiale, creano tuttavia anche nuove vulnerabilità. Esse possono costituire ghiotte occasioni per la criminalità informatica. Il rischio di subire una perdita di dati o di cadere vittime di estorsioni o spionaggio aumenta nel momento in cui il protocollo Internet (IP) diventa determinante all'interno della rete dell'edificio. Gli attacchi alle reti IP possono aggirare le funzioni di sicurezza dell'automazione degli edifici.

È dunque il momento di dedicare all'infrastruttura IT dell'automazione degli edifici la necessaria attenzione e di progettare e realizzare i nuovi impianti prestando attenzione alla sicurezza.

## 1.2 Finalità del documento

Le presenti linee guida illustrano ai progettisti, agli integratori di sistemi e agli informatici degli edifici come sia possibile realizzare, strutturare e gestire una rete dell'edificio sicura. Forniscono inoltre informazioni sulle competenze degli specialisti IT della committenza, dei progettisti, degli integratori e dei gestori. Infine, forniscono indicazioni e suggerimenti sulla realizzazione di un progetto KNX Secure.

Le presenti linee guida contengono informazioni generali. Le misure vanno adeguate caso per caso alle circostanze specifiche.

# 2 Smart building: i fattori trainanti in Svizzera

La digitalizzazione del parco edifici in Svizzera è ancora in una fase iniziale. Tuttavia, si fa sempre più pressante l'esigenza di progettare i nuovi edifici già con tecnologie intelligenti e di adeguare gli edifici esistenti. L'Internet of Things (IoT) e altri fattori trainanti alimentano questa tendenza:

- **Pressione dei costi:** la presenza di una sola rete all'interno dell'edificio semplifica la manutenzione riducendo i costi.
- **Autarchia energetica:** nel caso ideale, gli edifici smart producono e utilizzano autonomamente la loro energia. A tale scopo è necessario realizzare uno scambio di dati intelligente tra i dispositivi sia a livello di sistemi sia a livello di edificio (accoppiamento settoriale).
- **Industria 4.0:** per essere smart, gli stabilimenti produttivi richiedono anche accessi remoti. L'IT e l'OT (Operational Technology) devono crescere in parallelo.
- **Smart city:** in diverse città e quartieri si sviluppano approcci per una smart city. Il networking e le nuove tecnologie devono rafforzare l'efficienza, la sostenibilità e la convivenza delle persone.
- **Evoluzione tecnologica:** il (multi)cloud ibrido diventa il principio determinante delle architetture IT. L'intelligenza artificiale, i software di automazione, i nuovi approcci di sicurezza in rete come Zero Trust nonché l'aumento del numero di sensori, gli accessi rapidi senza fili (5G, Wi-Fi6) e le architetture IT intelligenti permettono di integrare gli edifici in strutture di reti più ampie sulla base di standard aperti.

Un'unica rete per tutti i servizi e gli impianti nell'edificio anziché più reti utilizzate in parallelo e basate su standard diversi: questa evoluzione sta prendendo piede per motivi economici ma anche perché semplifica la manutenzione e il controllo dei consumi energetici nell'edificio.

Tutti i servizi necessari utilizzano un'unica infrastruttura informatica e devono rispettare le prescrizioni di cibersicurezza della propria rete. Ciò consente la gestione a lungo termine dell'intera rete da un'unica fonte (il reparto IT) e permette di ottenere i certificati di cibersicurezza.

**Ethernet** Uno standard per la trasmissione di dati via cavo. Inizialmente sviluppata per le reti LAN (Local Area Network), oggi questa tecnologia viene utilizzata anche per le Wide Area Network (WAN). Per le applicazioni con elevati requisiti di affidabilità viene utilizzato il sistema Ethernet in tempo reale. Attualmente sono disponibili ampiezze di banda fino a 400 Gb/s. Le esigenze aumentano. Il nuovo standard Ethernet a 800 Gb/s è alle porte. Lo standard fino a 1,6 Terabit/s è in fase di sviluppo.

## 2.1 Regole del gioco fondamentali

Al reparto IT vengono assegnate nuove mansioni: alla gestione dei flussi di dati e delle reti si aggiunge la gestione delle reti dell'automazione degli edifici. Il reparto IT non deve solo garantire gli accessi sicuri dall'esterno (da remoto) ma anche i collegamenti e le strutture di rete nell'intero edificio. A tale scopo deve combinare in modo intelligente e sicuro il sistema **Ethernet** (cablato), il Wi-Fi 6 e la rete 5G.

Se un edificio fa parte della cosiddetta «infrastruttura critica», i requisiti relativi alla cibersicurezza sono ancora più elevati. Le prescrizioni informatiche diventano ancora più rigorose, anche in riferimento ai dispositivi.

# 3 IT per edifici smart

## 3.1 Realizzazione di un'infrastruttura IP sicura

Le tecnologie informatiche si basano sullo scambio di dati, oggi realizzato sulla base del protocollo Internet. Questo si verifica in qualunque ambiente informatico, nelle reti locali (LAN), nelle reti geografiche (WAN) nonché in Internet.

Esistono sempre meno dispositivi, memorie o dati circoscritti a livello locale e privi di collegamenti con l'esterno. L'evoluzione informatica si sviluppa verso un'architettura cloud che comprende più fornitori e cloud sia pubblici che privati (multicloud). A ciò si aggiungono strutture informatiche locali e dati che, ad esempio per ragioni giuridiche, non possono confluire nel cloud. Inoltre, sono sempre più diffuse le infrastrutture «edge», vale a dire ai margini della rete. In esse, i dati vengono elaborati in modo decentralizzato, esattamente nel luogo in cui sono necessari. Una **latenza** breve è importante.

**Latenza** I tempi di ritardo o di risposta sono una caratteristica di qualità importante dell'infrastruttura informatica e assumono una rilevanza diversa a seconda dell'applicazione: minore è la latenza, migliore risulta l'esperienza per l'utente.

L'IT per gli edifici smart deve pertanto soddisfare alcune condizioni. È strettamente collegata agli impianti tecnici dell'edificio e dispone di interfacce per la comunicazione con i dispositivi KNX.

Per garantire la sicurezza tecnica vigono i seguenti requisiti minimi:

- Collegamento Internet con indirizzo IP statico
- Router del provider Internet in modalità bridge con firewall
  - > Rete locale con indirizzo IP fisso e DHCP limitato
  - > Accessi limitati dalla WAN
  - > Servizi aperti (porte) solo sui dispositivi strettamente necessari per l'esercizio
  - > Accessi remoti solo tramite VPN (Virtual Private Network)
  - > Consentire solo password sicure. Ancor meglio: implementare l'autentificazione a più fattori come architettura standard o **Zero Trust**
  - > Limitare i punti di accesso Wi-Fi pubblici e l'accesso a TechNet/firewall

**Zero Trust** L'approccio classico di protezione della rete richiede che ciascun client esegua un'autentificazione per poter accedere alla rete e muoversi liberamente al suo interno. Con un'architettura Zero Trust, il paradigma cambia. Ogni client, utente e utilizzatore viene considerato non attendibile. Questo approccio incentrato sull'individuo e basato direttamente sui dati permette il costante controllo dei loro flussi.

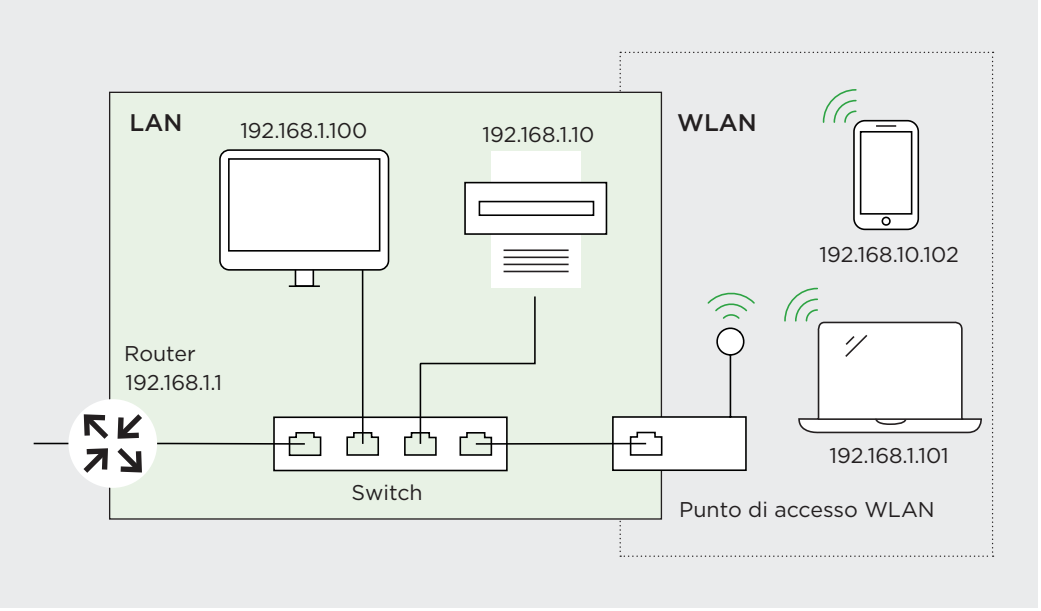



**Figura 3.1-1** Realizzazione di una rete semplice

## 3.2 Realizzazione di una rete sicura

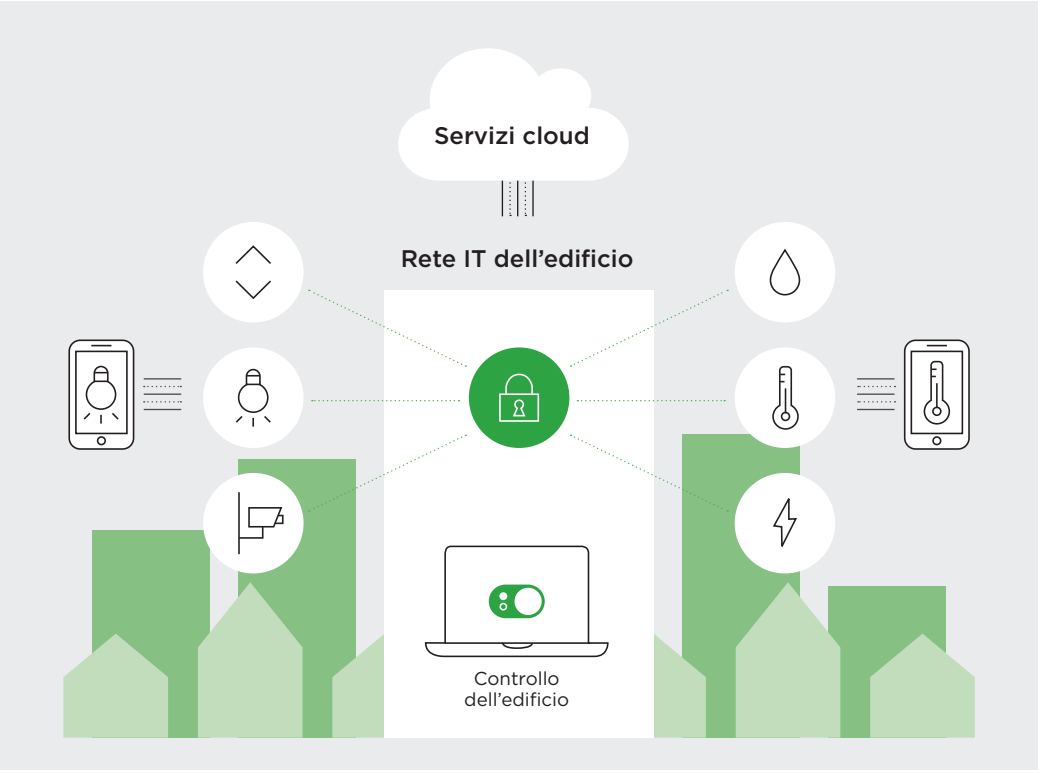
La complessità di una rete non va sottovalutata. Per realizzare un sistema affidabile è molto importante l'esperienza con le architetture di rete. Se non si dispone di tale competenza è necessario rivolgersi a un esperto di reti. Quest'ultimo dovrebbe lavorare in stretta collaborazione con il reparto IT, soprattutto se si tratta di realizzare un cloud privato.

Il cloud privato offre servizi IT tramite Internet o una rete privata per una ristretta cerchia di utenti. Lo smart building è una parte isolata di una rete più ampia ed è costituito da altri cloud pubblici o privati.

All'interno dello smart building, i vari impianti/componenti degli impianti devono poter comunicare tra di loro tramite una rete comune protetta dagli accessi non autorizzati.

Per l'edificio smart, ciò significa che i singoli «silos di rete» – così come realizzati in passato – non sono più al passo con lo stato dell'arte. Presentano troppi punti deboli e seguono inoltre un protocollo di sicurezza diverso a seconda del tipo di impianto. Alla luce della convergenza tra tecnica degli edifici e IT, il gruppo di operatori del mercato **IP-BLiS** raccomanda l'utilizzo unitario del protocollo Internet (IP) in tutta la rete. IP-BLiS non è una nuova organizzazione, bensì un'associazione all'interno della quale collaborano organizzazioni esistenti.

**IP-BLis** Organizzazione che riunisce diversi operatori dell'automazione degli edifici allo scopo di promuovere le reti IP sicure negli edifici.




Fonte: ip-blis.org BuildingTrend.png

**Figura 3.2-1** IP-BLiS promuove soluzioni basate su IP sicure, di livello superiore e armonizzate per lo smart building.

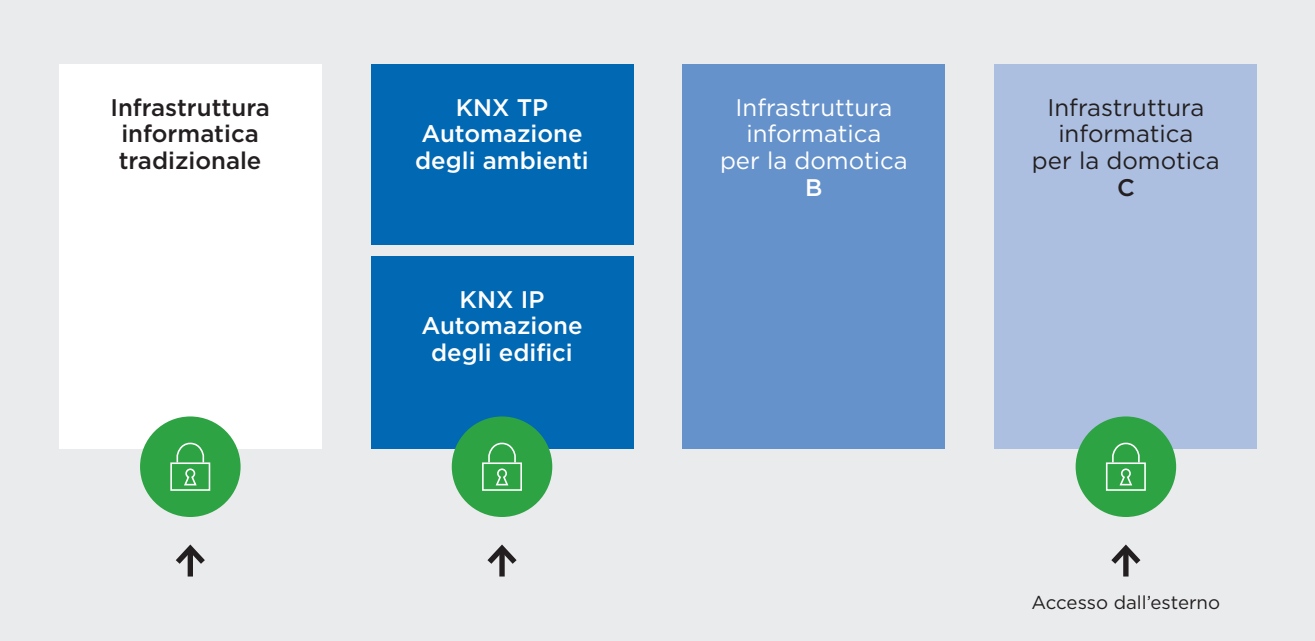



**Figura 3.2-2** Un'infrastruttura poco chiara e la presenza di piani di sicurezza diversi sono condizioni da evitare negli edifici.

Lo stato dell'arte prevede – come già descritto nell'introduzione – che le varie reti confluiscano in una rete unica. Ciò comporta, ovviamente, un relativo sforzo di coordinamento tra tutti i soggetti coinvolti. Un amministratore di rete può o deve prevedere la realizzazione di questo tipo di rete già durante la fase progettuale.

**Come realizzare reti IP sicure nell'edificio?**
Ciascun edificio necessita di una rete strutturata in modo specifico. In linea generale, le reti devono essere segmentate, vale a dire suddivise in varie sottoreti di dimensioni inferiori. Ciascuna sottorete può essere dotata di propri dispositivi di protezione e funzioni di controllo. Ciò fa sì che qualunque accesso non autorizzato rimanga circoscritto a livello di sottorete.

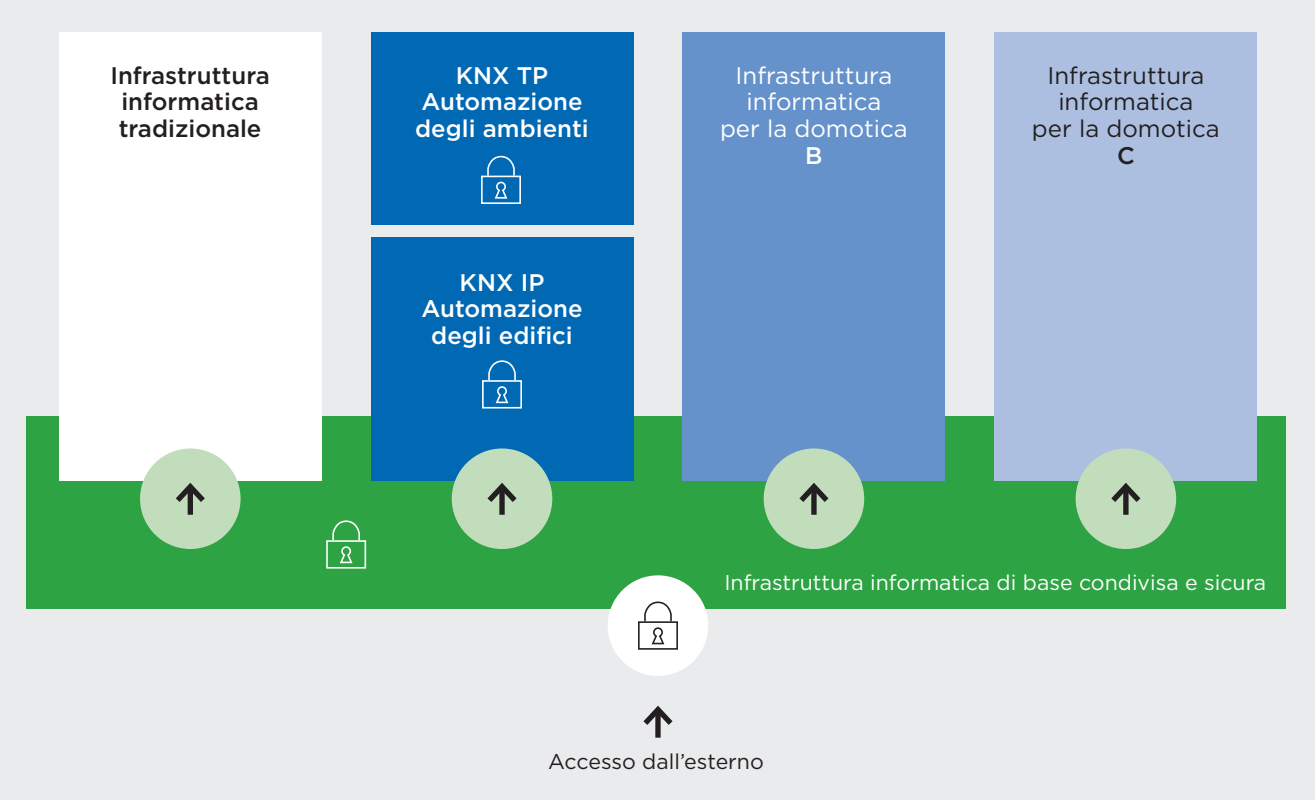



Figura 3.2-3 Va creata un'infrastruttura informatica di base condivisa, sicura e soprattutto coordinata.

Il passaggio successivo è **la virtualizzazione della rete.** Con una rete definita dal software (SDN), il controllo della rete viene affidato a un software. Quest'ultimo controlla tutti i dispositivi di rete in modo centralizzato. In questo tipo di rete, i singoli router e switch si limitano a garantire la trasmissione dei dati e non vanno più programmati singolarmente. Le reti possono anche essere fornite sotto forma di servizio dal cloud ed essere gestite centralmente. La **Network as a Service (NasS)** fornisce tutti i servizi IT necessari per gestire centralmente nel cloud il traffico dei dati all'interno dell'edificio e tra l'edificio e altre sedi.

Con concetti di rete quali **Zero Trust,** i team informatici proteggono gli edifici dagli accessi non autorizzati. Ciascun dispositivo terminale viene sostanzialmente considerato inattendibile e il traffico dati viene sottoposto a un controllo permanente. Questo paradigma di sicurezza senza password deve essere integrato sin dall'inizio nella progettazione della rete. Per l'accesso è inoltre necessaria un'**autenticazione a più fattori,** vale a dire che l'utente deve essere autorizzato tramite un secondo o persino un terzo canale (ad es. SMS).

**Come collaboriamo con il reparto IT?**
Il reparto IT deve essere coinvolto sin dalle prime fasi del progetto ed effettuare un'analisi della rete. Sulla base dell'esito di tale analisi viene definita la procedura successiva. Essa ha lo scopo di definire chi può accedere alla rete, con quale ruolo nonché a quali funzioni e a quali dati. Il reparto IT dovrebbe occuparsi anche del monitoraggio dell'automazione dell'edificio o della relativa rete. In tal modo, qualunque tentativo di accesso non autorizzato può essere individuato automaticamente sulla base di anomalie nel traffico di rete.

**Quali altri aspetti vanno considerati?**
Oggigiorno è difficile tracciare un chiaro perimetro degli edifici. I concetti di «dentro» e «fuori» non esistono più. Anche i facility manager talvolta accedono a determinate reti dall'esterno dell'edificio – rendendo necessari requisiti di sicurezza di rete ancor più elevati. L'SDN offre la base per l'integrazione di ulteriori sedi quali, ad esempio, altri edifici o uffici domestici all'interno di una rete comune.

I dispositivi Ethernet come gli switch e i router devono soddisfare i requisiti più elevati ed essere idonei all'impiego in sistemi SDN. Per le infrastrutture critiche, il settore offre hardware con livelli di sicurezza particolarmente elevati.

Ethernet è la tecnologia sulla quale si basano le reti via cavo e i protocolli di rete come **IP (Internet Protocol).** Ethernet trasferisce anche la corrente elettrica, ad esempio per il funzionamento dei sensori. Questi dispositivi devono essere dotati di protezione da sovratensione (SP, Surge Protection). Per le applicazioni nell'automazione viene utilizzato Ethernet in tempo reale. Gli adeguamenti tecnici assicurano che queste reti soddisfino i più elevati requisiti di affidabilità della comunicazione.

**Internet Protocol**
L'Internet Protocol (protocollo Internet, IP) costituisce la base della rete Internet e ormai della maggior parte delle reti di dati. I pacchetti di dati vengono elaborati indipendentemente dalla connessione. Le reti IP sono dinamiche ed eterogenee e pertanto relativamente protette dai guasti. Attualmente vengono impiegati i protocolli IPv4 e IPv6.

Nei sistemi di **Edge Computing,** i dati vengono elaborati localmente e non in un centro di calcolo – ad esempio negli edifici con sistemi informatici di nuova generazione. Ciò riduce i tempi di latenza, ad esempio per i robot che necessitano di dati in tempo reale. Tempi di latenza elevati aumenterebbero anche i rischi relativi ai dati nell'automazione.

I moderni switch semplificano l'integrazione di sistemi industriali e OT (Operational Technology) nelle reti di computer classiche e aprono la strada all'impiego di comprovate tecnologie di rete enterprise anche negli edifici.

Anche le reti senza fili (reti WLAN basate sullo standard Wi-Fi e 5G tramite rete mobile) devono rientrare tra gli aspetti considerati in fase di studio e progettazione dell'automazione degli edifici. A tale scopo sono necessarie una misurazione dell'edificio e un'accurata progettazione dei punti di accesso con le rispettive portate («copertura»).

# 4 Realizzazione sicura di un sistema di automazione degli edifici (KNX Secure)

## 4.1 KNX Secure

KNX Secure comprende tecnologie per il funzionamento sicuro dei sistemi KNX e per il networking ottimale con le reti IP. Queste tecnologie rendono sicure le installazioni KNX nei sistemi di automazione degli ambienti e degli edifici – a livello di intero impianto o in riferimento ad applicazioni specifiche.

KNX Secure non è un sistema fondamentalmente nuovo per gli integratori di sistemi KNX. KNX Secure comprende:

- **KNX IP Secure:** il flusso di dati KNX è protetto grazie alla crittografia completa nella rete IP.
- **KNX Data Secure:** il flusso di dati KNX è protetto grazie a crittografia e autenticazione sul cavo dati KNX a due fili o via radio.

Le due tecnologie possono essere combinate o impiegate in parallelo.

I dispositivi KNX Secure sono contrassegnati con la lettera «X», un lucchetto o un adesivo. Possono funzionare in modalità sicura o non sicura. Ciò rende l'installazione KNX flessibile in caso di modifiche o ampliamenti. Esiste anche la possibilità di un funzionamento misto. Il passaggio può anche avvenire in modo graduale, a condizione che i dispositivi KNX siano compatibili con lo standard KNX Secure.

> KNX Secure dovrebbe diventare il protocollo di riferimento per l'acquisto di nuovi dispositivi, in particolare per le topologie basate su IP.

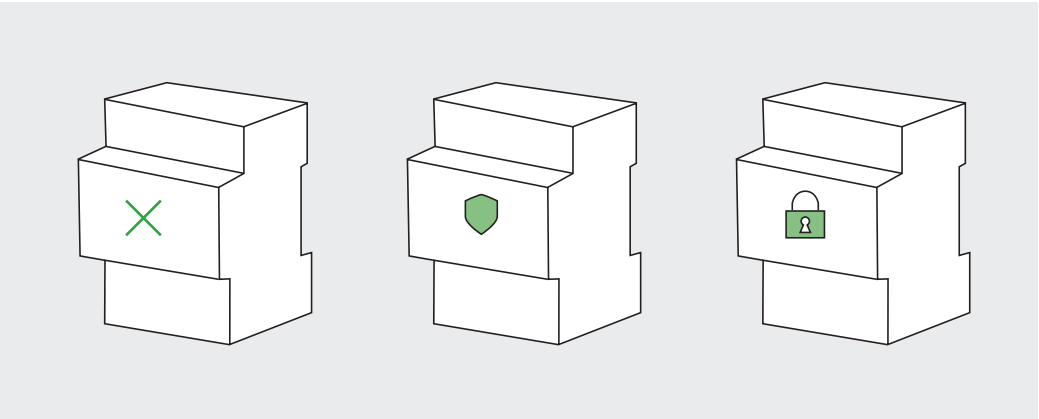


**Figura 4.1-1** dispositivi KNX Secure sono contrassegnati in diversi modi.

In ragione del formato più lungo dei telegrammi, i componenti di sistema utilizzati (ad esempio gli accoppiatori di area/linea) e le interfacce dati locali dell'ETS (ad esempio USB) devono supportare gli extended frame.

### 4.1.1 Certificati dei dispositivi

I dispositivi KNX Secure dispongono di un certificato apposto su ciascun dispositivo Secure sotto forma di codice QR.


**Figura 4.1-2** Esempio di certificato su un accoppiatore di linea. Un certificato del dispositivo ❶ è applicato in modo fisso sul dispositivo, il secondo ❷ certificato può essere rimosso durante la progettazione, prima dell'integrazione in un distributore.

Il certificato del dispositivo contiene il «codice iniziale del fabbricante».

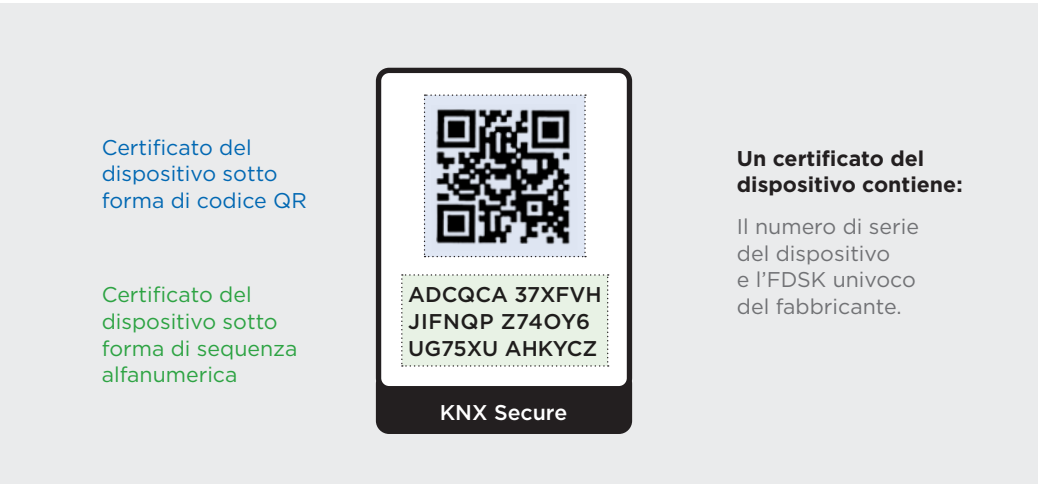



**Figura 4.1-3** Il certificato del dispositivo è applicato su ciascun dispositivo Secure sotto forma di codice QR. Contiene il «codice iniziale del fabbricante».

Si raccomanda di rimuovere il certificato del dispositivo dal prodotto dopo averlo scansionato nell'ETS e di conservarlo in un luogo sicuro (ad esempio nella documentazione relativa all'installazione).

## 4.1.2 Gestione dell’ETS

**ETS** L’ETS è il tool di configurazione unitario grazie al quale è possibile parametrizzare i dispositivi di oltre 500 fabbricanti a livello mondiale e realizzare i progetti KNX.

Durante la progettazione, i certificati dei dispositivi applicati sui dispositivi Secure devono essere importati nel rispettivo progetto **ETS.** L’importazione può avvenire con uno scanner, con la fotocamera del notebook, tramite digitazione sulla tastiera o un’app dedicata. Nel progetto ETS, per i dispositivi KNX Secure la funzione Secure è automaticamente attivata. L’ETS si occupa in background della gestione completa dei certificati dei dispositivi per il rispettivo progetto..

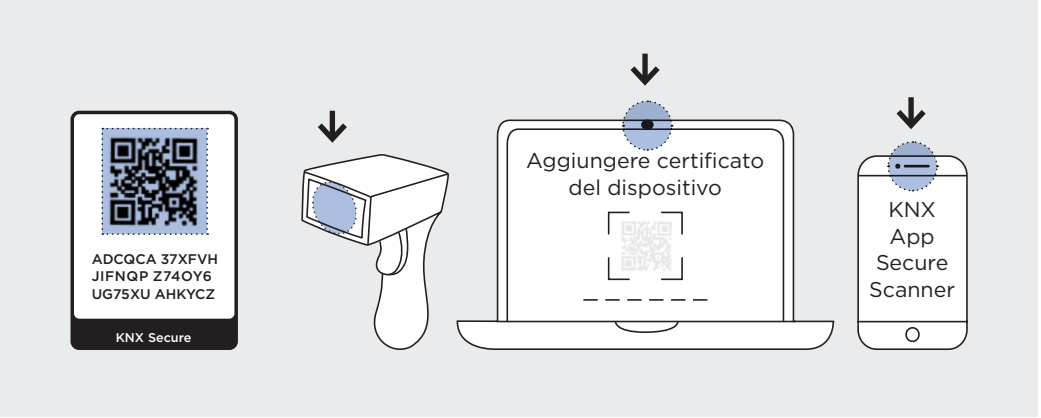



**Figura 4.1-4** I certificati dei dispositivi possono essere acquisiti grazie a uno scanner, alla fotocamera del notebook, a un’app dedicata o tramite digitazione sulla tastiera.

**FDSK** «Codice iniziale del fabbricante» (Factory Default Setup Key, FDSK). Questo codice è univoco per ciascun dispositivo e non può essere né cancellato, né modificato.

Durante il caricamento degli indirizzi fisici dei dispositivi KNX, l’ETS utilizza il numero di serie di ciascun dispositivo per associare l’**FDSK** importato al rispettivo dispositivo. Sulla base dell’FDSK, per ciascun dispositivo KNX il software genera in background nel progetto una chiave del dispositivo sicura e individuale (toolkey) che viene trasmessa al dispositivo KNX Secure durante la prima messa in funzione. La trasmissione della chiave avviene in forma crittografata al primo download con l’ausilio dell’FDSK. Qualunque successiva modifica a un dispositivo KNX Secure può essere effettuata esclusivamente con il relativo progetto ETS. L’FDSK non è più necessario, a meno che il dispositivo non venga ripristinato allo stato di fabbrica (tramite meccanismi specifici del fabbricante). Tutti i dati rilevanti ai fini della sicurezza impostati vengono dunque cancellati.

Per ciascun indirizzo di gruppo protetto collegato a un dispositivo KNX Secure e generato durante la progettazione, l’ETS genera una chiave di runtime segreta. Tutte le chiavi di runtime sono salvate nel progetto e visibili nel report «Sicurezza del progetto» (si veda il paragrafo 4.1.4).

Ciò vale per tutti i dispositivi cablati (TP), in radiofrequenza (RF) e basati su rete (IP).

## 4.1.3 Rappresentazione di KNX Secure nell’ETS

I dispositivi KNX Secure sono contrassegnati nella vista della topologia con il simbolo di uno scudo blu, in modo da essere facilmente distinguibili dai dispositivi KNX non sicuri. Con lo stesso simbolo dello scudo sono contrassegnati gli oggetti o gli indirizzi di gruppo collegati tra di loro tramite un’assegnazione sicura.

### 4.1.4 Password di progetto

Non appena in un progetto KNX nell'ETS viene inserito un dispositivo KNX Secure, il software ETS richiede l'impostazione di una password di progetto. Essa va annotata e **non** deve andare smarrita poiché, in caso contrario, l'accesso al progetto non sarà più possibile.

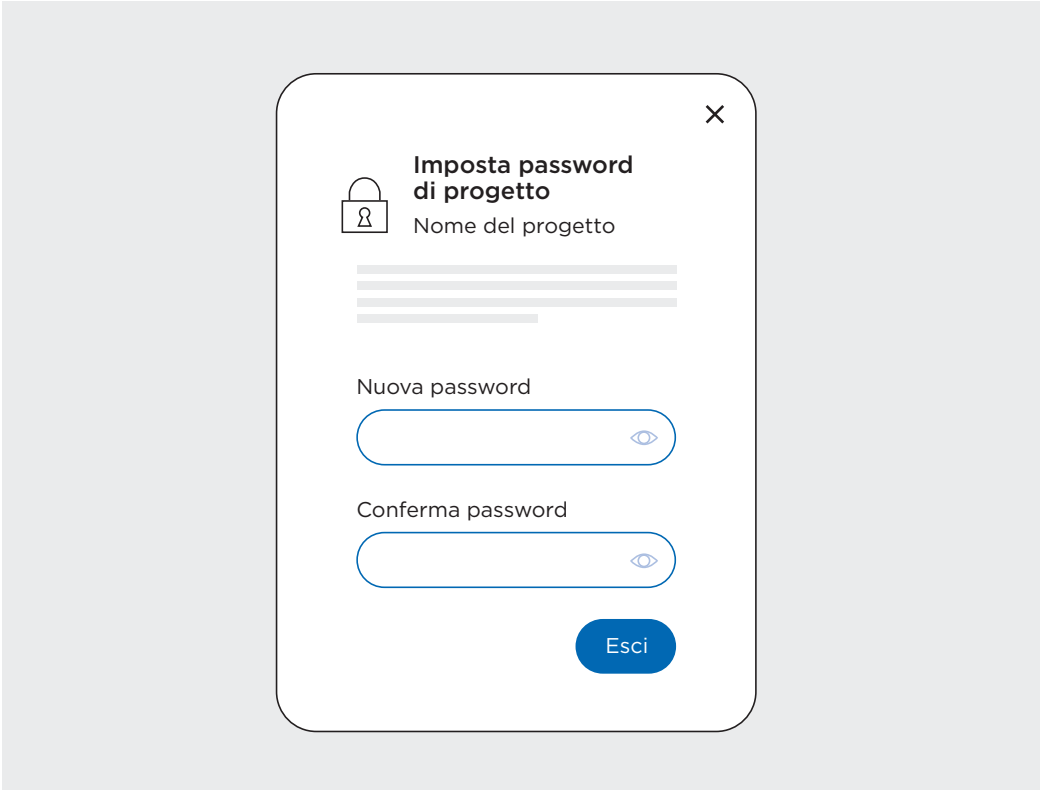



**Figura 4.1-5** La password di progetto dell'ETS va conservata in un luogo sicuro poiché, senza di essa, non è possibile ripristinare il progetto.

### 4.1.5 Secure Report dell'ETS

Dal menu «Rapporti» dell'ETS e da lì tramite la vista «Sicurezza del progetto» è possibile stampare tutti i dati sulla sicurezza relativi a ciascun progetto ETS. Nel report «Sicurezza del progetto» sono contenute le chiavi backbone, tutte le chiavi del dispositivo e – se sono presenti interfacce – anche i codici di autenticazione. Il report fornisce pertanto dati rilevanti per la sicurezza e va conservato in un luogo protetto. In caso di smarrimento del progetto ETS, queste informazioni sono perlomeno disponibili nella documentazione. Sono necessarie per poter rimettere in funzione i dispositivi dopo il ripristino. Il report «Sicurezza del progetto» va consegnato al gestore dell'edificio (committente) insieme agli altri dati di progetto.

### 4.1.6 Specifica standardizzata

**Standard ISO**
iso.org

I meccanismi di protezione specifici di KNX Secure si basano su algoritmi di sicurezza internazionali standardizzati conformi alla norma **ISO** 18033-3 e utilizzano la crittografia riconosciuta secondo AES 128 CCM.

**KNX**
knx.org

**KNX** Secure è inoltre standardizzato in Europa (nell'ambito della serie di norme EN 50090, parti 3-4) e a livello mondiale (secondo EN ISO 22510). KNX è pertanto il primo sistema di bus di campo al mondo a offrire un piano di sicurezza indipendente dal produttore per applicazioni per abitazioni ed edifici intelligenti. Esso offre la massima protezione dei dati attraverso l'autenticazione e la codifica della comunicazione dei dati.

KNX Data Secure utilizza la modalità CCM con crittografia AES a 128 bit (crittografia dati «Counter-Mode» con protezione dell'integrità «CBC-MAC-Mode») e chiavi simmetriche. Con una chiave simmetrica, sia il mittente sia il destinatario (o i destinatari) utilizzano la stessa chiave – il mittente per crittografare i messaggi in uscita (autenticazione e protezione dell'integrità) o il destinatario per verificare e decrittografare i messaggi in ingresso.

## 4.2 KNX Data Secure

KNX Data Secure codifica e autentica i telegrammi da dispositivo terminale a dispositivo terminale attraverso i canali di trasmissione KNX quali cavo a doppino intrecciato (twisted pair) e radiofrequenza. A tale scopo, tutti i componenti del sistema da proteggere devono essere dispositivi KNX Data Secure, indipendentemente dal fatto che siano collegati al sistema bus KNX tramite doppino intrecciato o radiofrequenza.

L'ETS assicura che gli indirizzi di gruppo sicuri vengano collegati solo con oggetti di comunicazione (dispositivi) compatibili con KNX Data Secure. Oltre a realizzare una protezione completa di intere aree KNX e linee KNX, con KNX Data Secure è possibile proteggere anche singole applicazioni KNX particolarmente a rischio.

Nella stessa topologia possono coesistere in parallelo sia funzioni sicure sia funzioni non sicure – persino all'interno del medesimo dispositivo KNX Data Secure. In altre parole, un dispositivo KNX Data Secure può avere sia oggetti di gruppo collegati a indirizzi di gruppo sicuri sia oggetti di gruppo con indirizzi di gruppo non sicuri.

Per l'utilizzo di KNX Data Secure è fondamentale tenere conto del fatto che – in ragione della chiave di sicurezza – i telegrammi trasmessi sulla linea bus sono più lunghi rispetto ai telegrammi standard. Già in fase di progettazione va quindi opportunamente organizzata la topologia, in particolare in riferimento al numero di dispositivi sicuri per linea. A partire dalla versione ETS 6 è possibile utilizzare gli accoppiatori di segmento con tabelle dei filtri grazie alla cui attivazione essi sono in grado di ripartire opportunamente il traffico del bus.

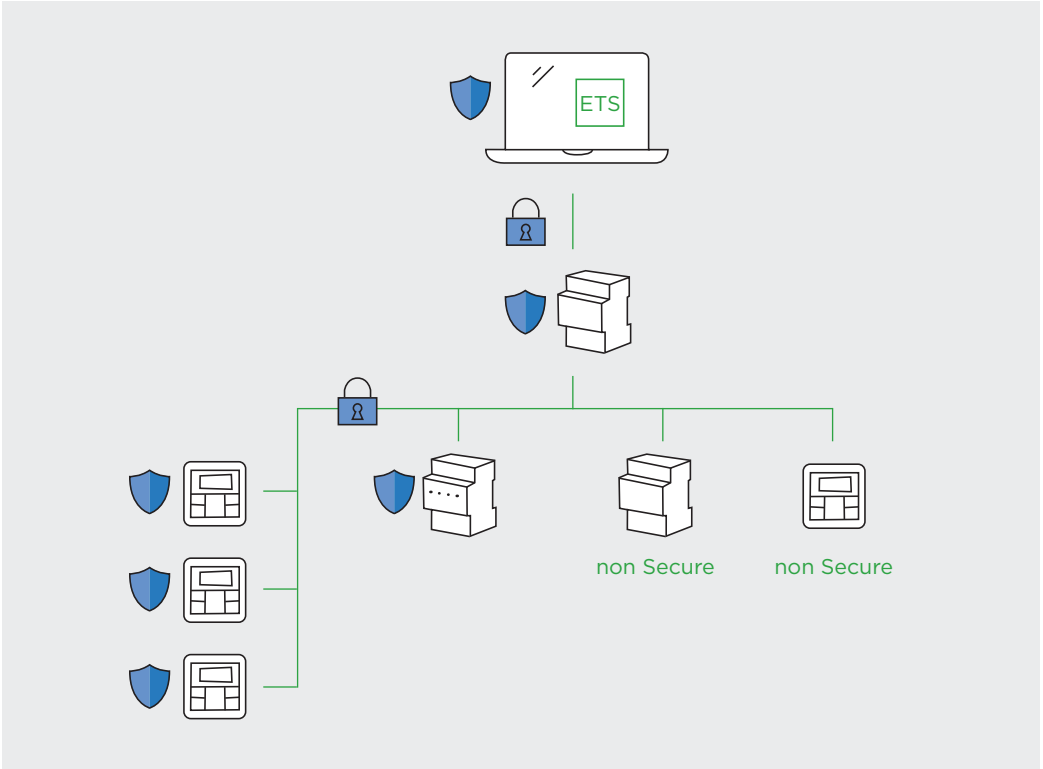



**Figura 4.2-1** KNX Data Secure: i telegrammi e i dispositivi KNX nella rete KNX sono crittografati e protetti. Non possono essere né letti, né manomessi o modificati da terzi non autorizzati nella rete.

## 4.3 KNX IP Secure

Con KNX IP Secure, tutti i telegrammi KNX scambiati tra i router KNX IP (o i dispositivi KNX IP) in un progetto vengono trasmessi in forma protetta e crittografata. I messaggi KNX inviati su IP tramite protocollo di tunneling o routing non possono quindi essere né letti né manomessi da terze parti, si veda anche figura 6.2-1 «Rappresentazione schematica di una rete sicura per la tecnica degli edifici». Per la crittografia, durante la configurazione del progetto l'**ETS** prepara la comunicazione IP dei router KNX IP in background.

**ETS** Con l'Engineering Tool Software ETS vengono configurati i dispositivi KNX. Il software ETS è indipendente dal fabbricante.

All'attivazione della «Messa in funzione sicura» nel router KNX IP, l'ETS genera una «chiave backbone» in background. Essa può essere richiamata in qualunque momento nell'ETS tramite il menu «Rapporti» > «Sicurezza del progetto». I componenti terzi – vale a dire i dispositivi, i sistemi e i gateway non configurati con il software di progettazione ETS – possono partecipare alla comunicazione sicura con l'ausilio di questa «chiave backbone».

Se l'impostazione «Messa in funzione sicura» nell'ETS viene disattivata e successivamente riattivata, a ogni attivazione l'ETS genera una nuova chiave backbone. Essa va aggiornata in tutti i dispositivi che comunicano con la linea dorsale KNX IP.

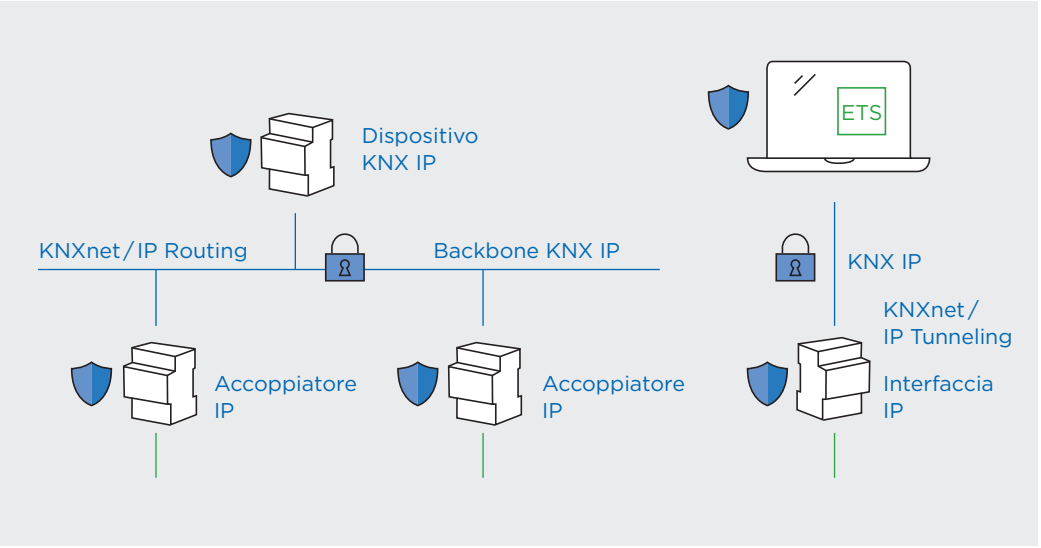



**Figura 4.3-1** KNX IP Secure: i telegrammi KNX nella rete IP (sia KNXnet/IP Routing sia KNXnet/IP Tunneling) sono crittografati e protetti. Non possono essere né letti né manomessi da terzi non autorizzati nella rete.

### 4.3.1 Router KNX IP

Un router KNX IP (si veda la fig. 4.3-2) è costituito da un collegamento a KNX TP che – attraverso i morsetti rossi e neri – conduce ai componenti KNX TP e da un collegamento alla linea principale realizzato con l'ausilio dell'IP (connettore RJ-45).

A livello IP, il router KNX IP dispone di una funzione di instradamento basata su KNXnet/IP Routing nonché di varie interfacce basate su KNXnet/IP Tunneling. Per ottenere una protezione corretta, KNX Secure deve essere obbligatoriamente attivato sia sul router sia su tutte le interfacce.

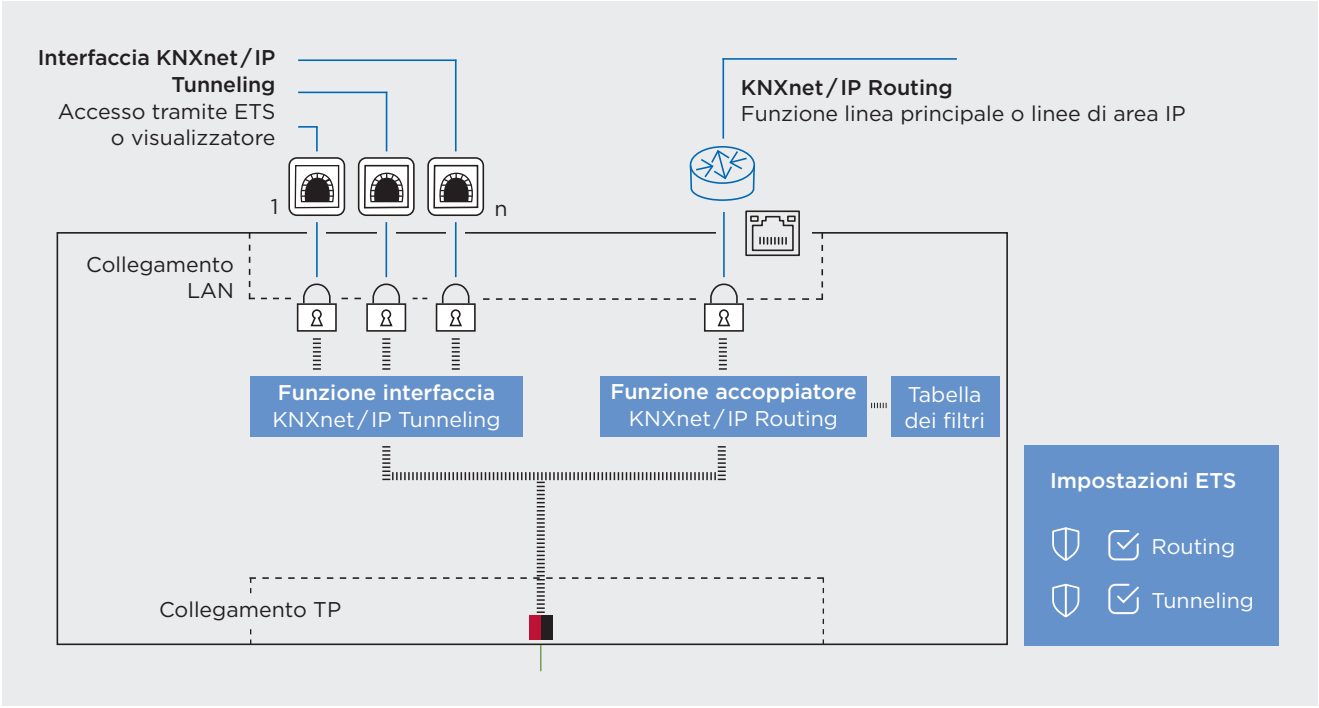



Figura 4.3-2 Struttura di un router KNX IP con le sue tre interfacce: KNXnet/IP Tunneling, KNXnet/IP Routing e KNX twisted pair (TP).

**Secure per la funzione di instradamento (KNXnet/IP Routing)**
I telegrammi KNX IP Routing sono crittografati e possono essere letti solo da dispositivi che dispongono della chiave backbone dell'ETS o configurati con o nello stesso progetto ETS. Anche con l'ETS è possibile accedere agli impianti KNX tramite KNXnet/IP Routing. Se la funzione Secure è attiva, l'accesso può tuttavia avvenire solo con il progetto ETS con il quale è stato configurato il router.

**Secure per la funzione di interfaccia IP (KNXnet/IP Tunneling)**
A seconda del fabbricante, i router KNX IP possono avere più interfacce KNXnet/IP Tunneling utilizzate per i visualizzatori o la comunicazione con altri impianti. Solo se anche tali interfacce KNXnet/IP Tunneling sono impostate nell'ETS su KNX Secure, la comunicazione IP è configurata in modo completamente sicuro. L'accesso al sistema può tuttavia avvenire soltanto con il rispettivo progetto ETS.

### 4.3.2 Interfacce KNX IP

Le interfacce KNX IP vengono utilizzate per i visualizzatori o la comunicazione con altri impianti. Esse fungono anche da interfacce con l'ETS.

**Secure per interfacce KNX IP**
Le interfacce KNXnet/IP Tunneling vanno impostate su KNX Secure nell'ETS. In questo caso, l'accesso tramite IP al sistema KNX è possibile soltanto tramite il progetto ETS oppure con un dispositivo (visualizzatore ecc.) che conosca il codice di autenticazione della rispettiva interfaccia.

## 4.4 Topologie KNX Secure

### 4.4.1 KNX Data Secure per tutto il progetto

La tecnologia KNX Secure permette ovviamente di realizzare installazioni KNX Secure in impianti KNX TP completi con più aree e linee. Anche in questo caso è possibile gestire dispositivi sicuri e non sicuri nella stessa topologia KNX.

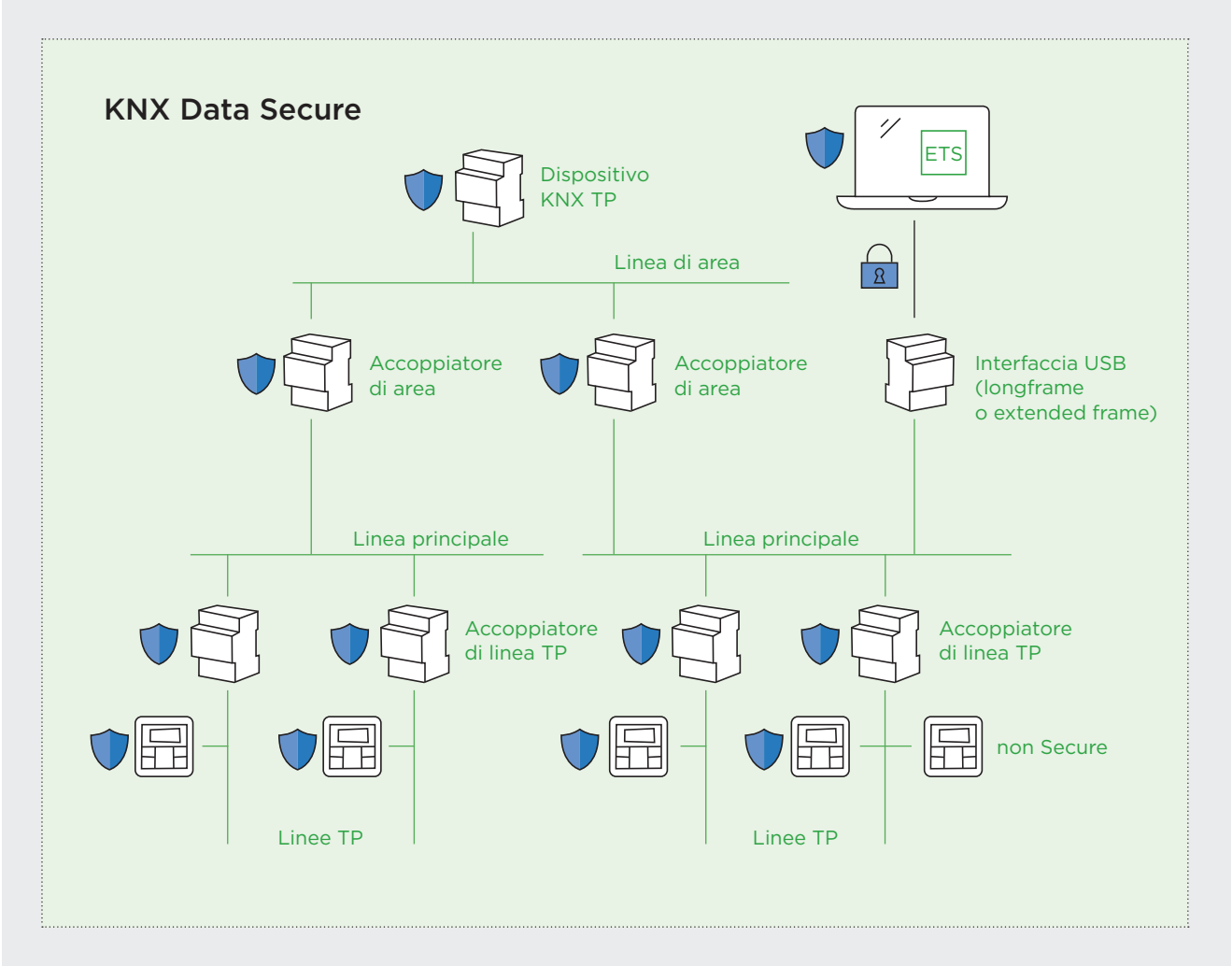



**Figura 4.4-1** Progetto KNX Data Secure su più linee e aree

### 4.4.2 Combinazione di KNX Data Secure e KNX IP Secure

Questa applicazione dovrebbe presto diventare lo standard soprattutto nei progetti di ampie dimensioni. KNX Data Secure e KNX IP Secure possono essere impiegati insieme in topologie IP/TP miste. Questa combinazione permette di proteggere in modo efficace aree e applicazioni critiche dell'automazione degli edifici indipendentemente dal tipo di accesso (IP, twisted pair o anche KNX-RF).

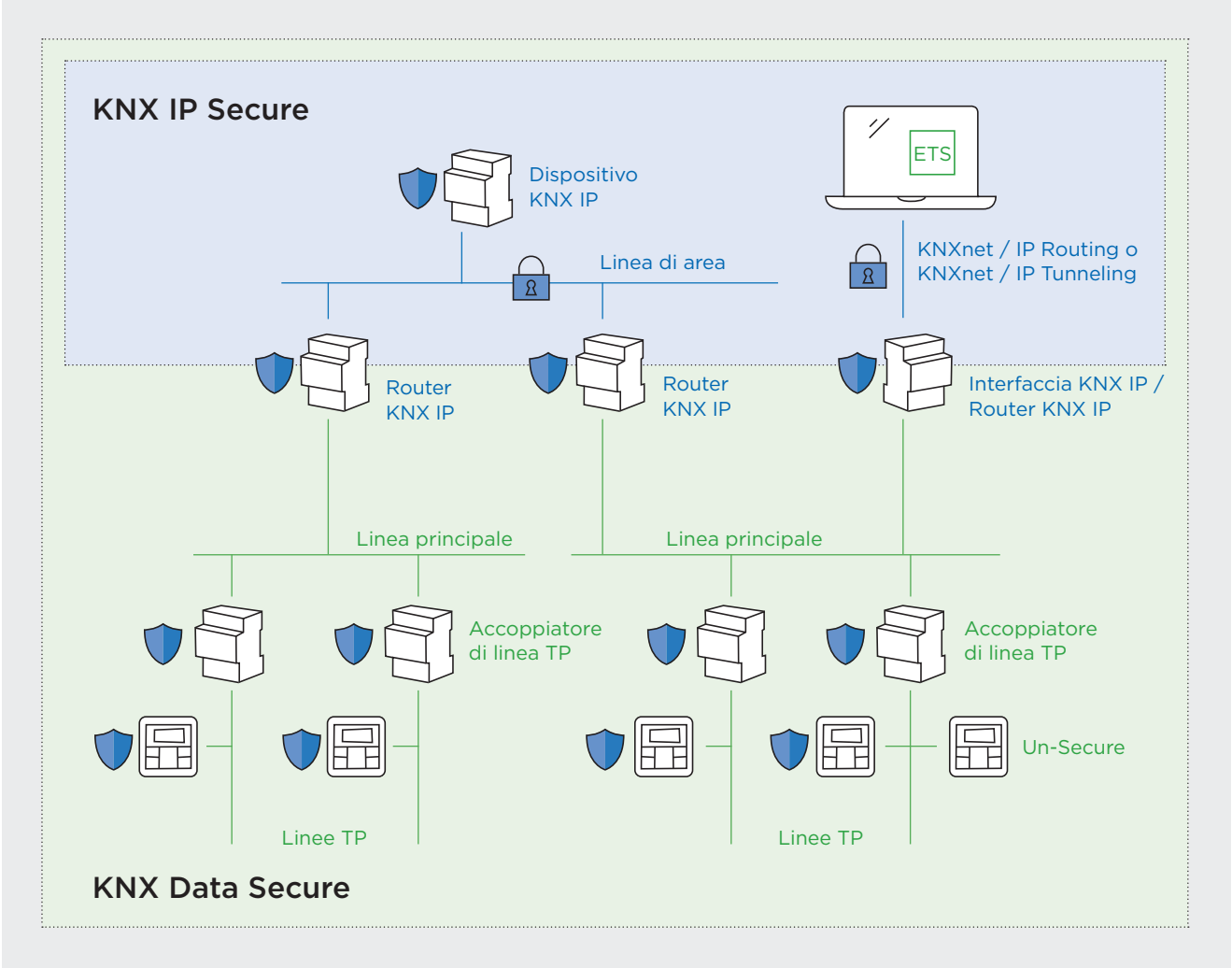



**Figura 4.4-2** KNX Data Secure e KNX IP Secure nello stesso progetto.

## 4.5 Termini importanti e definizioni

Termini importanti nell'ambito di KNX Data Secure e il loro significato

**Password di progetto**
Per poter programmare un dispositivo Secure con la modalità Secure attiva (oppure per attivare o disattivare la modalità Secure per il dispositivo Secure), nel progetto ETS deve essere attivata la «Messa in funzione sicura». Ciò è possibile solo se per il progetto ETS è stata preventivamente impostata una password di progetto.

**Certificato del dispositivo**
Codice QR sul dispositivo Secure. Contiene il «codice iniziale del fabbricante» (Factory Default Setup Key, FDSK) e il numero di serie del dispositivo.

**Factory Default Setup Key (FDSK)**
La Factory Default Setup Key (FDSK) di ciascun dispositivo compatibile con KNX Data Secure è unica al mondo e viene utilizzata per la prima messa in funzione del dispositivo. Ha una lunghezza di 128 bit e costituisce il codice iniziale del fabbricante di un dispositivo compatibile con KNX Data Secure. L'FDSK è contenuto nel certificato del dispositivo.

**Numero di serie**
Il numero di serie è un numero identificativo del fabbricante della lunghezza di 6 byte e funge da contrassegno univoco dei dispositivi KNX. Viene assegnato individualmente a ciascun dispositivo in fase di produzione (univoco per ciascun fabbricante a livello mondiale) e programmato nei dispositivi senza possibilità di modifica da parte dell'utente

**Chiave del dispositivo, toolkey**
La toolkey viene utilizzata esclusivamente dall'ETS per programmare un dispositivo compatibile con KNX Data Secure. È anch'essa lunga 128 bit, univoca per ciascun dispositivo nel progetto e sostituisce l'FDSK già dalla prima messa in funzione. La chiave del dispositivo viene in seguito utilizzata dall'ETS per qualunque operazione di programmazione in modalità sicura.

**Chiave di gruppo/Chiave di runtime**
Per garantire la comunicazione di runtime tramite indirizzi di gruppo con Data Secure, per la codifica e la decodifica dei telegrammi di gruppo vengono utilizzate chiavi di gruppo (group key). Ciascun indirizzo di gruppo in un progetto ETS è associato a una determinata chiave di runtime a 128 bit (chiave AES), a condizione che venga utilizzato l'indirizzo per la comunicazione sicura tra dispositivi KNX Data Secure. Un codice di autorizzazione nei telegrammi garantisce che soltanto i dispositivi del gruppo configurato possano scambiare dati.

**Chiave backbone**
Se come supporto backbone di un progetto ETS viene scelto l'IP e la sicurezza del backbone IP è attiva, l'ETS genera la chiave backbone per il progetto. L'ETS carica dunque questa chiave nell'accoppiatore KNX IP Secure e nelle interfacce KNX IP Secure del progetto (se queste ultime utilizzano la comunicazione sicura o hanno attivato la messa in funzione sicura). La chiave backbone e lo stato di attivazione sicura dei dispositivi Secure e dei canali di tunneling sono consultabili nel report «Sicurezza del progetto».

**Master reset**
Funzione per il ripristino di un dispositivo compatibile con KNX Secure alle condizioni di fabbrica. Eseguendo un master reset, tutte le impostazioni dell'utente vengono cancellate e viene riattivata la chiave originale (FDSK).

## 4.6 Riepilogo di KNX Secure

Per gli integratori di sistemi KNX, KNX Secure non è una novità assoluta, bensì un'estensione della tecnologia KNX esistente. KNX Secure comprende tecnologie per l'esercizio sicuro dei sistemi KNX tramite twisted pair (cavo a doppino intrecciato), radiofrequenza o reti IP. Queste tecnologie proteggono l'automazione degli ambienti e degli edifici contro gli attacchi informatici – per l'intero impianto o soltanto per applicazioni specifiche.

In un sistema KNX (progetto) possono essere utilizzati in parallelo singoli dispositivi KNX Secure e altri dispositivi non Secure. Anche gli indirizzi di gruppo attraverso i quali i dispositivi di un impianto comunicano gli uni con gli altri possono essere realizzati sotto forma di dispositivi Secure o non Secure. Tenendo conto delle specifiche del progetto e in accordo con la committenza, gli integratori (progettisti) stabiliscono quali indirizzi di gruppo KNX e dispositivi KNX andranno configurati come Secure e quali manterranno la configurazione convenzionale (non Secure).

KNX Secure impedisce:

- La possibilità di modifica dei parametri e delle impostazioni dei dispositivi con configurazione KNX Secure (sensori, attuatori ecc.) tramite un software ETS diverso da quello utilizzato per la creazione del progetto. L'accesso a tali dispositivi è possibile esclusivamente tramite il progetto ETS «originale» in cui sono memorizzate le chiavi del dispositivo (tool key) generate dall'ETS a partire dall'FDSK.
- La lettura o l'invio manuale sul bus da parte di terzi dei telegrammi KNX protetti con KNX Secure. Gli indirizzi di gruppo non sicuri in un sistema KNX possono continuare a essere registrati e manomessi anche se alcune parti del sistema sono eseguite con il protocollo Secure (eccezione nel caso di KNX IP Secure).
- La possibilità di interruzione o manomissione dei telegrammi KNX IP senza chiave backbone e chiave di progetto con KNX IP Secure. La comunicazione KNX tramite IP è completamente crittografata con AES 128 e dotata di una marcatura temporale.

Gli accoppiatori di segmento possono aiutare gli integratori a strutturare correttamente la topologia di un progetto KNX Secure. Possono rappresentare un ausilio importante per la distribuzione del traffico di telegrammi in singole zone.

## Consigli rapidi

In un'installazione KNX possono essere impiegati in parallelo i protocolli KNX IP Secure e KNX Data Secure.

In un impianto KNX possono essere impiegate in parallelo applicazioni sicure e non sicure. Non tutti i dispositivi devono essere protetti.

Se in un impianto vengono impiegati più router IP e uno di essi viene convertito a KNX IP Secure, anche tutti gli altri vanno convertiti a IP Secure.

Un oggetto di comunicazione di un dispositivo già collegato con un indirizzo di gruppo protetto non può più essere collegato con altri indirizzi di gruppo non protetti. Se nell'installazione non sono presenti proxy di sicurezza, questa regola vale per l'intera installazione. Con un proxy di sicurezza, la regola vale per i domini di sicurezza rilevanti.

All'interno dello stesso dominio di sicurezza, un indirizzo di gruppo deve essere semplice o sicuro per tutti gli oggetti di gruppo collegati. Se un dispositivo KNX non è Secure ma la sicurezza è imprescindibile, esso va sostituito con un dispositivo KNX Secure.

Le nuove funzioni di sicurezza possono essere perfettamente integrate anche negli impianti esistenti. KNX Secure è un'estensione compatibile verso l'alto: i dispositivi esistenti ignorano i messaggi KNX Secure.

## 4.7 Prospettiva su KNX IoT

KNX IoT viene impiegato esclusivamente sulle reti IP e sfrutta il protocollo TLS (Transport Layer Security) per proteggere il flusso di dati. A seconda dell'API utilizzato, le possibilità disponibili sono Ethernet, WLAN o thread. Ciò consente una crittografia end-to-end della comunicazione da un sensore fino al cloud.

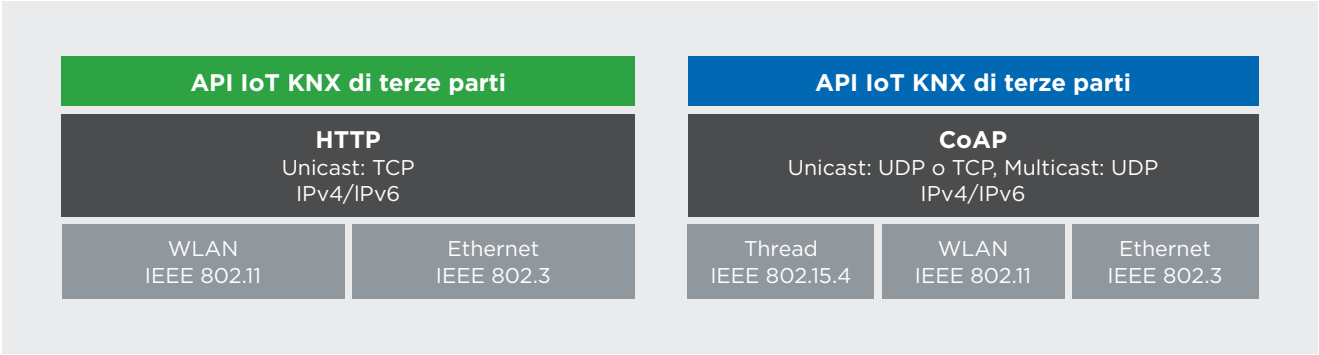



**Figura 4.7-1** Entrambe le varianti di KNX IoT (API di terze parti e Point API) utilizzano esclusivamente reti IP standard e rispettano le norme IEEE e IETF. In tal modo è possibile escludere problemi futuri con i reparti IT dei clienti.

### Consigli rapidi

Un'attenzione particolare va rivolta agli impianti nelle aree pubbliche, vale a dire in tutti i luoghi in cui le persone possono muoversi senza sorveglianza. In queste situazioni, anche i sistemi KNX cablati possono essere oggetto di attacchi.

Per gli impianti KNX che comunicano senza fili si raccomanda l'impiego di KNX Secure.

Se un impianto è connesso a Internet, l'impiego di un tunnel VPN per l'accesso tramite Internet è IMPRESCINDIBILE. Impiegando un'interfaccia KNX Secure con funzione di tunneling, è raccomandabile l'utilizzo di password forti suggerite dall'ETS, evitando di sostituirle con password deboli create dall'utente.

Nel caso di una backbone KNX IP e di altre reti IP è necessario ricorrere a una separazione delle VLAN. La rete KNX IP e altre reti devono poter comunicare soltanto tramite un idoneo firewall.

I dispositivi di automazione degli edifici devono essere facilmente adattabili all'ambiente informatico e supportare ad esempio l'assegnazione dinamica e fissa di indirizzi IP (DHCP) e la risoluzione dei nomi (DNS). Viene impedita la comunicazione tramite broadcast.

# 5 Cibersicurezza negli edifici e tecnica degli edifici

## 5.1 Fondamenti della cibersicurezza

La rete Internet è stata creata negli anni sessanta e strutturata in modo tale da essere protetta dai guasti, tuttavia senza tenere minimamente in considerazione la sicurezza dei server e delle reti. La criminalità digitale ci è andata a nozze. Nel tempo, il crimine informatico è diventato un business miliardario che, da un punto di vista economico, funziona esattamente come l'economia legale con fornitori, rivenditori e un efficiente «Servizio di assistenza clienti». Oggi non è dunque necessario essere hacker esperti per sferrare un attacco a un'impresa o a uno smart building: sono sufficienti i contatti giusti e una spiccata propensione al crimine.
Ne è dimostrazione il fatto che il numero delle violazioni della sicurezza è in costante aumento. Non è più questione di prevedere se si verrà presi di mira ma soltanto di capire quando ciò avverrà e quali conseguenze comporterà. Per tale ragione è necessario individuare quanto più rapidamente possibile questi inevitabili attacchi e adottare le opportune contromisure.

La cibersicurezza quale disciplina informatica si occupa di tutti gli aspetti della sicurezza e dei rischi correlati all'impiego di processi digitali. Sviluppa e attua misure, piani e linee guida allo scopo di proteggere i dispositivi e le reti collegati a Internet da accessi non autorizzati, furti di dati e manomissioni di qualsiasi genere.

Un attacco informatico è un attacco ostile a una rete IP di terzi e ai dispositivi terminali a essa collegati. Le finalità sono diverse. Un aumento significativo si è registrato negli attacchi ransomware, che codificano i dati e li rendono nuovamente disponibili solo dietro pagamento di un riscatto. Vengono sferrati anche attacchi per ragioni politiche, associati al furto di dati o alla manomissione di dispositivi terminali. Spesso gli hacker rimangono latenti nella rete per settimane prima di svelare le loro intenzioni.

Gli smart building rappresentano bersagli particolarmente interessanti, poiché offrono la possibilità di attaccare più imprese contemporaneamente e ottenere dall'attacco un bottino molto più cospicuo. Anche gli impianti OT sono spesso un bersaglio, ad esempio con l'interruzione di una rete elettrica o di una linea di produzione.

### 5.1.1 Forme di minaccia

Gli attacchi sfruttano diverse vulnerabilità che possono riguardare la rete, le applicazioni o i dispositivi terminali. Molto più semplice è invece nascondere software dannosi in e-mail fasulle oppure fornire link che inducono l'utente a cliccare, facendo in tal modo accedere l'hacker al proprio terminale. Il cosiddetto social engineering funziona persino per telefono: durante la conversazione, il personale delle aziende viene indotto a rivelare la propria password.

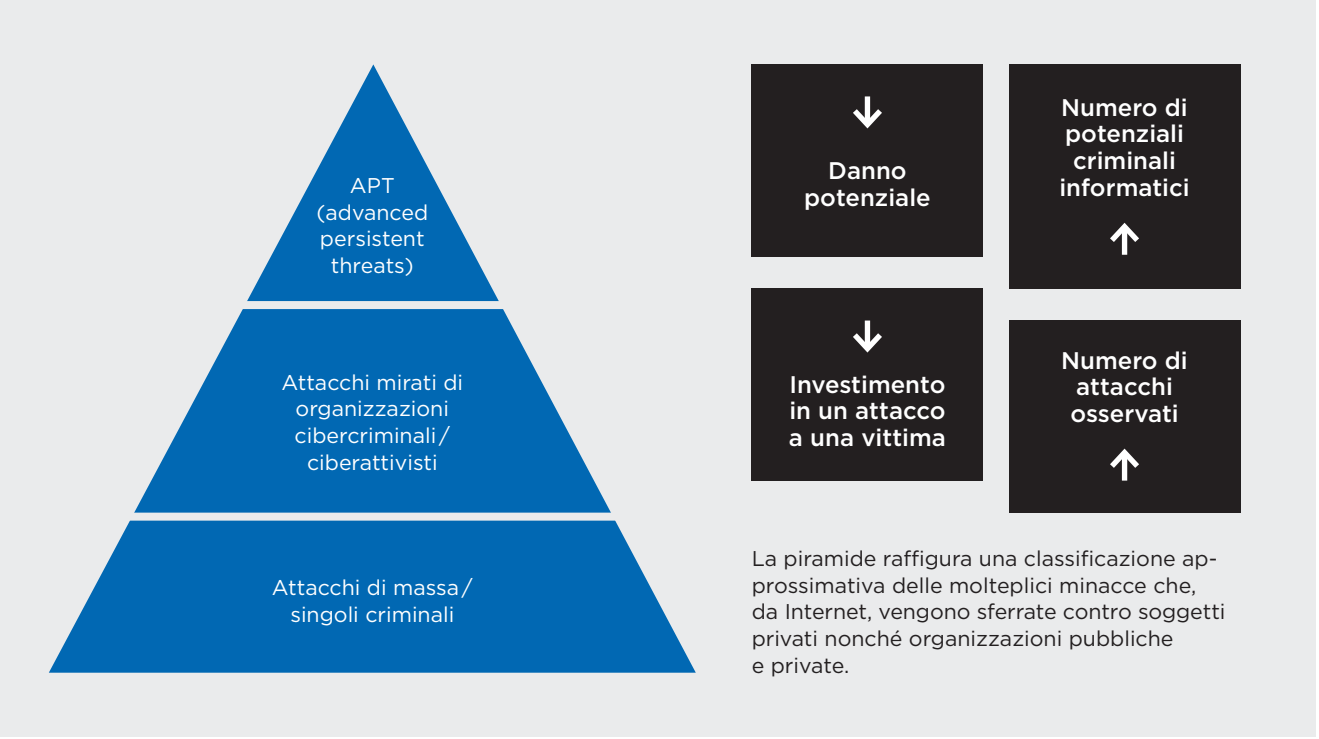



**Figura 5.1-1** Rappresentazione semplificata della piramide delle minacce secondo Sans, RecordedFuture

I confini tra le categorie di attacco sono labili.

- **APT:** attacchi con un elevato potenziale di danno, spesso preparati a lungo da attori statali. Vengono realizzati con il supporto di grandi risorse.
- **Attacchi mirati:** la criminalità digitale è mossa soprattutto da finalità finanziarie e prende di mira bersagli redditizi. Agisce perlopiù tramite estorsioni e furti di dati.
- **Singoli criminali:** per sferrare un attacco non è necessario essere hacker esperti. Gli attacchi di massa vengono messi a segno avvalendosi del modello crimeware as a service, con il noleggio di hackerware. Una volta realizzato l'attacco, l'autore e il fornitore dei servizi IT si spartiscono il denaro estorto. Altri motivi sono di natura politica (attivisti) oppure si tratta di prove di coraggio.

## 5.2 Nuovi piani di sicurezza

Sin dagli inizi delle reti IP, per gli utenti vige la raccomandazione di dotarsi di firewall (dispositivi per il blocco mirato del traffico di rete in ingresso) e software antivirus. Tutto ciò non è più sufficiente: oggi l'universo IP è un sistema complesso che consente di combinare cloud pubblici e privati in multicloud e vede sempre più spesso il personale aziendale lavorare dall'esterno della rete aziendale – ad esempio in home office – estendendo in tal modo sempre più il perimetro delle reti e rendendolo costantemente mutevole.

Risulta quindi necessario adottare un approccio «Security by Design» per tutti gli aspetti delle tecnologie informatiche, dallo sviluppo dei software all'architettura IT. I dati (le informazioni) vanno protetti in modo tale che solo le persone, le macchine o i computer autorizzati possano accedervi. L'identificazione, l'autorizzazione e la codifica del trasferimento dei dati sono meccanismi cruciali. In sintesi: chi comunica deve sempre conoscere con certezza l'identità della controparte.

Ne è un esempio Zero Trust. Non richiede più l'utilizzo di una password, poiché nessun dispositivo terminale e nessun utente viene più considerato affidabile. Ogni singola connessione dati viene valutata e autorizzata. Un approccio di cibersicurezza efficace e completo deve comprendere persone, processi, reti informatiche e altre tecnologie.

### Consigli di sicurezza generali

Mantenere i software sempre aggiornati. Ciò vale anche per i software operativi dei dispositivi.

Se si impiegano password: impostare password con caratteri speciali e numeri. È ad esempio possibile prendere i caratteri da una frase facile da ricordare selezionandoli in base a un preciso modello. Se disponibile, attivare l'autenticazione a più fattori. Utilizzare un gestore di password (ad es. quello presente nel browser) e non utilizzare in nessun caso la stessa password per più servizi IT.

Non lavorare mai al computer come amministratore.

Non fidarsi di nessun messaggio inatteso ricevuto tramite qualsiasi canale. Verificare i link, aprire gli allegati soltanto se si è certi della loro affidabilità o se sono stati verificati da uno scanner antivirus.

Scaricare i software soltanto dalle fonti ufficiali.

Modificare la password standard del fabbricante su ciascun nuovo dispositivo nella rete.

### 5.2.1 Ulteriori informazioni e link

- **Centro nazionale per la cibersicurezza:** www.ncsc.admin.ch
- **Swiss Cyber Defense DNA:** www.scd-dna.ch
- **MITRE ATT&CK:** tattiche, tecniche e procedure in caso di attacchi informatici www.attack.mitre.org
- **Database dei software dannosi noti:** www.attack.mitre.org/software
- **Cisco Cybersecurity:** www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
- **Cybersecurity Framework (NIST):** www.nist.gov/cyberframework
- **Cisco Talos Intelligence Group:** www.talosintelligence.com
- **Sito web indicante i dispositivi collegati a Internet:** www.shodan.io

## 5.3 Lo smart building quale cloud privato

L'odierna tecnica degli edifici è compatibile con l'IP e viene collegata alle reti, anche tramite Internet. Ciò comporta nuovi aspetti di sicurezza relativi agli edifici intelligenti. Entra dunque in gioco una nuova figura: lo specialista IT – che conosce i pericoli a livello di applicazioni e reti.

Le abitazioni, gli edifici commerciali e industriali diventano smart grazie all'automazione, ai sensori e all'intelligenza artificiale. Industria 4.0 significa sostanzialmente poter controllare intere linee di produzione tramite uno smartphone. L'Internet of Things (IoT) contribuisce con i dati a creare valore aggiunto e incrementi di efficienza per l'economia. In altre parole, gli approcci di rete e le tecnologie finora di tipo proprietario crescono insieme alle reti IP e, quindi, anche a Internet.

Le abitazioni sono improvvisamente divenute vulnerabili. I ladri non devono più scassinare porte o finestre ma cercare e sfruttare i punti deboli della rete. In un primo tempo può apparire innocuo se improvvisamente l'impostazione del regolatore del riscaldamento si alza, il televisore vi spia segretamente o la lavatrice si avvia. Ma cosa succederebbe se il vero obiettivo degli hacker fosse un altro? Se il loro intento fosse di prendere il controllo delle aree e dei dati più sensibili? Se nella WLAN sono presenti dispositivi come Alexa e simili, si rischia infatti di commettere sbadataggini e, ad esempio, aprire una porta smart e permettere ai ladri di accedere facilmente all'edificio.

### 5.3.1 L'ambiente IP pone un pericolo reale

Secondo studi di Cisco, entro il 2025 verranno installati 75 miliardi di dispositivi Internet of Things, spesso senza considerare gli aspetti relativi alla sicurezza. Con l'aumento del livello di intelligenza di abitazioni, uffici e appartamenti, aumenta anche il numero dei dispositivi collegati alla rete tramite IP che comunicano via cloud. Tra di essi rientrano ad esempio i contatori di acqua, gas e corrente elettrica, i dispositivi di illuminazione, gli impianti solari, i ventilatori, gli ascensori, i controlli degli accessi e molti altri. Lentamente si stanno diffondendo anche sistemi di protezione che, ad esempio, misurano l'occupazione degli ambienti e verificano le distanze. Essi generano dati estremamente preziosi per i criminali, che possono così mettere a segno i piani più loschi.

Spesso, gli edifici hanno una durata di vita di molti decenni e vengono progressivamente ammodernati; viene così a crearsi un mix di vecchie e nuove tecnologie che, spesso, presentano lacune sul piano della sicurezza. Raramente viene richiesta la consulenza di reparti IT che potrebbero mettere a disposizione le loro conoscenze in materia di flussi di dati e rischi relativi alla sicurezza informatica. Rimangono così molti interrogativi senza risposta: chi controlla le installazioni? Chi si occupa di aggiornare i dispositivi e gli elementi di comando quando sono disponibili nuove patch? È sufficiente un anello debole nella catena, un sensore che non viene più prodotto e sottoposto a manutenzione – ed ecco che un hacker ha già un piede nella porta.

Un edificio dotato di componenti di automazione è un sistema complesso ed eterogeneo che riunisce standard, tecnologie e processi diversi con numerose correlazioni. Gli elementi dell'automazione degli edifici sono estremamente interessanti per i criminali informatici. Un foro piccolissimo può facilmente trasformarsi in uno squarcio – per questo le lacunose recinzioni digitali delle aziende non sono minimamente sufficienti a proteggerle dalle estorsioni.

L'automazione degli edifici va quindi considerata una componente «vitale» delle costruzioni e adeguatamente protetta. Un ostacolo al riguardo è il fatto che ciascun edificio presenta caratteristiche architettoniche e tecniche diverse. Inoltre, spesso importanti componenti IT vengono installati senza alcuna protezione, sistemati nel

famoso sgabuzzino o sotto la scrivania, contrariamente a quanto avviene nei centri di calcolo, dove la protezione fisica dell'infrastruttura viene realizzata secondo le più rigorose misure di sicurezza.

### 5.3.2 Riflessioni fondamentali dalla prospettiva IT

La progettazione del servizio di automazione è fondamentale, così come la valutazione della sicurezza delle apparecchiature. Come in qualunque altro ambito, è necessario stabilire se i dispositivi dovranno essere utilizzati solo all'interno dell'edificio o se sarà necessario avvalersi anche di risorse da uno o più cloud. Qui spesso iniziano i problemi: questo aspetto, infatti, non viene quasi mai sottoposto alla valutazione di un integratore o del fabbricante, in quanto un edificio automatizzato viene generalmente gestito senza il coinvolgimento di un reparto IT. La sicurezza IT dell'automazione degli edifici viene relegata in secondo piano.

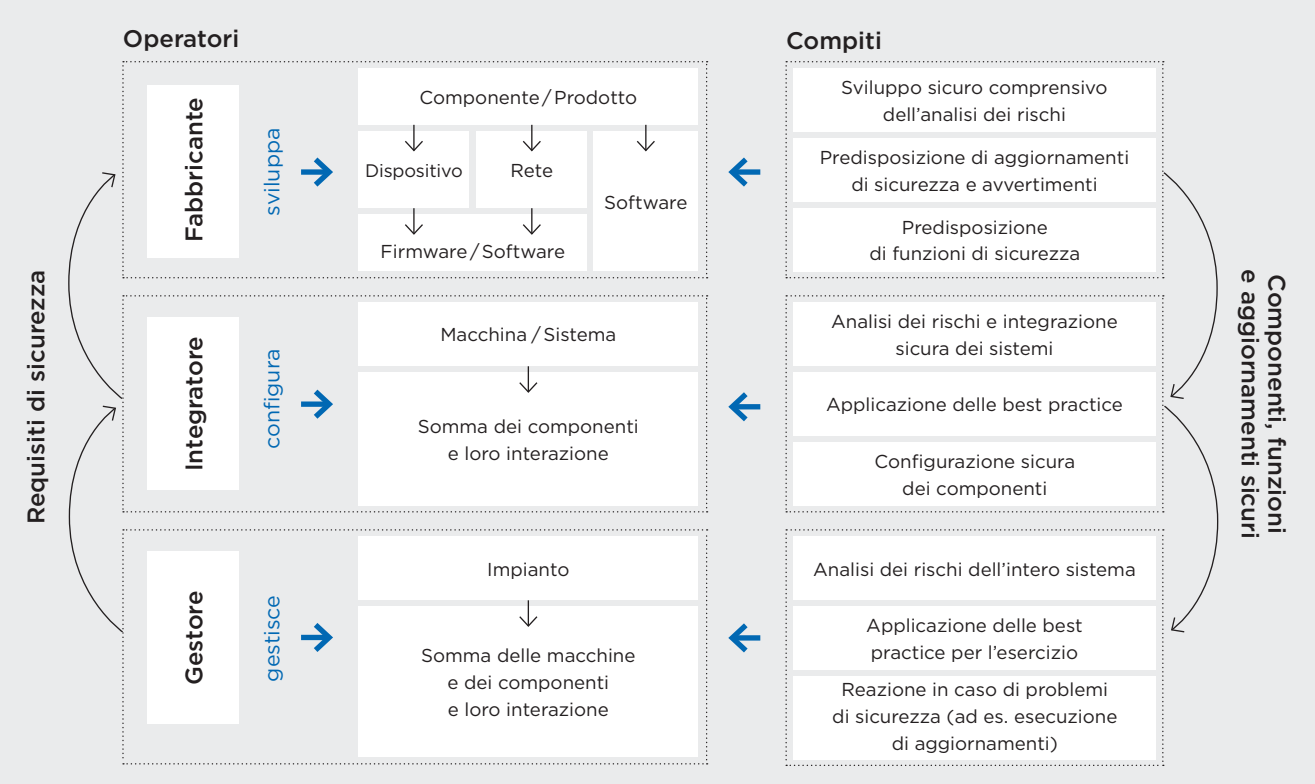
Quando tuttavia gli edifici diventano più che smart, l'IT e l'intelligenza artificiale offerte dal cloud diventano componenti a pieno titolo del sistema: vengono progettate reti intelligenti in grado di auto-controllarsi e di identificare le anomalie. La visibilità nella rete contribuisce inoltre alla sicurezza: gli edifici automatizzati, con i loro protocolli non IT, vengono integrati come cloud privati nei cloud ibridi delle imprese, che vengono controllati grazie a strumenti per garantire la massima trasparenza della rete. La progettazione di un edificio smart va dunque affrontata con la chiara intenzione di impostarlo come un nuovo centro di calcolo, un cloud privato.

Le cose non vanno però così. Servono nuovi approcci progettuali e nuovi standard di sicurezza a livello tecnologico, organizzativo e procedurale. Il progresso tecnico sul piano della sicurezza negli edifici è in ritardo rispetto agli sviluppi nei settori dell'IT e dell'OT (tecnologia operativa). Per entrambi, oggi vengono applicati i più elevati standard di sicurezza e sistemi automatizzati per il controllo degli accessi e dei flussi di dati. È giunto il momento di integrare gli edifici smart, di creare sistemi convergenti che vengano protetti in modo centralizzato e trasparente e da tecnologie sviluppate nonché applicate da specialisti. A richiederlo è un'economia digitalizzata in cui le persone vanno protette indipendentemente dal luogo fisico in cui lavorano. Proprio negli ambienti di lavoro ibridi del «new normal», gli edifici dovrebbero provvedere direttamente a garantire la protezione delle persone nei processi informatici e di lavoro.

## 5.4 Raccomandazioni operative

La protezione degli edifici intelligenti dai pericoli derivanti dall'ambiente IP presuppone una stretta collaborazione tra specialisti in automazione degli edifici e specialisti IT. Congiuntamente, essi creano un cloud privato, una rete accessibile sulla base di regole rigorose e costituita da diverse sottoreti. I flussi di dati devono essere controllati per individuare eventuali anomalie e vanno regolarmente eseguiti aggiornamenti e correzioni degli errori.

È dunque necessaria una collaborazione tra fabbricanti, integratori e gestori. Il primo passaggio dovrebbe essere costituito da una valutazione approfondita e da un'analisi dei dati e dei rischi.



Fonte: ZVEI

**Figura 5.4-1** I requisiti di sicurezza nell'edificio devono essere soddisfatti da tre operatori che lavorano fianco a fianco e condividono le rispettive conoscenze specialistiche.

### 5.4.1 Supporto del reparto IT

Solo le esperte e gli esperti IT dispongono del know-how e dell'esperienza per garantire l'esercizio sicuro delle reti IP e la gestione di complesse infrastrutture multicloud, vale a dire di combinazioni di cloud privati e pubblici. I moderni ambienti IT sono basati su cloud; i confini tra archiviazione a livello locale e archiviazione in cloud sono labili. Un'attenta valutazione dell'edificio consente di definirne la strutturazione, i processi e le funzioni smart. Da ciò è possibile dedurre le opportune misure per un esercizio sicuro.

I reparti IT devono, in definitiva, considerare l'automazione degli edifici come il loro compito principale. L'automazione dev'essere conforme agli standard.

### 5.4.2 Reti sicure e flessibili

Le reti moderne sono gestite da software e segmentate. Comprendono sedi sia interne che esterne. Possono essere reti Wi-Fi, 5G ed Ethernet, reti locali, reti di campus o reti geografiche.

Un controller gestisce tutte le funzioni e regola il flusso di dati su tutti i segmenti della rete. Queste sottoreti creano aree protette e bloccano i criminali informatici abbastanza a lungo da permetterne una tempestiva individuazione. Gli asset, i dispositivi terminali e i flussi di comunicazione devono essere registrati, classificati e la rete deve essere adeguatamente segmentata. Ad esempio, i dispositivi dell'automazione non devono assolutamente avere accesso a server interni.

Tutti gli accessi devono essere controllati in tempo reale. Con l'approccio Zero Trust, anche nell'edificio è sempre possibile sapere chi ha eseguito l'accesso, con quale terminale e a quali risorse. L'intelligenza artificiale applicata alle reti è in grado di rilevare variazioni nel traffico o nei pattern e di far scattare l'allarme.

### 5.4.3 Piano di cibersicurezza

Per qualunque futura installazione è necessario il confronto con un esperto in cibersicurezza. Un'infrastruttura IT standardizzata e ampiamente automatizzata ne agevola il controllo e permette al reparto IT di concentrarsi sulle proprie competenze chiave, ad esempio occupandosi dell'individuazione e dell'eliminazione preventive dei thread prima che possano rappresentare un pericolo.

Nello smart building si applicano gli stessi principi validi in ambito IT: i punti di interconnessione sulla rete devono essere protetti, le patch e i dispositivi terminali devono essere gestiti. Un efficace piano di cibersicurezza deve inoltre contemplare una gestione intelligente dei dati, grazie alla quale i dati produttivi – e quindi critici – vengono salvati in tempo reale anche su altri supporti (backup) e, in caso di emergenza, possono essere rapidamente ripristinati.

### 5.4.4 Formazione delle persone negli edifici smart

In ambito IT vale il principio secondo cui la cultura della sicurezza deve essere una filosofia di vita, poiché più dell'80 percento delle violazioni della sicurezza è di origine umana. Le persone rivelano le proprie password, cliccano su ogni link e aprono gli allegati spianando la strada alla criminalità digitale che, in tal modo, riesce a infiltrarsi nelle reti tramite e-mail contenenti software dannosi. Gli utenti degli smart building devono pertanto esser consapevoli del fatto che l'ambiente in cui si muovono è critico sotto il profilo della sicurezza. Come per le esercitazioni antincendio, devono conoscere i pericoli reali e la situazione generale delle minacce.

### 5.4.5 Le norme come fondamento

Per un esercizio IT sicuro negli edifici, le norme vigenti devono costituire il fondamento per lo sviluppo di piani di protezione. L'ISO/IEC Joint Technical Committee (JTC1) elabora la famiglia di norme ISO/IEC 27000 per i sistemi informatici. L'IEC Technical Committee 65 (TC 65) pubblica lo standard IEC 62443 per i sistemi OT.

Queste due norme – in combinazione con le corrispondenti certificazioni di conformità e controprove – sono pilastri importanti di un piano di cibersicurezza efficace e completo per gli edifici smart.

## 5.5 Standard

Per la sicurezza negli smart building esistono alcuni standard e linee guida fondamentali. Sulla loro base vengono elaborati piani di sicurezza individuali.

- **Guida alla verifica della cibersicurezza:** www.isaca.de
- **Sicurezza informatica nell'automazione degli edifici (IT Security for Building Automation and Control Systems, VDMA 24774):** www.vdma.org

**Norme rilevanti**

- **Livelli di sicurezza IEC 62443:** i compiti rilevanti per la sicurezza riguardano l'intero ciclo di vita di un impianto. La serie di norme internazionali sulle «reti di comunicazione industriali – sicurezza IT per reti e sistemi» descrive gli aspetti tecnici e procedurali della sicurezza informatica industriale.
- **ISO/IEC 27001:** sistema di gestione della sicurezza delle informazioni con una persona responsabile dell'applicazione nei processi interni all'azienda.
- **ISO/IEC 2700x Reihe:** gli standard da 0 a 5 descrivono tutti gli elementi della sicurezza informatica.
- **ISO/IEC 15408:** valutazione e certificazione dei prodotti IT
- **ETSI Standard EN 303645:** il nuovo standard per la sicurezza IoT definisce la sicurezza informatica nell'Internet of Things (ad es. sensori).

## 5.6 Tipi di crittografia

La crittografia protegge la riservatezza, l'autenticità e l'integrità dei dati. La crittografia si basa sul metodo di conversione da testo in chiaro a testo codificato dipendente da una chiave. Il testo codificato può essere letto solo impiegando la chiave segreta. A tale scopo è possibile ricorrere a un software o a un hardware. Esistono diversi tipi di crittografia: simmetrica, asimmetrica o ibrida.

I processi di crittografia simmetrici sono efficienti e rapidi. La stessa chiave viene utilizzata sia per la codifica che per la decodifica. I processi asimmetrici lavorano con coppie di chiavi formate da una chiave pubblica (pubblicamente nota) e da una chiave privata. Le due chiavi sono accoppiate su base matematica. I messaggi crittografati con la chiave pubblica possono essere decrittografati solo con la chiave privata del destinatario. I processi ibridi combinano entrambe le metodologie. La prima crittografia viene eseguita con una chiave casuale e di tipo usa e getta.

Gli obiettivi di protezione comunemente perseguiti con la crittografia fanno sì che, in un messaggio, vengano garantite:

- la possibilità di lettura solamente da parte di una determinata persona;
- l'effettiva provenienza dalla persona che dichiara di esserne il mittente;
- l'assenza di modifiche durante la trasmissione.

La crittografia è dunque un importante fattore di un piano di sicurezza completo per le tecnologie informatiche e le reti: da un lato, il trasporto dei dati viene crittografato; dall'altro, i due «partecipanti alla conversazione» (persona, software, macchina, dispositivo terminale) vengono autenticati.

La crittografia end-to-end è la crittografia completa del flusso di dati tra più stazioni intermedie e reti da un dispositivo terminale all'altro. Costituisce la situazione ideale di un servizio IT sicuro.

**Nelle reti IP sono comunemente diffusi i seguenti meccanismi di sicurezza:**

- **AES (Advanced Encryption Standard):** l'AES lavora con chiavi aventi una lunghezza di 128, 192 o 256 bit e costituisce un meccanismo molto sicuro e dalle elevate prestazioni. Con chiavi da 256 bit è praticamente inattaccabile.
- **TLS (Transport Layer Security):** navigazione sicura tramite https:// e traffico e-mail sicuro tramite smtps. Il protocollo utilizza la crittografia asimmetrica con AES.
- **WPA 2/3:** utilizzo sicuro delle reti mobili tramite Wi-Fi 5 o 6 su base AES.
- **SHA:** famiglia di algoritmi che assicura l'autenticità dei dispositivi (sicurezza del certificato).
- **VPN (Virtual Private Network):** le connessioni di rete private crittografate possono essere realizzate in diversi modi. Creano un tunnel di dati virtuale che attraversa varie reti. Viene perlo-più utilizzato lo standard IPsec, spesso anche TLS.
- **IPsec (Internet Protocol Security):** famiglia di protocolli per la comunicazione protetta su reti IP non sicure. Si impiegano diversi processi di crittografia e algoritmi.

# 6 Avvertenze sulla pianificazione di progetti di automazione degli edifici sicuri

## 6.1 Conoscenze specialistiche IP e collaborazione

Per portare la sicurezza in un edificio smart a un livello ottimale è necessario operare in base a una procedura coordinata e completa. Il presente documento descrive molti degli aspetti da considerare.

La sicurezza KNX comprende anche la sicurezza IP, la protezione del flusso di dati proveniente dall'esterno e che scorre all'interno dell'edificio. In altre parole, lo smart building non è un'isola KNX in mezzo al grande mare dei dati. È esposto alle stesse tempeste che colpiscono qualsiasi altro sistema e organizzazione in Internet.

Detto in gergo tecnico: in uno smart building viene creato un cloud privato che potrebbe persino essere parte di un ambiente multicloud più grande.

Per gli installatori/trici, lo sviluppo della sicurezza negli edifici smart comporta l'acquisizione di nuove conoscenze specialistiche in campo IP oppure la collaborazione con corrispondenti specialisti. Se il progetto prevede il coinvolgimento dei reparti IT delle imprese, essi vanno consultati sin dalla fase iniziale.

## 6.2 Compiti della progettazione tecnica degli edifici

### 6.2.1 Definizione delle condizioni generali

I progettisti (dell'automazione degli edifici) devono definire insieme alla committenza e al rispettivo reparto IT le condizioni generali. Esse comprendono il piano degli indirizzi IP, le prescrizioni per la scelta di hardware, router e password nonché la loro gestione e molto altro. Va inoltre stabilito che KNX IP Secure sia il nuovo standard per il trasferimento di informazioni KNX su infrastrutture IP. Ne è riportato un esempio al Capitolo 6.3.

### 6.2.2 Identità e gestione delle autorizzazioni

Chi ha o necessita di accesso agli impianti, quando, dove e con quali modalità? E chi gestisce tali accessi? Le progettiste e i progettisti devono definire tali aspetti sin dalle prime fasi del progetto. La VPN potrebbe essere una possibilità per gli accessi esterni, poiché non vi sarebbero sicuramente più porte aperte! Si dovrà inoltre tenere conto di fasi progettuali quali la realizzazione, l'esercizio e la manutenzione.

### 6.2.3 Chiara strutturazione del progetto

A fronte delle crescenti esigenze di networking che caratterizzano gli smart building, si rende sempre più importante una strutturazione chiara e comprensibile del progetto, degli indirizzi e dell'IP. La responsabilità della coordinazione di progettazione e applicazione ricade su progettisti di impianti elettrici, di edifici e dell'informatica degli edifici.

**I loro compiti comprendono in particolare:**

- La suddivisione e la strutturazione logica dell'impianto (topologia, aree e linee) in considerazione del traffico di telegrammi.
- L'elaborazione di uno schema di base che documenti con precisione la topologia KNX e IP.
- Rientrano pertanto nella documentazione anche lo schema IP e il piano IP con tutti i segmenti di rete, i numeri IP e le interfacce.
- Vanno inoltre documentate anche la gestione delle password e la loro assegnazione.
- È inoltre molto importante che per ciascun progetto sia presente un piano di assegnazione degli indirizzi, come descritto nelle direttive progettuali di KNX Swiss.

Questi principi di progettazione consentono di pianificare e applicare in modo ottimale la topologia e la sicurezza di un'installazione tecnica degli edifici costituita da componenti KNX e IP.

### 6.2.4 Fondamenti della sicurezza

La sicurezza dell'installazione KNX o IT va considerata in ogni fase. Indicazioni importanti a tal riguardo sono contenute anche nell'opuscolo KNX Secure della KNX Association sul sito knx.org.

**In sintesi, è necessario considerare i seguenti punti:**

- I sistemi di automazione funzionano sempre tramite reti dedicate (VLAN) dotate di dispositivi hardware propri (router, switch ecc.).
- La segmentazione della rete blocca il movimento laterale degli aggressori.
- Sono necessarie tutte le caratteristiche di sicurezza delle reti IP: filtri MAC, crittografia, password forti o autenticazione a più fattori, reti Wi-Fi 6 con crittografia WPA3 e nomi SSID che non permettano di risalire all'hardware.
- Ricorso all'indirizzo IP multicast di KNX con un indirizzo diverso dall'indirizzo standard.
- Nessuna porta aperta dei dispositivi KNX verso Internet.
- Bloccare per quanto possibile l'accesso dall'esterno (gateway di default «0»).
- Accesso esterno a KNX solo tramite VPN o altri accessi sicuri contemplati nell'estensione dello standard KNX.
- Evitare il traffico superfluo: i router devono opportunamente bloccare gli indirizzi sorgente e non devono consentire il broadcasting e le connessioni punto-punto.
- Impostare e utilizzare l'ETS in modo sicuro.

### 6.2.5 Piano esemplificativo per un'automazione degli edifici sicura

Come precedentemente affermato, in uno smart building la rete viene utilizzata da molti «gruppi di partecipanti». Dal punto di vista dell'automazione degli edifici è necessario assicurare che tutte le aree – anche le aree di rete a monte – siano protette dagli accessi non autorizzati.

L'esempio seguente mostra come può essere strutturata una rete di questo tipo. L'immagine non ha alcuna pretesa di completezza ma intende unicamente fornire aiuto nell'elaborazione di piani generali della tecnica e dell'informatica degli edifici per un progetto.

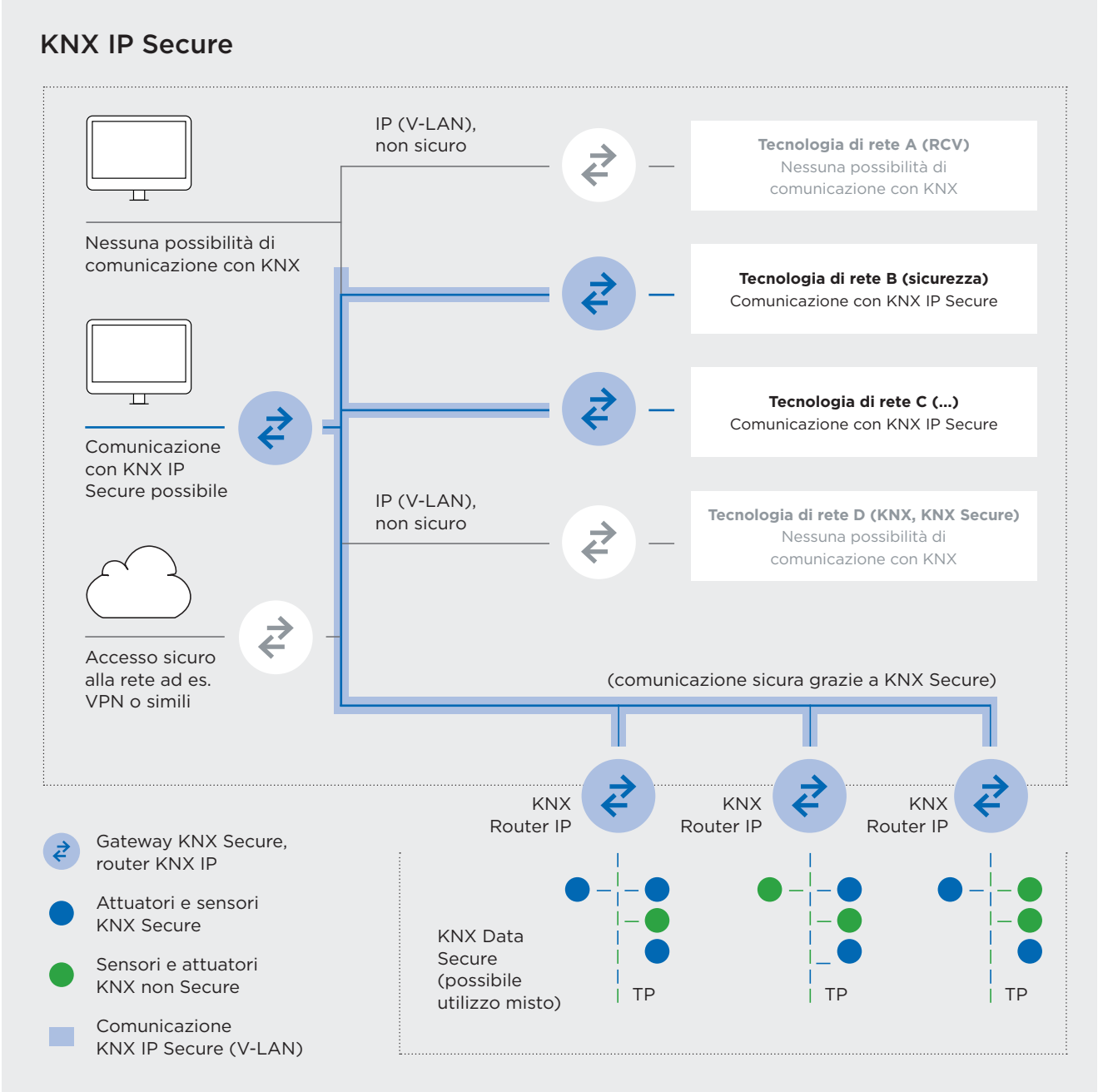



**Figura 6.2-1** Rappresentazione schematica di una rete sicura per la tecnica degli edifici

## 6.3 Svolgimento di un progetto KNX Secure

Lo schema seguente mostra, in una semplice panoramica, la procedura per realizzare correttamente un progetto KNX Secure. Esso descrive in linea di massima gli aspetti da prevedere in ciascuna fase SIA e le tempistiche ideali per l'attivazione della crittografia nell'intero progetto ETS. Insieme all'ausilio di progettazione KNX Swiss e alle direttive progettuali KNX Swiss, gli integratori di sistemi KNX e i progettisti di impianti elettrici e di sistemi informatici per gli edifici dispongono di validi strumenti per realizzare con successo i propri progetti.

### Consiglio rapido

Un'ultima osservazione: se tutti i partner progettuali comunicano con gli stessi standard – così come avviene con KNX – il successo del progetto KNX Secure o di una rete informatica sicura dell'edificio è garantito.

## Panoramica dello svolgimento di un progetto KNX Secure

**KNX Preparazione**
Fasi SIA 1 + 2

**KNX Progettazione**
Fase SIA 3

**KNX Appalto**
Fase SIA 4

**KNX Realizzazione**
Fase SIA 5

**KNX Gestione**
Fase SIA 6

Attivazione di KNX Secure

**Inizio del progetto / Preparazione**
Decisione relativa all'impiego di KNX Secure nel progetto
- Definizione dei principi di base e delle responsabilità per l'elaborazione del piano di cibersicurezza / sicurezza

**Progettazione**
Elaborazione del piano di cibersicurezza / sicurezza per KNX / IT
- Definizione degli aspetti da eseguire con KNX Secure o senza di esso
- (non Secure)
- Definizione della gestione dei certificati dei dispositivi («raccolta» dei codici QR (certificati dei dispositivi), archiviazione, selezione della procedura per l'importazione nell'ETS, flusso dei documenti ecc.)
- Preparazione della documentazione KNX Secure
  Considerazione del carico del bus, definizione della topologia

**Appalto**
- Integrazione del piano di cibersicurezza / sicurezza KNX e dell'IT nel capitolato d'appalto
- Definizione delle voci di onorario per la cibersicurezza (KNX e IT) e i servizi necessari
  Preparazione della documentazione KNX Secure

**Creazione del progetto ETS**
- Preparazione del progetto KNX Secure
- Impostazione e documentazione della password di progetto ETS
- Registrazione strutturata nell'ETS delle chiavi del dispositivo KNX Secure secondo il piano elaborato (scanner, fotocamera del notebook, app ecc.)
  Importante: coordinamento in un unico progetto ETS in caso di più team (personale esterno, freelance ecc.)
- Considerazione del carico del bus

**Messa in funzione del progetto**
- KNX Secure pronto (tutti i certificati dei dispositivi sono stati importati) ma non ancora attivato
- Verifica della completezza di tutti i documenti KNX Secure
- Considerazione del carico del bus, attivazione obbligatoria delle tabelle dei filtri

**Ultimazione del progetto di base**
Messa in funzione del progetto, informazione ai clienti finali

*Periodo per adeguamenti o modifiche*

**Data di revisione e adeguamento**
Adeguamenti o integrazioni conformi alle richieste del cliente

**Attivazione di KNX Secure nel progetto ETS**
Attivazione della modalità KNX Secure nell'ETS (password predefinita e documentata). ATTENZIONE! In caso di smarrimento, la password non potrà più essere recuperata!
- Ricaricamento dell'applicazione di tutti i router IP.
- Ricaricamento anche delle applicazioni di tutti i dispositivi TP KNX Secure in modalità Secure (si veda la cartella dinamica «Dispositivi modificati» nell'ETS).

**Consegna del progetto definitivo**
Consegna della documentazione KNX Secure al cliente finale comprensiva di tutte le informazioni Secure come password ecc. (si veda anche la scheda informativa «File di configurazione ETS»)
- Esecuzione del backup del file di progetto compresa l'archiviazione sicura con password di progetto

Creazione del documento

## 6.4 Mezzi ausiliari per l’assistenza progettuale

In stretta collaborazione con operatori esperti rientranti nella cerchia dei propri soci, l’associazione KNX Swiss elabora varie documentazioni tecniche – in forma di schede informative, linee guida e ausili di progettazione – destinate ad assicurare una corretta progettazione, strutturazione e gestione dei progetti. Il loro scopo è quello di ottimizzare ulteriormente i progetti KNX attuali e futuri, dalla progettazione alla realizzazione fino alla relativa gestione.

### 6.4.1 Direttive progettuali KNX Swiss

Le direttive progettuali KNX Swiss rappresentano un mezzo ausiliario prezioso per garantire la qualità dei progetti KNX. Contengono importanti informazioni di base e proposte per un ottimale design progettuale, in quanto la corretta strutturazione di un impianto KNX è determinante per smart home o smart building perfettamente funzionanti. Le direttive progettuali supportano gli integratori di sistemi nella strutturazione chiara delle informazioni nell’ETS e nell’identificazione unitaria degli elementi.


**Figura 6.3-1** Direttive progettuali KNX Swiss: Realizzazione strutturata di progetti KNX

### 6.4.2 Ausilio di progettazione KNX

In Svizzera, la procedura di svolgimento dei progetti edili viene suddivisa nelle fasi e nelle sottofasi previste dal Modello di prestazioni della Società svizzera degli ingegneri e degli architetti (SIA). Per ciascuna di queste fasi, l'ausilio di progettazione KNX Swiss mette a disposizione liste di controllo esaustive che indicano chiaramente quali lavori devono essere eseguiti e quando questi vanno svolti nonché a quali domande è necessario rispondere e in quale momento. Le liste di controllo trattano anche il tema KNX Secure, vale a dire il tema delle reti informatiche sicure negli edifici. I contenuti dell'ausilio di progettazione si basano principalmente sull'esperienza pluriennale dei partner KNX, degli integratori di sistemi KNX e dei progettisti di impianti elettrici che realizzano per la propria clientela impianti ottimali, privi di errori ed efficienti dal punto di vista energetico.


**Figura 6.3-2** Ausilio di progettazione KNX Swiss: Progettazione e realizzazione strutturata di progetti KNX

www.knx.ch

## Gruppo di progetto e autori

KNX Secure è in continua evoluzione, quindi i vostri contributi e le vostre aggiunte sono sempre benvenuti. Aiutateci a mantenere questa guida aggiornata. Saremmo molto lieti di leggere i commenti di tutto il settore.

www.knx.ch/secure
knx@knx.ch

**Autori**

- Bruno Habegger, com:agentur
- René Senn, raum consulting

**Con la collaborazione di**

- Beat Bebi, Feller SA
- Thomas Roth, Maneth Stiefel AG
- Stefan Balsiger, Siemens Svizzera SA
- Klaus Wächter, Siemens AG
- Christoph Koch, Cisco Schweiz

KNX NATIONAL SWISS

**Segretariato KNX Swiss**
Bahnhofstrasse 88
8197 Rafz