KNX

NETx AUTOMATION

All-in-one

Building management software for medium-sized and enterprise building automation projects

Building management systems for providing security in existing KNX projects:

organizational measures and device monitoring

NETxAutomation Software GmbH

Austrian, globally active company
–
founded in 2001

Our customers

- Electrical planner
- Electricians
- System integrators

20
years of experience

100+
countries represented

500,000+
projects with over 500,000 data points

8,000+
active licenses

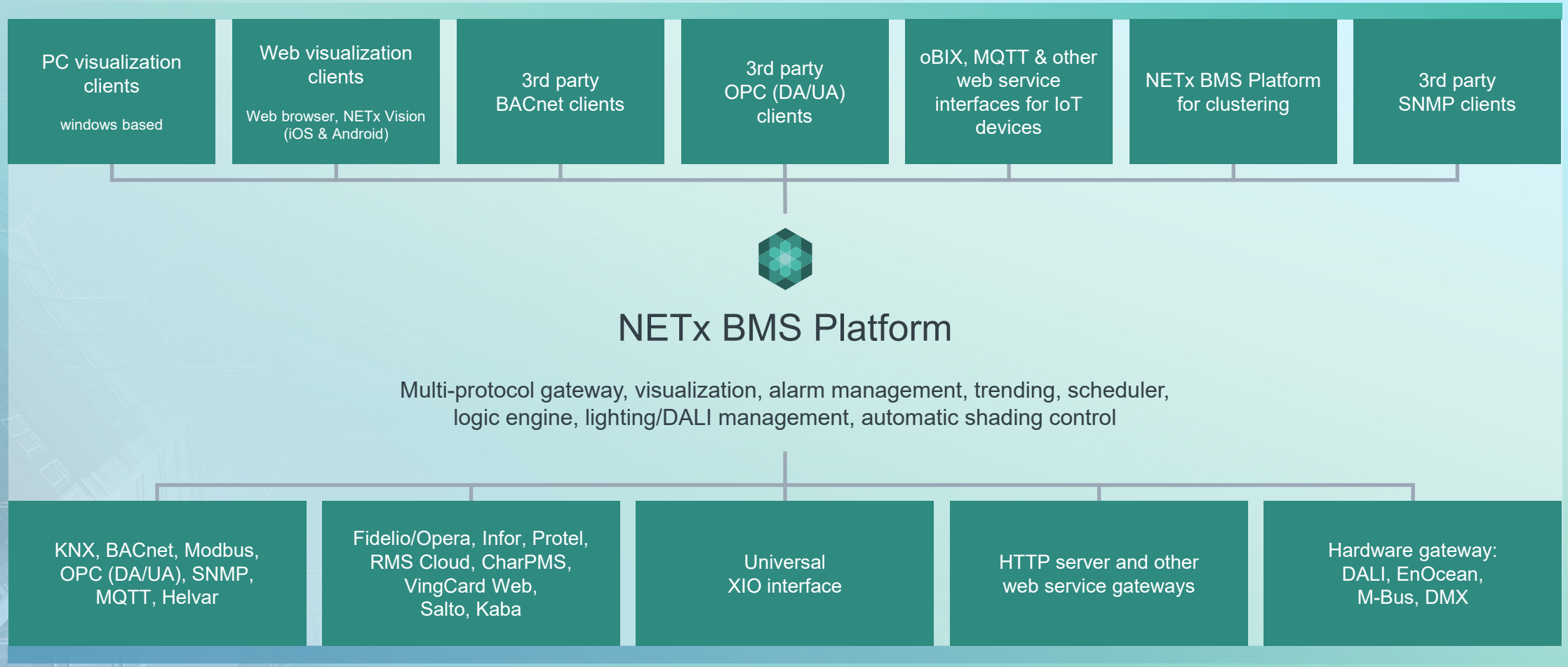
40
intern. sales- and R&D Partner

Software solutions for building automation systems

Management applications: visualization, energy reporting, automatic shading control, lighting control, project support

Integration of heterogeneous building automation networks: building management system platform (BMS Platform), OPC server

NETx BMS Platform



Why is security important?

NETx AUTOMATION

Is security important in the home and building automation domain?

- “Why should I bother if anyone turns my lights on or off?”
- “If someone wants to know my room temperature, I have no objections”

Security-critical services

- Access control
- Intruder alarms

Vandalism acts may have massive economic impact

- Complete wide shutdown of system in hotel
- Security attacks in functional buildings
- Mass panic in public spaces (e.g., lighting system in concert hall)
- Hospital (e.g., lighting system in emergency room)
- Building system may be entrance point to other (more critical) systems (e.g. hotel management systems)

KNX security

What about security in building automation?

All protocols (KNX, Modbus, BACnet, proprietary solutions) are or were prone to security attacks

The good news is that new security standards are available for KNX

KNX data security

Secure communication for all KNX media

KNX IP security

Additional security measures for KNX over IP networks

KNX security

Is KNX security enough?

Yes, it uses state of the art cryptographic technologies which is used in other application domains (TLS/SSL, e banking, …)

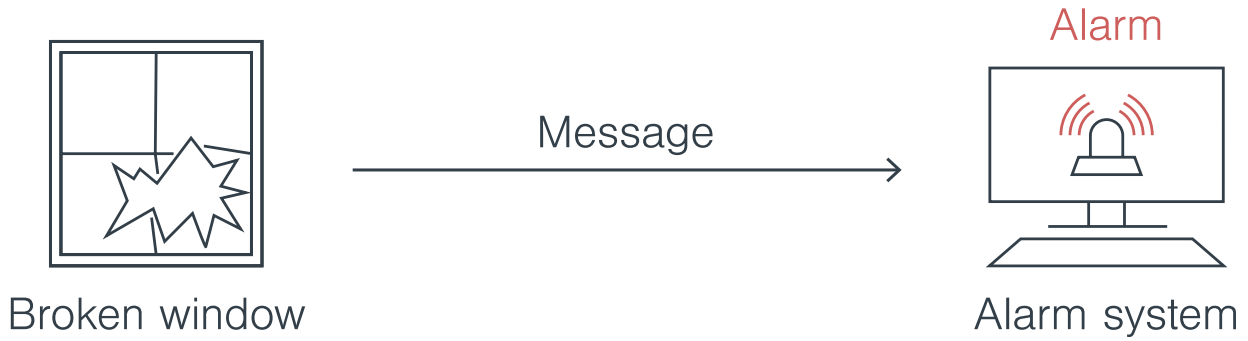
But:

What about existing KNX projects that use non-secure KNX devices?

Secure communication is not enough

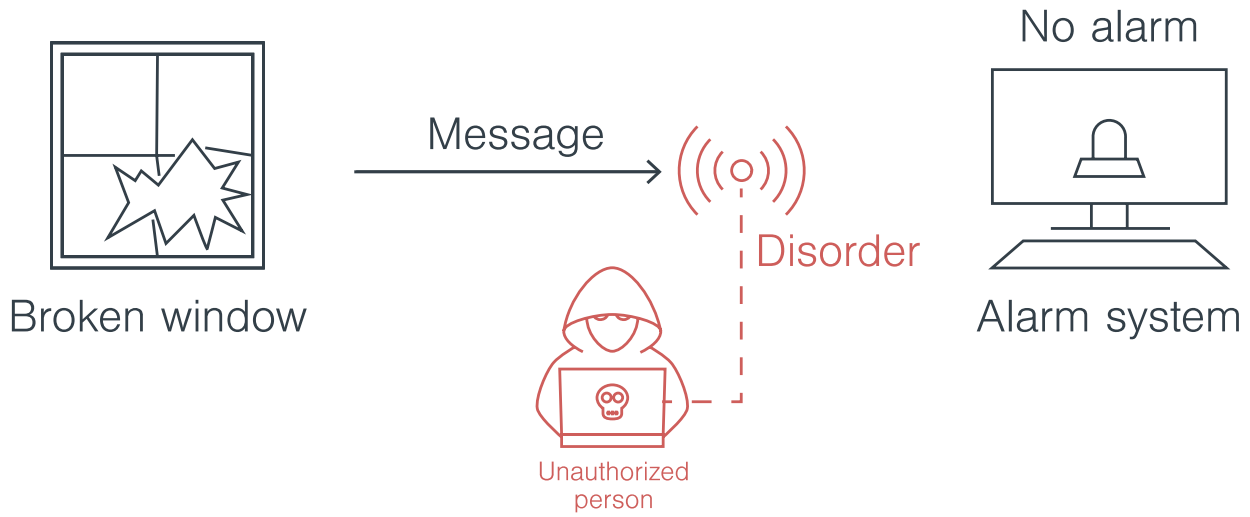
Secure communication is not enough

Example:	Denial-of-service attack in alarm system	Glass breakage sensor message when window is broken



Secure communication is not enough

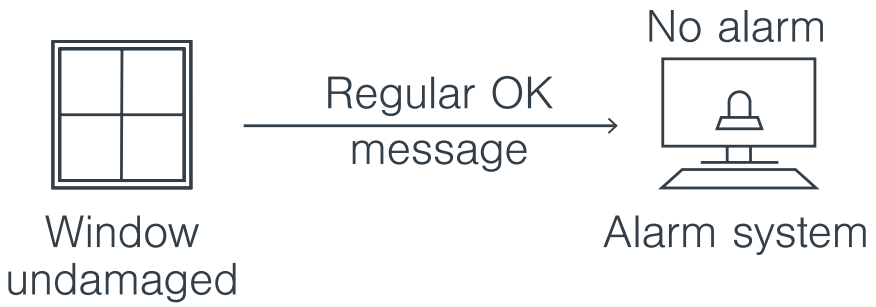
Denial-of-service attack in alarm system	Glass breakage sensor message when window is broken



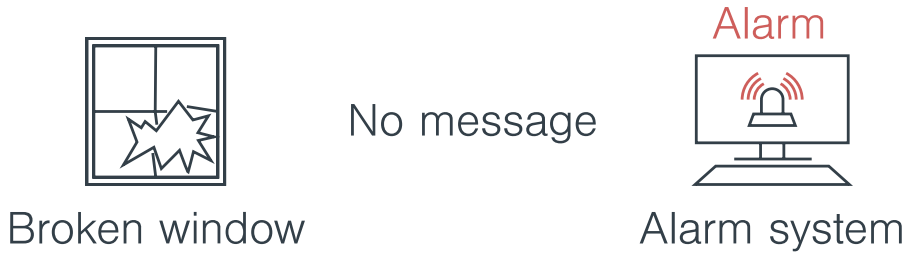
Secure communication is not enough

NETx AUTOMATION

More secure solution:
sensor sends “OK” message periodically



If message is missing alarm is raised



Secure existing KNX projects

Use organizational measures!

- Isolate building automation networks
- Use defence-in-depth methods
- Train the electrical engineers and integrator to use technologies in a right and secure

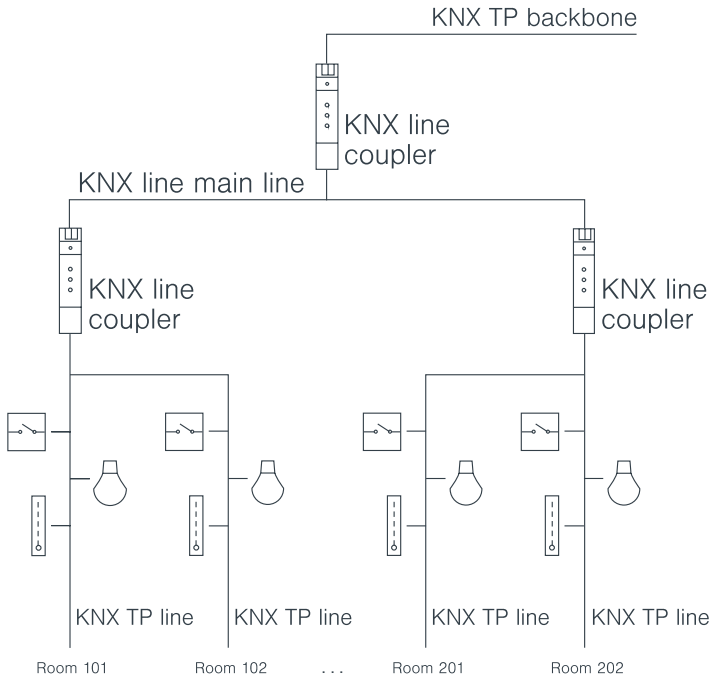
Use additional software tools at the building management level

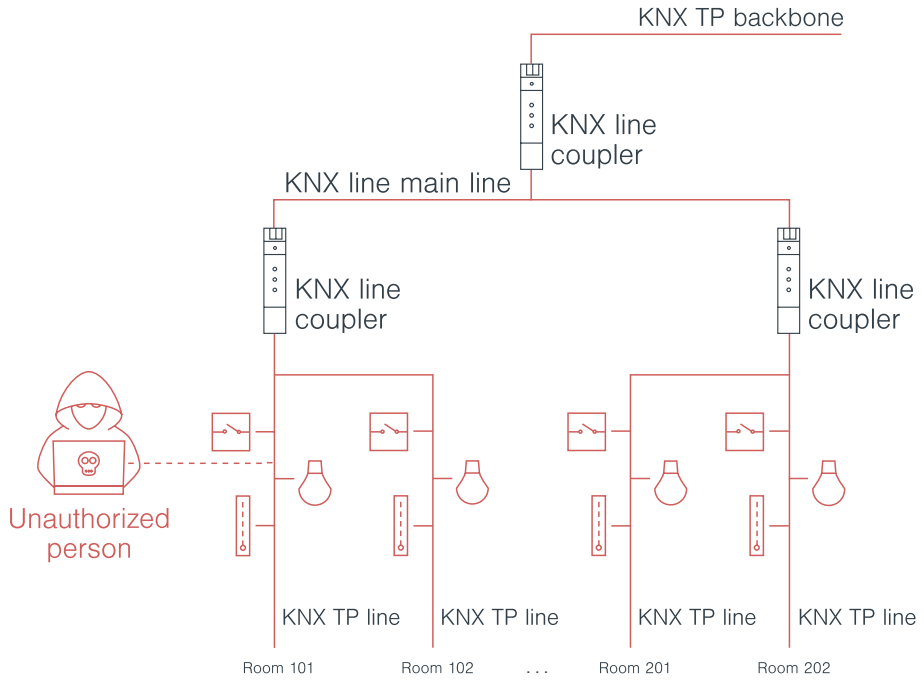
Building management systems that provide additional countermeasures against security attacks

Intrusion detection	Device monitoring and logging	Alarm systems	Visualizations that support TLS connections

Defence in depth in hotel projects

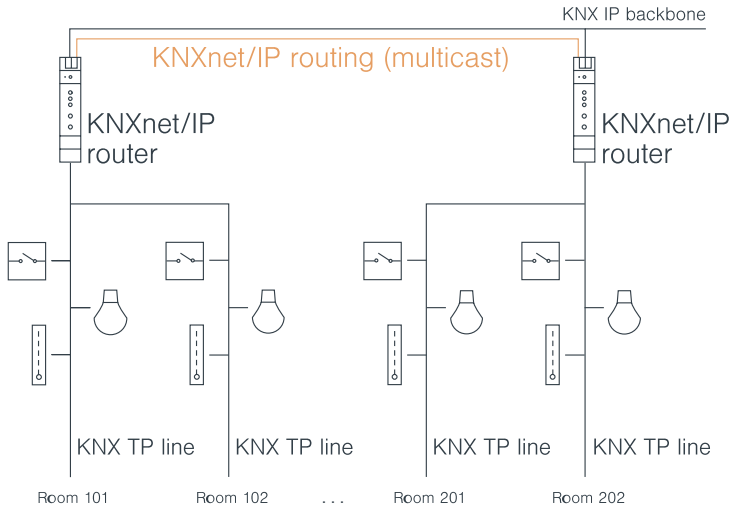
Insecure integration

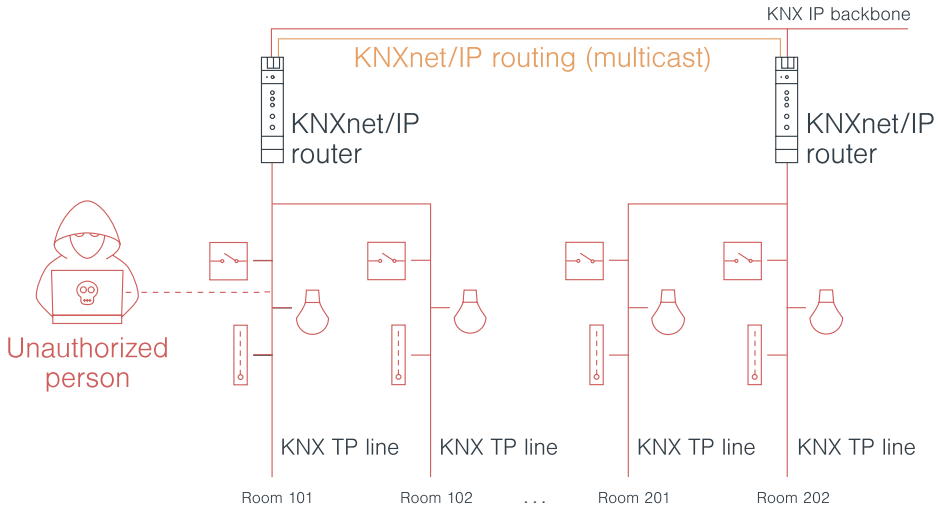




Defence in depth in hotel projects

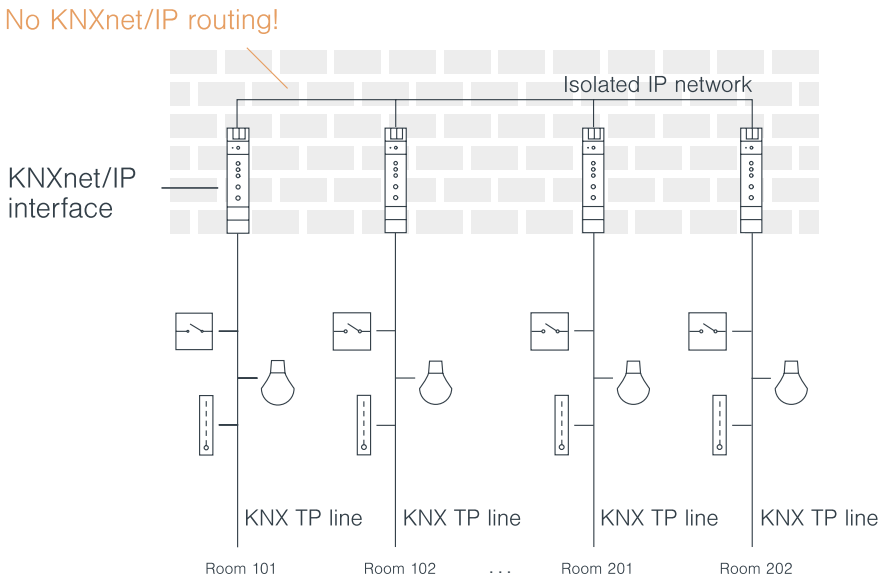
Better, but still insecure

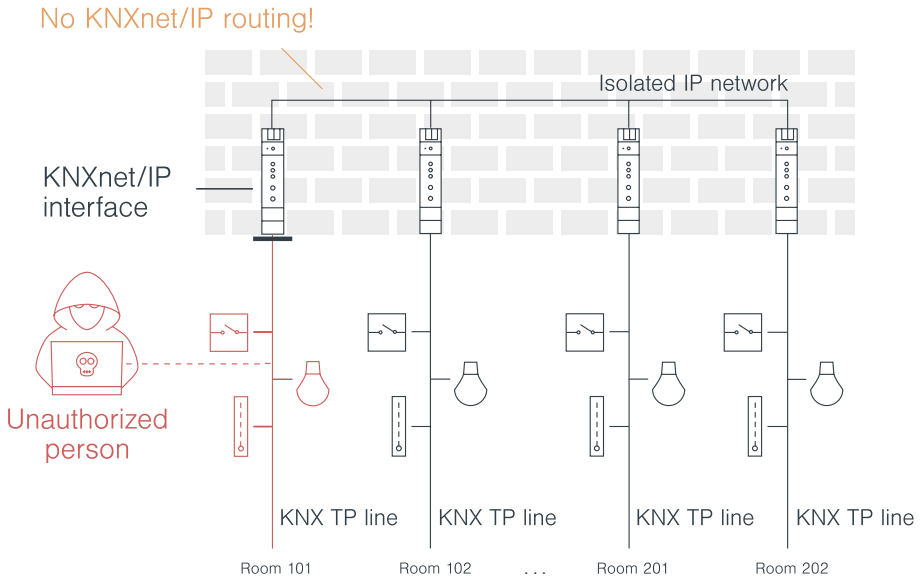




Defence in depth in hotel projects

Security by isolated rooms





Defence in depth in hotel projects - security by isolated rooms

No KNX communication between rooms is necessary

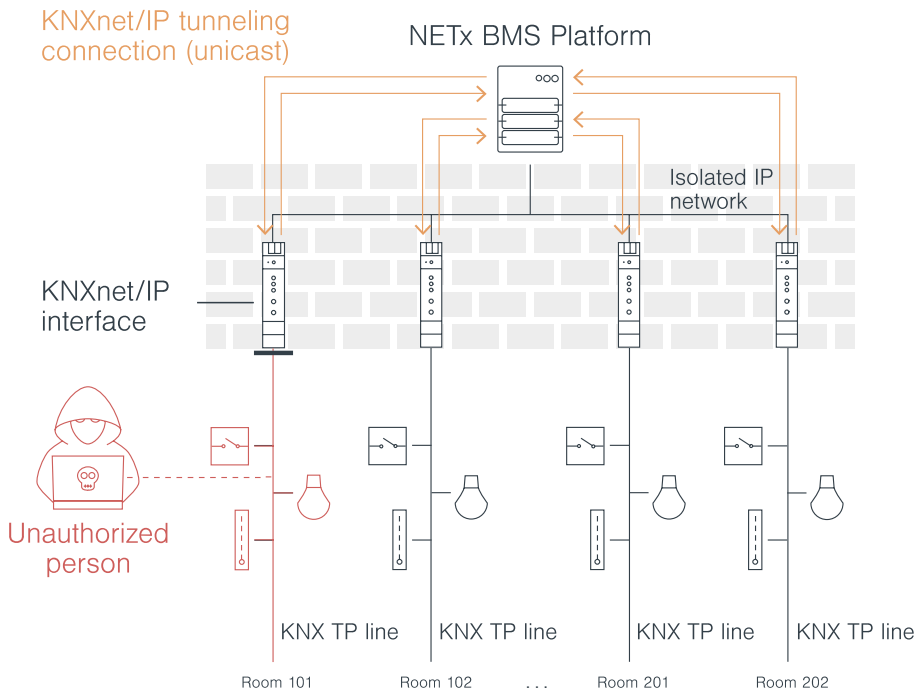
- No KNXnet/IP routing is necessary
- KNXnet/IP interfaces instead of KNXnet/IP routers can be used (much cheaper)

What about central commands like changing set points?

- Using Building Management System (BMS) software

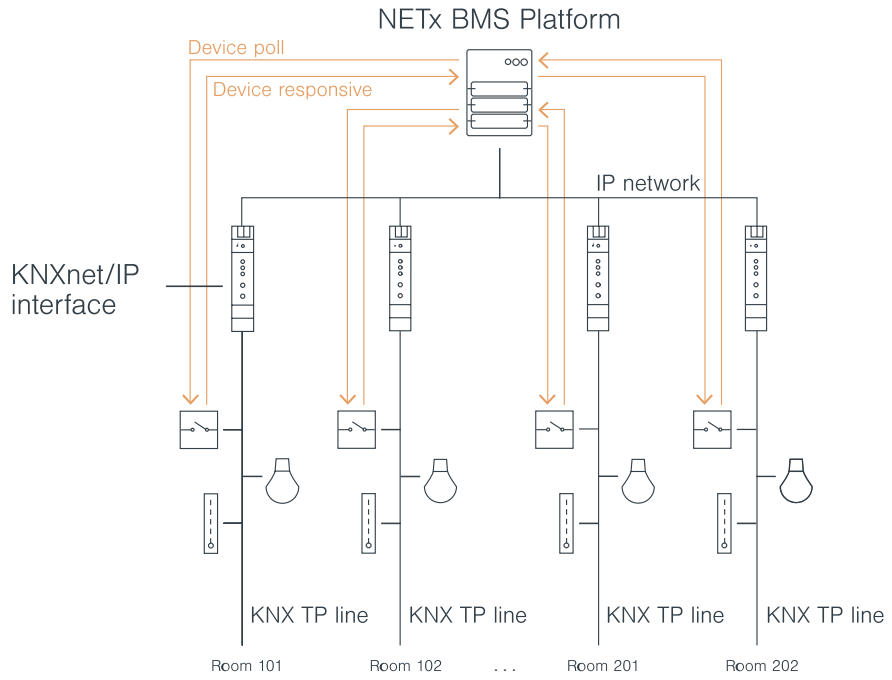
Defence in depth in hotel projects

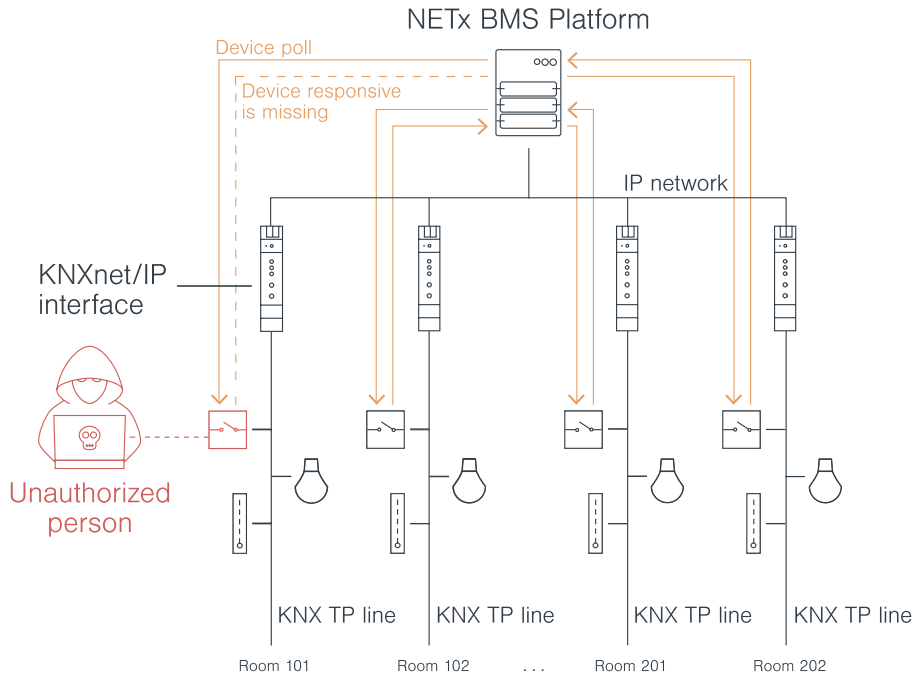
Secure central management using BMS solution



Intrusion detection with BMS

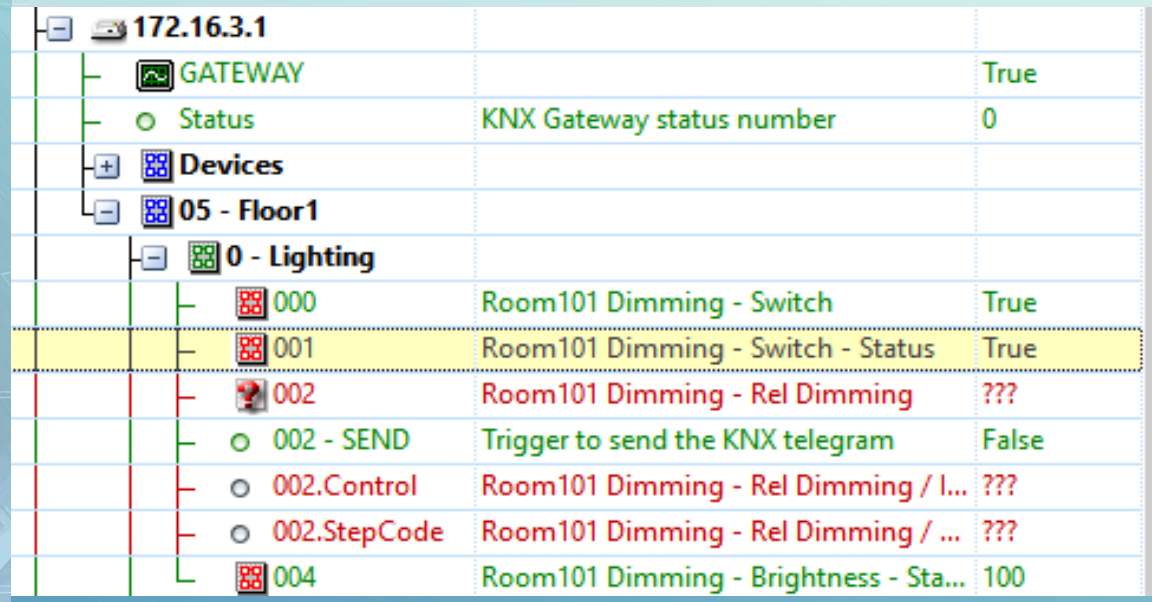
Device monitoring

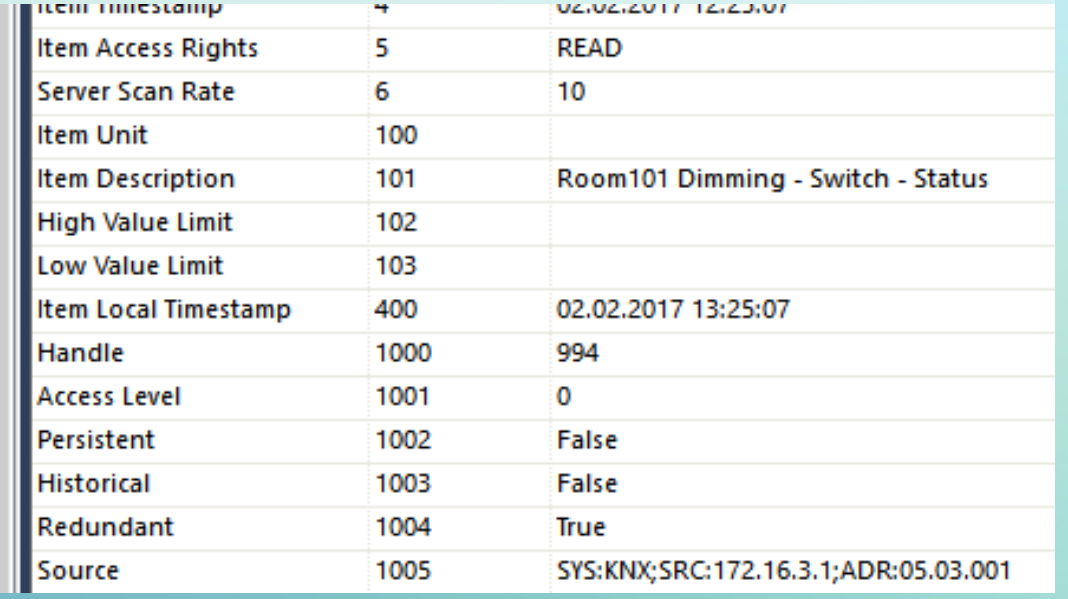




Intrusion detection with BMS

Device polling using KNX management request	If device is not responding within appropriate time, alarm is raised	No bandwidth problem due to multiple point-to-point tunnelling connections	Data source information is also available

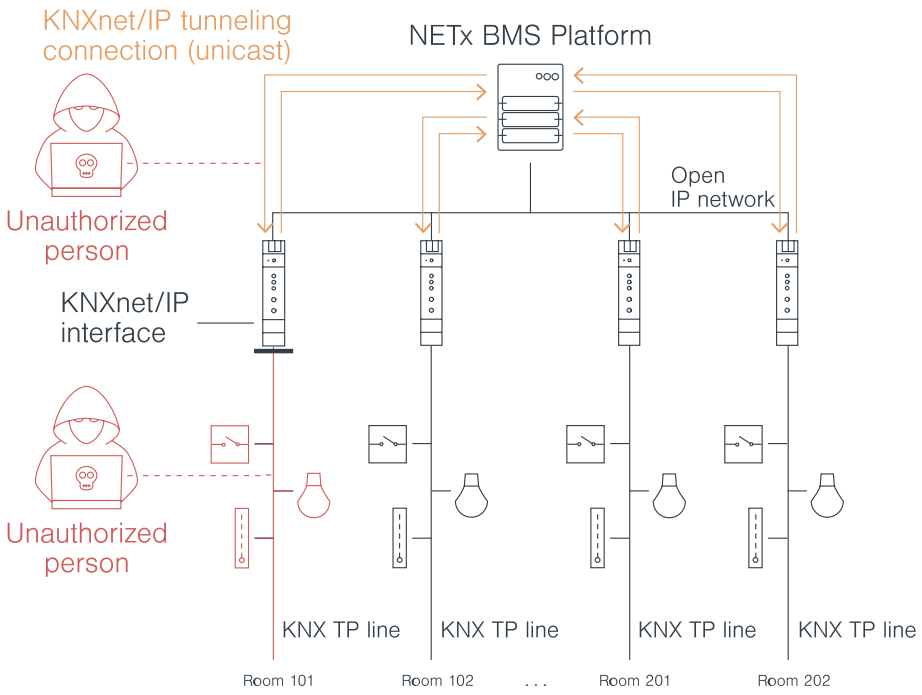




Isolation of the IP network

What to do if the IP network can not be isolated?

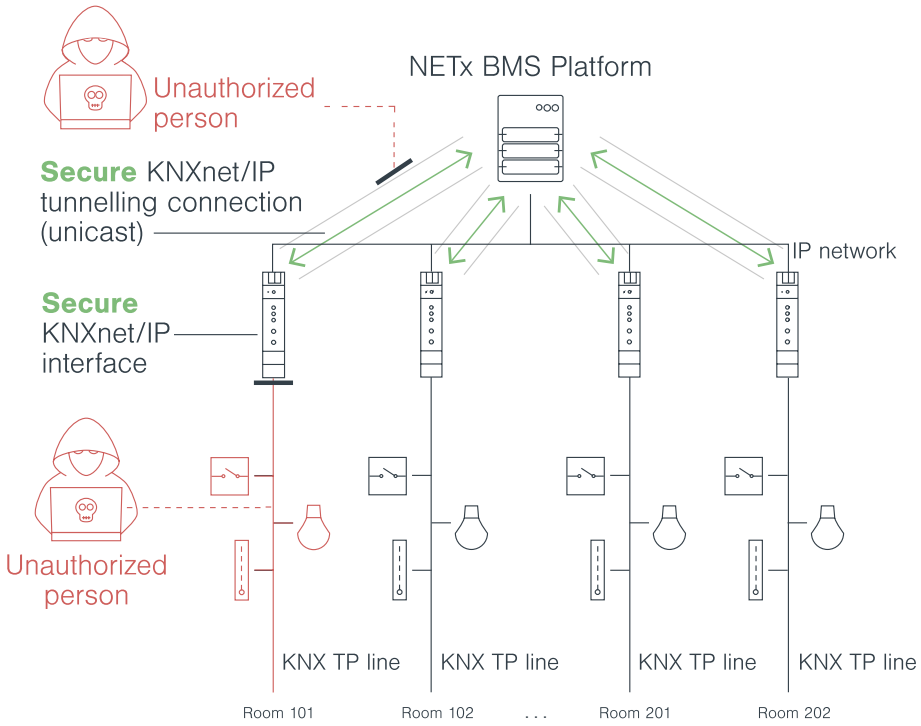
Using KNX security standard: secure KNXnet/IP tunnelling



Secure KNXnet/IP tunnelling

New KNXnet/IP security protects communication between BMS Platform and KNXnet/IP routers and interfaces

Malicious users with access to IP network cannot disturb KNXnet/IP communication

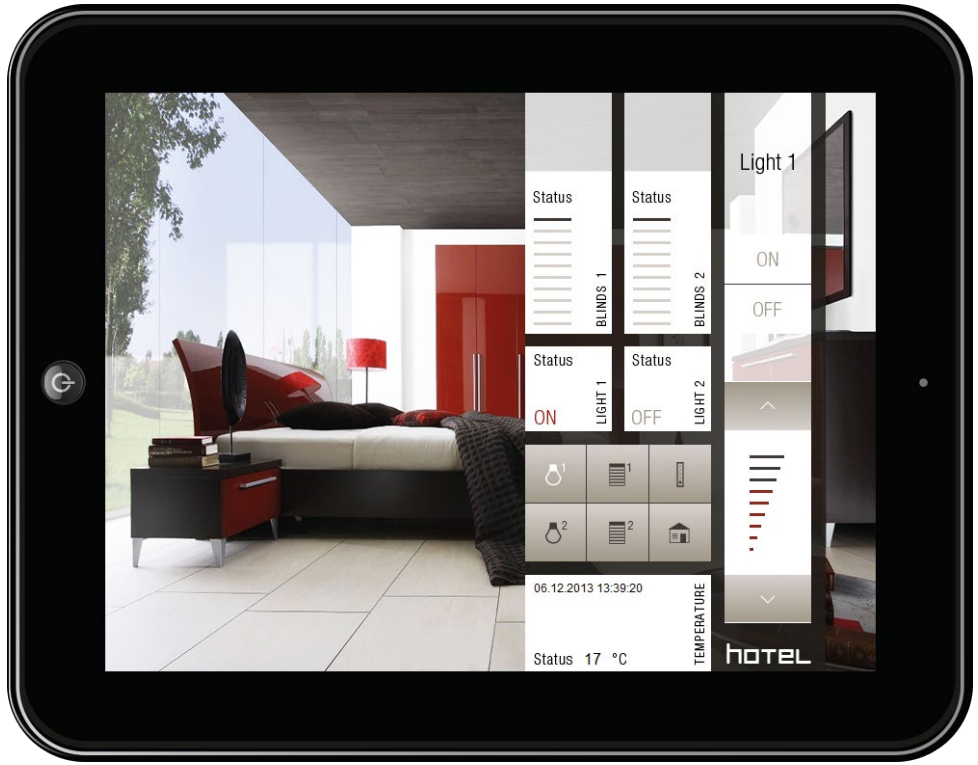


Secure visualization with NETx BMS Platform

NETx BMS Platform provides web-based visualization

Pure HTML5 and JavaScript https support using TLS

Username/password authentication



Secure KNXnet/IP tunnelling driver

NETx AUTOMATION

Available for NETx BMS Platform

Secure KNXnet/IP tunnelling

Can be used with new secure KNXnet/IP routers and interfaces

NETx AUTOMATION

www.netxautomation.com