Building management systems for providing security in existing KNX projects: Organizational measures and device monitoring

Part 2: Security in existing KNX projects

To avoid security lapses in existing KNX projects, different organizational measures can be used:

- Using defense-in-depth-methods
- Isolation of building automation networks
- Training of electrical engineers and integrators to use technologies in a right and secure way

The following additional software tools at the building management level can increase security:

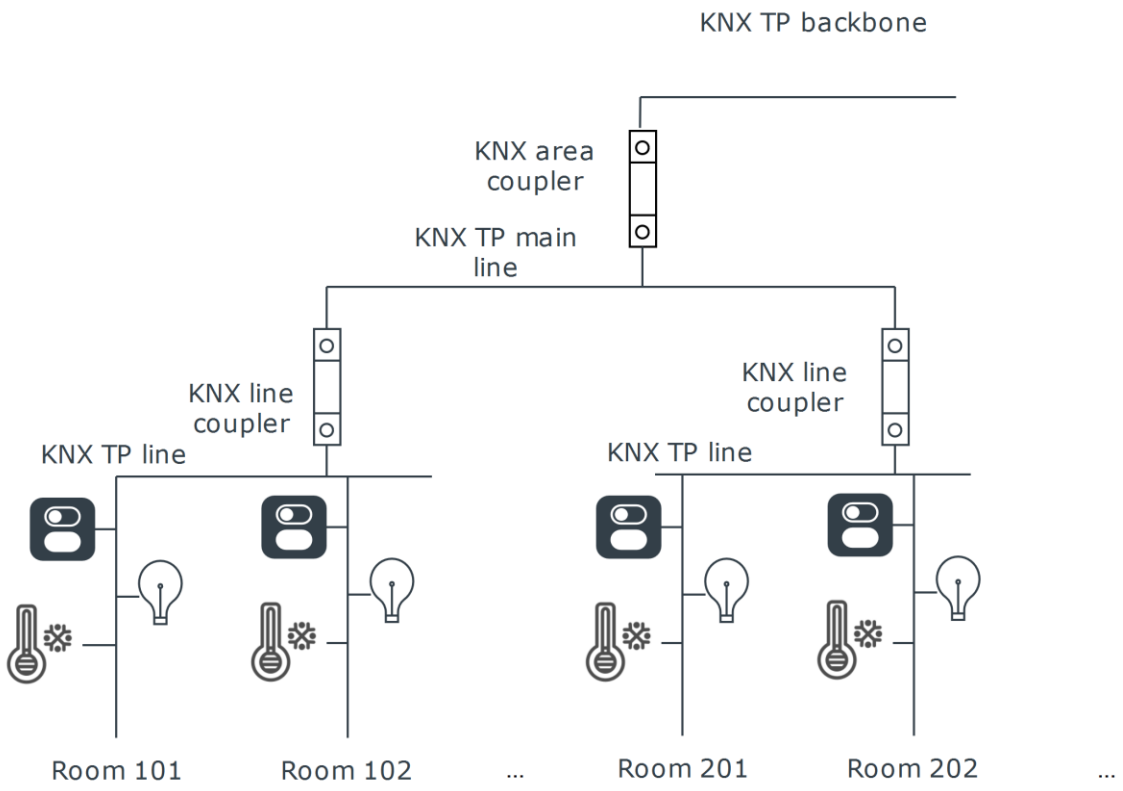
- Intrusion detection
- Alarm systems
- Device monitoring and logging
- Visualization, that support TLS/SSL connections

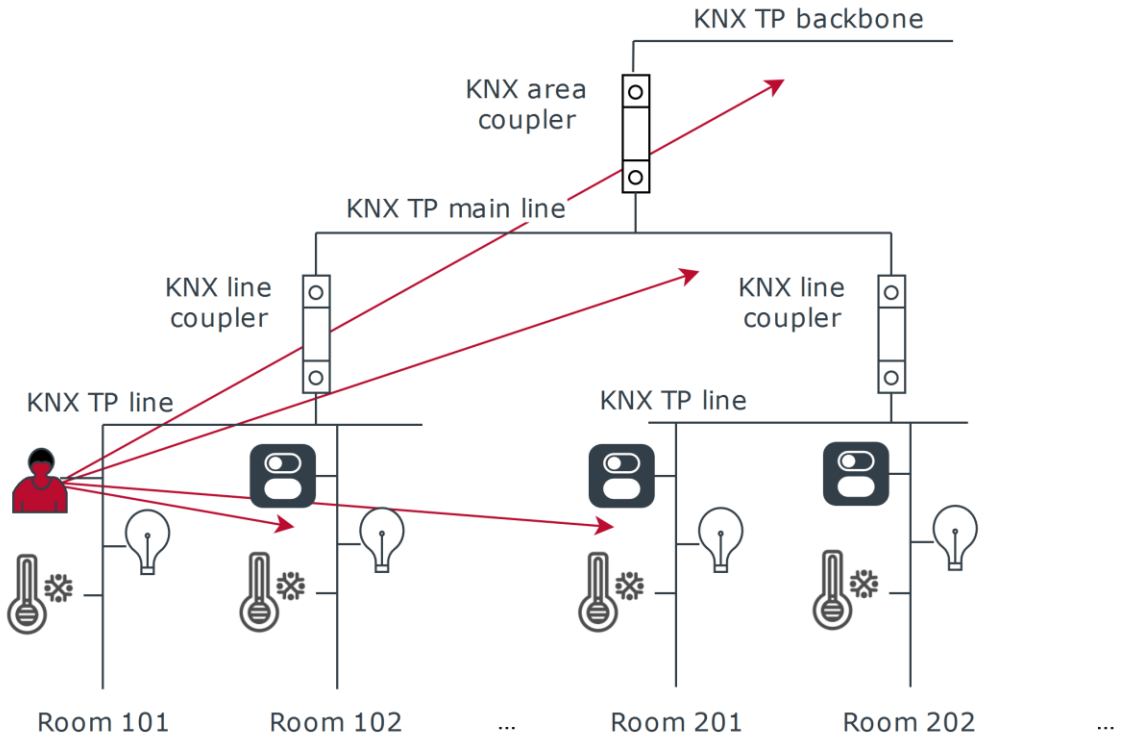
The following examples will show you how to make existing building automation projects secure.

Defense in Depth in hotel projects

Example 1: Insecure integration

The image below shows the typical structure of a building automation system using are and line couplers. An invader might get access to the whole KNX network by e.g. removing a KNX device he can access the according BUS cable. In principle area and line coupler have the task to filter the data traffic, but sometimes filtering is not possible (e.g. central visualization at the backbone) or deactivated.

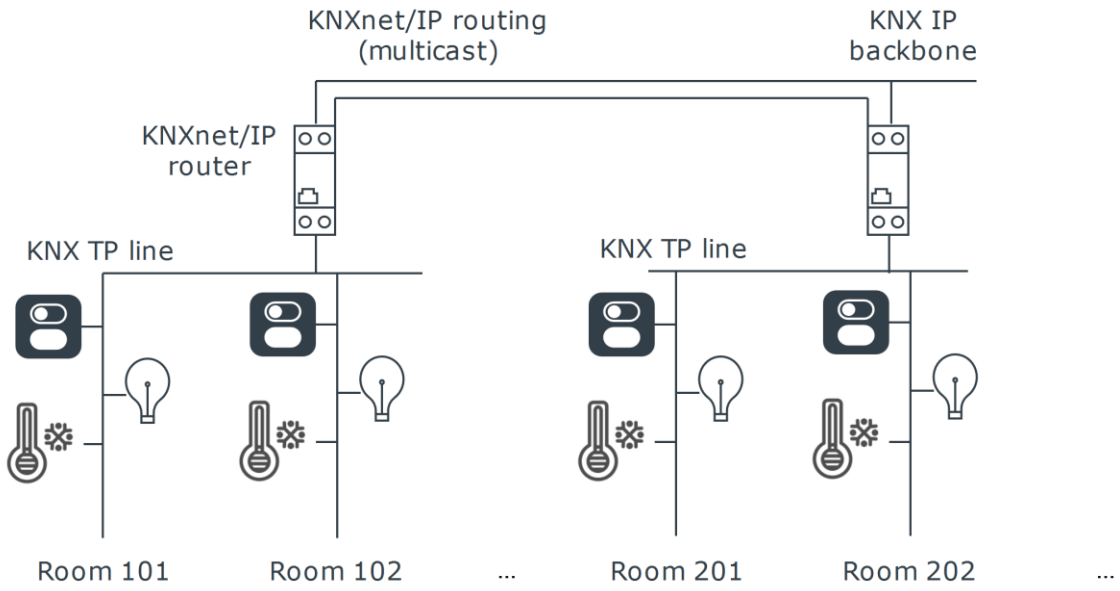

KNX TP backbone
KNX area coupler
KNX TP main line
KNX line coupler
KNX line coupler
KNX TP line
KNX TP line
Room 101
Room 102
...
Room 201
Room 202
...


KNX TP backbone
KNX area coupler
KNX TP main line
KNX line coupler
KNX line coupler
KNX TP line
KNX TP line
Room 101
Room 102
...
Room 201
Room 202
...

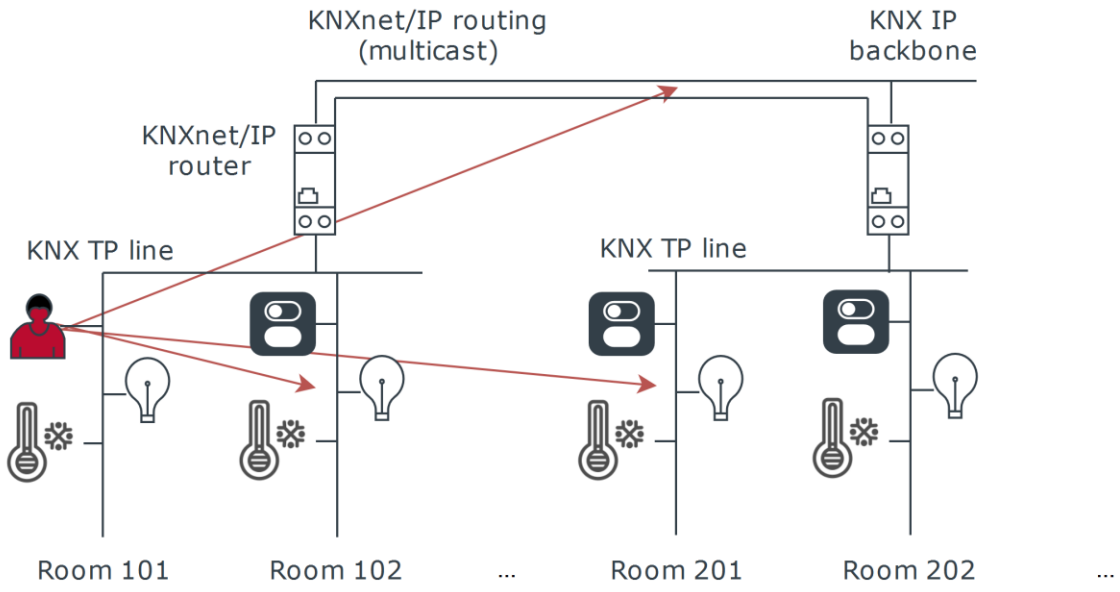
Isolation of building automation networks

Example 2: Better, but still insecure

A better way is using KNXnet/IP routers like shown in the following image.

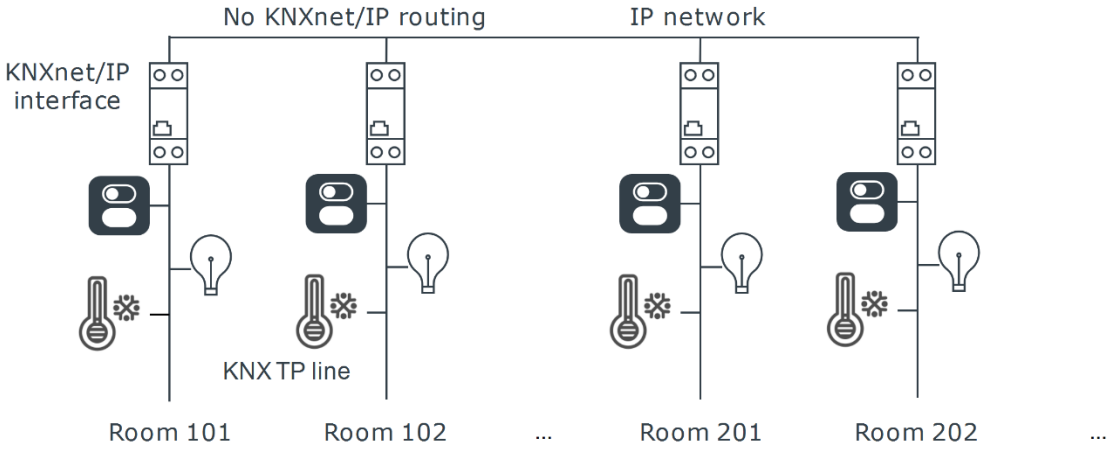


Also in this scenario, it is possible for an invader to access the whole KNX network. Even though, KNXnet/IP routers have filter option, their usage is often limited.

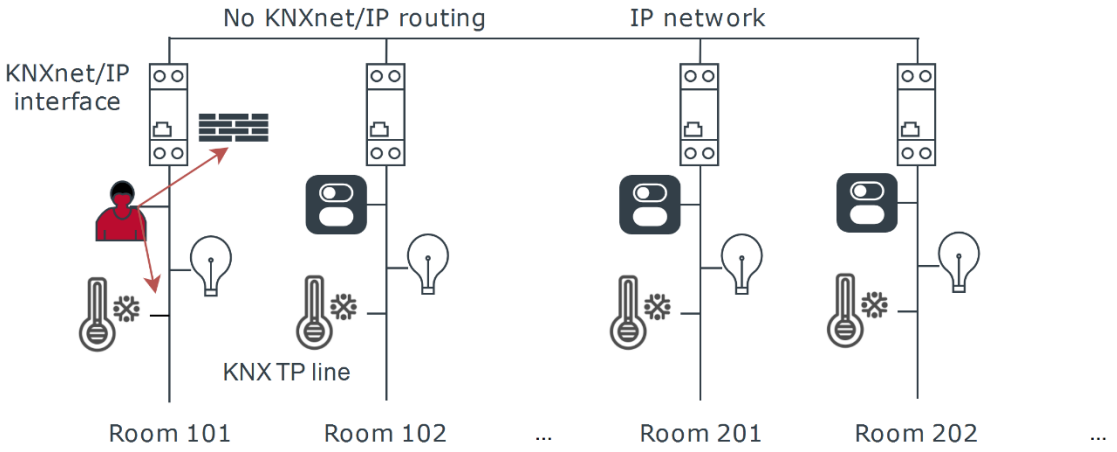


Example 3: Security by isolated rooms

While the two previous examples failed to provide complete security, this scenario provides a significant minimization of security vulnerabilities. Each room uses its own KNX line. To link these lines to the management system above (e.g. visualization) KNXnet/IP interfaces can be used.



Since a KNX communication between the individual rooms is not necessary, KNXnet / IP routing can be dispensed with. For this reason, KNXnet/IP routing within the KNXnet/IP routers should be deactivated. Alternatively, much cheaper KNX interfaces can be used. An attacker is thus restricted to the devices of the hacked room, which gives him no advantage since he has access to his room function anyway. There is no danger to the rest of the system, however, because the attacker is, so to speak, insulated.



But what about central commands like changing the set point, if the communication between the rooms is missing? The best solution is to use sophisticated building management software.

Part 1: Status of security in building automation

Part 3: Secure building automation through management solution (NETx BMS Server)