



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

NETxAutomation

- Austrian company that is operating world-wide
- Founded in 2001

100,000

Projects with 100,000+ data points

16

16 years of experience in building automation

40

Customers in 40+ countries

Software solutions for building automation systems

- Integration of heterogenous building automation networks: Building Management System (BMS) platform, OPC server
- Management applications: visualization, energy reporting, automatic shading control, lighting management, project support

Customers are

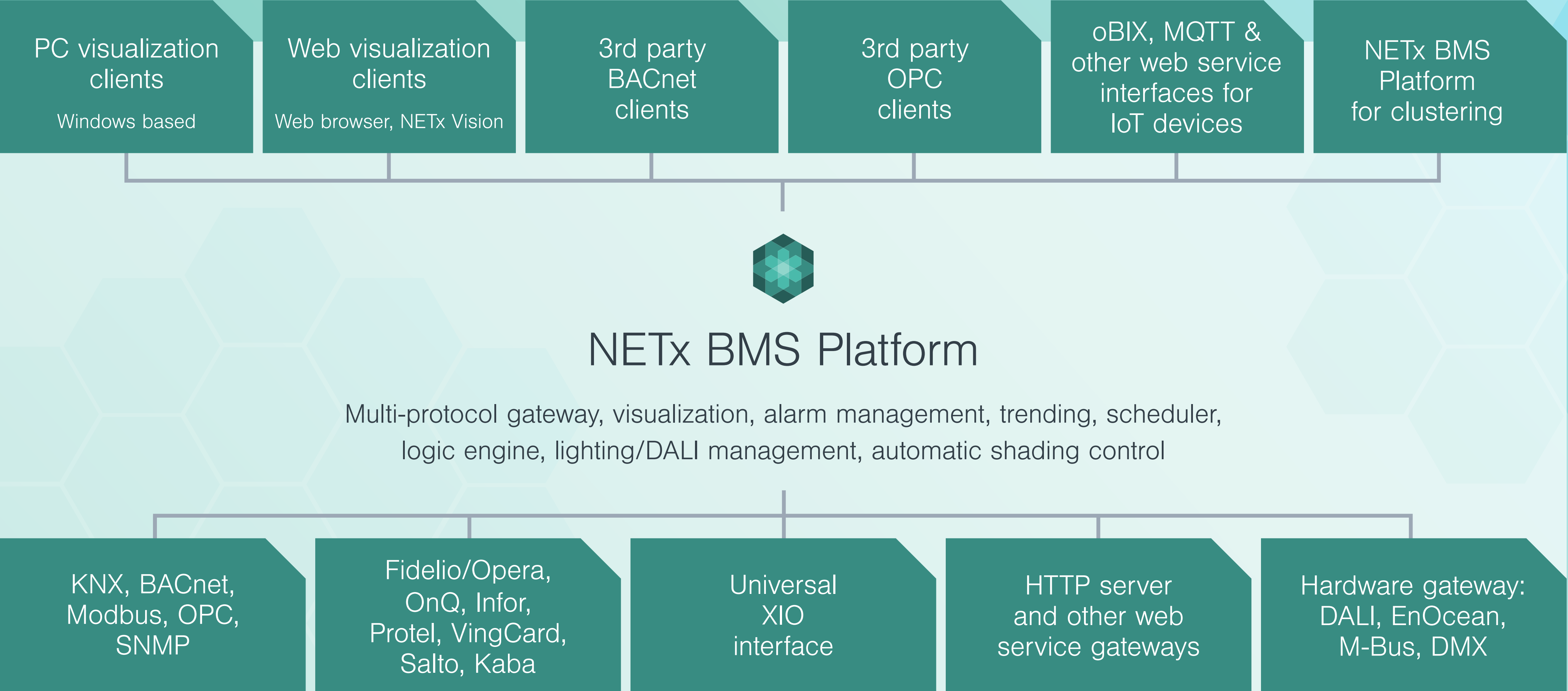
- electrical consultants
- electrical engineers
- system integrators

6,000

6,000+ realized projects

36

36+ international sales, solution and R&D partners



PC visualization clients
Windows based

Web visualization clients
Web browser, NETx Vision

3rd party BACnet clients

3rd party OPC clients

oBIX, MQTT & other web service interfaces for IoT devices

NETx BMS Platform for clustering



NETx BMS Platform

Multi-protocol gateway, visualization, alarm management, trending, scheduler, logic engine, lighting/DALI management, automatic shading control

KNX, BACnet, Modbus, OPC, SNMP

Fidelio/Opera, OnQ, Infor, Protel, VingCard, Salto, Kaba

Universal XIO interface

HTTP server and other web service gateways

Hardware gateway: DALI, EnOcean, M-Bus, DMX

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)

What about security in building automation?

All protocols (LonWorks, 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

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?

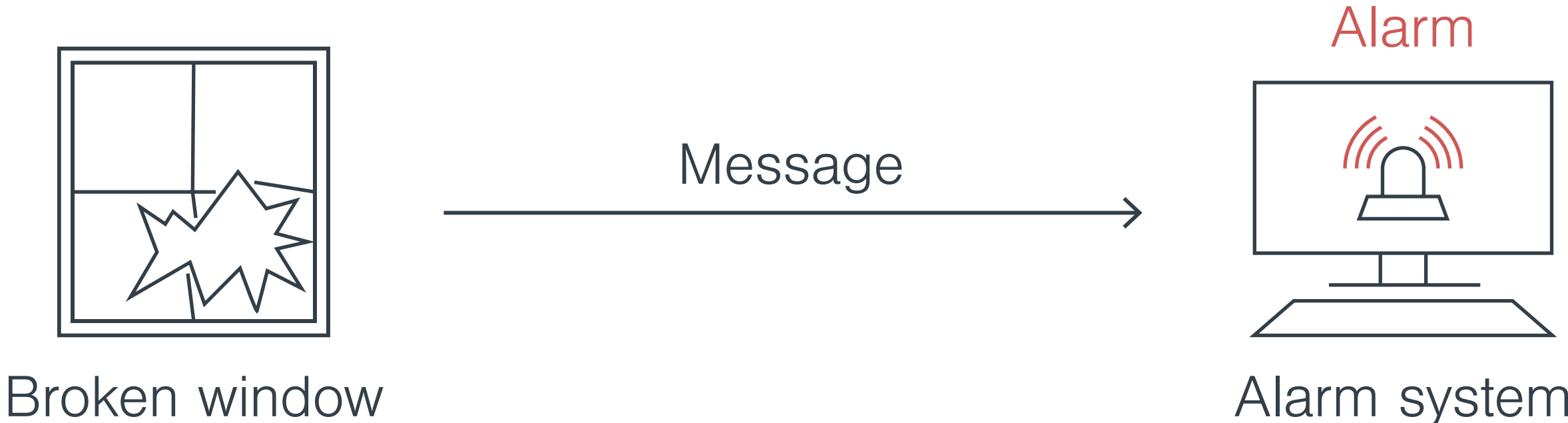
Secure communication is not enough

Secure communication is not enough

Example:

Denial-of-service attack in alarm system

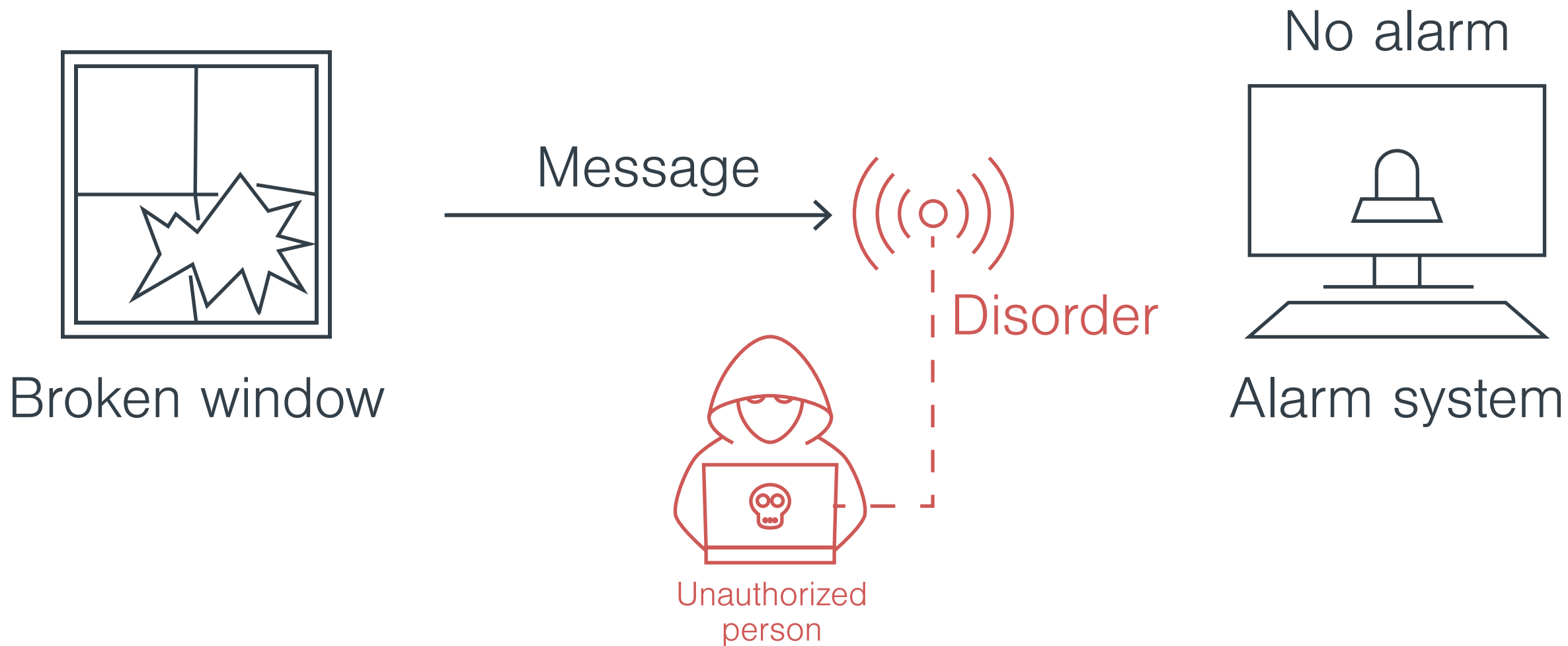
Glass breakage sensor message when window is broken



Secure communication is not enough

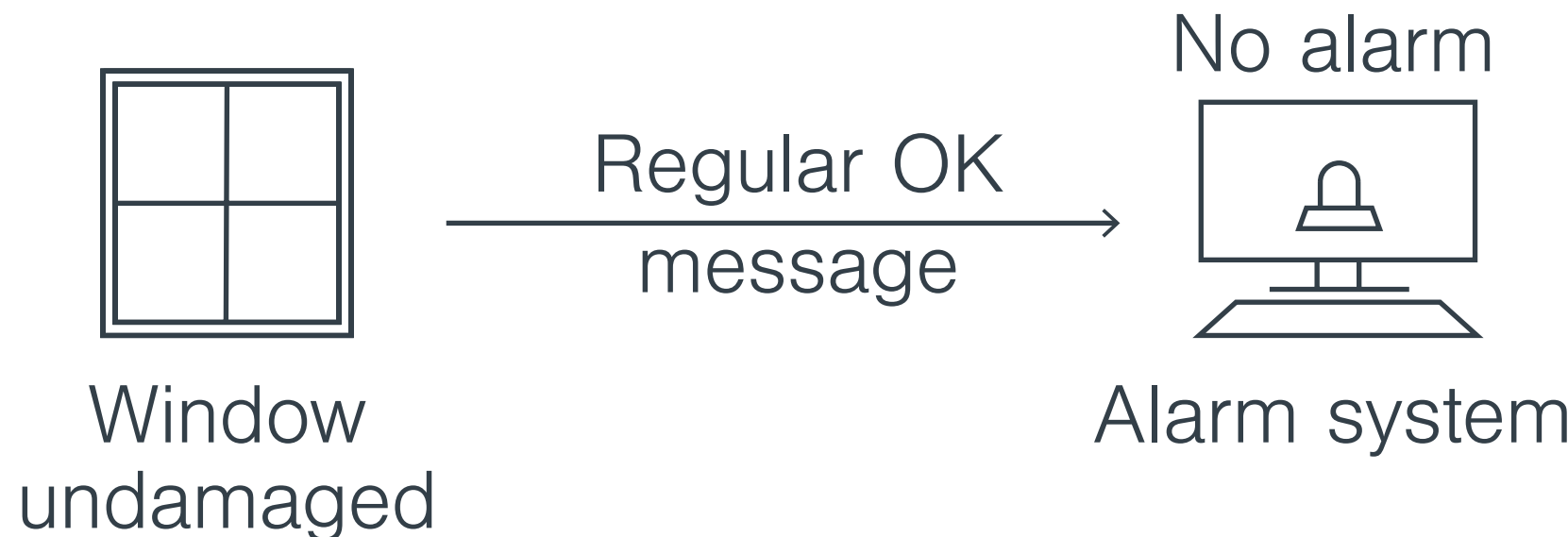
Jamming attack fully breaks alarm system

Message is not received by alarm system

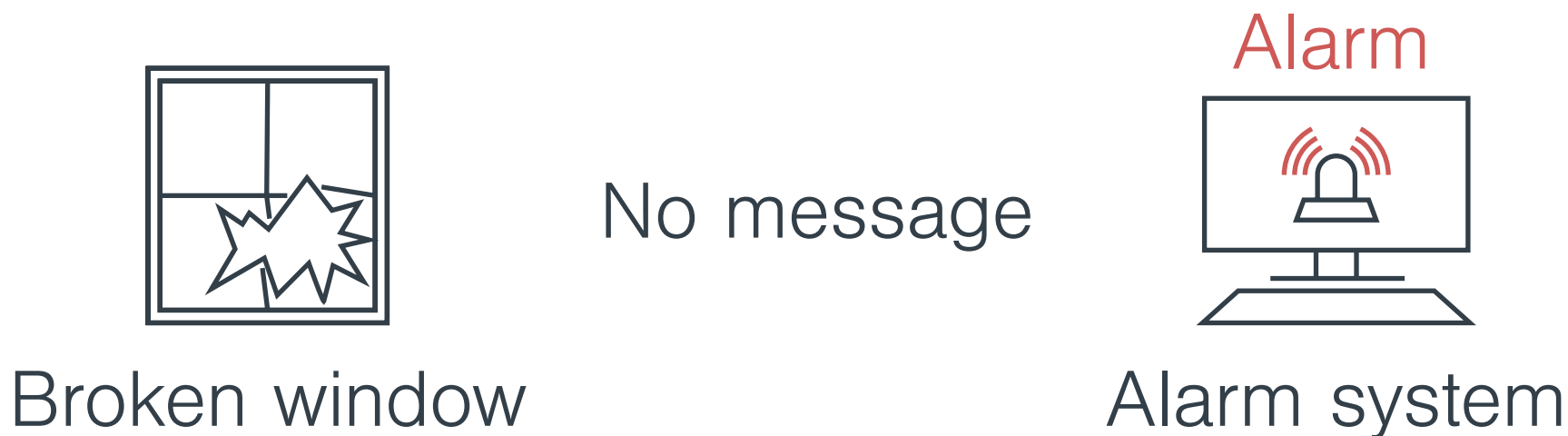


Secure communication is not enough

More secure solution: sensor sends "OK" message periodically



If message is missing alarm is raised



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

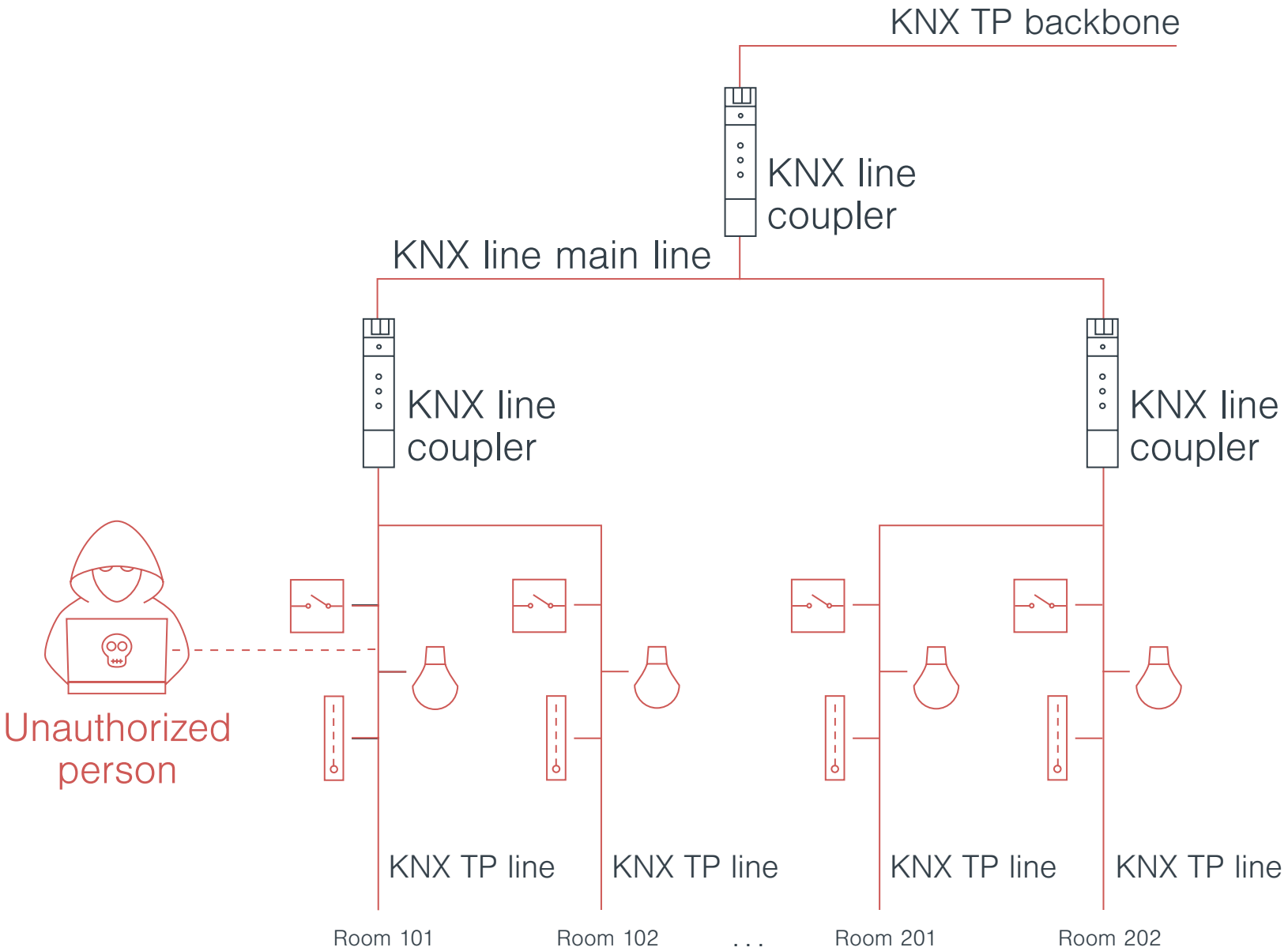
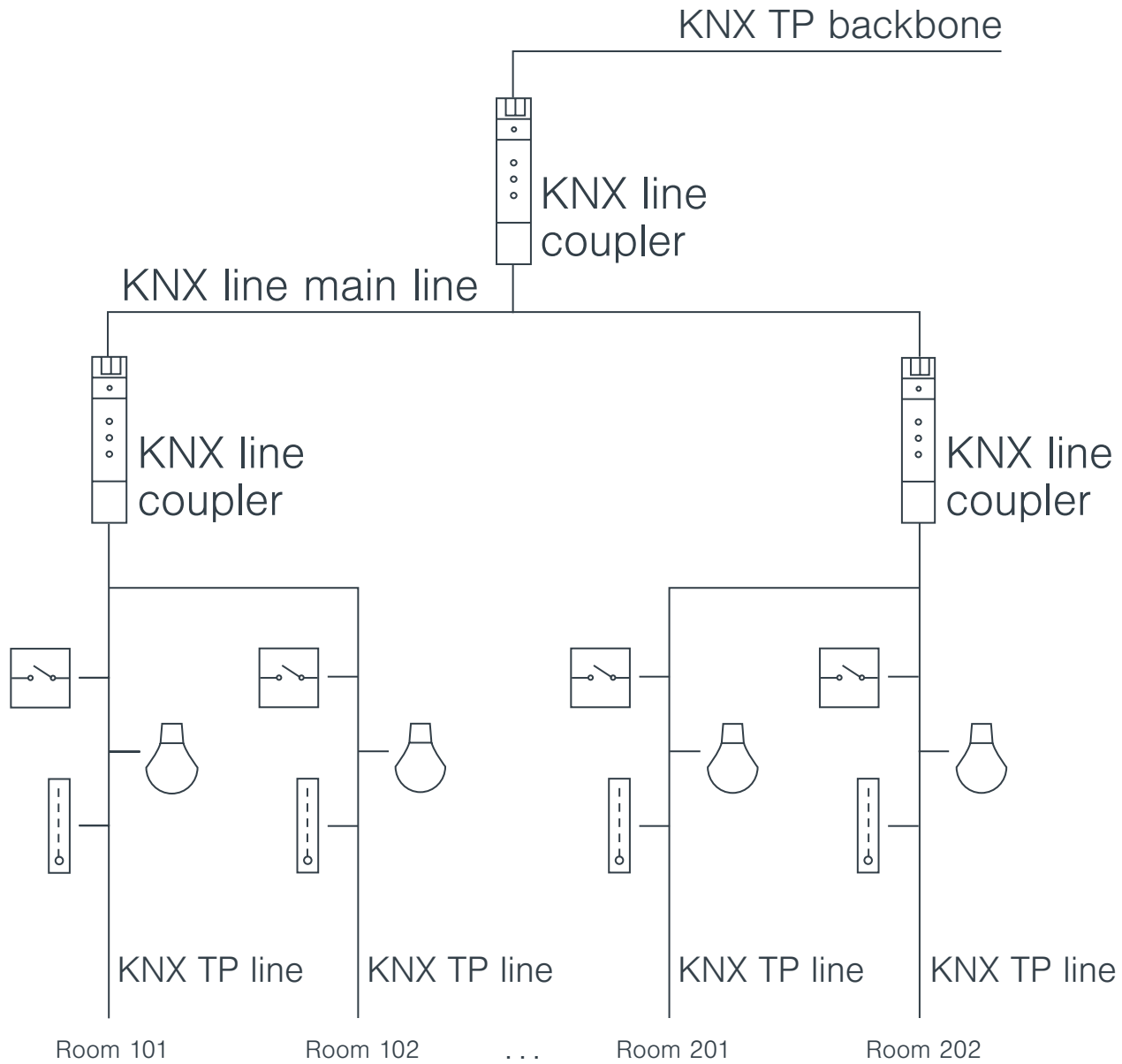
Intrusion detection

Device monitoring
and logging

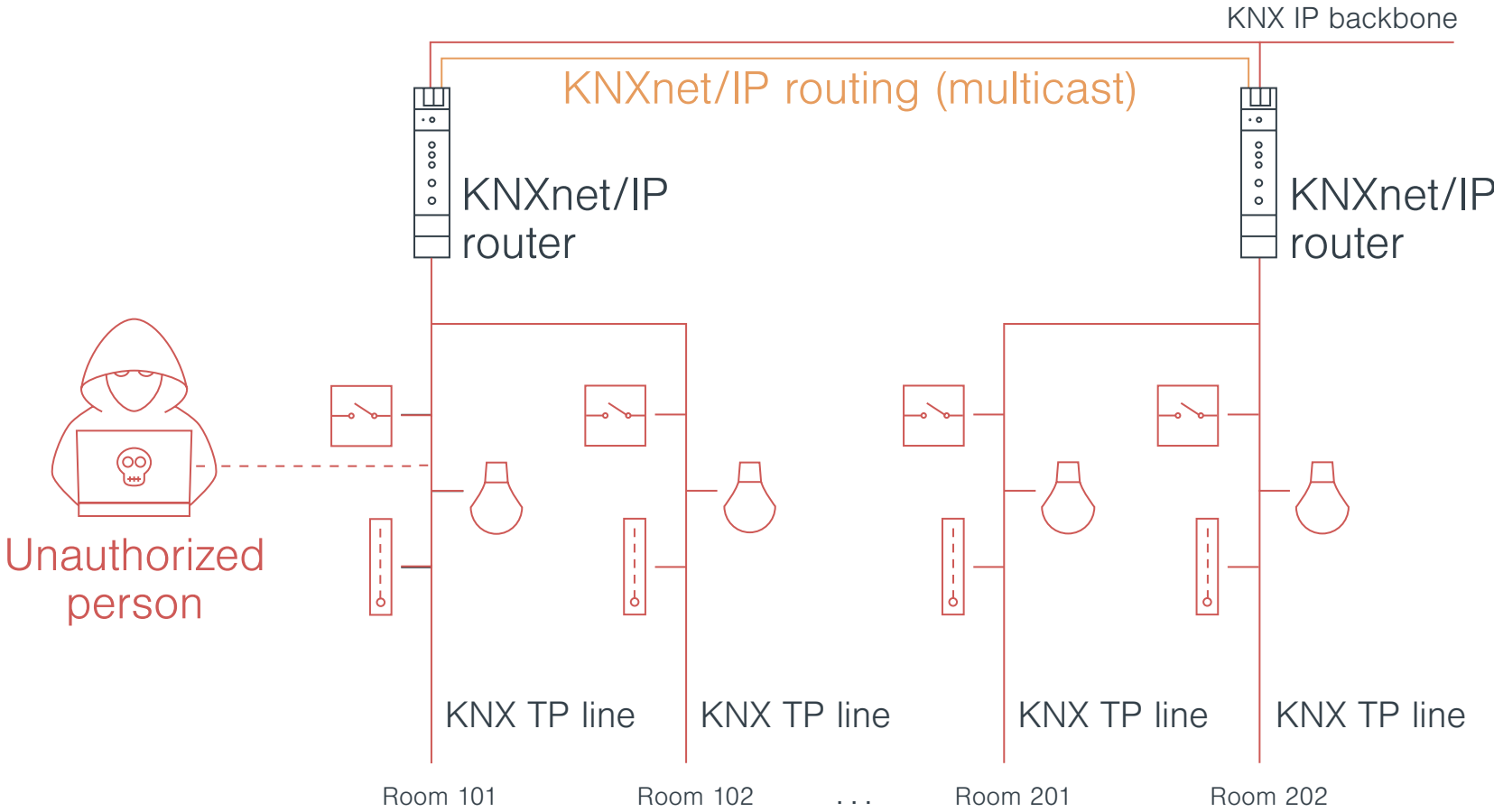
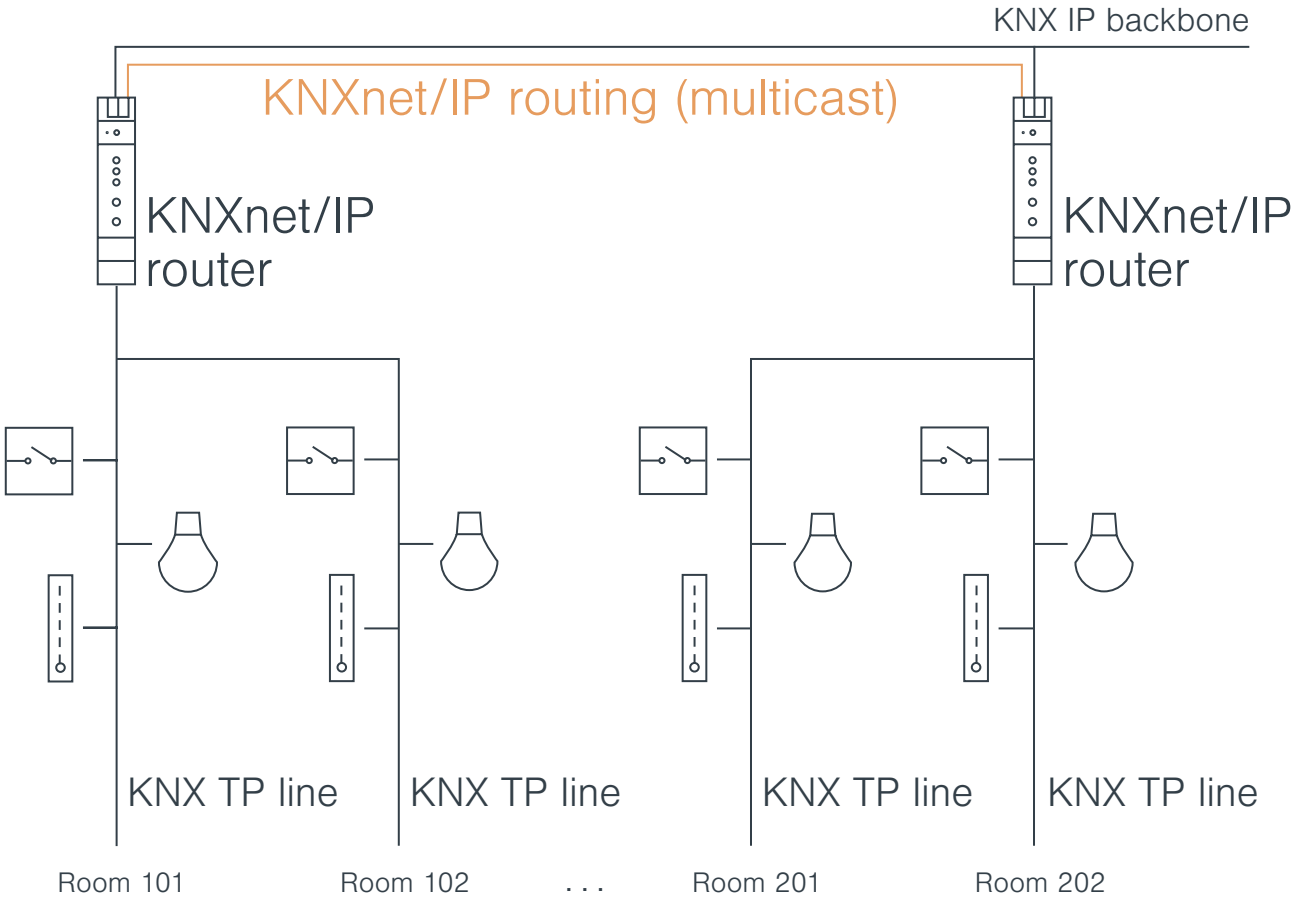
Alarm systems

Visualizations that
support TLS/SSL
connections

Insecure integration

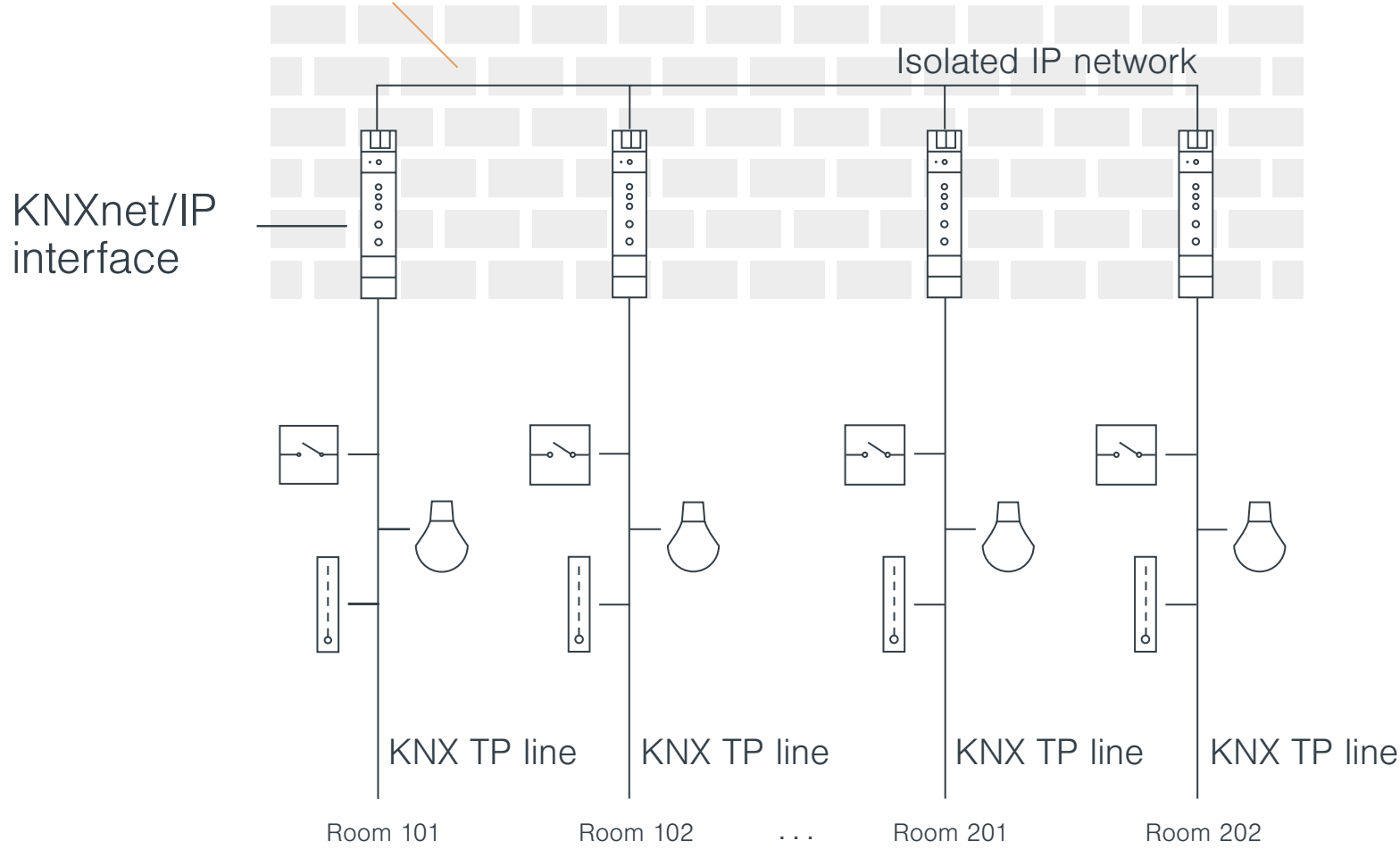


Better, but still insecure

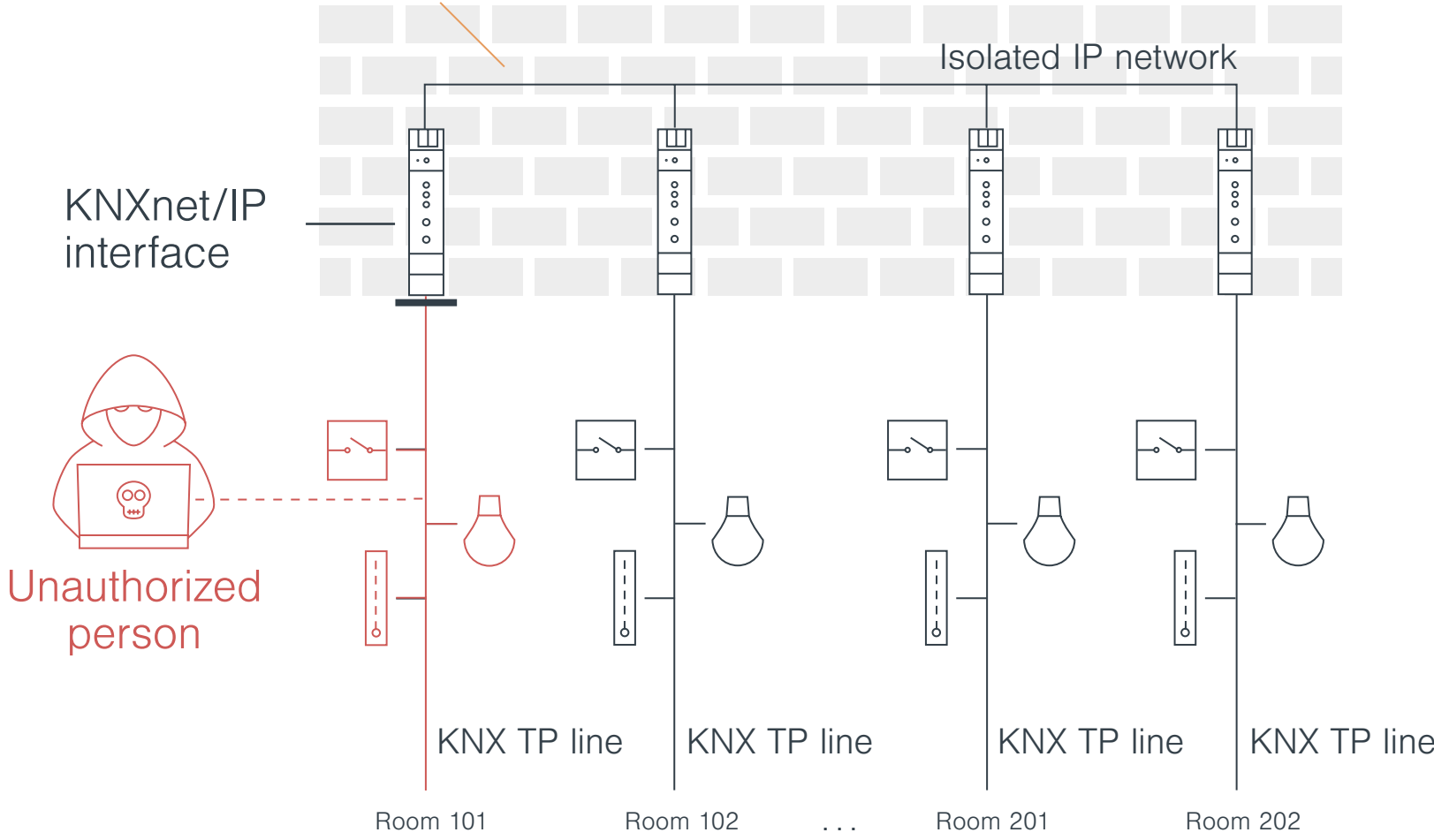


Security by isolated rooms

No KNXnet/IP routing!



No KNXnet/IP routing!



Security by isolated rooms

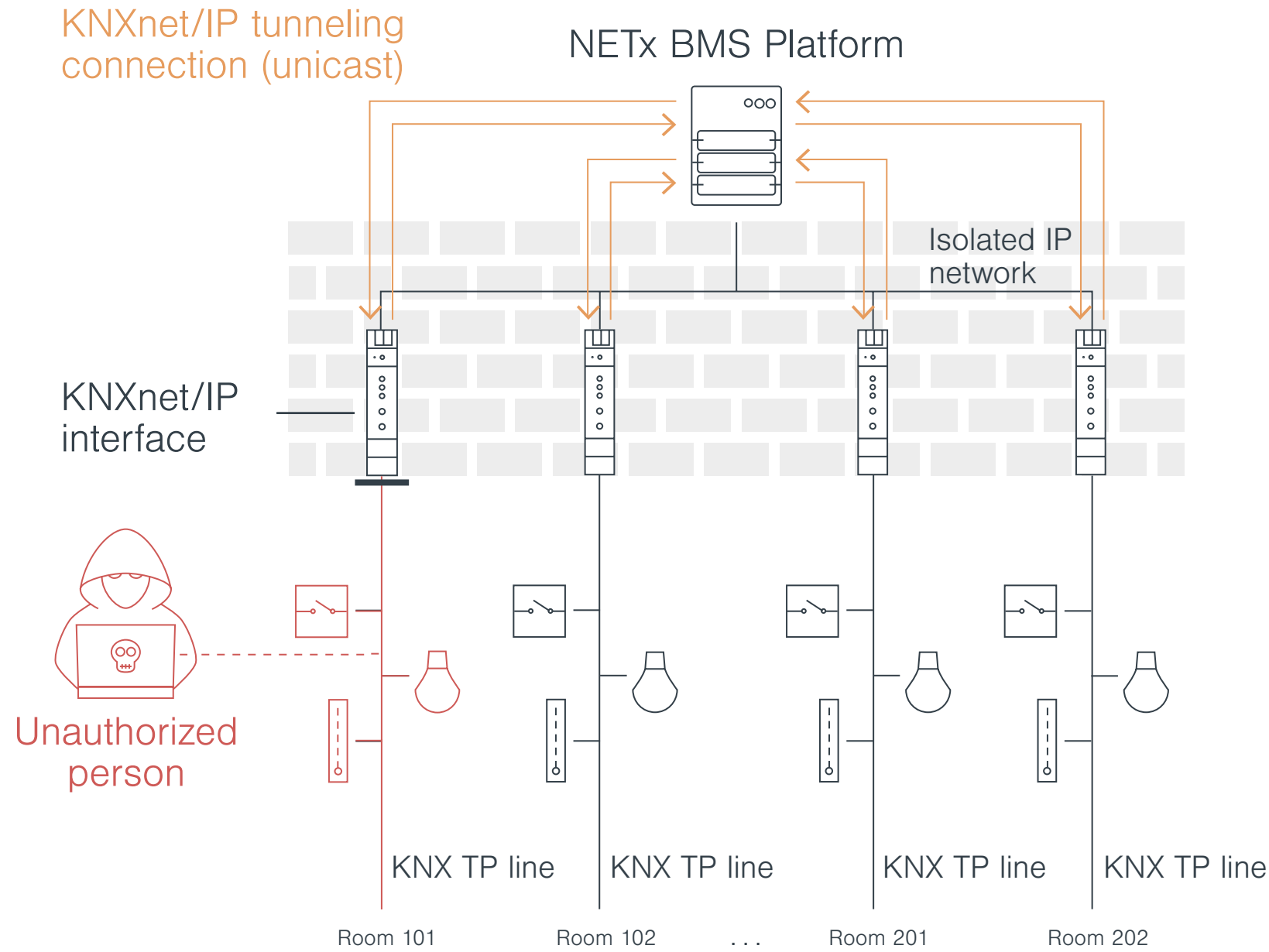
No KNX communication between rooms is necessary

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

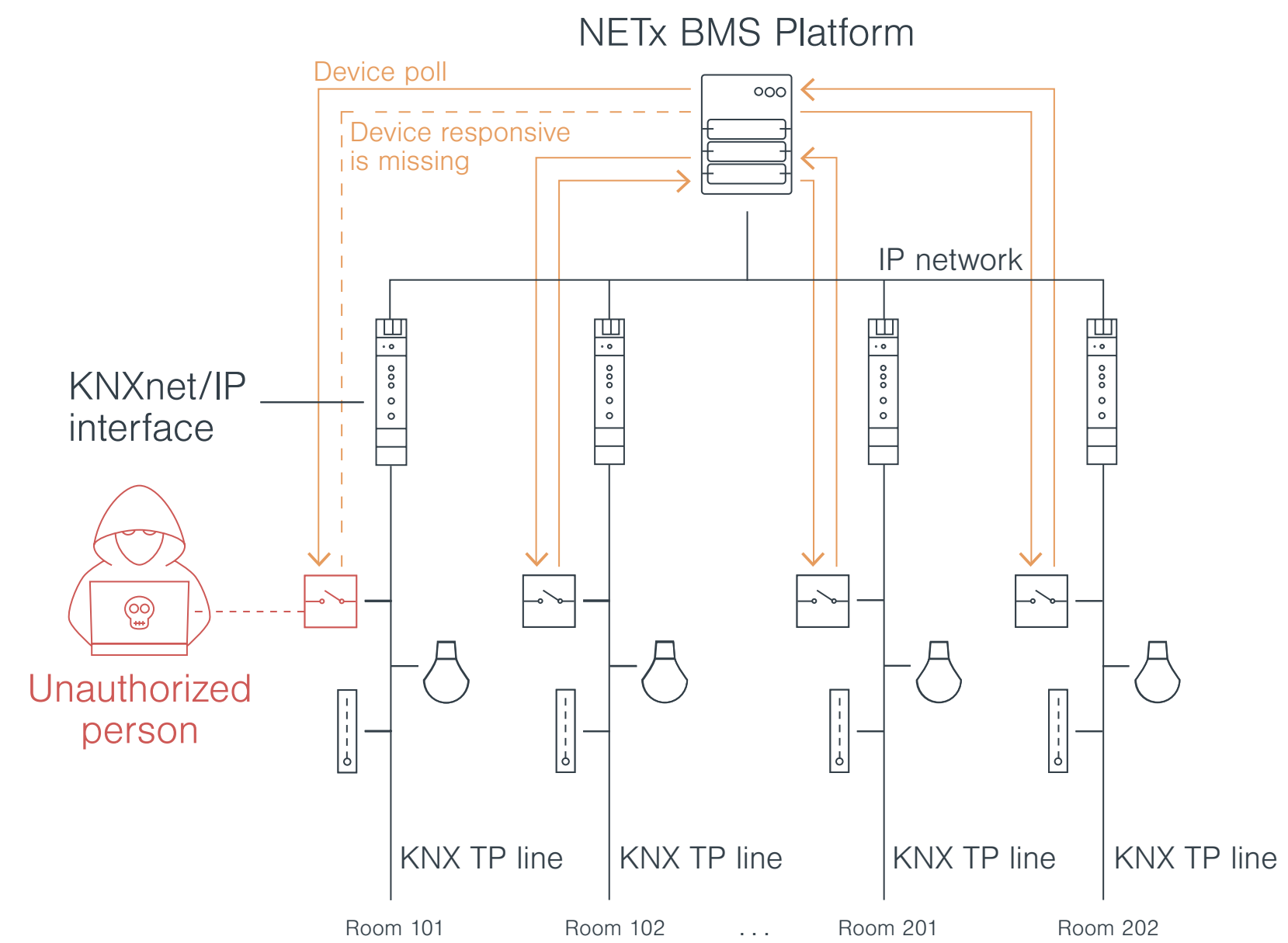
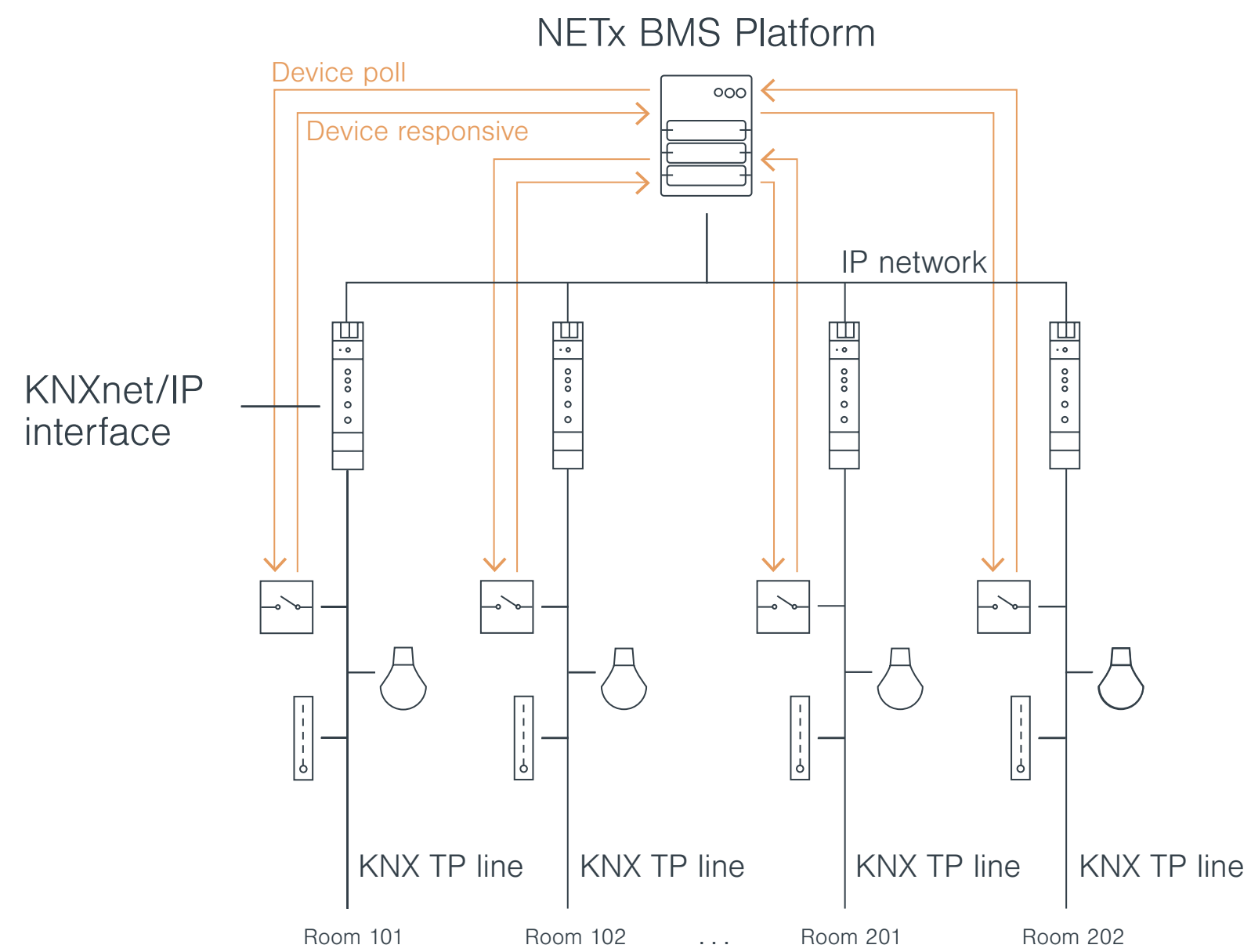
What about central commands like changing set points?

Using Building Management System (BMS) software

Secure central management using BMS solution



Device monitoring



Device polling using KNX management request

If device is not responding within appropriate time, alarm is raised

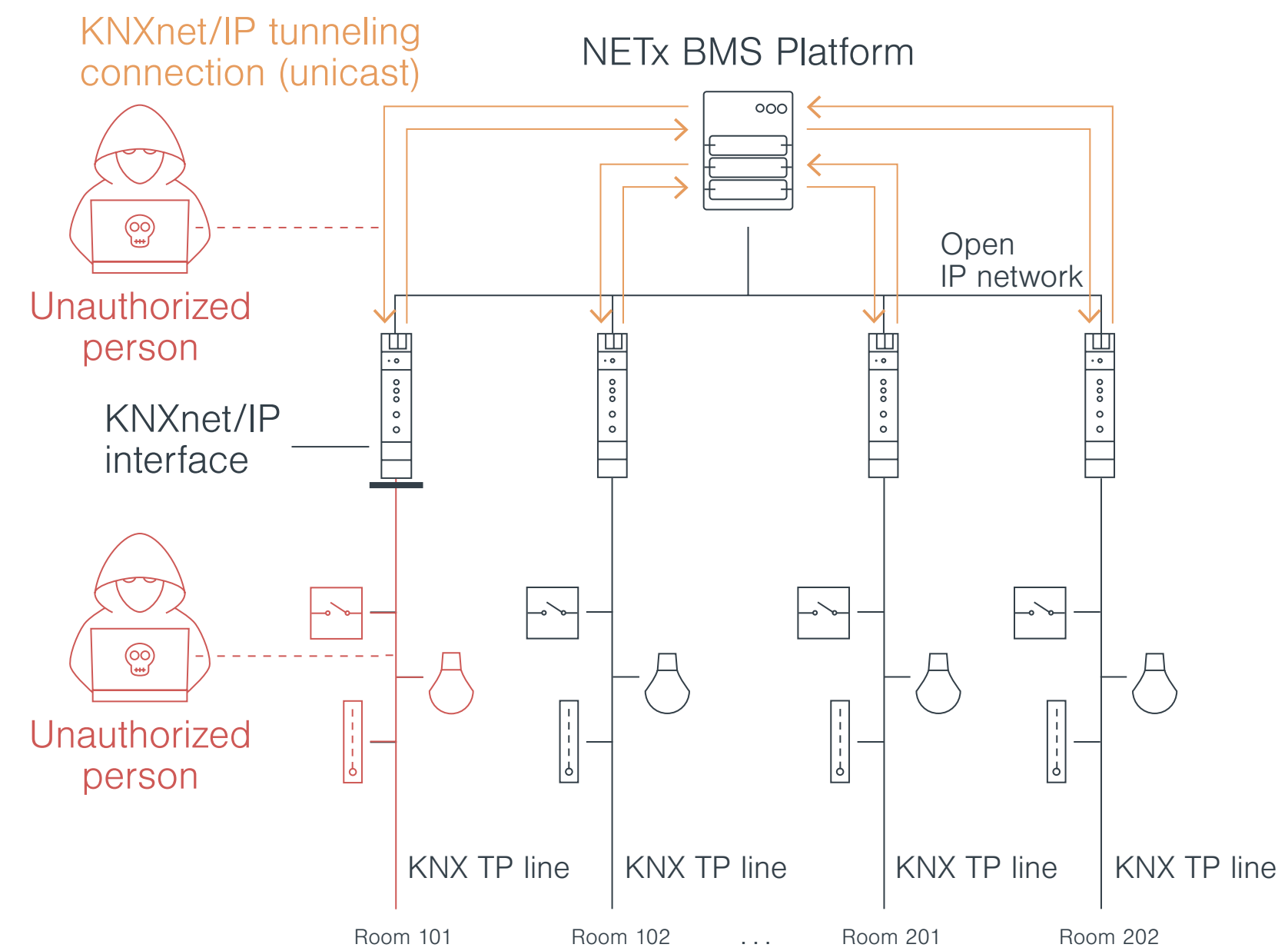
No bandwidth problem due to multiple point-to-point tunnelling connections

Data source information is also available

172.16.3.1			Item timestamp	4	02.02.2017 12:23:07
+	GATEWAY		Item Access Rights	5	READ
o	Status	KNX Gateway status number	Server Scan Rate	6	10
+	Devices		Item Unit	100	
-	05 - Floor1		Item Description	101	Room101 Dimming - Switch - Status
-	0 - Lighting		High Value Limit	102	
-	000	Room101 Dimming - Switch	Low Value Limit	103	
-	001	Room101 Dimming - Switch - Status	Item Local Timestamp	400	02.02.2017 13:25:07
-	002	Room101 Dimming - Rel Dimming	Handle	1000	994
o	002 - SEND	Trigger to send the KNX telegram	Access Level	1001	0
o	002.Control	Room101 Dimming - Rel Dimming / l...	Persistent	1002	False
o	002.StepCode	Room101 Dimming - Rel Dimming / ...	Historical	1003	False
-	004	Room101 Dimming - Brightness - Sta...	Redundant	1004	True
			Source	1005	SYS:KNX;SRC:172.16.3.1;ADR:05.03.001

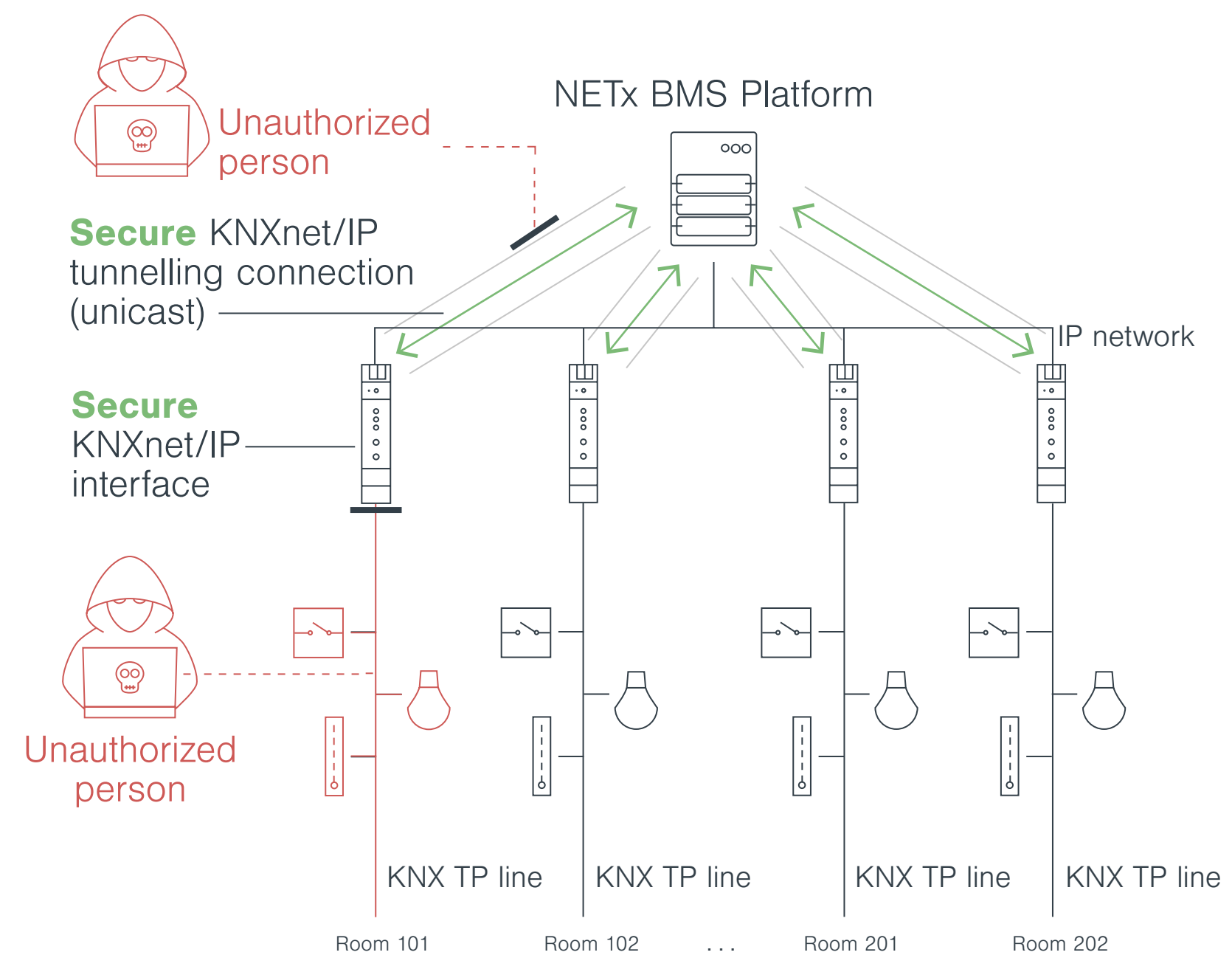
What to do if the IP network can not be isolated?

Using KNX security standard:
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

Available for NETx BMS Platform

Secure KNXnet/IP tunnelling

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

www.netxautomation.com