

Modul 5: Intelligens épületek

Intelligens szabályozás és automatizálás

IT Biztonság

Standardizált kommunikációs
protokollok

Prof. Dr.-Ing. Sabine Hoffmann

Christoph Degel



Erasmus+

Az Európai Unió
Erasmus+ programjának
társfinanszírozásával



STU

SLOVAK UNIVERSITY OF
TECHNOLOGY IN BRATISLAVA

TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN

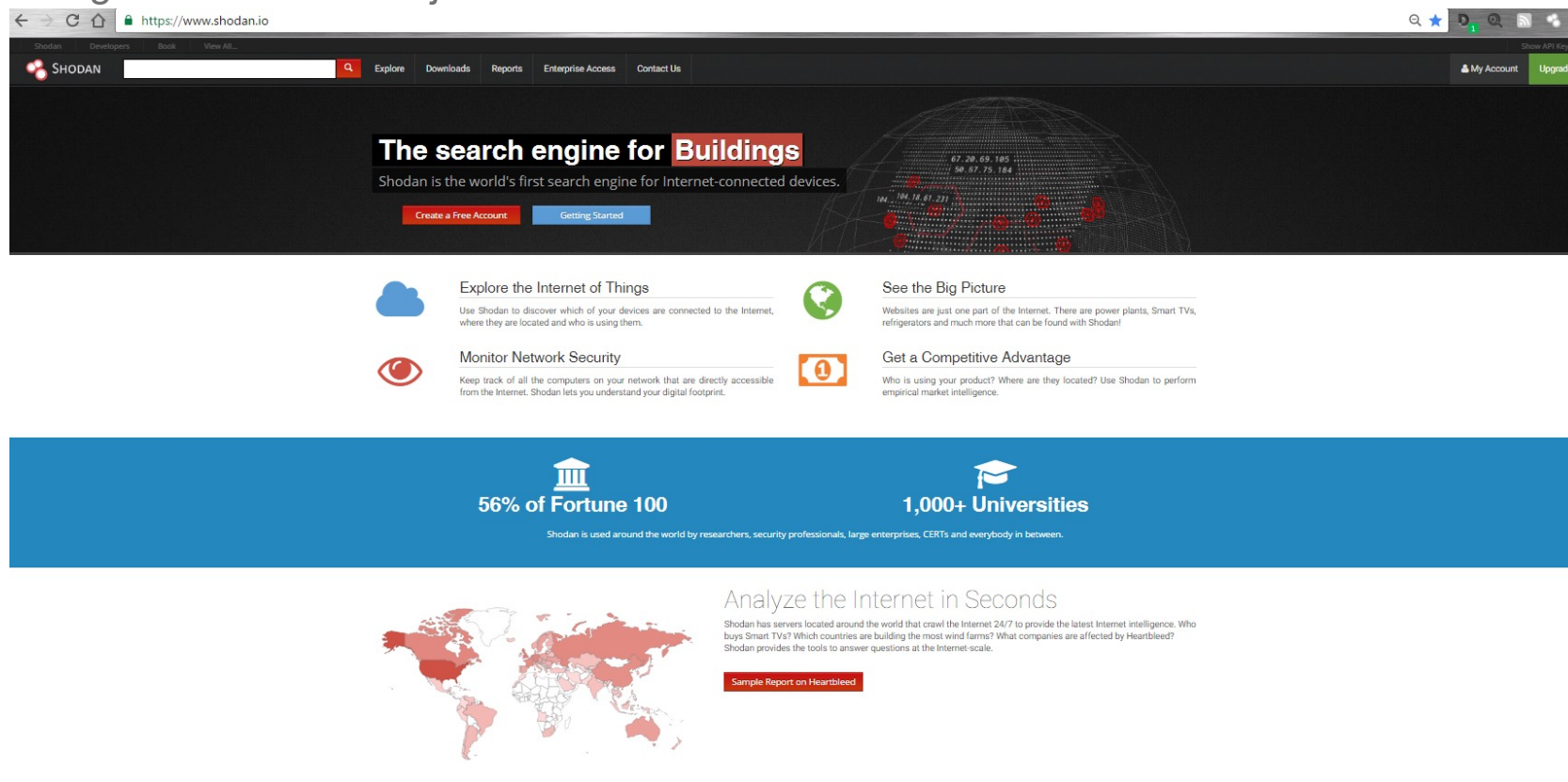


IT Biztonság

IT Biztonság

Shodan

A Shodan a világ első keresőmotorja az internetre csatlakoztatott eszközök számára



The screenshot shows the Shodan website homepage. The browser address bar displays <https://www.shodan.io>. The website has a dark theme with a navigation bar at the top containing links for Shodan, Developers, Blog, and View All. A search bar is prominently displayed. Below the navigation bar, a large banner features the text "The search engine for Buildings" and "Shodan is the world's first search engine for Internet-connected devices." To the right of this text is a graphic of a globe with red dots representing connected devices. Below the banner, there are four main sections, each with an icon and a title: "Explore the Internet of Things" (cloud icon), "See the Big Picture" (globe icon), "Monitor Network Security" (eye icon), and "Get a Competitive Advantage" (person icon). Each section contains a brief description of its functionality. Below these sections is a blue banner with two statistics: "56% of Fortune 100" and "1,000+ Universities", both accompanied by icons (a building and a graduation cap respectively). Below the blue banner, there is a world map with red dots indicating server locations, and a section titled "Analyze the Internet in Seconds" with a brief description of Shodan's capabilities and a link to a "Sample Report on Heartbleed".

Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices don't always require authentication - it isn't part of the protocol!



Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

[Explore Modbus](#)



S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

[Explore Siemens S7](#)



DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

[Explore DNP3](#)



The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

[Explore Niagara Fox](#)



BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

[Explore BACnet](#)



EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

[Explore EtherNet/IP](#)



Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

[Explore GE-SRTP](#)



The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

[Explore HART-IP](#)



PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

[Explore PCWorx](#)



MELSEC-Q Series use a proprietary network protocol for communication. The devices are used by equipment and manufacturing facilities to provide high-speed, large volume data processing and machine control.

[Explore MELSEC-Q](#)



FINS, Factory Interface Network Service, is a network protocol used by Omron PLCs, over different physical networks like Ethernet, Controller Link, DeviceNet and RS-232C.

[Explore OMRON FINS](#)



The protocol the Crimson v3.0 desktop software uses when communicating with the Red Lion Controls G306a human machine interface (HMI).

[Explore Crimson v3](#)



Over 250 device manufacturers from different industrial sectors offer automation devices with a CODESYS programming interface. Consequently, thousands of users such as machine or plant builders around the world employ CODESYS for automation tasks.

[Explore Codesys](#)

IEC 60870-5-104

IEC 60870 part 5 is one of the IEC 60870 set of standards which define systems used for SCADA in electrical engineering and power system automation applications.

[Explore IEC 60870-5-104](#)

ProConOS

ProConOS is a high performance PLC run time engine designed for both embedded and PC based control applications.

[Explore ProConOS](#)

Szabványosított protokollok szerinti szűrés

IT Biztonság

Shodan

The screenshot displays the Shodan search engine interface. The search bar at the top contains the query 'port:47808 country:DE'. The left sidebar shows various filters and statistics, including 'TOTAL RESULTS: 254', 'TOP COUNTRIES' (Germany: 254), 'TOP CITIES' (Frankfurt am Main: 99), 'TOP ORGANIZATIONS' (Amazon.com: 94), and 'TOP PRODUCTS' (PMC BACnet Building Contr...: 8). The main content area lists search results for three IP addresses: 87.146.218.150, 138.201.43.29, and 178.27.164.153. Each result includes details such as the instance ID, object name, vendor name, application software, firmware, model name, and a description. The first result is for 'Deutsche Telekom AG' in Brackenheim, Germany. The second result is for 'Hetzner Online GmbH' in Germany. The third result is for 'Vodafone Kabel Deutschland' in Augsburg, Germany. The interface also features a 'New Service' banner for 'Shodan Monitor' and a 'Try out the new be' button.

Shodan Developers Monitor View All... Show API Key Try out the new be

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
254

TOP COUNTRIES

Germany 254

TOP CITIES

Frankfurt am Main 99
Hamburg 7
Munich 4
Weissach 3
Schwarzenbek 3

TOP ORGANIZATIONS

Amazon.com 94
Deutsche Telekom AG 56
Vodafone DSL 18
Unitymedia Business 10
Versatel Deutschland 7

TOP PRODUCTS

PMC BACnet Building Contr... 8
PCO1000WB0 8
DDC420 5
Version 9 4
PXC100-E.D + PXA40-T / HW... 4

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

87.146.218.150
p5792da96.dip01-lpcconnect.de
Deutsche Telekom AG
Added on 2020-05-27 05:51:16 GMT
Germany, Brackenheim

Instance ID: 0
Object Name: WAGO_BAC
Vendor Name: WAGO Kontakttechnik GmbH & Co. KG
Application Software: 117662
Firmware: 01.01.23(07)
Model Name: 750-831

BACnet Broadcast Management Device (BBMD):
172.16.201.20:47808
192.160.40.59:47808
172.16.201.201:47808

138.201.43.29
whocares
Hetzner Online GmbH
Added on 2020-05-27 07:14:04 GMT
Germany

echo

178.27.164.153
ipb21ba499.dynamic.kabel-deutschland.de
Vodafone Kabel Deutschland
Added on 2020-05-27 10:33:34 GMT
Germany, Augsburg

Instance ID: 77000
Object Name: pCOWeb77000
Location: Unknown
Vendor Name: Carel S.p.A.
Application Software: 2.15.2A
Firmware: A1.5.0 - B1.2.4
Model Name: PC01000WB0
Description: Carel BACnet Gateway

3.121.218.238
ec2-3-121-218-238.eu-central-1.compute.amazonaws.com
Amazon.com
Added on 2020-05-27 10:59:23 GMT
Germany, Frankfurt am Main

Instance ID: 200
Object Name: enteliBUS Manager-Touch 200
Vendor Name: Delta Controls
Application Software: V3.40
Firmware: 612850
Model Name: eBMGR-TCH

BACnet Broadcast Management Device (BBMD):
172.30.64.1:47808

Foreign Device Table (FDT):
83.236.208.18:53617:ttl=60:timeout=59

Példa: Németországban üzemelő BACnet-es berendezések

As an example a search for BACnet devices in Germany was performed

IT Biztonság

Shodan

Shodan

Developers

Monitor

View All...

Show API Key

Try o

 **SHODAN**

port:47808 country:"DE"

Q

Home

Explore

Downloads

Reports

Pricing

Enterprise Access

Exploits

Maps

Share Search

Download Results

Create Report

TOTAL RESULTS

254

TOP COUNTRIES



Germany254

TOP CITIES

Frankfurt am Main99

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

87.146.218.150

p5792da96.dip0.t-ipconnect.de

Deutsche Telekom AG

Added on 2020-05-27 05:51:16 GMT

 Germany, Brackenheim

ics

Instance ID: 0

Object Name: WAGO_BAC

Vendor Name: WAGO Kontakttechnik GmbH & Co. KG

Application Software: 117662

Firmware: 01.01.23(07)

Model Name: 750-831

BACnet Broadcast Management Device (BBMD):

172.16.201.20:47808

192.160.40.59:47808

172.16.201.201:47808

IT Biztonság

Az Ethernet-alapú hálózatok kihívása a BA-ban

Az IT biztonság jogi alapjai Németországban: :

- BSI – Szövetségi Információbiztonsági Hivatal
- ITSiG - Az IT biztonsági törvény, 2015. július
- KRITIS - Az informatikai biztonsági törvény végrehajtásáról szóló rendelet 2016. május 3-án lépett hatályba (energetikai, informatikai és távközlési ágazatok).
- VDMA Gépészeti ipar
- TKG – Távközlési törvény
- BDSG – Törvény az adatvédelmi törvény potosításáról
- GDPR - Általános adatvédelmi rendelet



IT Biztonság

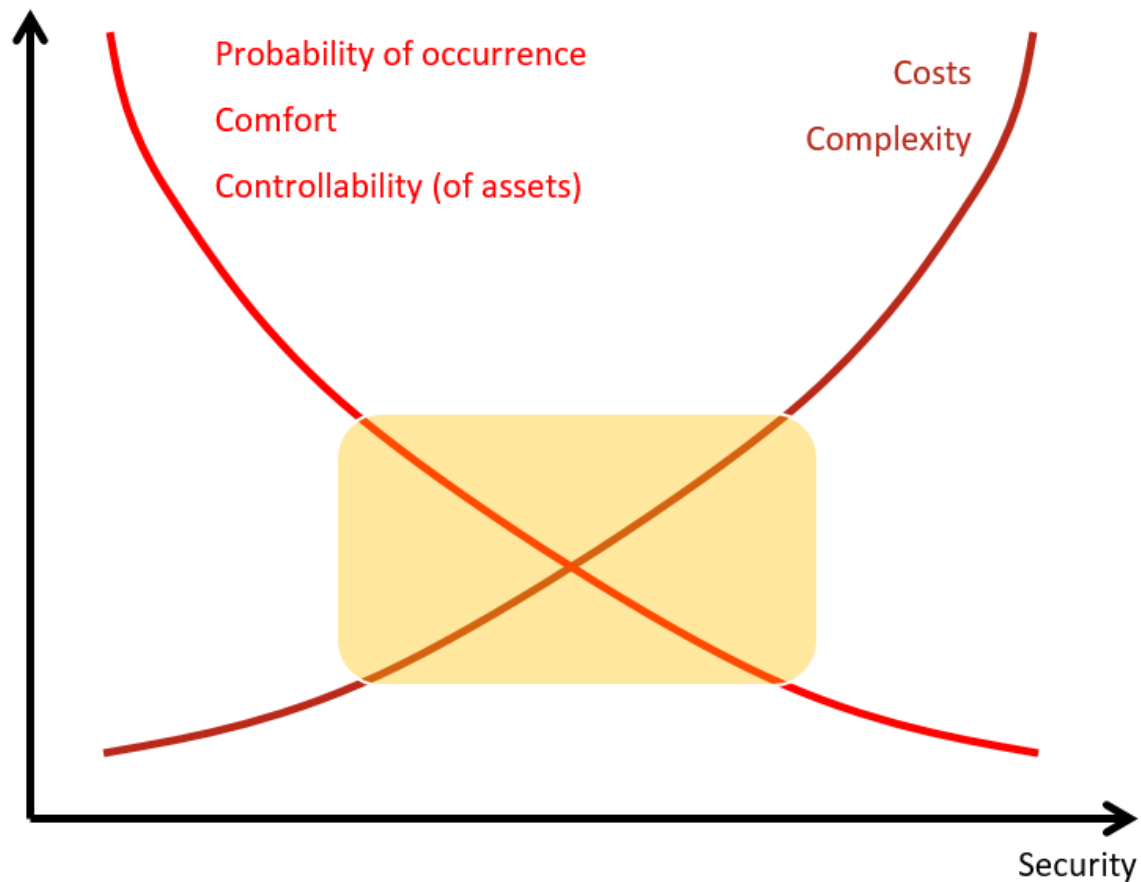
Az Ethernet-alapú hálózatok kihívása a BA-ban

Minél magasabbak a biztonsági követelmények, annál nagyobbak a költségek és az összetettség.

A növekvő összetettség a kényelem és az irányíthatóság csökkenését eredményezheti.

Meg kell találni az egyensúlyt a jogi követelmények keretein belül.

-> Kockázatelemzés



IT Biztonság

Az Ethernet-alapú hálózatok kihívása a BA-ban

Az Ethernet-alapú infrastruktúra ma már szabványos:

- A fejlesztés előnyei:
 - A BA-rendszerekhez való kapcsolódási pontok az informatikai hardveren
 - Az információ több rendszer / alkalmazás számára is elérhető
 - Nagy infrastruktúrák kombinálhatók a WAN-szabványok segítségével
- Hátrányok:
 - A BA-infrastruktúrához való hozzáférés (túl) könnyen megvalósítható
 - a szabványos protokollok lehetővé teszik, hogy illetéktelenek kezeljék a rendszert.

IT Biztonság

Az Ethernet-alapú hálózatok kihívása a BA-ban

A megváltozott kommunikációs infrastruktúra elemzése:

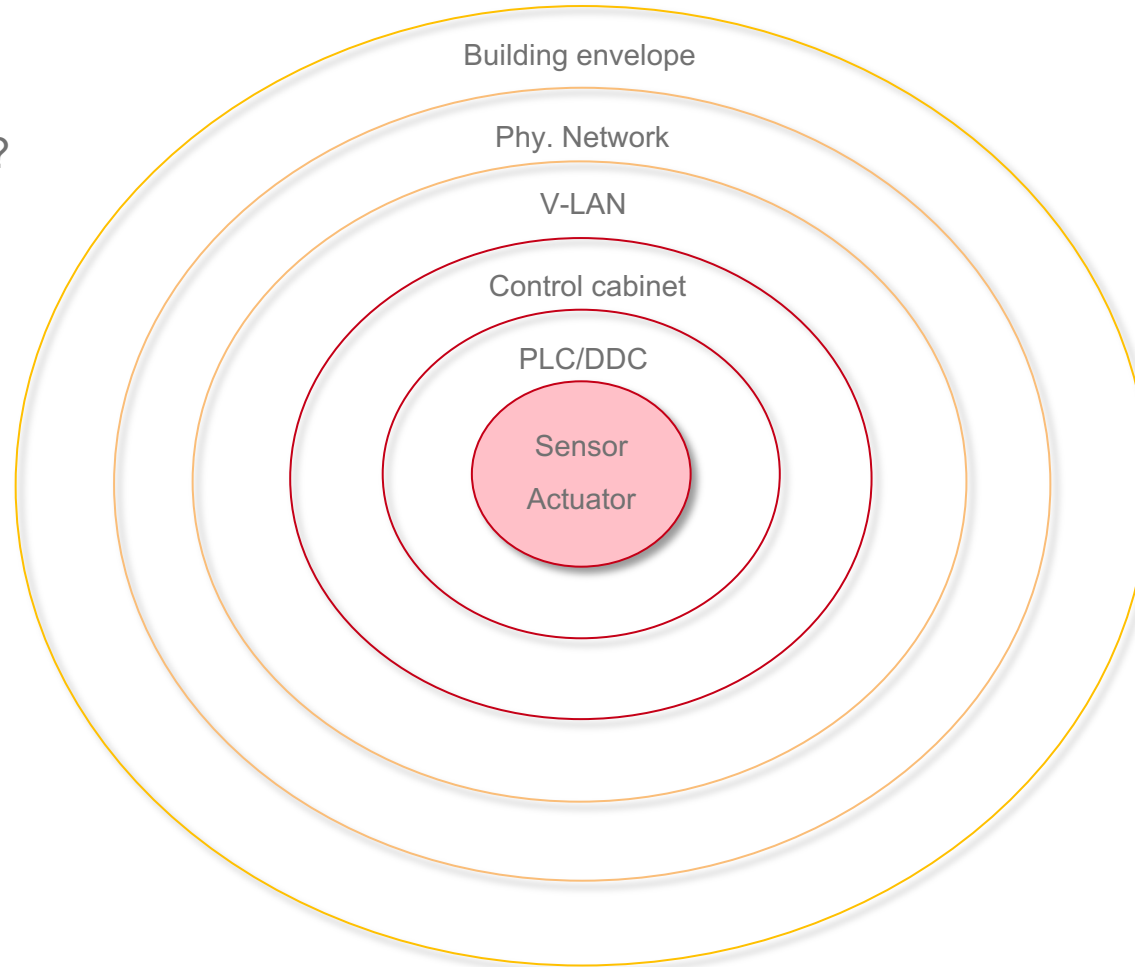
- A jelenlegi tervezés a BA-funkciókra és nem a hálózatfizikára összpontosít:
 - Szobaautomatizálás, ICE technológia, biztonságtechnika, egyéb rendszerek
 - A hangsúly az egyes funkciókon és azok kölcsönhatásán van.
 - A hálózati infrastruktúrát gyakran elhanyagolják
- Hogyan kell figyelembe venni az új infrastruktúrát?
 - Ez a "funkció nélküli technológia" karbantartást igényel?
 - Minden működik. Van ok a cselekvésre?
 - Az informatikai részleg vagy az épületgépészeti részleg kezelje a hálózatot?
 - ...



IT Biztonság

Az Ethernet-alapú hálózatok kihívása a BA-ban

Milyen veszélyek fenyegethetik az informatikai környezetből a BA-t is?

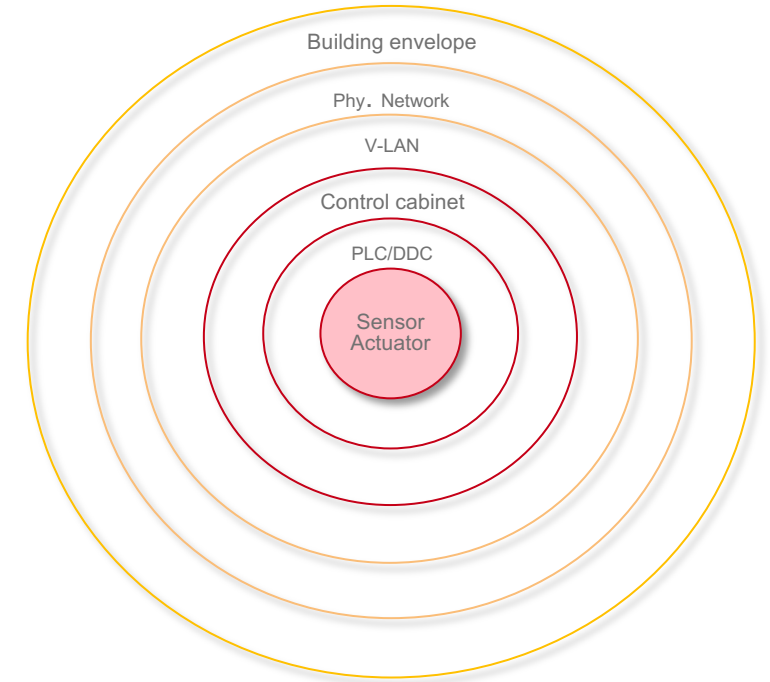


IT Biztonság

Az Ethernet-alapú hálózatok kihívása a BA-ban

Milyen veszélyek fenyegethetik az informatikai környezetből a BA-t is?

- Károk vagy fenyegetések a hálózaton belül
 - Hozzáférés a BA-rendszerhez
 - Adatok és információk lekérdezése
 - A rendszer/berendezés szándékos megzavarása vagy manipulálása
-
- A hálózaton kívülről érkező károk vagy fenyegetések
 - gondatlanul konfigurált távoli hozzáférés egy üzemrészhez
 - UPnP (Universal Plug and Play) az eszközök gyártófüggetlen vezérléséhez)



IT Biztonság

Az Ethernet-alapú hálózatok kihívása a BA-ban

Problémás terület: UPnP (Universal Plug and Play)

Az UPnP az Internet Gateway Device (IGD) protokollt használja, hogy a felhasználó számára egyszerű módon utasítsa a routereket, hogy nyissanak meg portokat és továbbítsák az internetről érkező kéréseket egy internethez csatlakoztatott számítógéphez (vagy eszközhöz).

Az UPnP-t csak a helyi hálózat hálózati interfészein szabad engedélyezni, és nem szabad, hogy az internetről elérhető legyen. 2013 januárjában a bostoni Rapid7 biztonsági cég bejelentette, hogy egy 6 hónapos projekt keretében UPnP eszközök után kutatott az interneten. A 81 millió IP-cím között 1500 gyártó 6900 termékét találták meg, amelyek válaszoltak az internetről érkező UPnP-kérésekre. Az eszközök 80%-a otthoni internet-hozzáférést biztosító router, a többi eszköz nyomtatók, webkamerák és megfigyelő kamerák. Az UPnP protokoll segítségével ezekhez az eszközökhöz lehet hozzáférni, illetve manipulálni őket. Translated with www.DeepL.com/Translator (free version)

IT Biztonság

Az Ethernet-alapú hálózatok kihívása a BA-ban

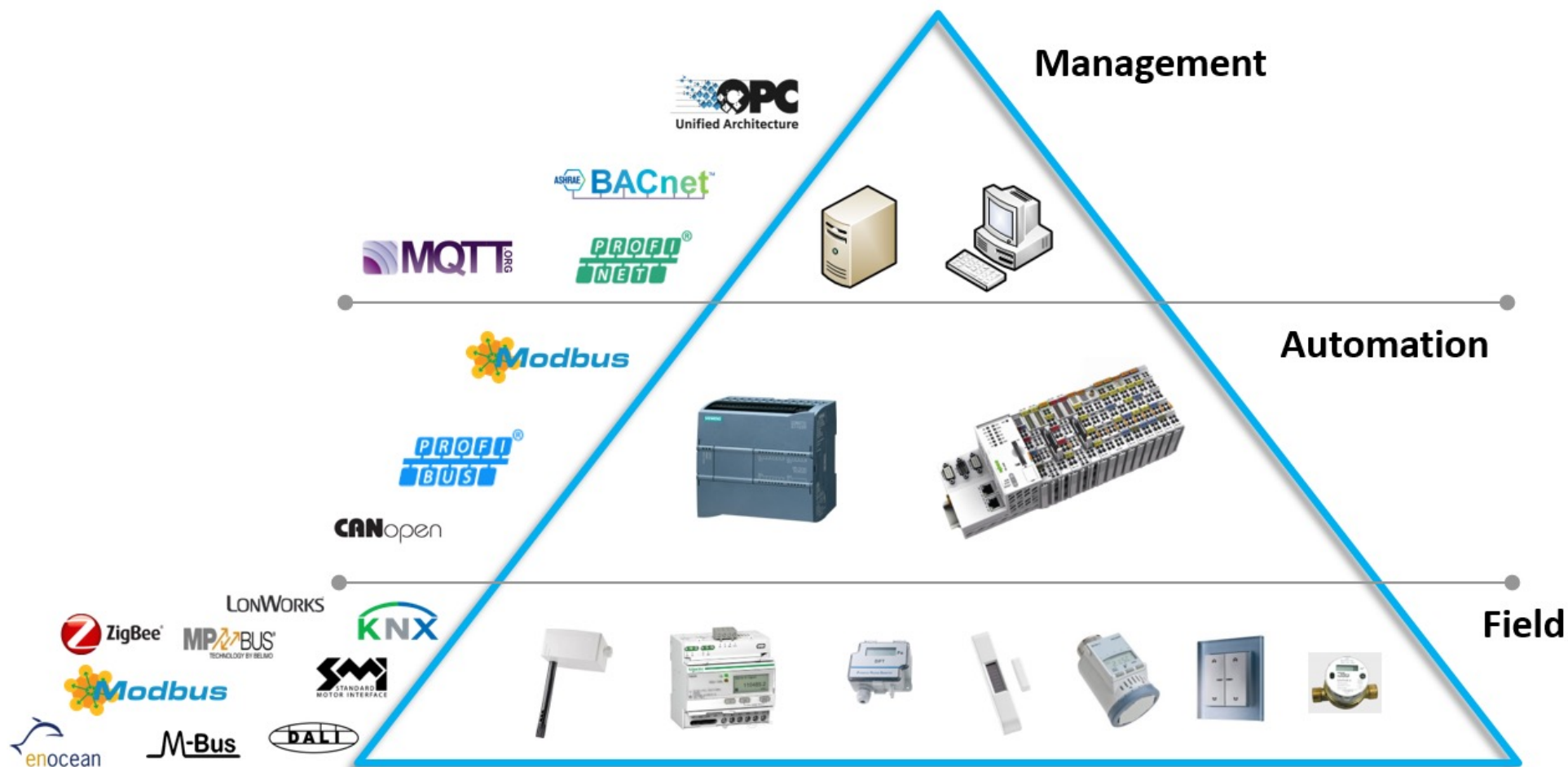
Problémás terület: Jelszavak

- Válassz komplex jelszót
- Ne használj neveket
- Ne jegyezz fel jelszavakat
- Használj különböző jelszavakat
- Az egyszerű jelszavak elkerülendőek (lásd ábra)
- Légy kreatív!
 - Cseréld a betűket számokra: LEED → 1337
 - "I get up in the morning and brush my teeth." → Password "lguitmabmt"
- Változtasd meg az előre beállított jelszavakat
- Véd a képernyővédőt jelszóval



IT Biztonság

BA protokollok and IT biztonság területén



IT Biztonság

Protokollok és bus rendszerek

Modbus:

- Nincsenek biztonsági mechanizmusok vagy hitelesítés
- Az 502-es port a megfelelő infrastruktúrával blokkolható



BACnet:

- Jelenleg nincsenek biztonsági mechanizmusok vagy hitelesítés
- Az objektumok szabadon hozzáférhető BACnet szkennelrel olvashatók.
- A prioritásokon keresztül akár kapcsolási műveletek is lehetségesek
- Nagyszámú port használata bonyolítja a kizárást



OPC and OPC-UA:

- OPC - Klasszikus biztonsági mechanizmusok nélkül
- Az OPC-UA a protokollon alapuló, tanúsítványalapú biztonsági mechanizmusokkal rendelkezik.



IT Biztonság

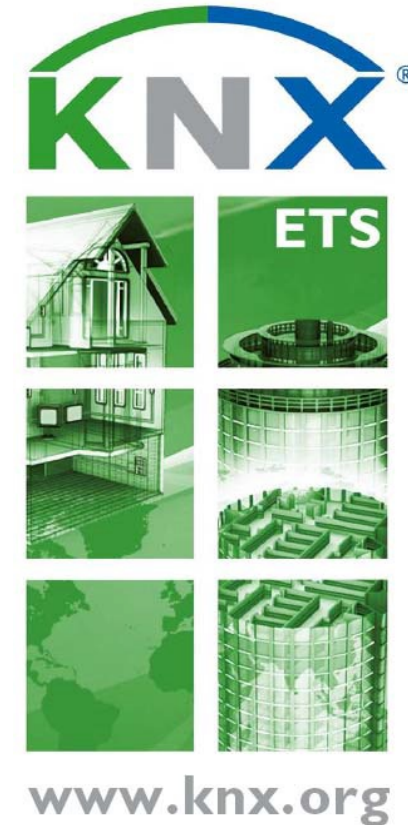
Protokollok és bus rendszerek

KNX

- Klasszikusan nincsenek biztonsági mechanizmusok
- Kétvezetékes buszon keresztüli hozzáférés az épület számos pontján lehetséges
- Az új telepítések - KNX Secure! (IP router)

KNX Secure

- Bemutatva: a frankfurti Light&Building 2016 rendezvényen
- Csak ETS5.5 és magasabb verziószámmal elérhető
- KNX IP Secure - biztosítja az IP résztvevők közötti kapcsolatot.
- KNX Data Security - biztosítja a kapcsolatot a TP résztvevők között.
- A kulcsok bevitele az ETS-be a telepítő által

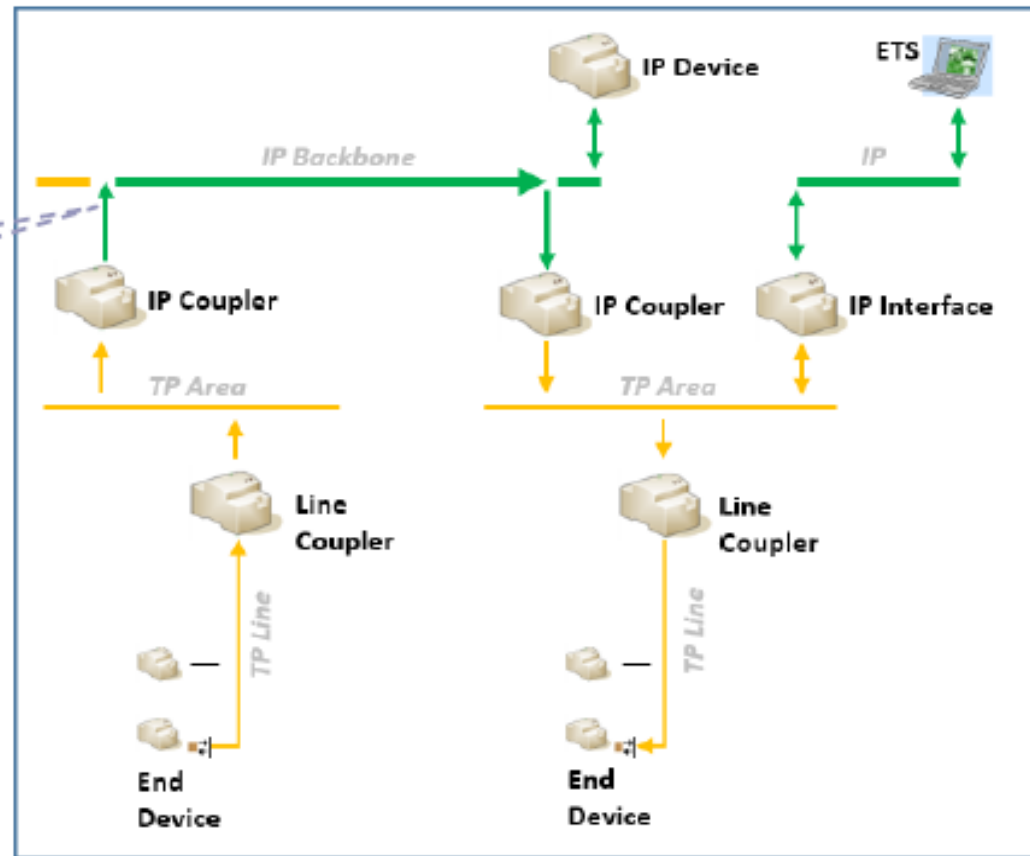


Technology Concept, IP Secure

KNX IP Secure secures the entire KNXnet/IP telegram

All KNX telegrams between two (or more) IP couplers are **secured**

- unsafe communication
- safe communication

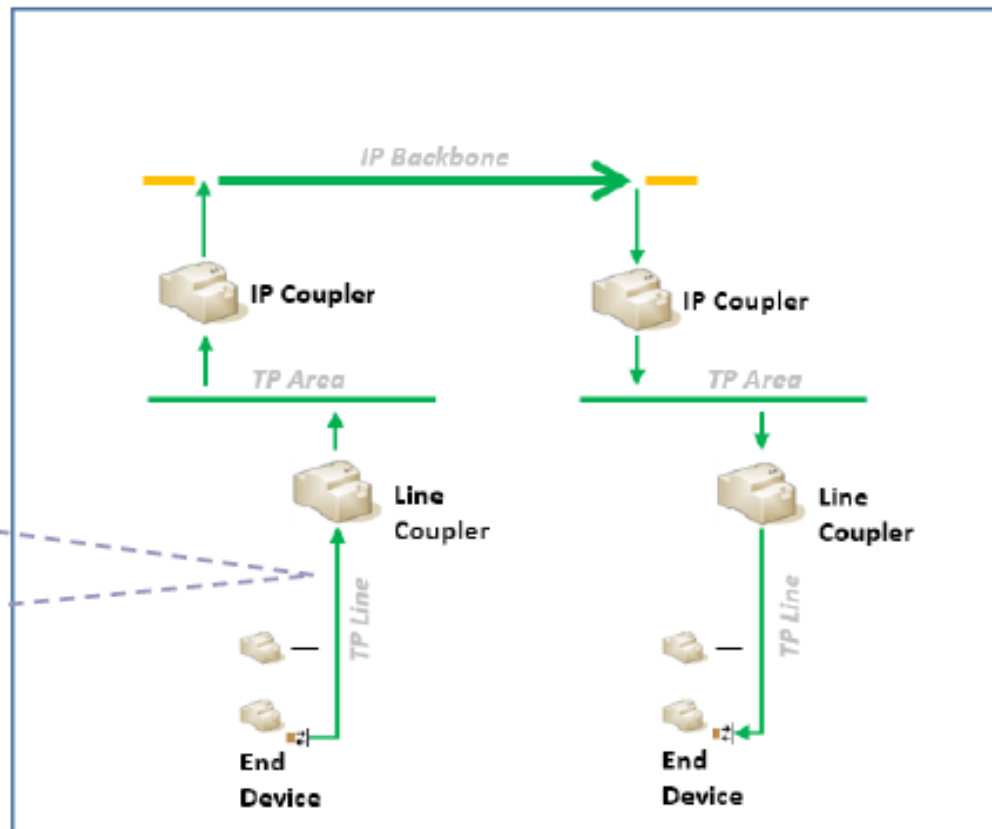


Technology Concept, Data Secure

KNX Data Secure only secures the APCI and the user data

The group communication of a certain station (one or more comm. objects) to other comm. Objects is **secured**

- unsafe communication
- safe communication

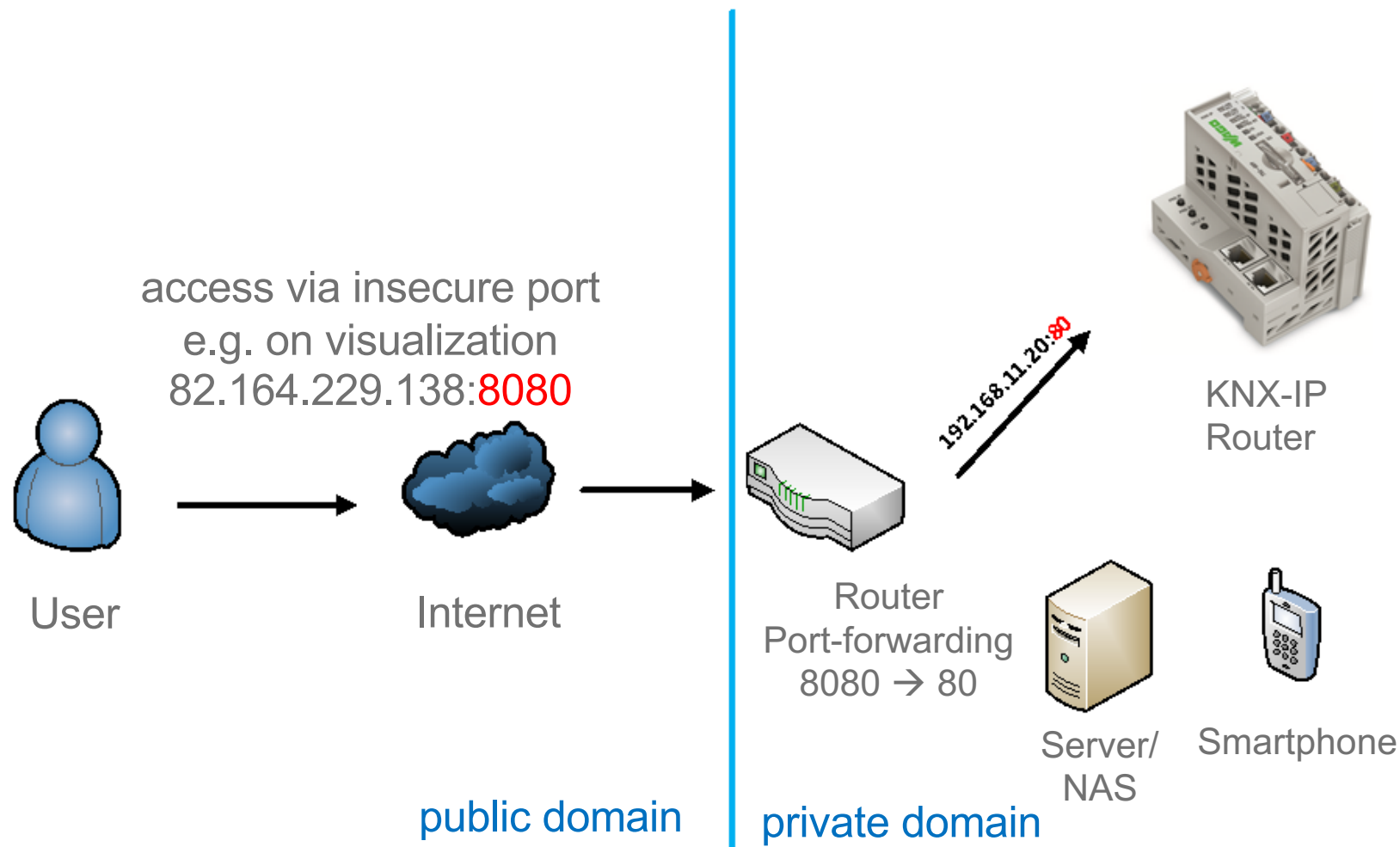


IT Biztonság

PORT továbbítás vs. VPN kapcsolat

Port továbbítás:

- Nem biztosított kapcsolat
- Közvetlen hozzáférés a privát területhez
- Több eszköz több nyitott port
- A HTTPS csak a kapcsolatot biztosítja, további hitelesítés szükséges a végberendezésen.
- Bizonytalan SSL/TLS verziók, ha van ilyen

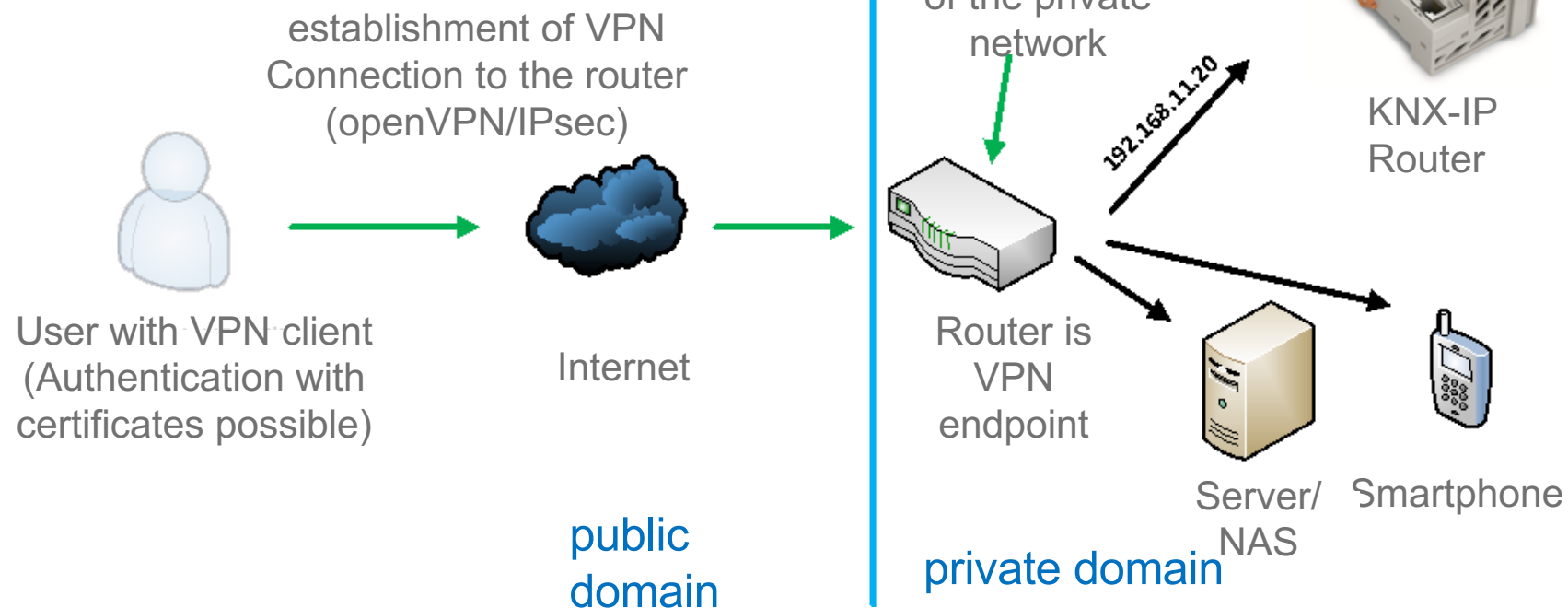


IT Biztonság

PORT továbbítás vs. VPN connection

VPN (Virtual Private Network) kapcsolat:

- Biztonságos kapcsolat
- Szükség esetén hitelesítés tanúsítványokon keresztül
- Nincs átláthatóság a külvilág felé
- Bármennyi kapcsolat lehetséges
- Bonyolultabb a beállítása
- Speciális hardverre lehet szükség
- AES256 titkosítás Gyakorlatilag visszafejthetetlen 2018-tól kezdve

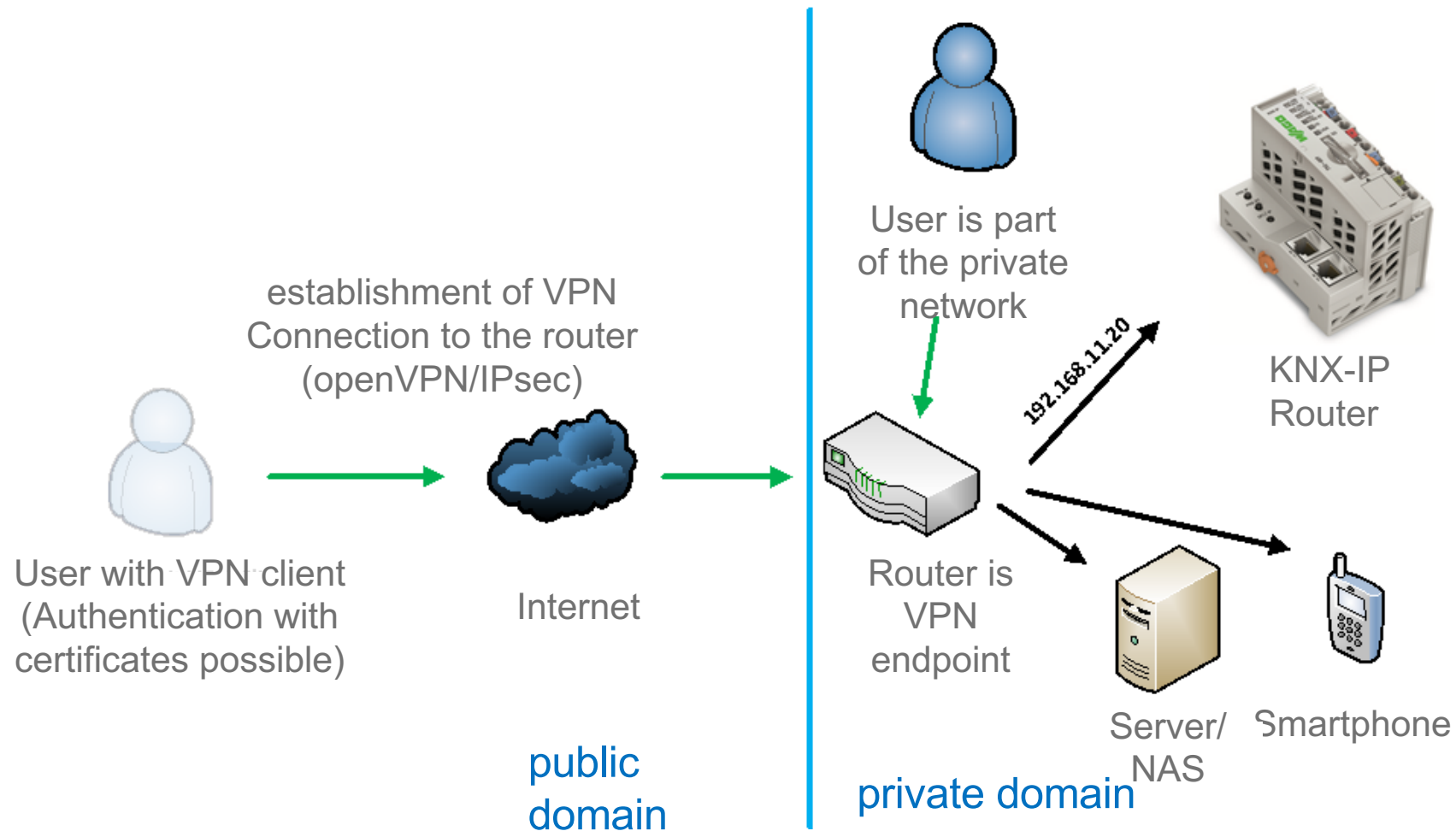


IT Biztonság

PORT továbbítás vs. VPN connection

VPN kapcsolat:

- Csak egy hozzáférési pont
- Jobb ellenőrzés
- Az adatok változatlanok
- Állandóan titkosított kapcsolat
- Hitelesítés, ki jelentkezik be
- A privát tartomány része



IT Biztonság

PORT továbbítás vs. VPN connection

VPN technológia:

- IPsec (IP-Security)
 - Az IP protokoll kiterjesztése
 - Az ISO/OSI modell 3. rétegén (internetes réteg)
 - Fejlett konfiguráció
- OpenVPN
 - Nyílt VPN implementáció
 - Az ISO/OSI modell 4. rétegén (Transport Layer)
 - Erős közösség
 - Megvalósítások számos operációs rendszerhez
 - Egyszerű adminisztráció

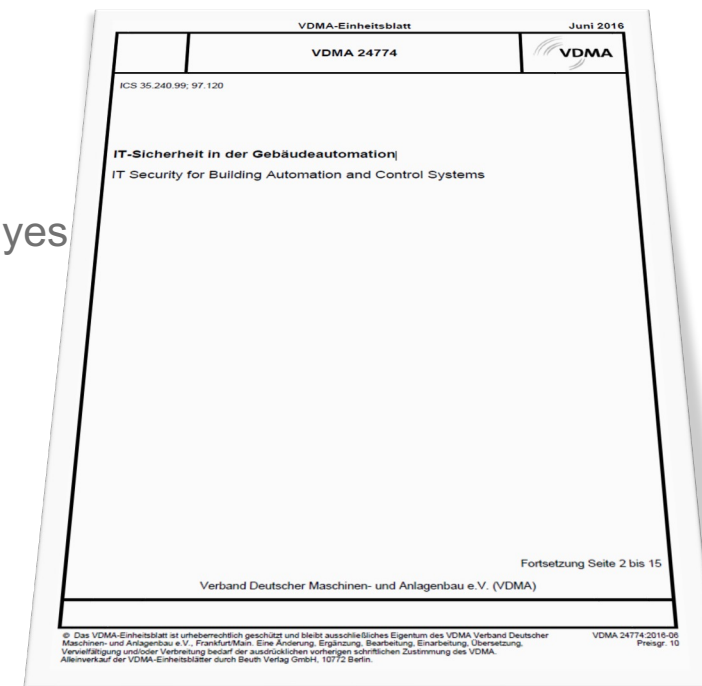


IT Biztonság

Ajánlások és segítségnyújtás

Milyen ajánlások orvosolhatják a helyzetet?

- VDMA 24774 szabvány
- A BSI biztonsági kapuk koncepciója
- és a LARS ICS (Light and Right Security for Industrial Control System - könnyű és helyes vezérlőrendszerek számára)
- EN ISO 16484 Épületautomatizálási rendszerek
- EN 13321-2 Nyílt adatkommunikáció (KNXnet/IP)
- EN 14908 Vállalatsemleges adatkommunikáció (LON)



IT Biztonság

Ajánlások és segítségnyújtás

- VDMA 24774 szabvány
 - VA meglévő és új épületekre vonatkozó intézkedési javaslatok
 - Alapvető ajánlások
 - Jogok kezelése / jelszavas védelem
 - A kommunikáció titkosítása
 - Az eszközök tűzfala (előzetes konfiguráció)
 - Ellenőrzési nyomvonal funkciók
 - Frissítés / frissítések
 - Projekttervezési szabályok
 - Kockázatelemzés / gyengeségelemzés
 - biztonsági mentési koncepció
 - Karbantartás és távoli hozzáférés

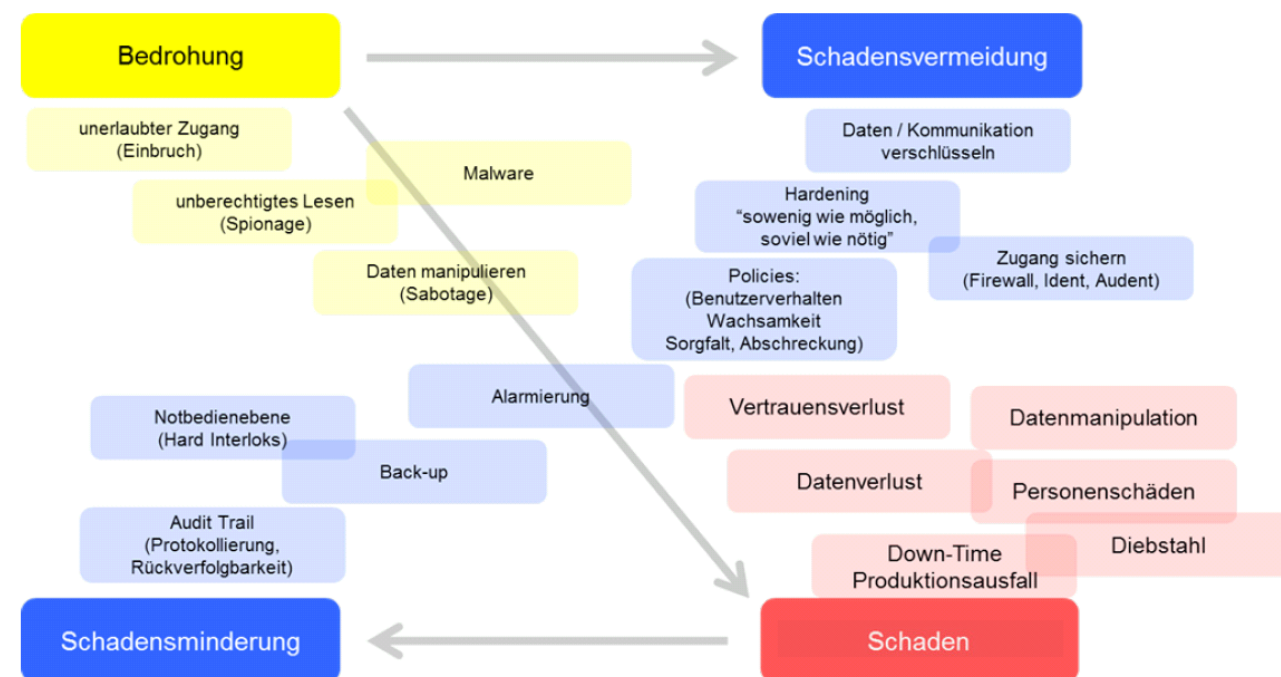


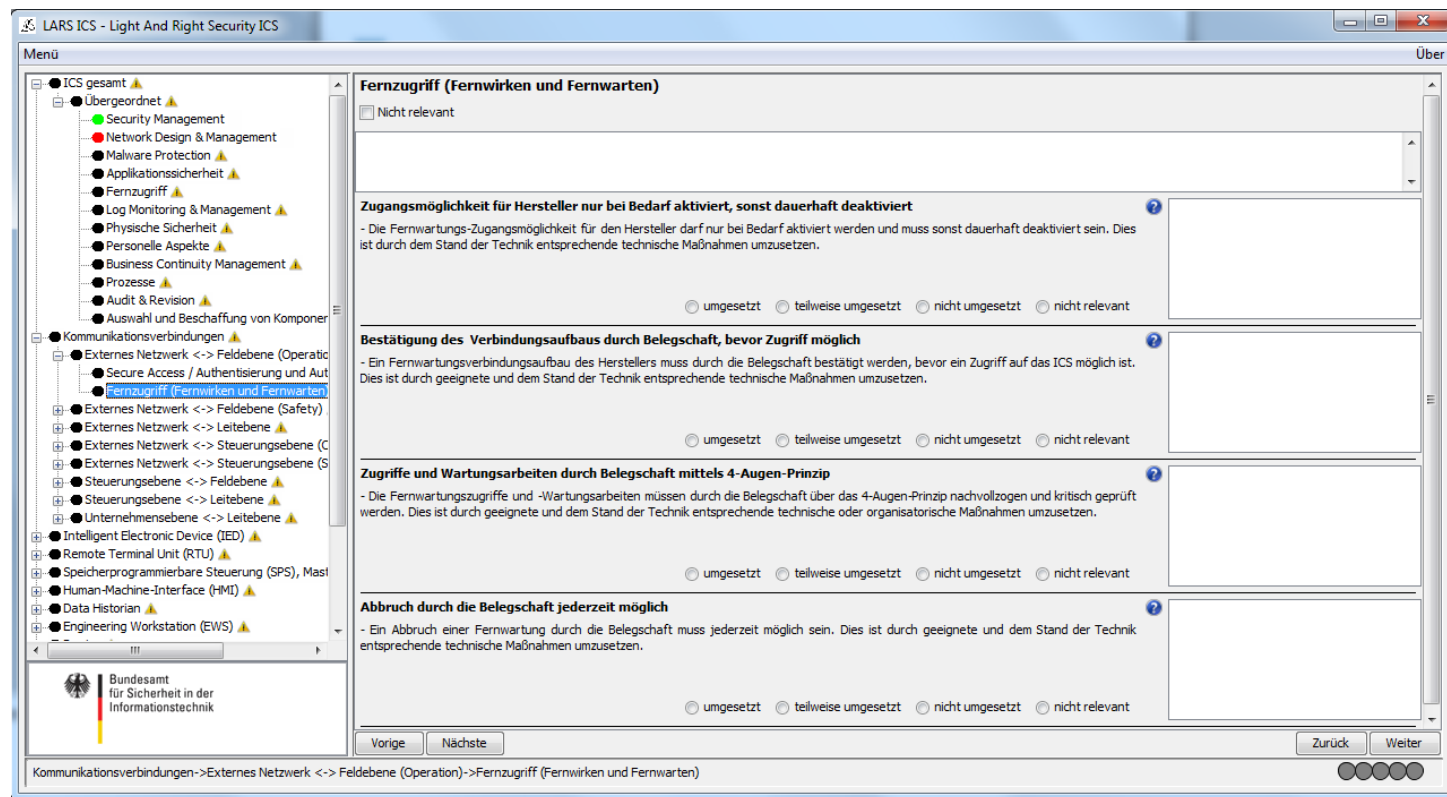
Bild 1 – Bedrohung - Gegenmaßnahmen in der Gebäudeautomation im IT-Umfeld

Das VDMA-Einheitsblatt soll Planer, Errichter und Betreiber dabei unterstützen Maßnahmen für IT-Sicherheit von neuen oder schon errichteten GA-Systemen umzusetzen. Dies betrifft den gesamten Lebenszyklus, inklusive Wartung, Service und Rückbau.

IT Biztonság

Ajánlások és segítségnyújtás

- LARS ICS (Light and Right Security for Industrial Control System)
 - Kritikus infrastruktúrák értékelő eszköze
 - Eszközök rögzítése
 - Jelentéskészítés



Standardizált kommunikációs protokollok

Standardizált kommunikációs protokollok

A gyártók összekapcsolhatósága

- Mindenki saját alkalmazást fejleszt a termékéhez
- A rendszerek önmagukban is nagyon jól működnek

Problémák

- Az alkalmazások nem kompatibilisek egymással
- Nincs szabványosított "nyílt" interfész
- Ezért nincs interakció a különböző eszközök között
- Intelligens integrációs platformok hiánya
- Az informatikai biztonságot erősen figyelmen kívül hagyják az egyszerűség javára

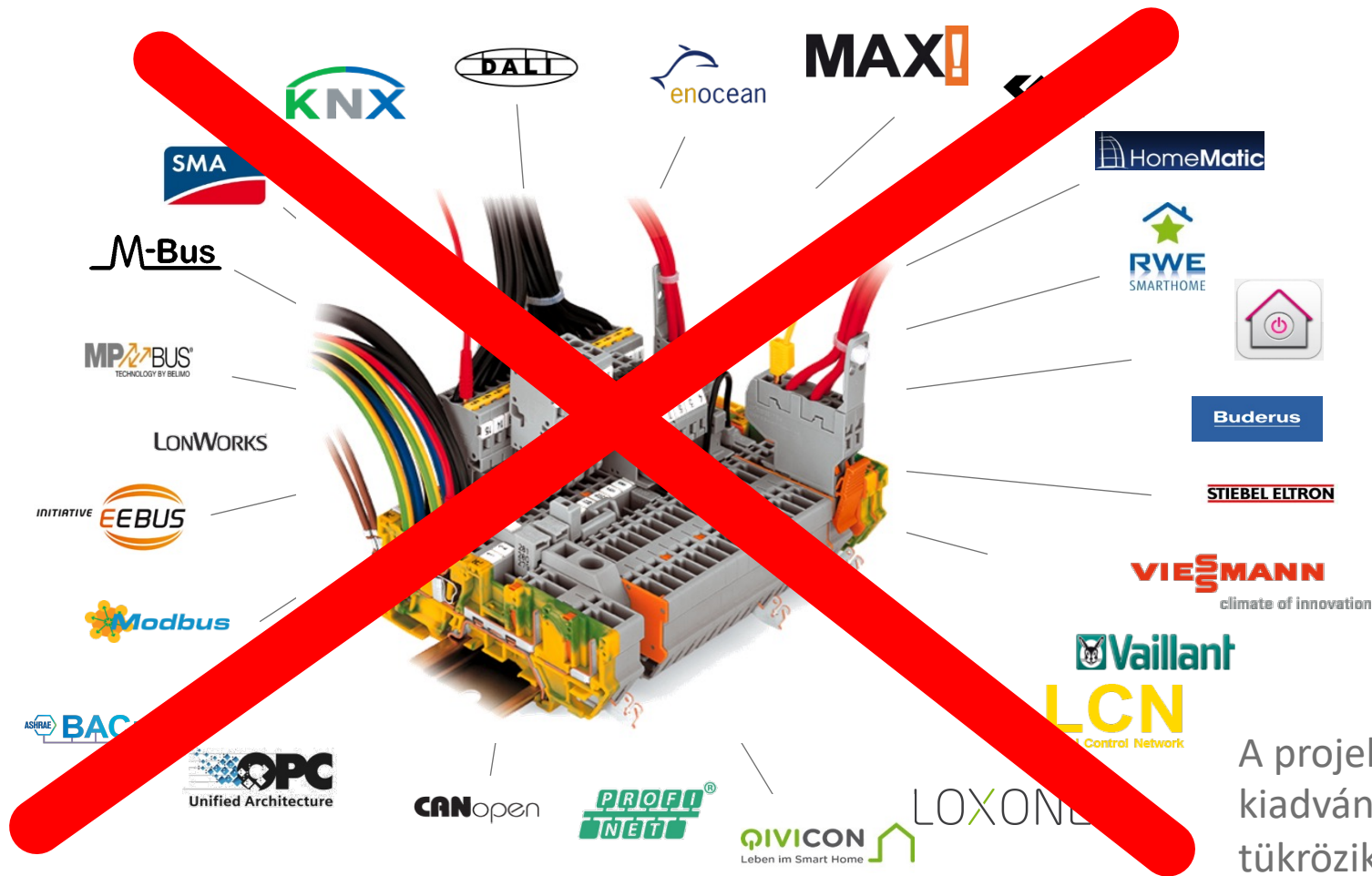


Standardizált kommunikációs protokollok

Miért csak szabványosított protokollokat kell használni??

- Világszerte (részben) szabványosított protokollok
- Az épületgépészet és az ipar különböző protokollokat használ
- Nagyon sok termék különböző gyártóktól egy protokollhoz
- A know-how elterjedt az ágazatbana rendszertől függően nagy integrációs erőfeszítés lehetséges
- nincs univerzális kapcsolat valamennyi protokoll között

Standardizált kommunikációs protokollok



There is no "Egg-laying woolmilk pig" yet



[<https://www.pinterest.de/pin/352688214560668227/>]

A projektet az Európai Bizottság támogatta. A kiadványban megjelentek nem szükségszerűen tükrözik az Európai Bizottság nézeteit.