

**BMS is destroyed
by "smart button"**

I am working at



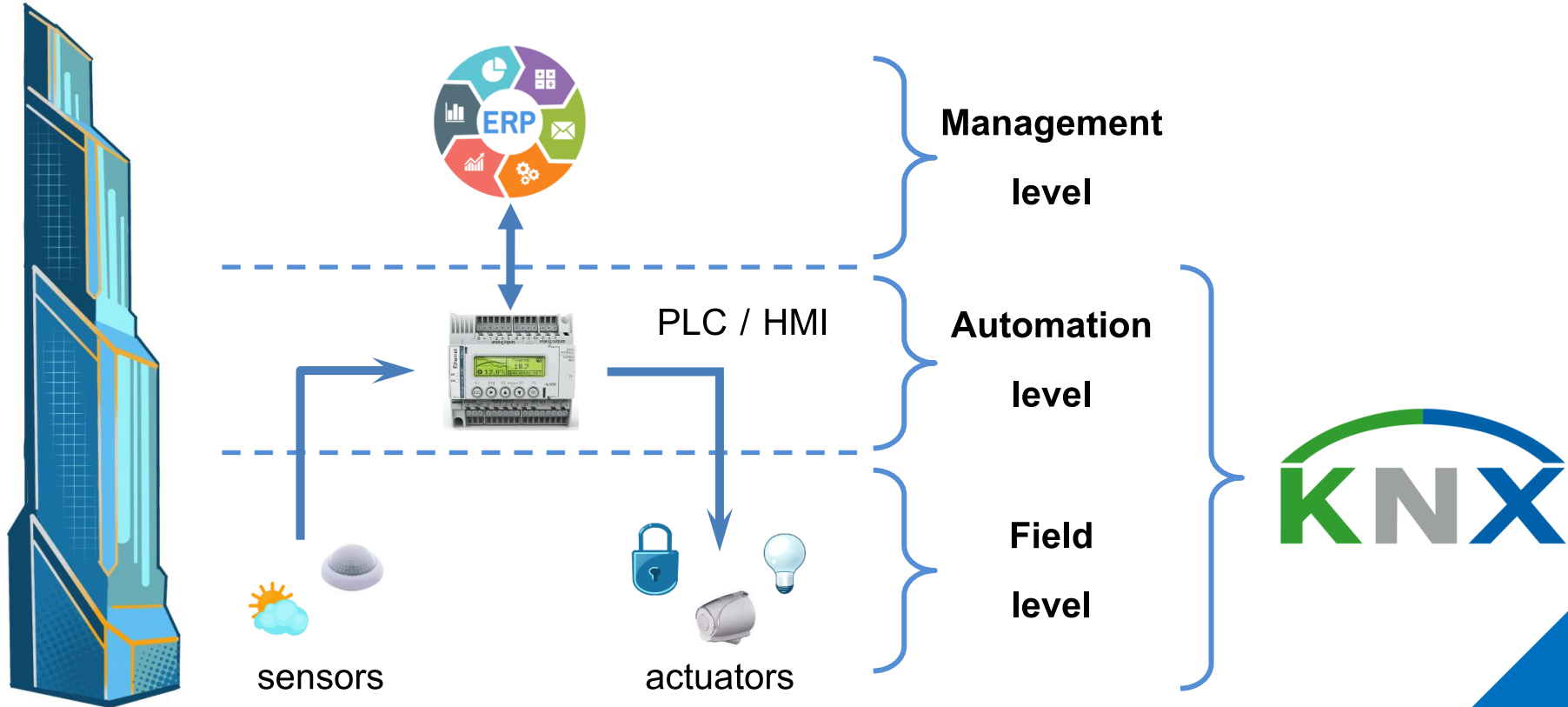
- **Specialize in ICS security of embedded devices**
- **Dedicate a lot of time to programming industrial controllers for ICS**
- **Took part in smart home development projects**

- **What is BMS**
- **Introduction to KNX**
- **Ideal world**
- **Real world**



What is BMS

Building Management System - BMS



BMS is destroyed by "smart button"



Reduce power consumption



Control operation of different systems

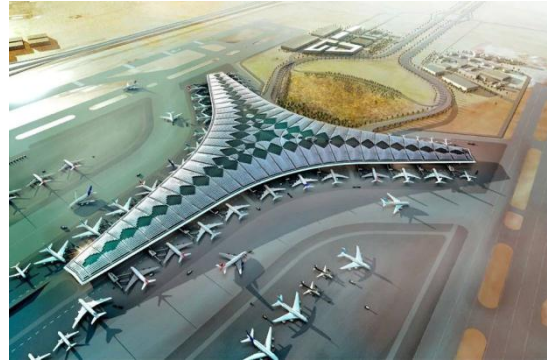


Ensure visitors' comfort





Asia Square



**Al Maktoum
International Airport**



**Welt Museum
Wien**



**Heating,
Ventilation and Air
Conditioning**



Indoor presence detection



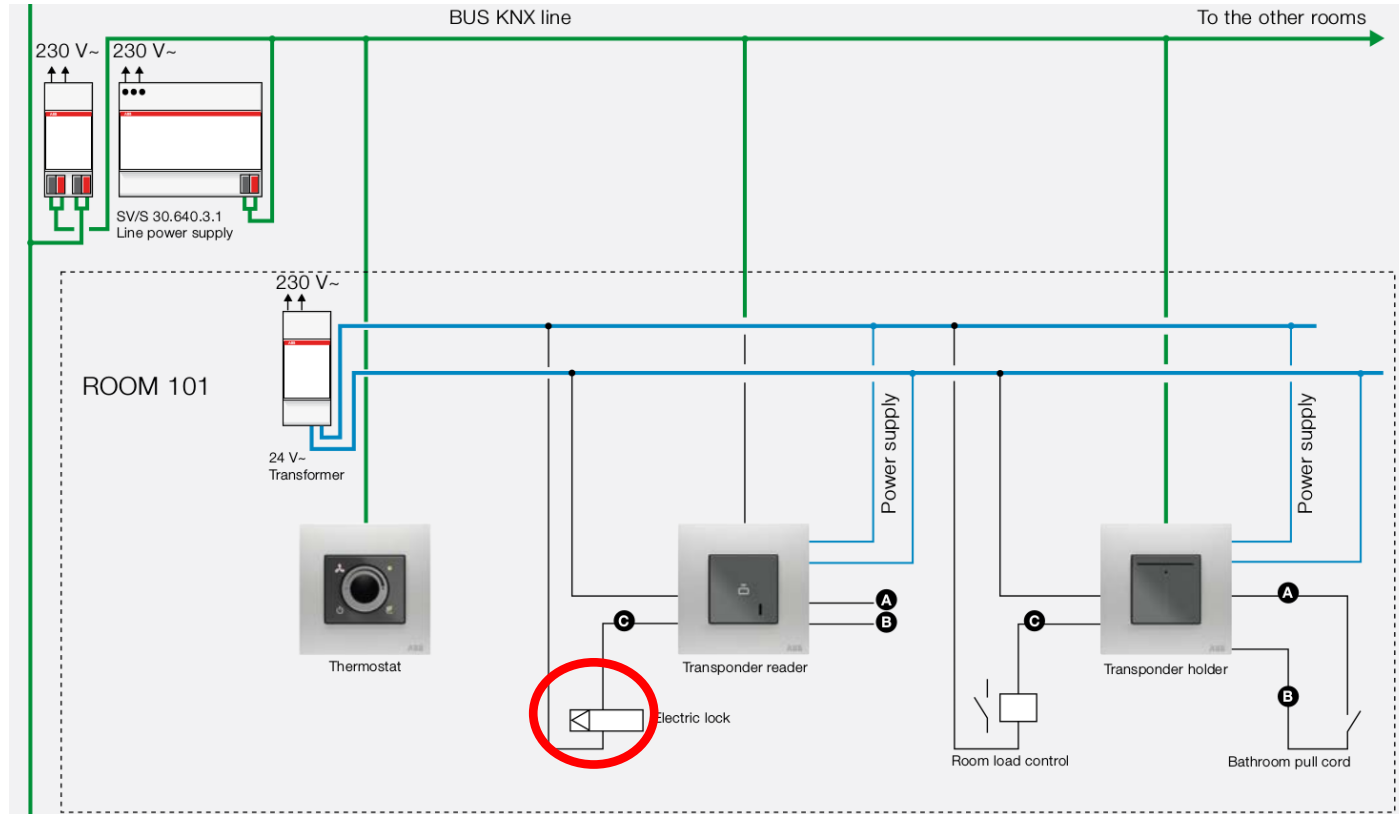
Room Thermostat



Transponder reader

....

ABB KNX solutions for hotel applications



Introduction to KNX

KNX - TP

(Twisted pair)



9600 bit/s

KNXnet/IP



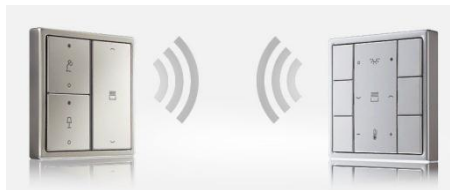
KNX - PL

Power Line (PL110)



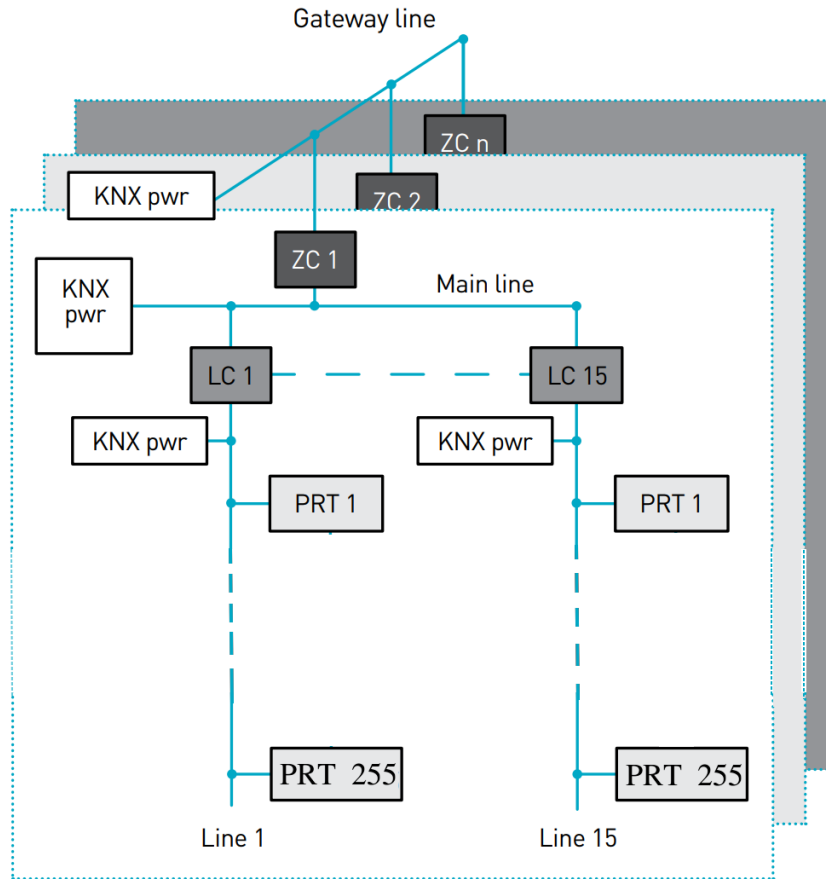
1200 bit/s

KNX - RF



16384 bit/s

868 MHz

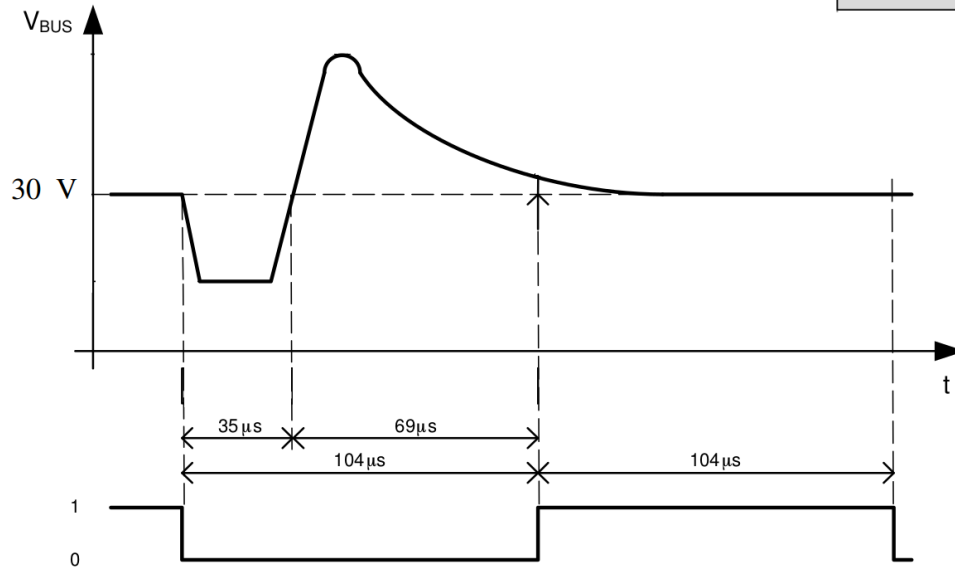


max 15 areas

1 area – max 15 lines

1 line – max 255 nodes

Control field	Source address	Receiver address	N_PDU		Check field
8 bit	16 bit	16 bit	8 bits	T_PDU	8 bit
				6 bits	A_PDU





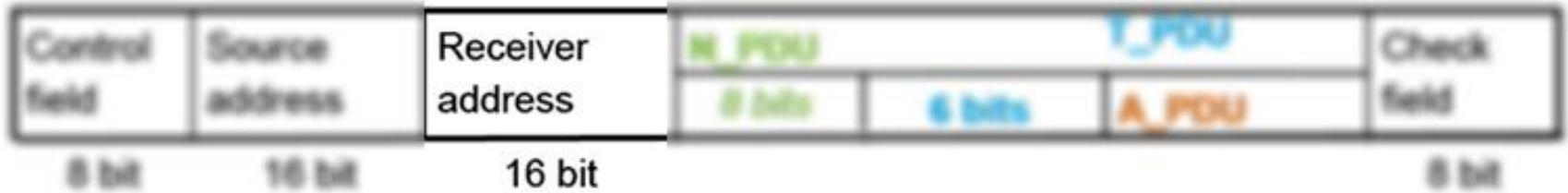
Control byte

		Byte 0							
		Control byte							
		8	7	6	5	4	3	2	1
		1	0	1	1	2	1	0	0
Priority						1	1	Low	
						0	1	High	
						1	0	Alarm	
						0	0	System	
Repeated				1	No				
				0	Yes				



Byte 1								Byte 2									
Source address								Source address									
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1		
4	3	2	1	4	3	2	1	8	7	6	5	4	3	2	1		
								n	n	n	n	n	n	n	n	0..255	node
				n	n	n	n	0..15								line	
n	n	n	n	0..15												area	

Source address



Byte 1 Receiver address								Byte 2 Receiver address							
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
0	4	3	2	1	1	0	9	8	7	6	5	4	3	2	1
					n	n	n	n	n	n	n	n	n	n	n
					0..2047										
					n n n n 0..15										

Receiver address

Byte 1 Receiver address								Byte 2 Receiver address							
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
0	4	3	2	1	3	2	1	8	7	6	5	4	3	2	1
								n	n	n	n	n	n	n	n
					0..255										
					n	n	n	0..7							
					n n n n 0..15										

It depends on Group Address Style



NPCI



Byte 5	
NPCI	
	8 7 6 5 4 3 2 1
	1 3 2 1 4 3 2 1
Length	n n n n 0..15
Routing counter	n n n 0..7
(DAF)	1 Group addressed telegram
	0 Individual addressed telegram

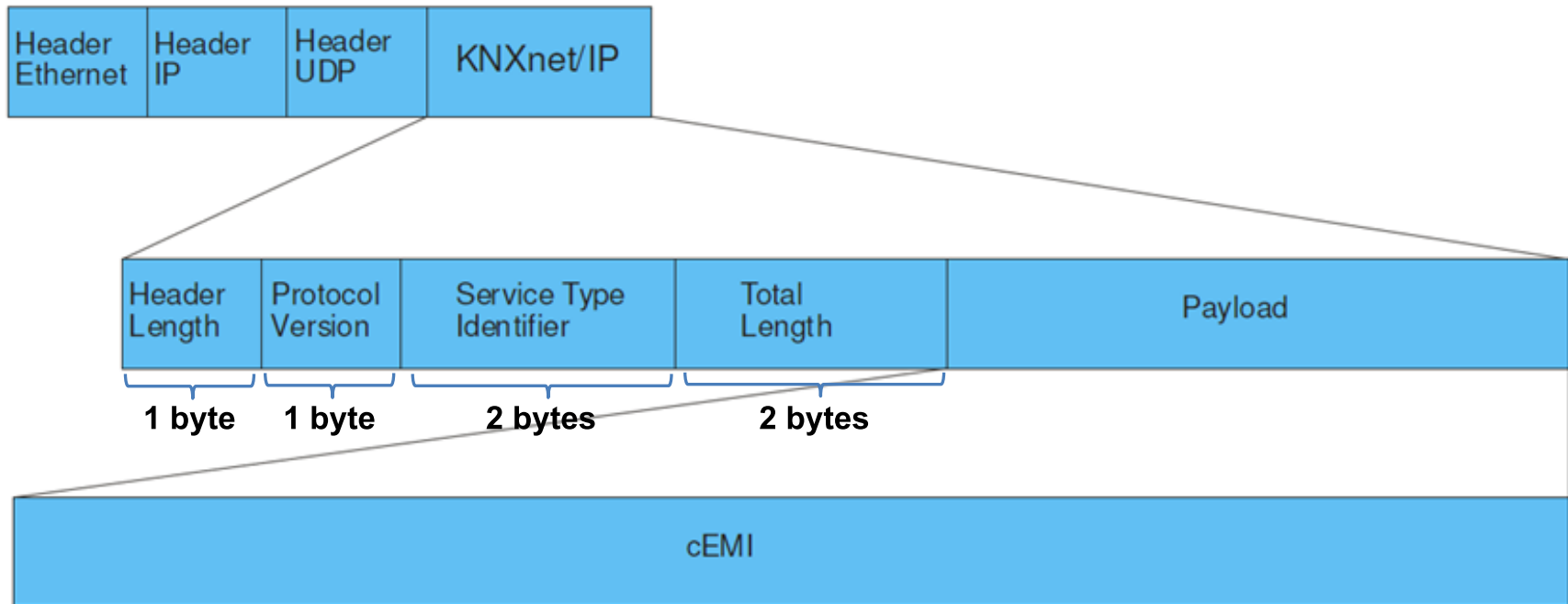


TPCI / APCI

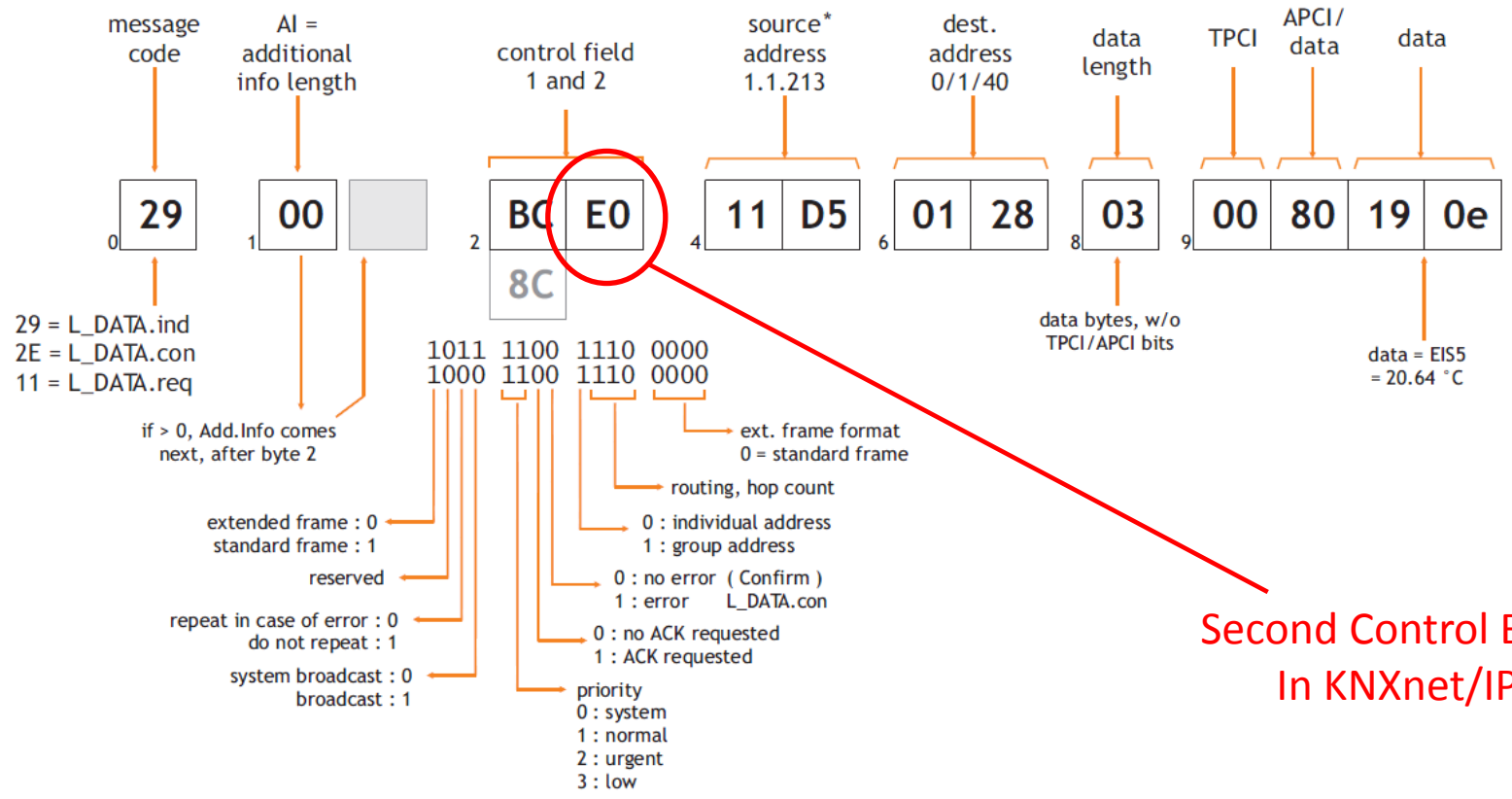
		Byte 6 TPCI / APCI								Byte 7 APCI							
		8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
		2	1	4	3	2	1	4	3	2	1	6	5	4	3	2	1
APCI								x	x	x	x	x	x	x	x	x	x
sequence number				n	n	n	n	0..15									
TPCI	0 0	UDT (Unnumbered Data Packet)															
	1 0	UCD (Unnumbered)															
	0 1	NDT (Numbered Data Packet)															
	1 1	NCD (Numbered Control Data)															

APCI	Name
0011	IndividualAddrWrite
0100	IndividualAddrRequest
0101	IndividualAddrResponse
0110	AdcRead
0111	AdcResponse
1000	MemoryRead
1001	MemoryResponse
1010	MemoryWrite
1011	UserMessage
1100	MaskVersionRead
1101	MaskVersionResponse
1110	Restart
1111	Escape





Multicast @ 224.0.23.12:3671

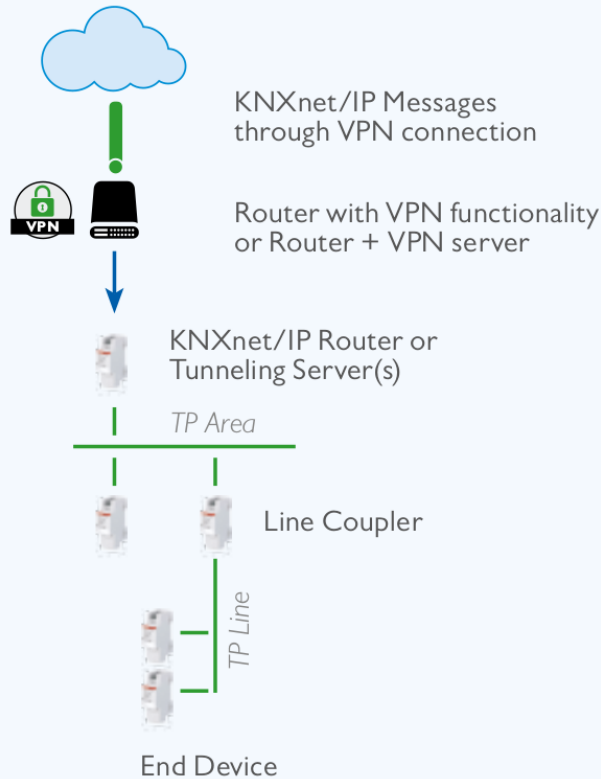


Second Control Byte
In KNXnet/IP

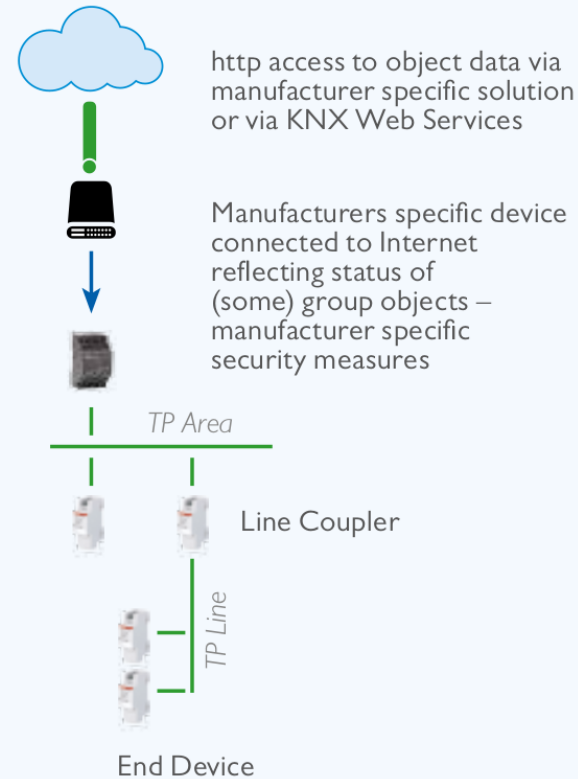


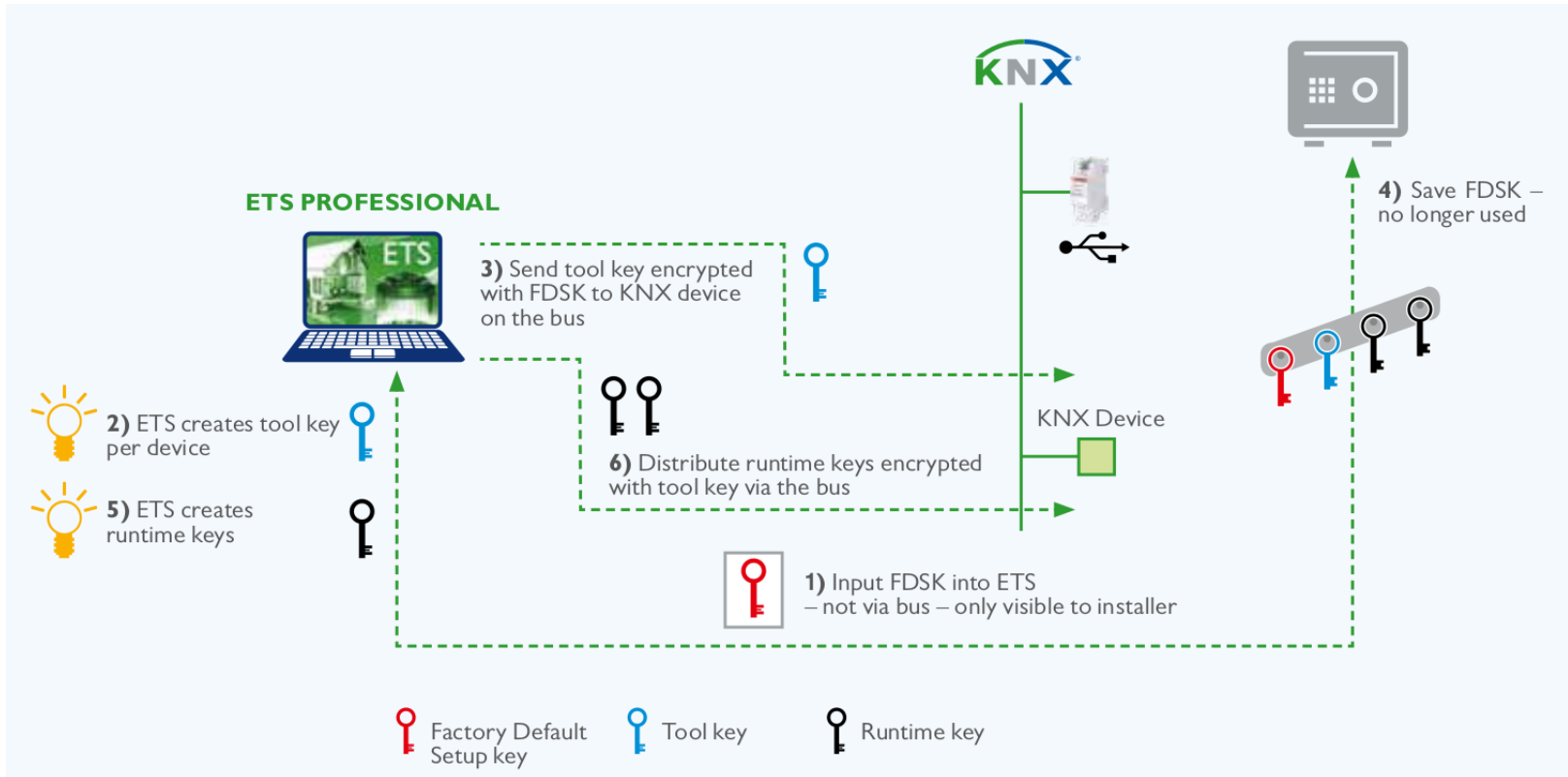
Ideal world

RECOMMENDED A



RECOMMENDED B





KNX Position Paper on Data Security and Privacy

The screenshot shows the ETS5 software interface. The 'Topology' window displays a network tree on the left and a table of network elements in the center. A blue arrow labeled '1' points to the 'Topology Backbone' folder. The 'Properties' window on the right shows configuration for the selected element, with a blue box and arrow labeled '2' highlighting the 'Security' dropdown menu.

Area	Name	Description	Mainline Me	Domain Address
1	New area		IP	-

Manufacturer	Name	Order Number	Medium	Application	Version
ABB	IPR/S3.1.1 IP-Router,REG	2CDG 110 175 R0011	TP,IP	IP-Router/2.0	1.0

Properties

Settings Comments Information

Backbone Name

Backbone area

Description

Status: Unknown

Backbone Medium: IP

Network Latency: WAN (< 2s)

Multicast Address: 224.0.23.12

Security: On

Bus Connection: None

Find and Replace

Workspaces

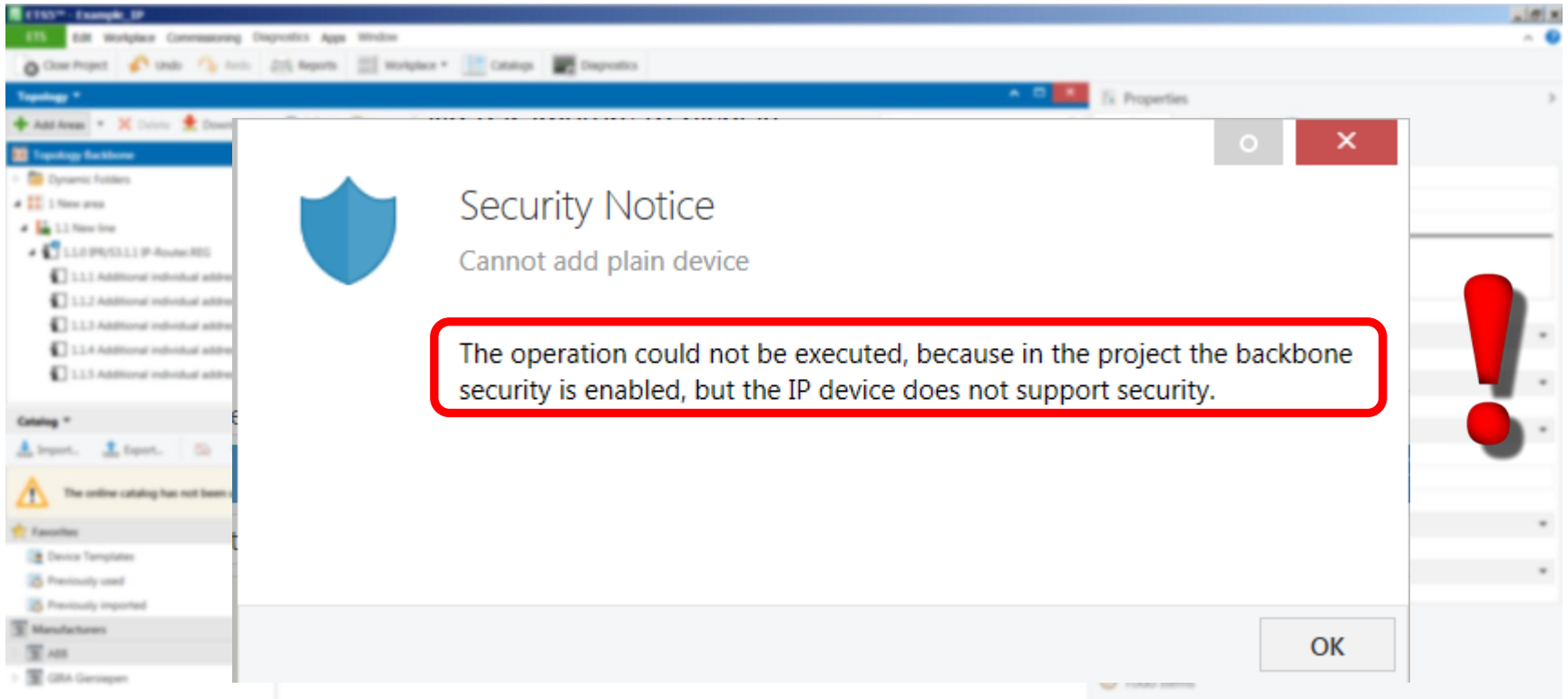
Todo Items

ETS5 provides security connection


HOWEVER ...

BMS is destroyed by "smart button"

Real world



ETS5 provides security connection



[Register](#)
[Sign In](#)

[Results](#)

[Map](#)

[Metadata](#)

[Report](#)

[Docs](#)

Quick Filters

For all fields, see [Data Definitions](#)

Autonomous System:

- 24 COMCAST-7922 - Comcast Cable Communications, LLC
- 15 ATT-INTERNET4 - AT&T Services, Inc.
- 8 HIGG
- 7 CENTURYLINK-US-LEGACY-QWEST - CenturyLink Communications, LLC
- 6 TNF-AS

[More](#)

Protocol:

HTTP/1	151	80/http
Date:	101	443/https
Server	64	21/ftp
X-POWE	57	23/telnet
Set-Co	49	22/ssh

[More](#)

Tag:

- 188 http
- 99 https
- 64 ftp
- 57 telnet
- 49 ssh

[More](#)

```
<neau>
<title
</nead
<body>
```

IPv4 Hosts

Page: 1/8 Results: 194 Time: 128ms

50.247.4.218 (50-247-4-218-static.hfc.comcastbusiness.net)

- COMCAST-7922 - Comcast Cable Communications, LLC (7922) Ferndale, Michigan, United States
- LOYTEC electronics GmbH LIP-ME201C 443/https, 47808/bacnet, 80/http
- 47808.bacnet.device_id.vendor.official_name: LOYTEC Electronics GmbH

BUILDING CONTROL
SCADA

96.65.136.164 (96-65-136-164-static.hfc.comcastbusiness.net)

- COMCAST-7922 - Comcast Cable Communications, LLC (7922) Sarasota, Florida, United States
- LOYTEC electronics GmbH LINX-203 21/ftp, 22/ssh, 23/telnet, 443/https, 47808/bacnet, 80/http
- 47808.bacnet.device_id.vendor.official_name: LOYTEC Electronics GmbH

BUILDING CONTROL
EMBEDDED
SCADA

96.65.136.162 (96-65-136-162-static.hfc.comcastbusiness.net)

- COMCAST-7922 - Comcast Cable Communications, LLC (7922) Sarasota, Florida, United States
- LOYTEC electronics GmbH LIOB-584 21/ftp, 22/ssh, 23/telnet, 443/https, 47808/bacnet, 80/http
- 47808.bacnet.device_id.vendor.official_name: LOYTEC Electronics GmbH

BUILDING CONTROL
EMBEDDED
SCADA

87.144.182.71 (p5790B647.dip0.t-ipconnect.de)

- DTAG Internet service provider operations (3320) Unterfoehring, Bavaria, Germany
- 443/https, 80/http
- loytec.local
- 443.https.tls.certificate.parsed.issuer.organization: LOYTEC electronics GmbH

h)
erland

93.146.245.98 (net-93-146-245-98.cust.vodafone51.it)

- VODAFONE-IT-ASN (30722) Rome, Latium, Italy
- LOYTEC electronics GmbH LVIS-3ME15-A1 21/ftp, 22/ssh, 23/telnet, 443/https, 47808/bacnet, 5900/vnc, 80/http
- 47808.bacnet.device_id.vendor.official_name: LOYTEC Electronics GmbH

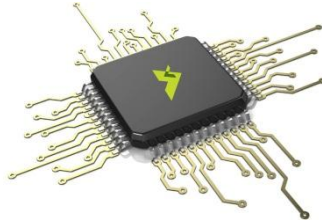
BUILDING CONTROL
EMBEDDED
REMOTE_DISPLAY
SCADA
VNC

50.208.3.241

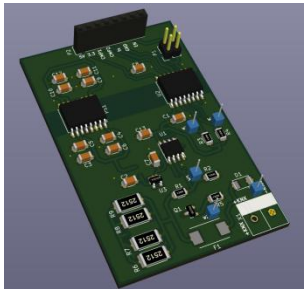
- COMCAST-7922 - Comcast Cable Communications, LLC (7922) Denver, Colorado, United States
- LOYTEC electronics GmbH LVIS-3ME15-G1 22/ssh, 443/https, 47808/bacnet, 80/http



stand-alone device



**“smart” transceiver
(NCN5120 or E981.03)**



Design self-transceiver

ETS software



**Press button to switch
“Program mode”**

Commit/configure node



pwnknx

connection



Ethernet (via IP gateway)



Ethernet/Wi-Fi (based on esp32)



KNX-TP (based on esp32)

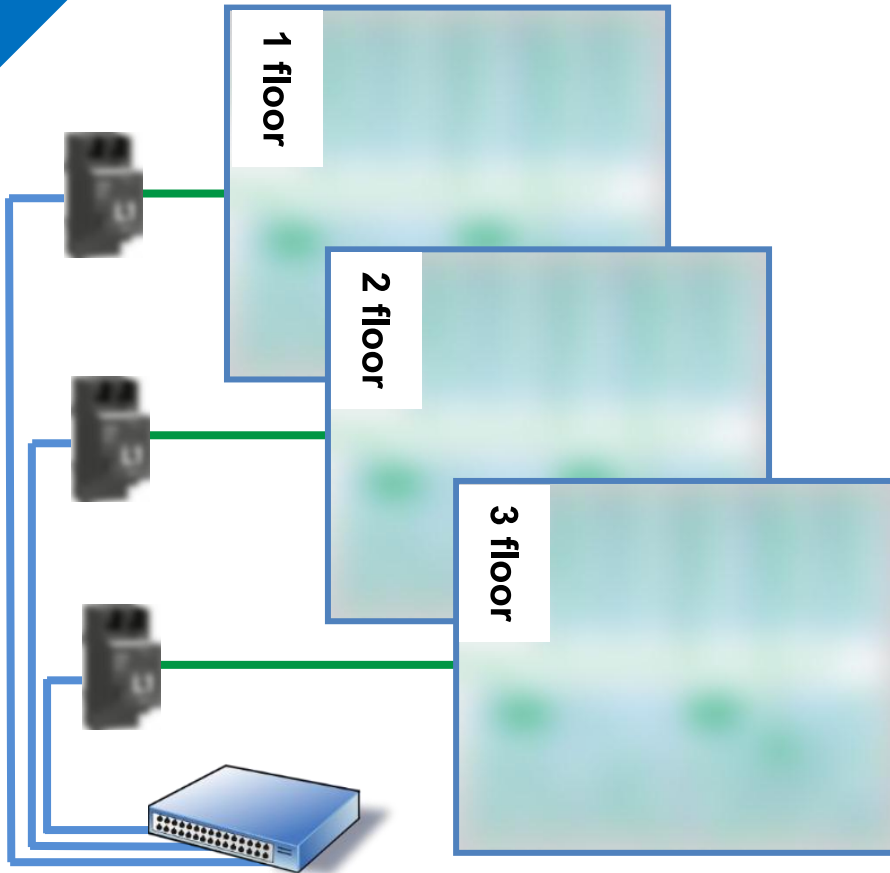


<https://github.com/Xarlan/pwnknx>



pwnknx

- **sniff** To get information about number line, address format, which used
- **scan** To find all nodes in a line, because ETS5 sometimes can't display all of them
- **read** Read configuration from node (APCI "memory read")
- **write** Write configuration to node (APCI "memory write")
- **set_key** Set the authorization key (APCI "Escape" + extended APCI bits)

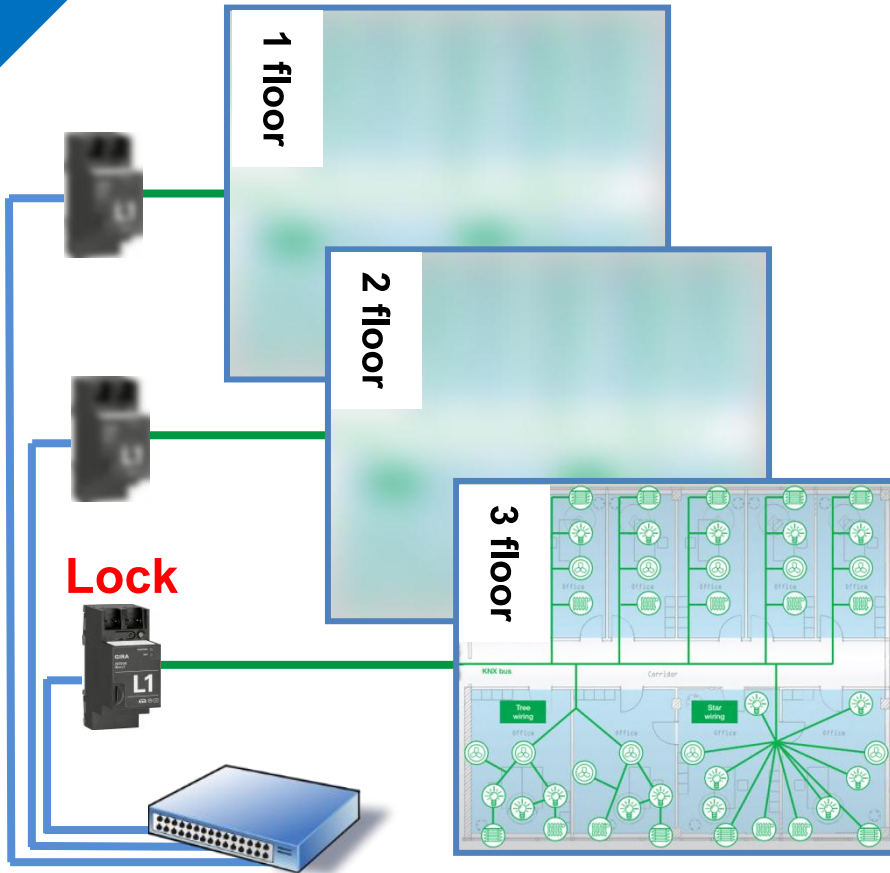


Connect **anywhere** to KNX TP

- Listen the traffic and slightly understand the type of devices
- Replay attack

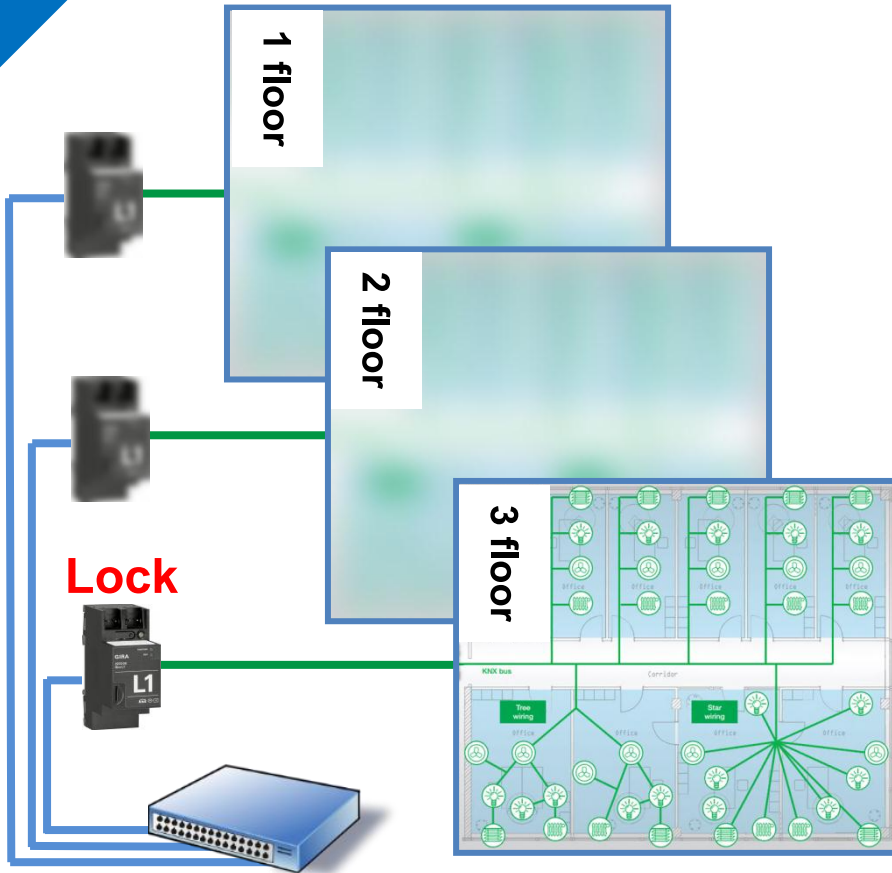


— Ethernet
— KNX-TP



- Discover KNX-TP segment
- Manage nodes in current KNX-TP segment





- Use APCI “Read memory” to get info

IP 192.168.1.222

Mask 255.255.255.255

Gateway 192.168.1.1

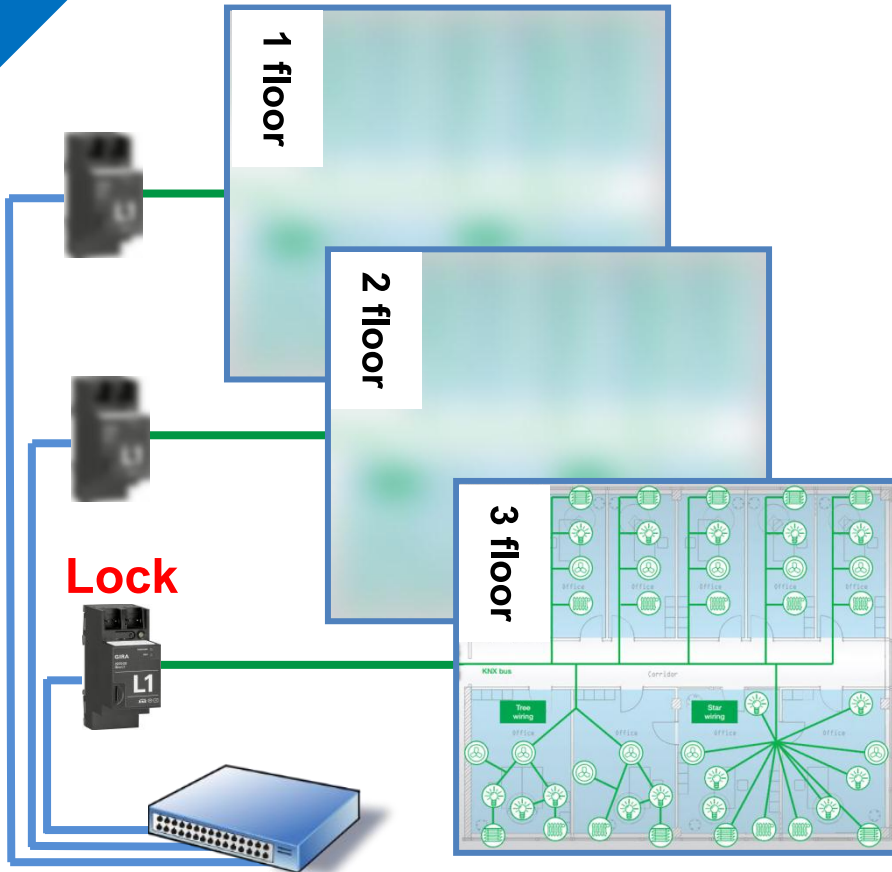
Status router Lock or Unlock

...

```

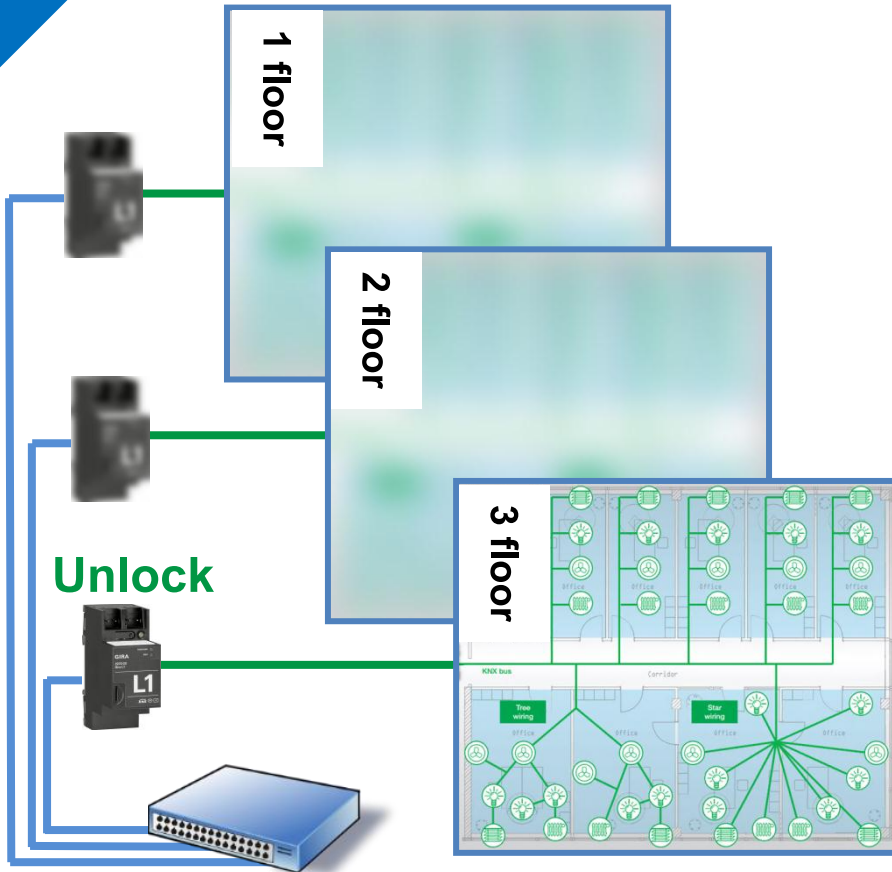
0140h: 00 01 00 00 00 00 C0 A8 01 DE FF FF FF 00 C0 A8 .....A".byyy.A"
0150h: 01 01 5E 1A 0E 1A 08 10 00 00 00 FF 00 00 00 00 ..w.....y....
0160h: 00 00 00 00 00 00 00 33 0D A8 58 0A AF 42 59 4B .....3."X."BYK
0170h: 21 04 78 62 01 01 01 00 00 06 00 07 00 08 00 0B !.xb.....
0180h: 00 51 C3 06 00 07 03 FF FF FF FF FF FF FF FF FF .QÃ....yyyyyyyyy
    
```

— Ethernet
— KNX-TP



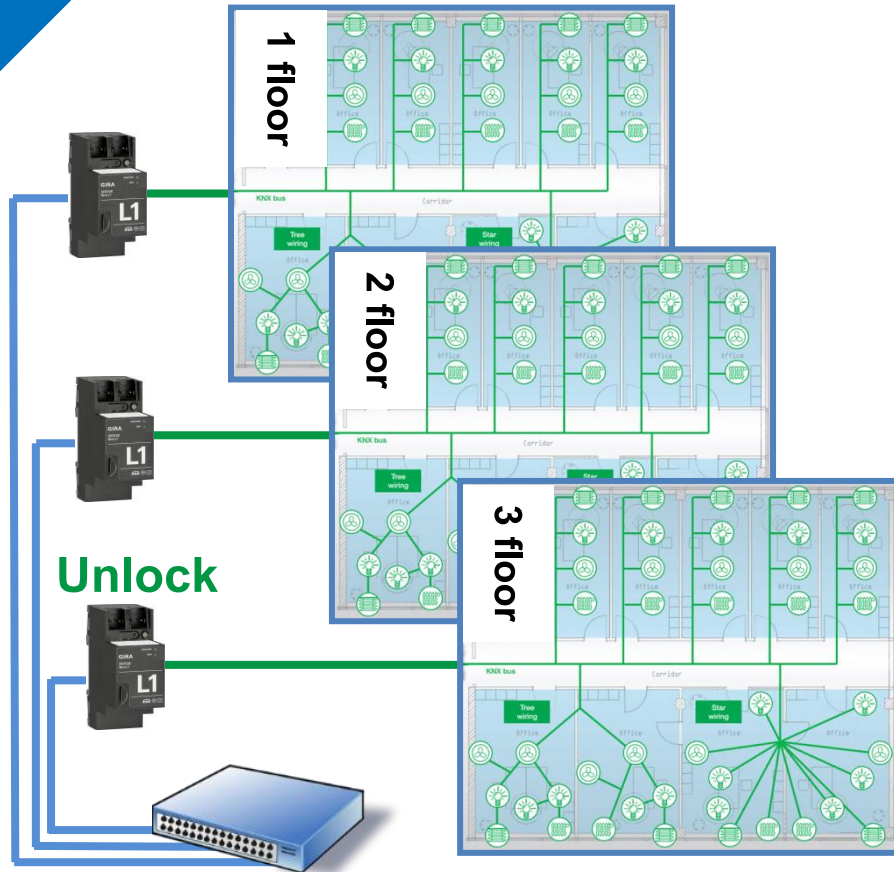
- Use APCI “Write memory” to change the configuration node or IP router

— Ethernet
— KNX-TP



- Use APCI “Write memory” to change the configuration node or IP router

— Ethernet
— KNX-TP

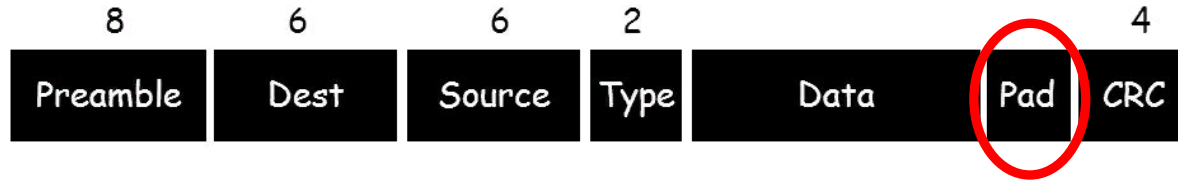


- Discover and manage all nodes in KNX-TP & KNXnet/IP

— Ethernet
— KNX-TP

- **APCI “User Message”**
we can to send up to 69 bytes, not 15 bytes,
some router can transfer 69 bytes form knx-tp to KNXnetIP
- **Padding for Ethernet frame**

Ethernet Frame Format



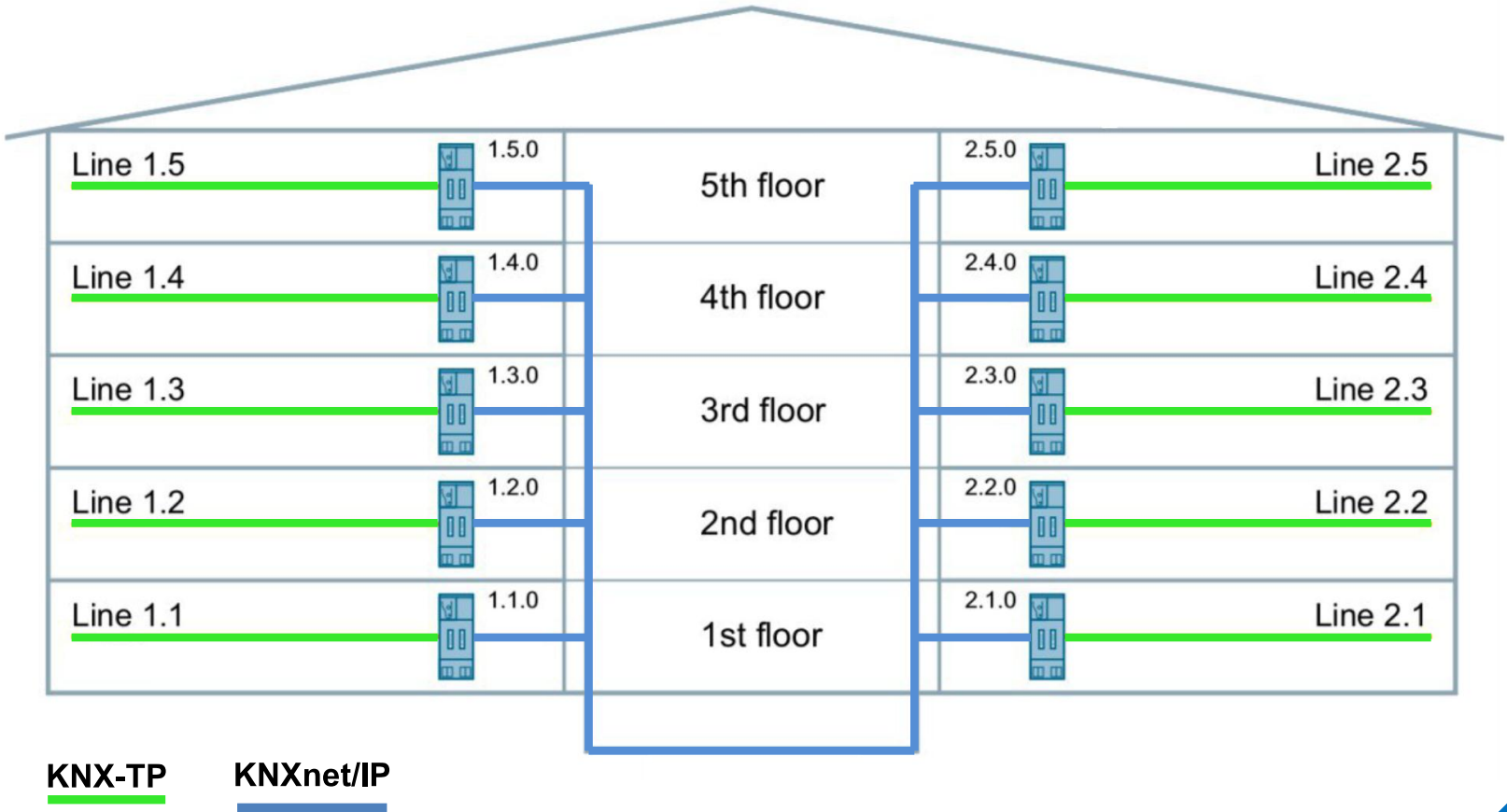
for some KNX IP router don't forget about



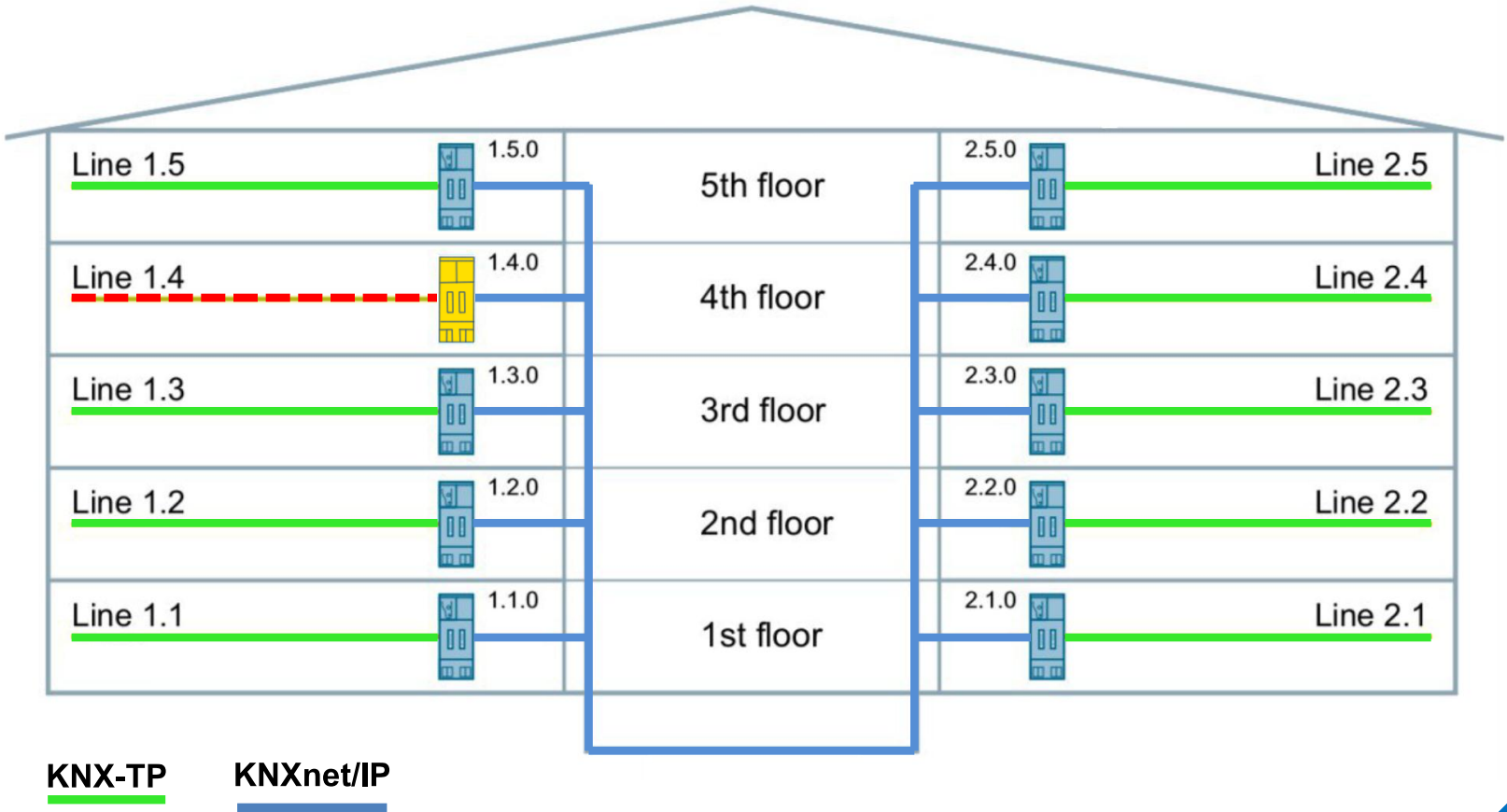
- **No needed to switch to “program mode”**
in ETS5 you need switch to “program mode” to change configuration of node
in real life – use APCI “memory read/write” without “key authorization”

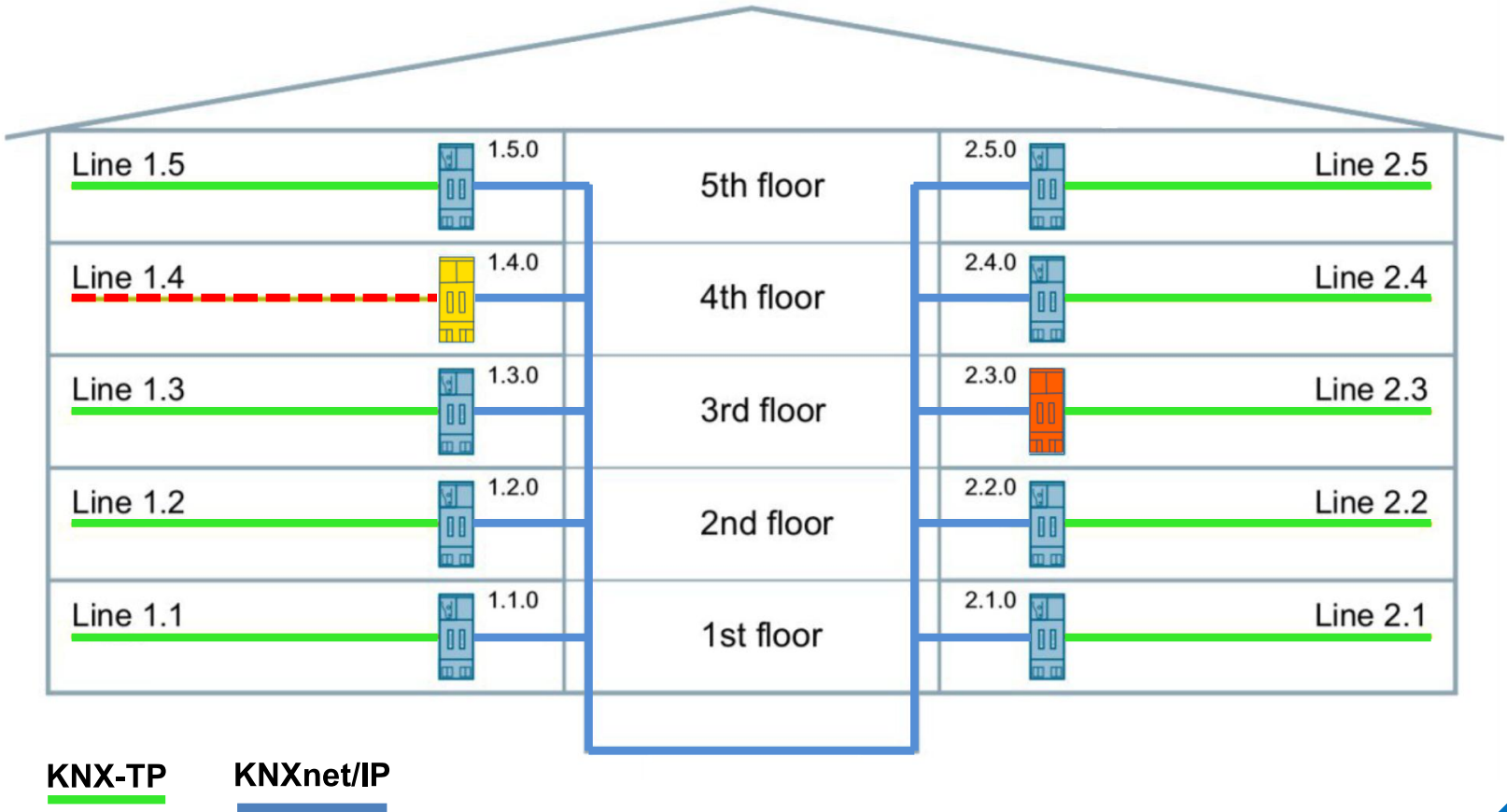
- **APCI “Escape” + Key authorization**
use to “memory access-protection”
However, some nodes can confirm that the
authorization key was changed,
but in reality nothing happened!!!





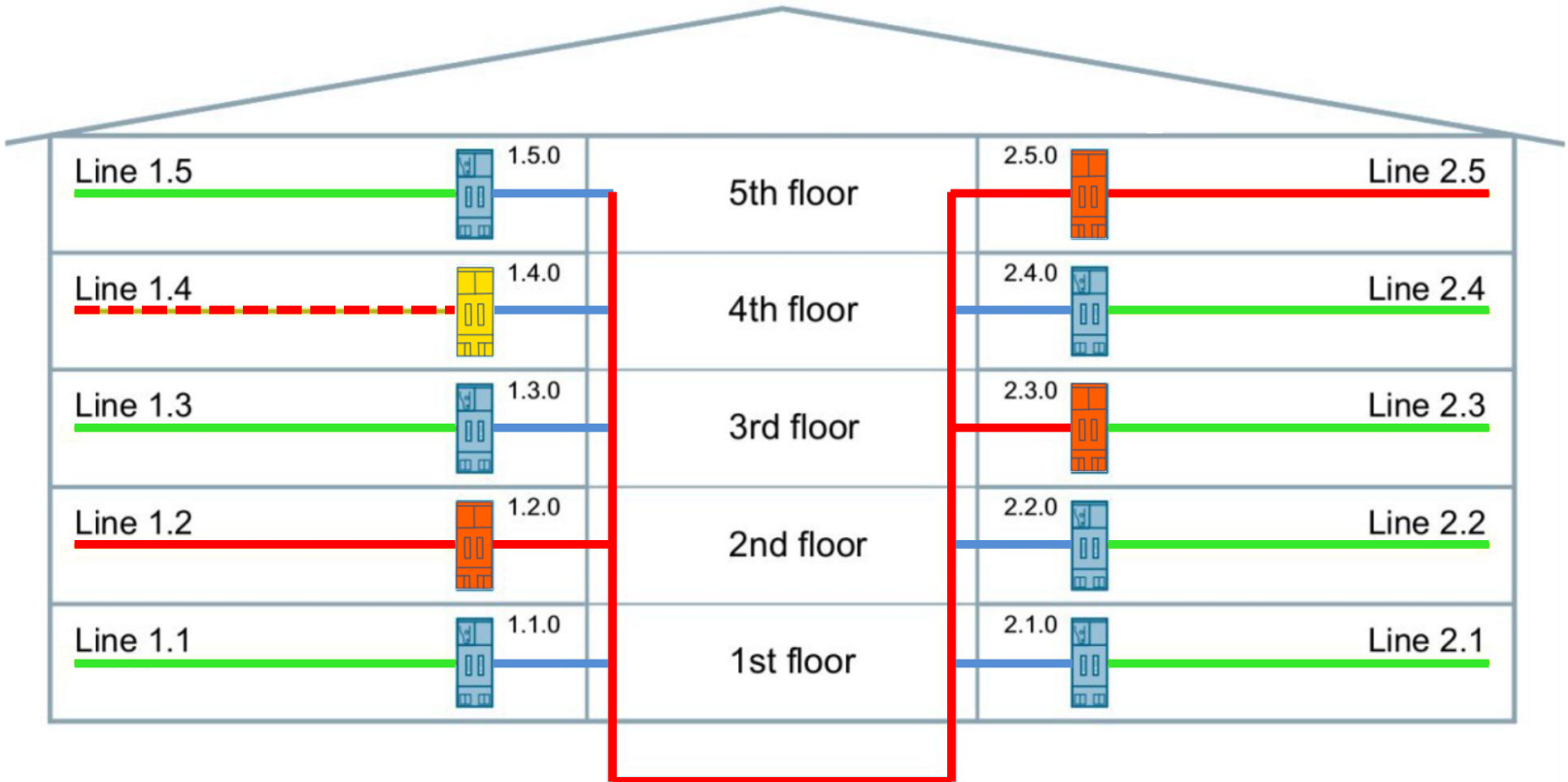
KNX-TP KNXnet/IP





KNX-TP

KNXnet/IP



KNX-TP KNXnet/IP

How to update firmware on IP router from field side ?

Use APCI “User Message”

- to read firmware:

APCI = 0x2C0 (User Message)

Data = [0xXX, ..., 0xXX]

where

0xXX – the part of firmware

- to write firmware:

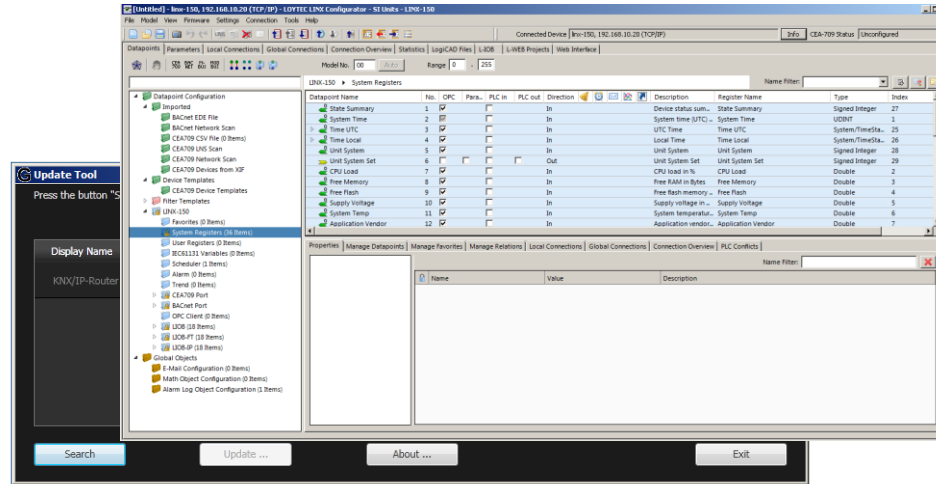
APCI = 0x2C2 (User Memory Write)

Data = [0xXX, ..., 0xXX]

where

0xXX – the part of firmware

How to get control over the device Connect to the Ethernet

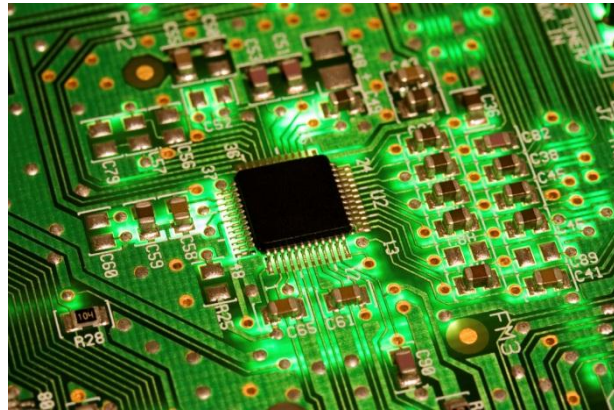


Update

Run
“vendor name”
Update Tool

Possible MCU:

- ATmega128
- AT91SAM9G20
- NXP LPC2366



Possible OS:

- Nut/OS
- Linux
- Custom firmware



Possible transceiver:

- FZE1066
- EIB-TP-UART-IC
- E981.03

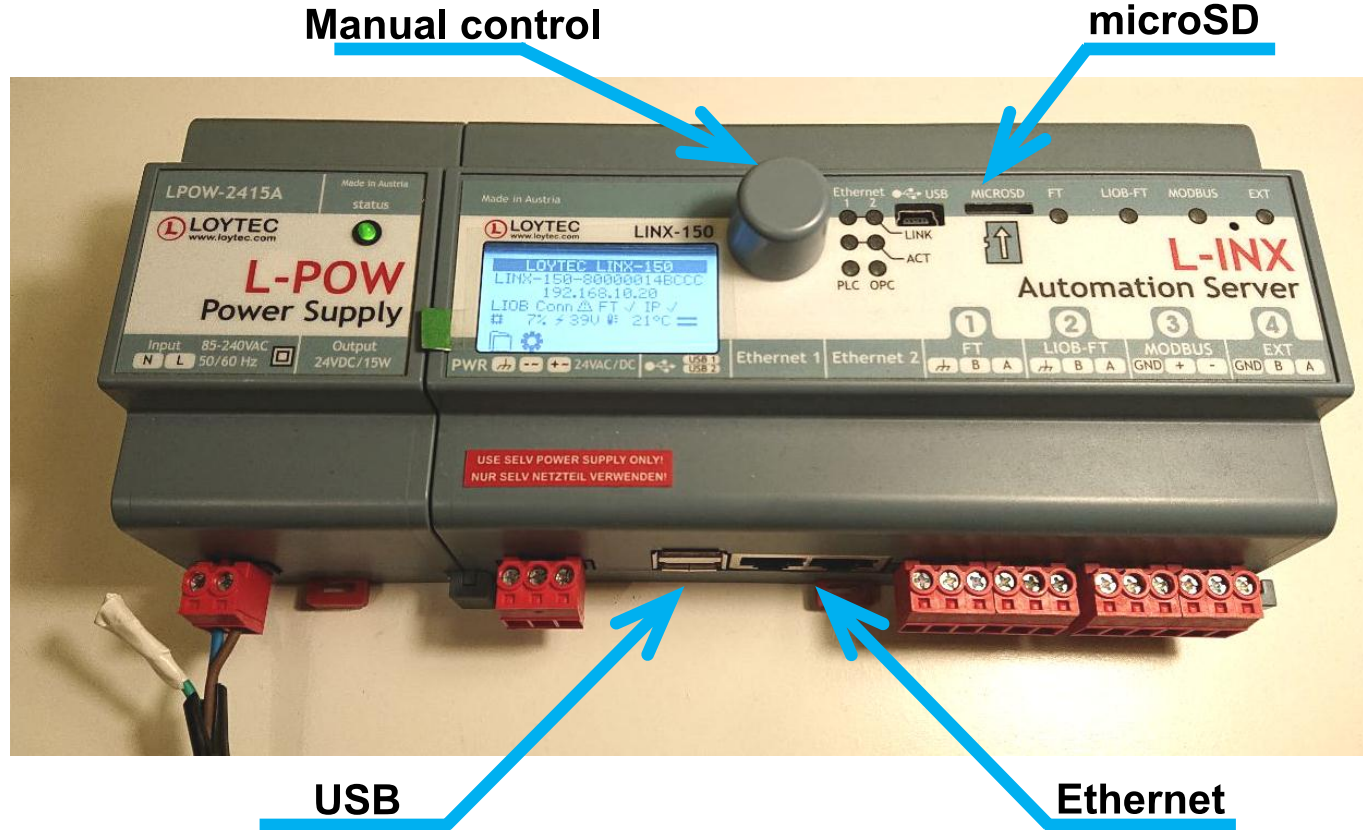


Linx 150



- programmable automation stations
- program connectivity functions to concurrently integrate:
 - CEA-709 (LonMark Systems);
 - BACnet;
 - KNX;
 - Modbus;
 - M-Bus

Linx 150



Manual control

microSD

USB

Ethernet

Linx 150



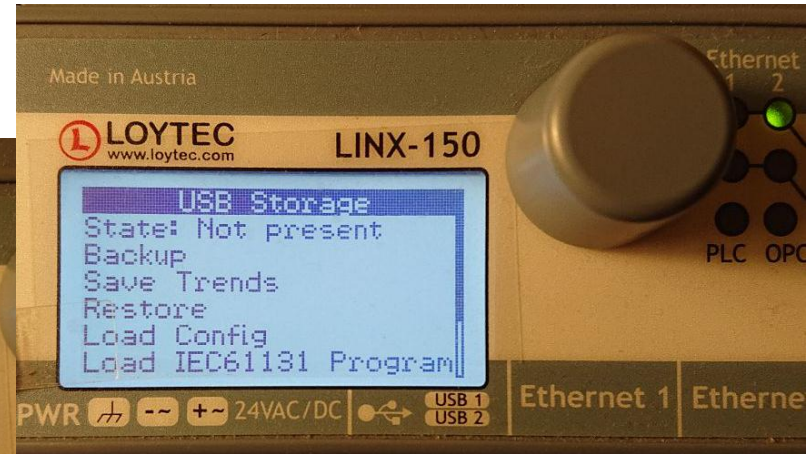
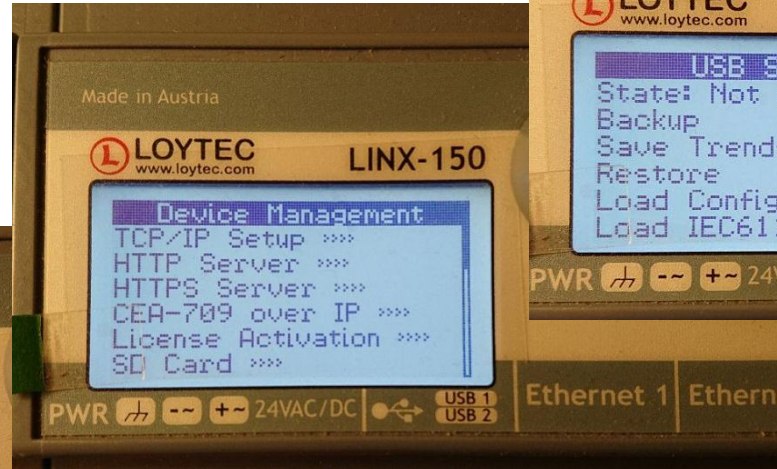
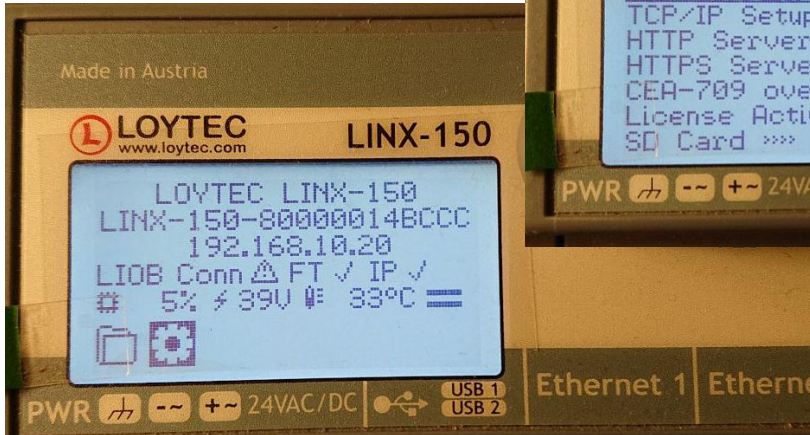
Serial

38,400 bps / 8 data bits /
no parity / 1 stop bit / no handshake

Manual

Ethernet

- http web server
- ftp
- ssh
- ...



You can do anything!!!

Linx 150



192.168.10.20 192.168.10.20 - Device Info

LOYTEC **Device Info**

networks under control

LINX-150
guest
192.168.10.20:53

Device Info
Data
Commission
Config
Statistics
L-WEB
L-IOB
Documentation
Reset
Contact
Logout

General Info

Product	LINX-150, firmware 6.1.2	2017-04-06 16:14:00
Hostname	LINX-150-80000014BCCC, 192.168.10.20	
Serial number	017906-80000014BCCC	
Free RAM, swap, flash	28376 KB, 65532 KB, 155684 KB	
CPU, temp, supply	6%, 33°C, 39.4V	
NTP status	out-of-sync	
Uptime	01:53:29	

Device Status

Warning

- Hardware: Supply voltage (39.4 V) too high
- Network: NTP out of sync
- L-IOB status: LIOB-Connect (X), LIOB-FT (✓), LIOB-IP (✓)
- IEC61131 status: Logic stopped (X), I/O driver active (✓)
- IEC61131 program source: No program on device
- Port 1: CEA-709 (✓)
- Port 2: LIOB-FT (✓)
- Port 3: Disabled
- Port 4: Disabled
- LIOB: LIOB-Connect (✓)
- USB: Disabled
- Ethernet 1 (LAN): no link (X), 192.168.10.20

Ethernet 1 (LAN) services:
 ✓ VNC for LCD UI, ✓ FTP, ✓ Telnet, ✓ SSH
 ✓ Global Connections (CEA-852), ✓ LIOB-IP
 ✓ Web UI, ✓ HTTP, ✓ HTTPS, ✓ Modbus TCP
 ✓ KNXnet/IP, ✓ BACnet/IP, ✓ RNI 0 (CEA-709)
 ✓ SNMP, ✓ OPC XML-DA

Ethernet 2 (WAN): connected (✓), switched (✓)
 Wireless 1: Disabled
 Wireless 2: Disabled

Firmware Info

	Primary (ACTIVE)	Fallback
Firmware	LINX-AT91 Primary Image	LINX-AT91 Fallback Image
Version	6.1.2	4.5.0
Build date	2017-04-06 16:14:00	2012-04-27 14:00:13

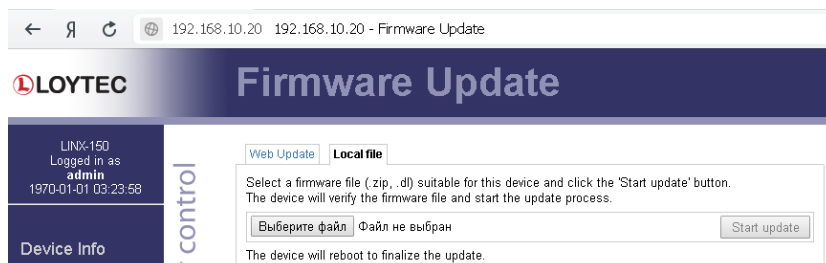
Project Information

Project file	HVahuPlant001_V2.linx	<input type="checkbox"/> Remote config
Project name	AHU System HVplant001	

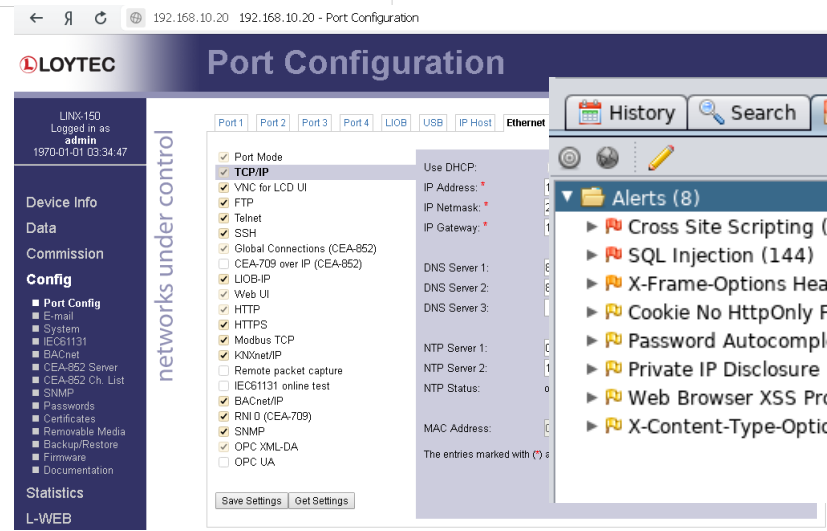
A lot of information
for guest

Account: admin

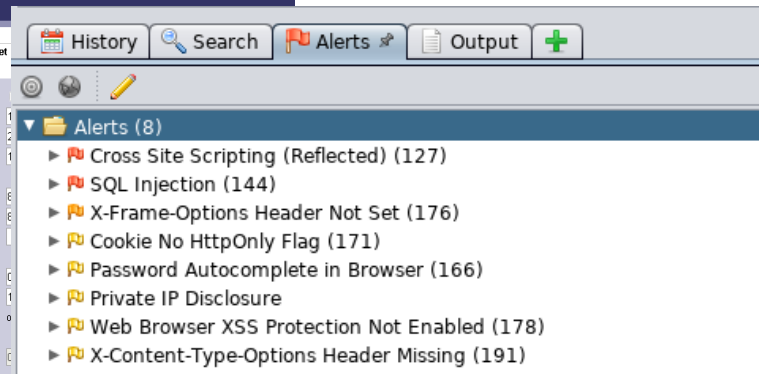
Password: loytec4u



networks under control



networks under control



Don't forget, that the communication happens via HTTP, FTP

LINX-150
Logged in as
admin
1970-01-01 04:16:43

Device Info
Data
Commission
Config

- Port Config
- E-mail
- System
- IEC61131
- BACnet
- CEA-852 Server
- CEA-852 Ch. List
- SNMP
- **Passwords**
- Certificates
- Removable Media
- Backup/Restore
- Firmware
- Documentation

networks under control

Enter the desired passwords for the administrator, operator and guest accounts.
The administrator has full access to the device, whereas a guest can only view the status information but not change the configuration.
In order to clear a password leave the password field empty.

Account

New password:

Retype password:

min: 1 symbol

max: 15 symbols

Analyze `/etc/init.d/S35firewall` and other network settings

```
fw_start()
{
    local ssh_port
    local ftp_port

    # Get SSH port from registry
    ssh_port=$(ltreg --read | egrep "sys.srv.sshd.0.port=0x[0-9a-f]+" | sed 's/.*///')

    # Get FTP port from registry
    ftp_port=$(ltreg --read | egrep "sys.srv.ftpd.0.port=0x[0-9a-f]+" | sed 's/.*///')
    if [ -z "$ftp_port" ]; then
        ftp_port=21
    else
        ftp_port=$(( $ftp_port ))
    fi

    # Reload FTP conntrack module
    rmmod nf_conntrack_ftp
    modprobe nf_conntrack_ftp ports=$ftp_port

    fw_clear

    ##### RAW #####

    # Disable conntrack on local interface
    iptables -t raw -A PREROUTING -i lo -j CT --notrack
    iptables -t raw -A OUTPUT -o lo -j CT --notrack

    ##### INPUT #####

    # Allow local interfaces
    iptables -A INPUT -i lo -j ACCEPT
    iptables -A INPUT -i usb0 -j ACCEPT

    # Allow related
    iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

    # Application input chain
    iptables -N INPUT_APP
    iptables -A INPUT -j INPUT_APP

    # Allow ssh if registry is not readable
    if [ -z "$ssh_port" ]; then
        iptables -A INPUT -m state --state NEW --proto tcp --dport 22 -j ACCEPT
    fi
}
```

NOT

rules in *iptables*

fail2ban

sshguard

if you miss - engage in brute force




















linx_at91_6_4_6_20190213_1030.dl

Download from official web site

<https://www.loytec.com/de/support/download/linx-150>



linux_at91_6_4_6_20190213_1030.dl

 base_1.6.0-2_arm.opk	1,9 MB	Debian package
 bmstp_4.4.122_5.2.2-2_arm.opk	18,2 kB	Debian package
 bootstrap-loytec9g20_3.2-2_arm.opk	5,5 kB	Debian package
 dropbear_2018.76-1_arm.opk	191,2 kB	Debian package
 fcgi_2.4.0-10_arm.opk	21,3 kB	Debian package
 freetype_2.7.1-1_arm.opk	282,4 kB	Debian package
 hostapd_2.6-3_arm.opk	408,9 kB	Debian package
 iptables_1.6.1-1_arm.opk	293,4 kB	Debian package
 iw_4.9-1_arm.opk	64,8 kB	Debian package
 jpeg_1.5.1-1_arm.opk	100,2 kB	Debian package
 libconfig_1.5-2_arm.opk	47,3 kB	Debian package
 libftdi1_1.3-1_arm.opk	25,2 kB	Debian package
 libnl_3.2.27-1_arm.opk	234,2 kB	Debian package
 libpng_1.6.28-1_arm.opk	90,6 kB	Debian package
 libstdc++_6.0.22-1_arm.opk	395,4 kB	Debian package
 libusb_1.0.20-1_arm.opk	39,8 kB	Debian package
 lighttpd_1.4.49-1_arm.opk	292,4 kB	Debian package

A lot of Debian package

+

Loytec package

Linux Kernel 3.18.45

CVE-2019-xxxx

CVE-2018-xxxx

dropbear_2018.76-1

CVE-2018-15599

proftpd_1.3.5d-1

CVE-2017-7418

sudo_1.8.19p2-1

CVE-2017-1000368

CVE-2017-1000367



```

; /firmware $ file linx_at91_primary.exe
linx_at91_primary.exe: ELF 32-bit LSB executable, ARM, EABI5 version 1 (SYSV),
dynamically linked, interpreter /lib/ld-uClibc.so.0, not stripped
    
```

```

/firmware $ readelf -l linx_at91_primary.exe

Elf file type is EXEC (Executable file)
Entry point 0xe2f08
There are 7 program headers, starting at offset 52

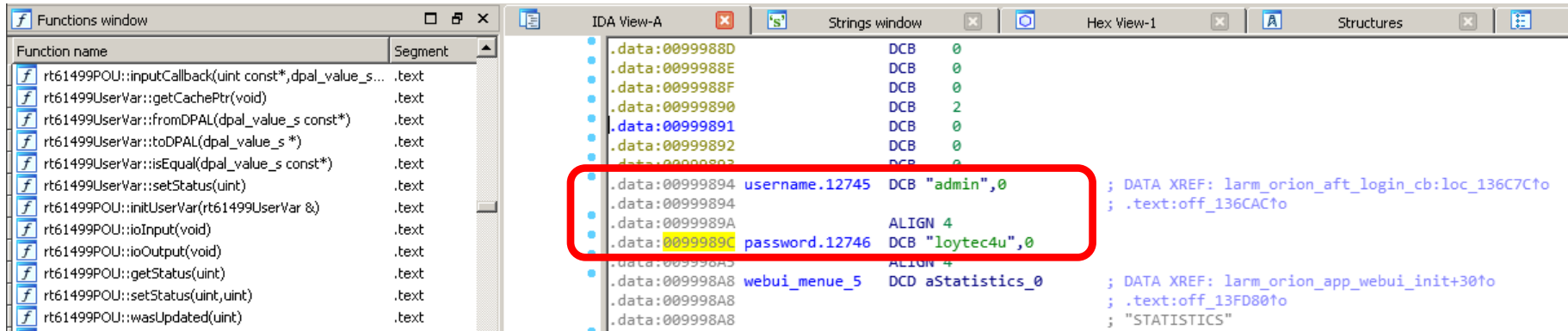
Program Headers:
Type           Offset       VirtAddr     PhysAddr     FileSiz MemSiz  Flg Align
EXIDX          0x95abb8    0x0096abb8   0x0096abb8   0x1d3d0 0x1d3d0  R   0x4
PHDR           0x000034    0x00010034   0x00010034   0x000e0 0x000e0  R E  0x4
INTERP        0x000114    0x00010114   0x00010114   0x00014 0x00014  R   0x1
      [Requesting program interpreter: /lib/ld-uClibc.so.0]
LOAD           0x000000    0x00010000   0x00010000   0x977f8c 0x977f8c  R E 0x10000
LOAD           0x978000    0x00998000   0x00998000   0x12718 0x1dfc28  RW  0x10000
DYNAMIC        0x978014    0x00998014   0x00998014   0x00170 0x00170  RW  0x4
GNU_STACK     0x000000    0x00000000   0x00000000   0x00000 0x00000  RWE 0x10

Section to Segment mapping:
Segment Sections...
00      .ARM.exidx
01
02      .interp
03      .interp .hash .dynsym .dynstr .gnu.version .gnu.version_r .rel.dyn .rel
.plt .init .plt .text .fini .rodata .ARM.exidx .ARM.exidx .eh_frame
04      .init_array .fini_array .jcr .dynamic .got .data .flashdata .bss
05      .dynamic
06
    
```

File doesn't stripped

Stack may be executable

/usr/bin/linux_at91_primary.exe



The screenshot shows the IDA Pro interface with the following windows:

- Functions window:** Lists various functions such as `rt61499POU::inputCallback`, `rt61499UserVar::getCachePtr`, `rt61499UserVar::fromDPAL`, `rt61499UserVar::toDPAL`, `rt61499UserVar::isEqual`, `rt61499UserVar::setStatus`, `rt61499POU::initUserVar`, `rt61499POU::ioInput`, `rt61499POU::ioOutput`, `rt61499POU::getStatus`, `rt61499POU::setStatus`, and `rt61499POU::wasUpdated`.
- Strings window:** Displays a list of strings with their memory addresses and attributes. A red box highlights the following entries:
 - `username.12745` DCB "admin",0 ; DATA XREF: larm_orion_aft_login_cb:loc_136C7C↑ ; .text:off_136CAC↑
 - `password.12746` DCB "loytec4u",0

Hardcoded password and user

Private key

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEogIBAAKCAQEAzcmM//qGwD0iJaJ
```

`/var/lib/opcua/certificatestore/server/private`
`/etc/lighttpd/ssl/`

The same “*Private Key*”

for different version of firmware

Perhaps the same “*Private Key*”

for different devices

```
-----END RSA PRIVATE KEY-----
```



What is it Linx 153 firmware ???

Linx 153
firmware

Some new specific package for Linx 153

Old packages from Linx 150
with older version

for example "*proftpd*"

- ***“Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment.”*** by Jesus Molina
- ***“Security for KNXnet/IP”*** by Daniel Lechner, Wolfgang Granzer, Wolfgang Kastner
- **Hacking Intelligent Buildings: Pwning KNX & ZigBee Networks**

<https://conference.hitb.org/hitbsecconf2018ams/sessions/hacking-intelligent-buildings-pwning-knx-zigbee-networks/>

Conclusion

- **DoS for any node in KNX network**
- **Opportunity to manage any device in KNX**
- **Change router configuration**
- **Update firmware for some node via knx-tp**
- **No checks are present in during update**
- **Using not secure protocols (http, ftp) to communicate with Linx 150**
- **Using old packages in Linx 150**



- **KNX Position Paper on Data Security and Privacy**

GIRA

Productdefinition

1.4 KNX Secure

The KNX IP router is prepared for KNX Secure from index status I14 in combination with Firmware 3.3 (additional firmware update required). The necessary FDSK (Factory Default Setup Key) is located as a label on the side of the KNX IP router and is also included as a Secure Card.

Important notes

- Store the Secure Card carefully.
- We recommend that you remove the label on the device for maximum security.
- Restoration is not possible if the FDSK is lost.



Gratitude

- **Dimitrii Viktorov, CTO, SENSORMATICA LLC**

<https://sensormatica.ru>



- **Kees Jongenburger**

@KankFFdoen



egor21@gmail.com

@Xarlan