Building Automation and Control – Hacking Subsidized Energy Saving System

Stephen Hilt, Philippe Lin

2015/9/18-19

TREND MICRO

Securing Your Journey to the Cloud

$ whoami

- Philippe Lin
- Staff engineer in Trend Micro
- BACnet newbie

$ whoami

- Stephen Hilt
- Senior threat researcher, Trend Micro
- 10 years ICS security exp

Disclaimer

- Do not probe / scan / modify the devices that you don't own.
- Do not change any value without permission.
- It's a matter of LIFE AND DEATH.
- Beware! Taiwanese CRIMINAL LAW.

Photo courtesy of Wikimedia, CC0.

BACnet –
Building Automation and Control networks

BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control, lighting control, access control, and fire detection systems and their associated equipment. http://en.wikipedia.org/wiki/BACnet

Building Automation?

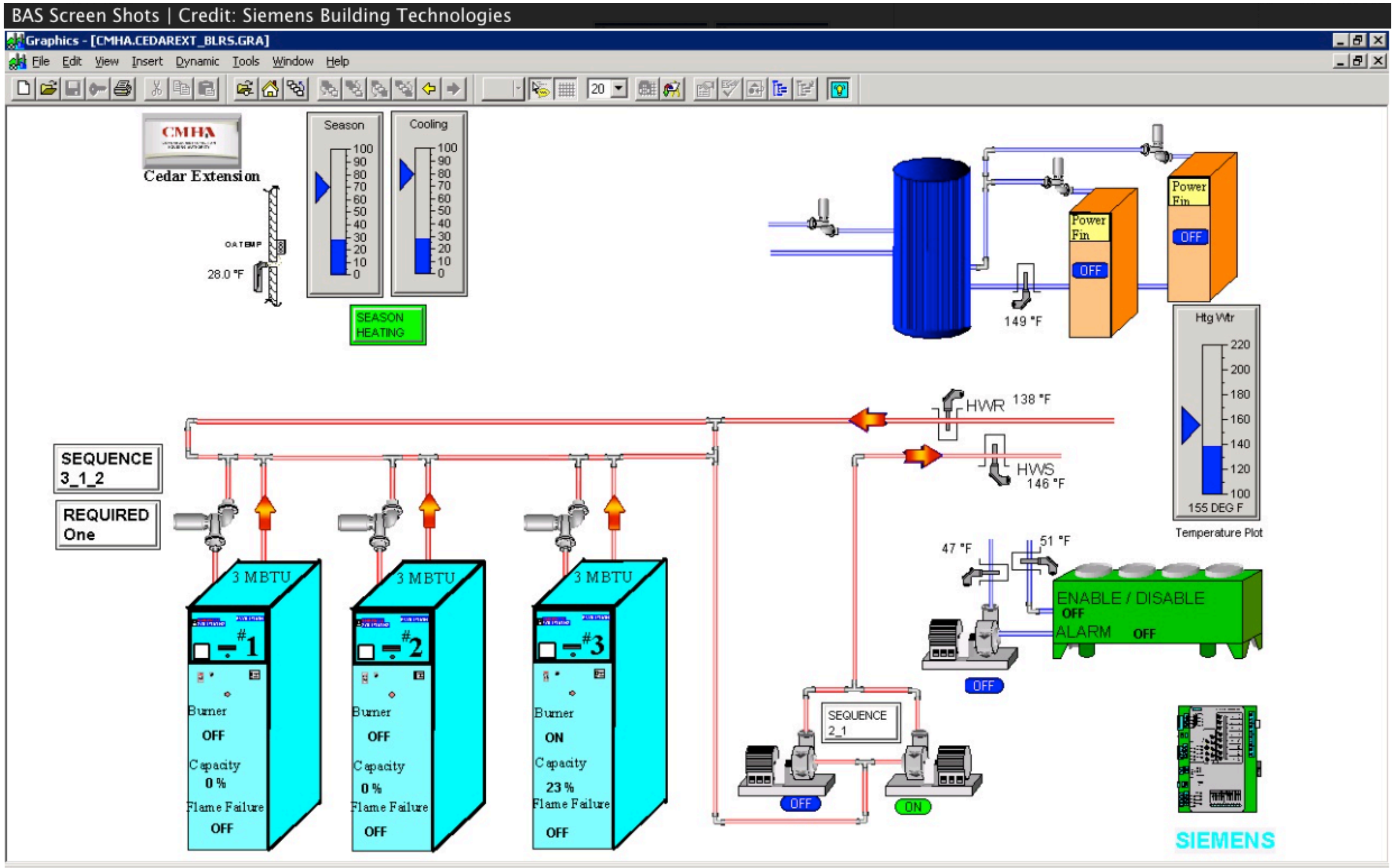


Image from
http://buildipedia.com/aec-pros/facilities-ops-maintenance/case-study-cuyahoga-metro-housing-authority-utilizes-bas
Credit: Siemens Building Technologies

Building Automation!

Photo courtesy of Chien Kuo Senior High School.

ANSI/ASHRAE 135-2001

Table 12-12. Properties of the Device Object Type

Property Identifier	Property Datatype	Conformance Code
Object_Identifier	BACnetObjectIdentifier	R
Object_Name	CharacterString	R
Object_Type	BACnetObjectType	R
System_Status	BACnetDeviceStatus	R
Vendor_Name	CharacterString	R
Vendor_Identifier	Unsigned16	R
Model_Name	CharacterString	R
Firmware_Revision	CharacterString	R
Application_Software_Version	CharacterString	R
Location	CharacterString	O
Description	CharacterString	O
Protocol_Version	Unsigned	R
Protocol_Revision	Unsigned	R
Protocol_Services_Supported	BACnetServicesSupported	R
Protocol_Object_Types_Supported	BACnetObjectTypesSupported	R
Object_List	BACnetARRAY[N]of BACnetObjectIdentifier	R
Max_APDU_Length_Accepted	Unsigned	R
Segmentation_Supported	BACnetSegmentation	R
Max_Segments_Accepted	Unsigned	O[1]
VT_Classes_Supported	List of BACnetVTClass	O[2]
Active_VT_Sessions	List of BACnetVTSession	O[2]
Local_Time	Time	O[3,4]
Local_Date	Date	O[3,4]
UTC_Offset	INTEGER	O[4]
Daylight_Savings_Status	BOOLEAN	O[4]
APDU_Segment_Timeout	Unsigned	O[1]
APDU_Timeout	Unsigned	R
Number_Of_APDU_Retries	Unsigned	R
List_Of_Session_Keys	List of BACnetSessionKey	O
Time_Synchronization_Recipients	List of BACnetRecipient	O[5]
Max_Master	Unsigned(1..127)	O[6]
Max_Info_Frames	Unsigned	O[6]
Device_Address_Binding	List of BACnetAddressBinding	R
Database_Revision	Unsigned	R
Configuration_Files	BACnetARRAY[N] of BACnetObjectIdentifier	O[7]
Last_Restore_Time	BACnetDateTime	O[7]
Backup_Failure_Timeout	Unsigned16	O[8]
Active_COV_Subscriptions	List of BACnetCOVSubscription	O[9]
Profile_Name	CharacterString	O

ICS Protocols

Modbus

dnp Distributed Network Protocol

OPC

SIEMENS

IEC

BACnet

LonWorks

- ICS – Industrial Control Systems
- SCADA – Supervisory Control and Data Acquisition
- DCS – Distributed Control Systems

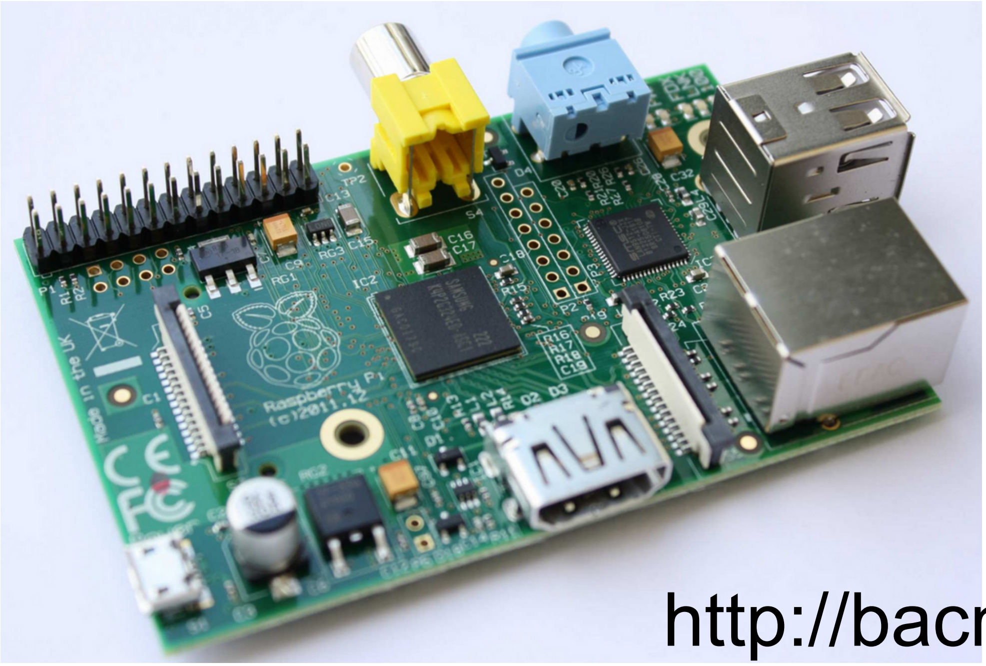
(Most) ICS Protocols

Authentication

Encryption

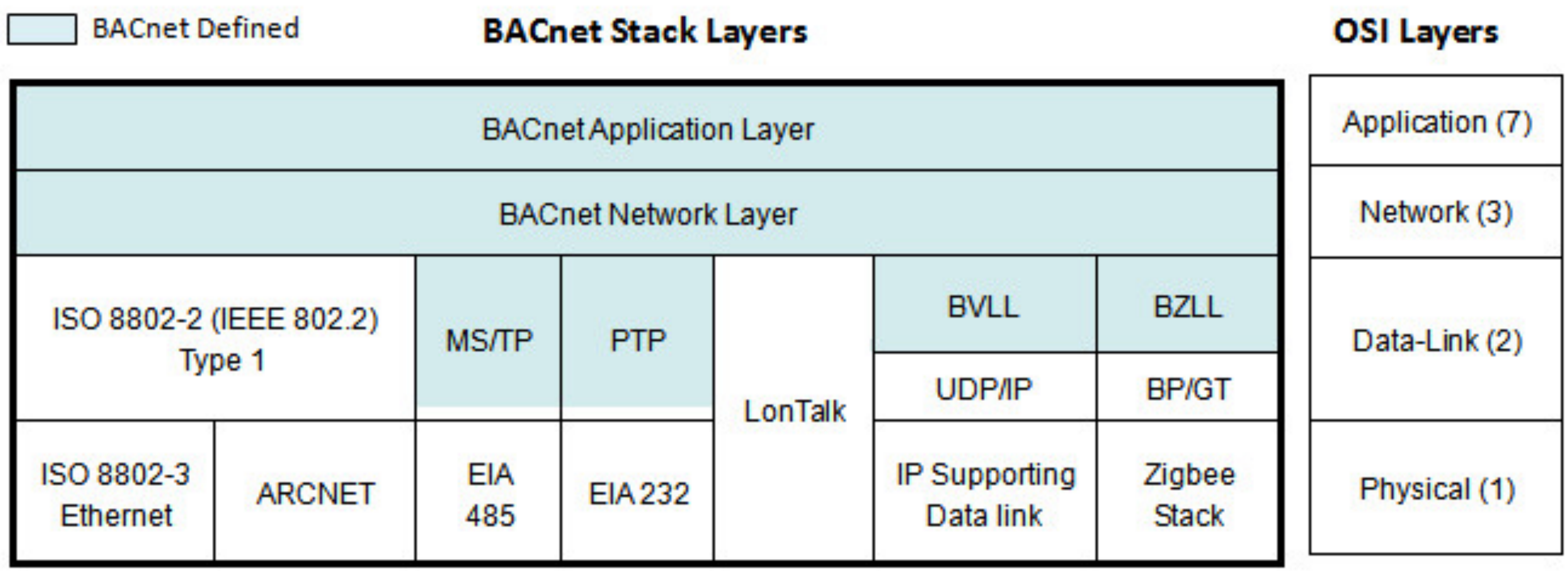
Data Integrity

Homemade BACnet



http://bacnet.sourceforge.net/

BACnet Layers map to OSI



Credit: icpdas.com

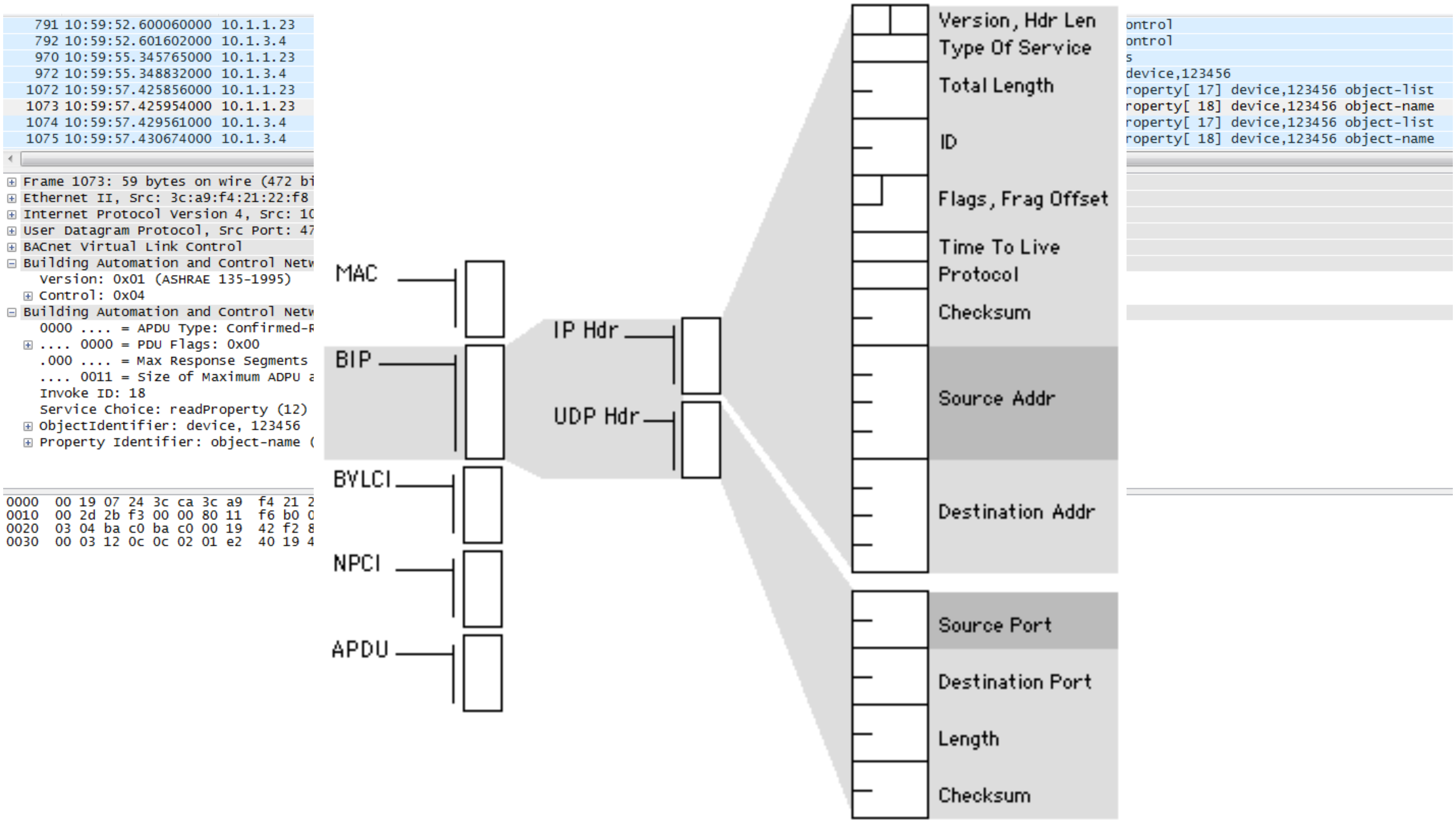
BACnet/IP

791	10:59:52.600060000	10.1.1.23	10.1.3.4	BVLC	48 BACnet Virtual Link Control
792	10:59:52.601602000	10.1.3.4	10.1.1.23	BVLC	60 BACnet Virtual Link Control
970	10:59:55.345765000	10.1.1.23	10.1.3.4	BACnet-APDU	54 Unconfirmed-REQ who-Is
972	10:59:55.348832000	10.1.3.4	10.1.1.23	BACnet-APDU	73 Unconfirmed-REQ i-Am device,123456
1072	10:59:57.425856000	10.1.1.23	10.1.3.4	BACnet-APDU	61 Confirmed-REQ readProperty[17] device,123456 object-list
1073	10:59:57.425954000	10.1.1.23	10.1.3.4	BACnet-APDU	59 Confirmed-REQ readProperty[18] device,123456 object-name
1074	10:59:57.429561000	10.1.3.4	10.1.1.23	BACnet-APDU	64 Complex-ACK readProperty[17] device,123456 object-list
1075	10:59:57.430674000	10.1.3.4	10.1.1.23	BACnet-APDU	75 Complex-ACK readProperty[18] device,123456 object-name

```
⊞ Frame 1073: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0
⊞ Ethernet II, Src: 3c:a9:f4:21:22:f8 (3c:a9:f4:21:22:f8), Dst: 00:19:07:24:3c:ca (00:19:07:24:3c:ca)
⊞ Internet Protocol Version 4, Src: 10.1.1.23 (10.1.1.23), Dst: 10.1.3.4 (10.1.3.4)
⊞ User Datagram Protocol, Src Port: 47808 (47808), Dst Port: 47808 (47808)
⊞ BACnet Virtual Link Control
⊟ Building Automation and Control Network NPDU
    Version: 0x01 (ASHRAE 135-1995)
  ⊞ Control: 0x04
⊟ Building Automation and Control Network APDU
    0000 .... = APDU Type: Confirmed-REQ (0)
  ⊞ .... 0000 = PDU Flags: 0x00
    .000 .... = Max Response Segments accepted: Unspecified (0)
    .... 0011 = Size of Maximum ADPU accepted: Up to 480 octets (fits in an ARCNET frame) (3)
    Invoke ID: 18
    Service Choice: readProperty (12)
  ⊞ ObjectIdentifier: device, 123456
  ⊞ Property Identifier: object-name (77)
```

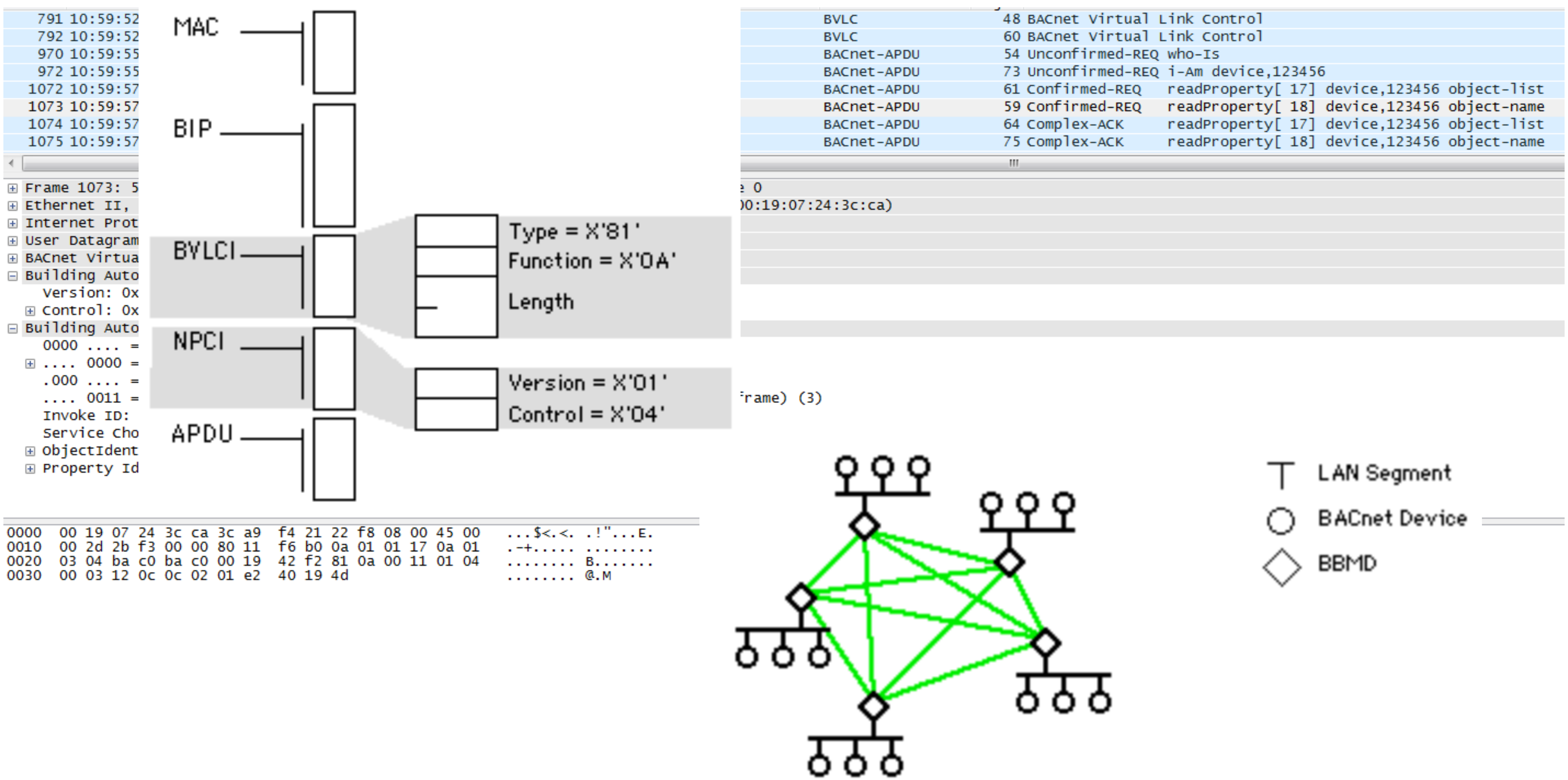
```
0000  00 19 07 24 3c ca 3c a9  f4 21 22 f8 08 00 45 00   ...$<.<. .!"...E.
0010  00 2d 2b f3 00 00 80 11  f6 b0 0a 01 01 17 0a 01   .-+..... ........
0020  03 04 ba c0 ba c0 00 19  42 f2 81 0a 00 11 01 04   ........ B.......
0030  00 03 12 0c 0c 02 01 e2  40 19 4d                  ........ @.M
```

BACnet/IP = UDP + BVLL + NPDU + APDU + …



Charts courtesy of http://www.bacnet.org/Tutorial/BACnetIP/default.html

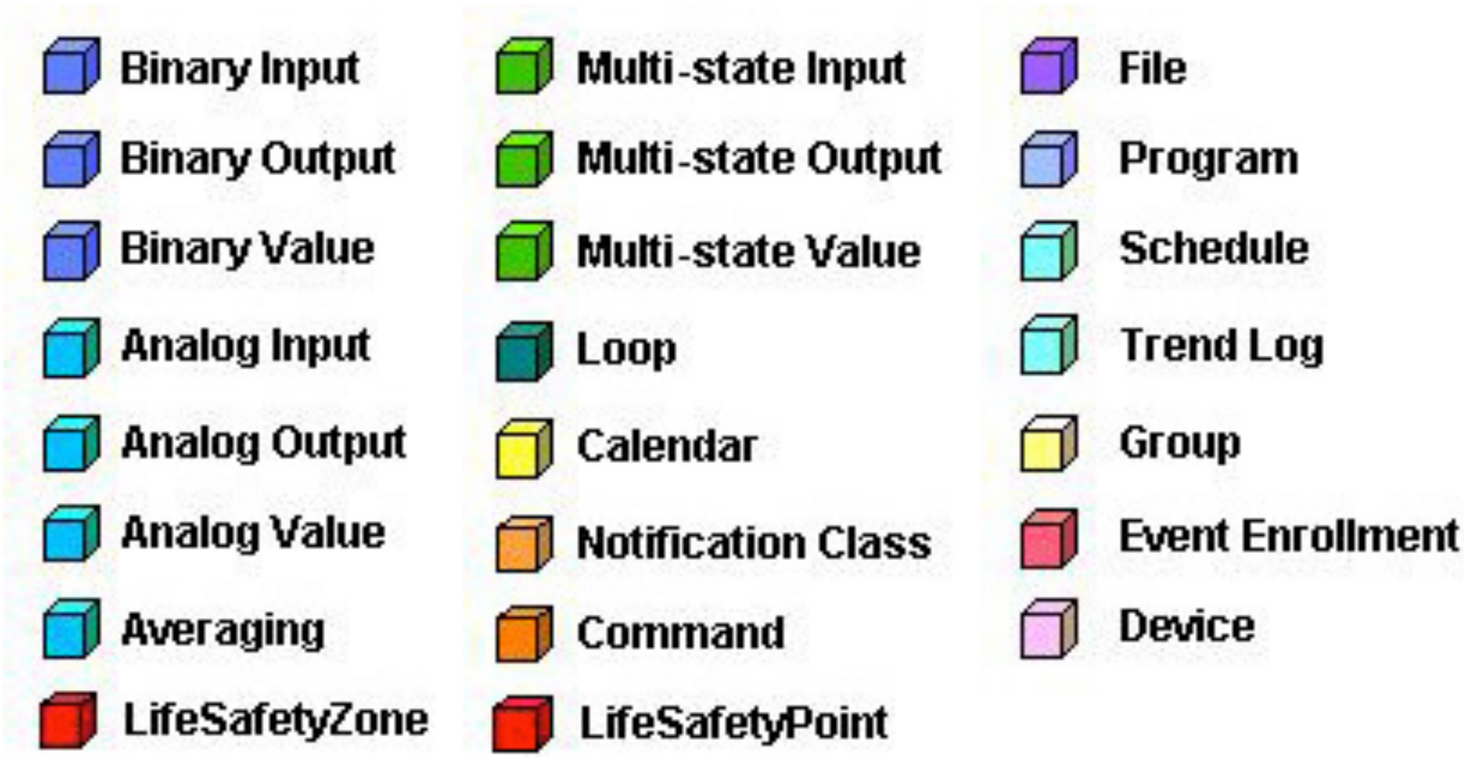
BACnet/IP = UDP + BVLL + NPDU + APDU + …



BBMD = BACnet broadcast management device

Charts courtesy of http://www.bacnet.org/Tutorial/BACnetIP/default.html

BACnet Objects



Credit: www.bacnet.org

BACnet-discover-enumerate.nse (1)

Object Name Packet Sent == 810a001101040005010c0c023FFFFF19**4d**

object-identifier	(75),
object-list	(76),
object-name	(77),
object-property-reference	(78),
object-type	(79),

→ 77 == 0x4d

Source: **ANSI/ASHRAE Standard 135-2001**

Source code:
https://github.com/digitalbond/Redpoint/blob/master/BACnet-discover-enumerate.nse

BACnet-discover-enumerate.nse (2)

- Other Read Properties To Try
  - 810a001101040005010c0c023FFFFF19xx
    - Vendor ID: 120 (0x78)
    - Description: 28 (0x1c)
    - Firmware: 44 (0x2c)
    - Application Software: 12 (0x0c)
    - Model Name: 70 (0x46)
    - Location: 58 (0x3a)
    - Object Identifier: 75 (0x4b)

Source code:
https://github.com/digitalbond/Redpoint/blob/master/BACnet-discover-enumerate.nse

BACnet-discover-enumerate.nse (3)

```
|   Vendor ID:
|   Object-identifier:
|   Firmware:
|   Application Software:
|   Object Name:
|   Model Name:
|   Location:
|   Broadcast Distribution Table (BDT):
|_  Foreign Device Table (FDT): Empty Table
```

Vendor ID: A registered BACnet Vendor

Object-identifier: unique identifier of the device. If the Object-Identifier is known, it is possible to send commands with BACnet client software, including those that change values, programs, schedules, and other operational information on BACnet devices.

```
# nmap --script BACnet-discover-enumerate.nse -sU  -p 47808 140.112.xx.xx
```

BACnet-discover-enumerate.nse (3)

```
|   Vendor ID:
|   Object-identifier:
|   Firmware:
|   Application Software:
|   Object Name:
|   Model Name:
|   Location:
|   Broadcast Distribution Table (BDT):
|_  Foreign Device Table (FDT): Empty Table
```

Broadcast Distribution Table (BDT) : A list of the BACnet Broadcast Management Devices (BBMD) in the BACnet network. This will identify all of the subnets that are part of the BACnet network.

Foreign Device Table (FDT): A list of foreign devices registered with the BACnet device. A foreign device is any device that is not on a subnet that is part of the BACnet network, not in the BDT. Foreign devices often are located on external networks and could be an attacker's IP address.

Map Out Connections

```
Nmap scan report for 140-127-xxx-xxx.n**k.edu.tw (140.127.xxx.xxx)
Host is up (0.00050s latency).
PORT      STATE SERVICE
47808/udp open  BACNet -- Building Automation and Control Networks
| bacnet-info:
|   Vendor ID: Siemens Schweiz AG (Formerly: Landis & Staefa Division Europe) (7)
|   Vendor Name: Siemens Building Technologies Inc.
|   Object-identifier: 0
|   Firmware: 3.7
|   Application Software: INT0370
|   Object Name: 25OC0001874
|   Model Name: Insight
|   Description: BACnet Device
|   Location: PC
|   Broadcast Distribution Table (BDT):
|     140.127.xxx.xxx:47808
|     140.127.xxx.xxx:47808
|     172.18.9.254:47808
|_  Foreign Device Table (FDT): Non-Acknowledgement (NAK)
```

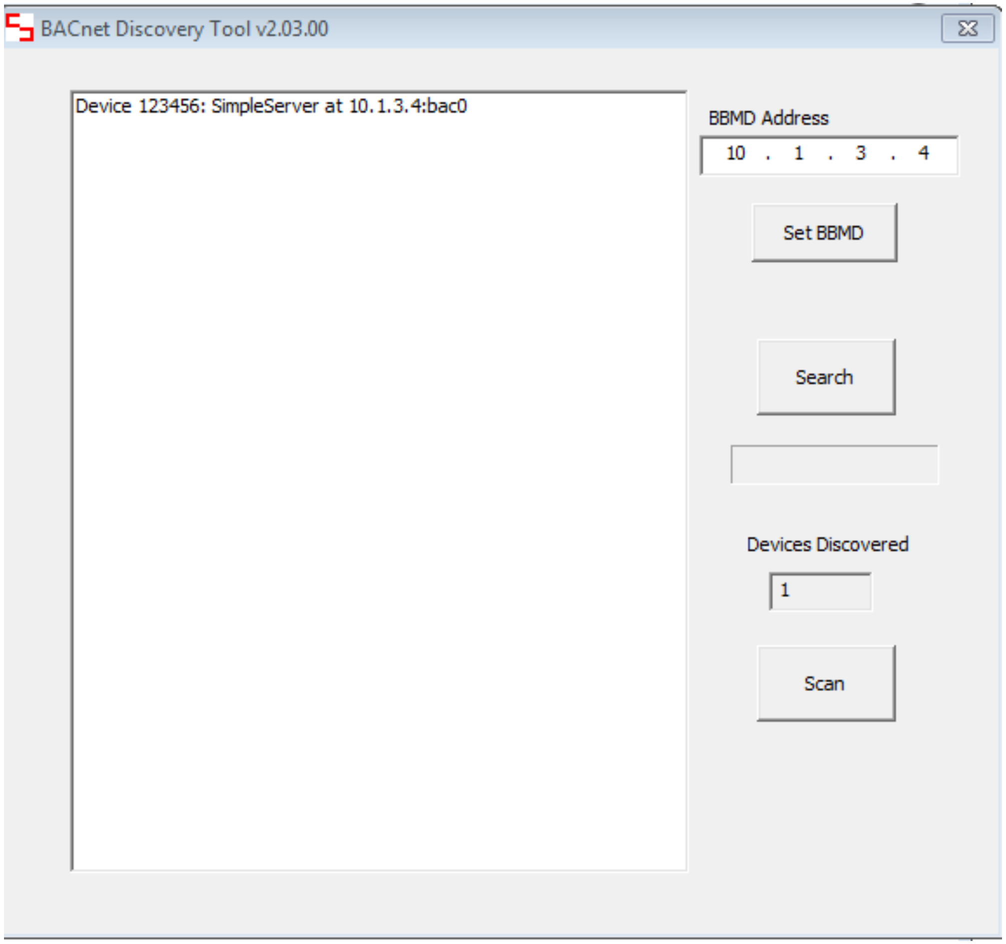
FDT → NAK!

```
Nmap scan report for 140-127-xxx-xxx.n**k.edu.tw (140.127.xxx.xxx)
Host is up (0.00050s latency).
PORT      STATE SERVICE
47808/udp open  BACNet -- Building Automation and Control Networks
| bacnet-info:
|   Vendor ID: Siemens Schweiz AG (Formerly: Landis & Staefa Division Europe) (7)
|   Vendor Name: Siemens Building Technologies Inc.
|   Object-identifier: 0
|   Firmware: 3.7
|   Application Software: INT0370
|   Object Name: 25OC0001874
|   Model Name: Insight
|   Description: BACnet Device
|   Location: PC
|   Broadcast Distribution Table (BDT):
|     140.127.xxx.xxx:47808
|     140.127.xxx.xxx:47808
|     172.18.9.254:47808
|_  Foreign Device Table (FDT): Non-Acknowledgement (NAK)
```

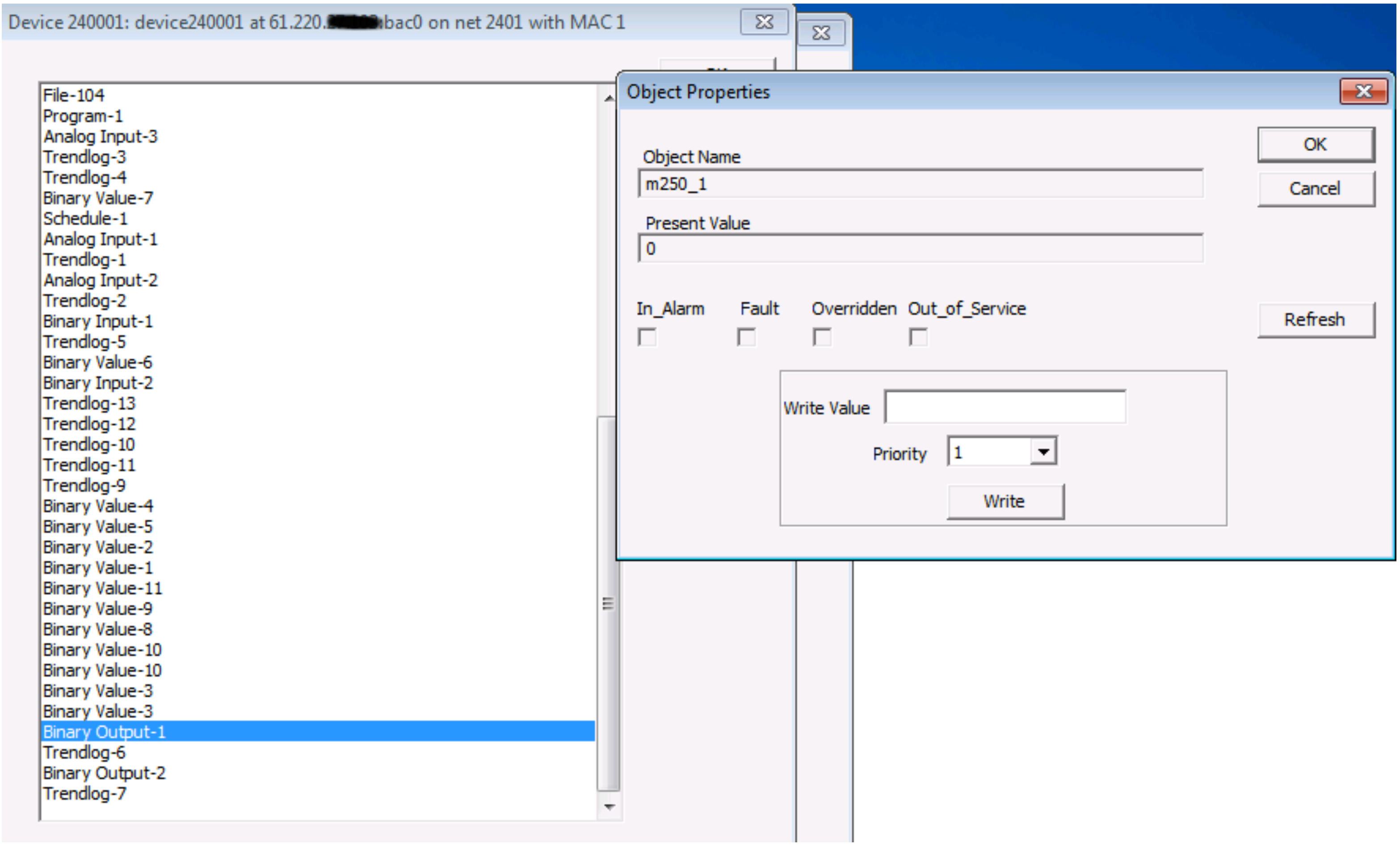
Let’s Gather MORE Information

- Systems Require you to Join the Network as a Foreign Device to Enumerate Devices that are attached, as well as points
  - Once Registered in FDT, perform a Who-is message
  - Parse I-Am responses
  - …
  - Profit?

BACnet Discovery Tool (BDT)

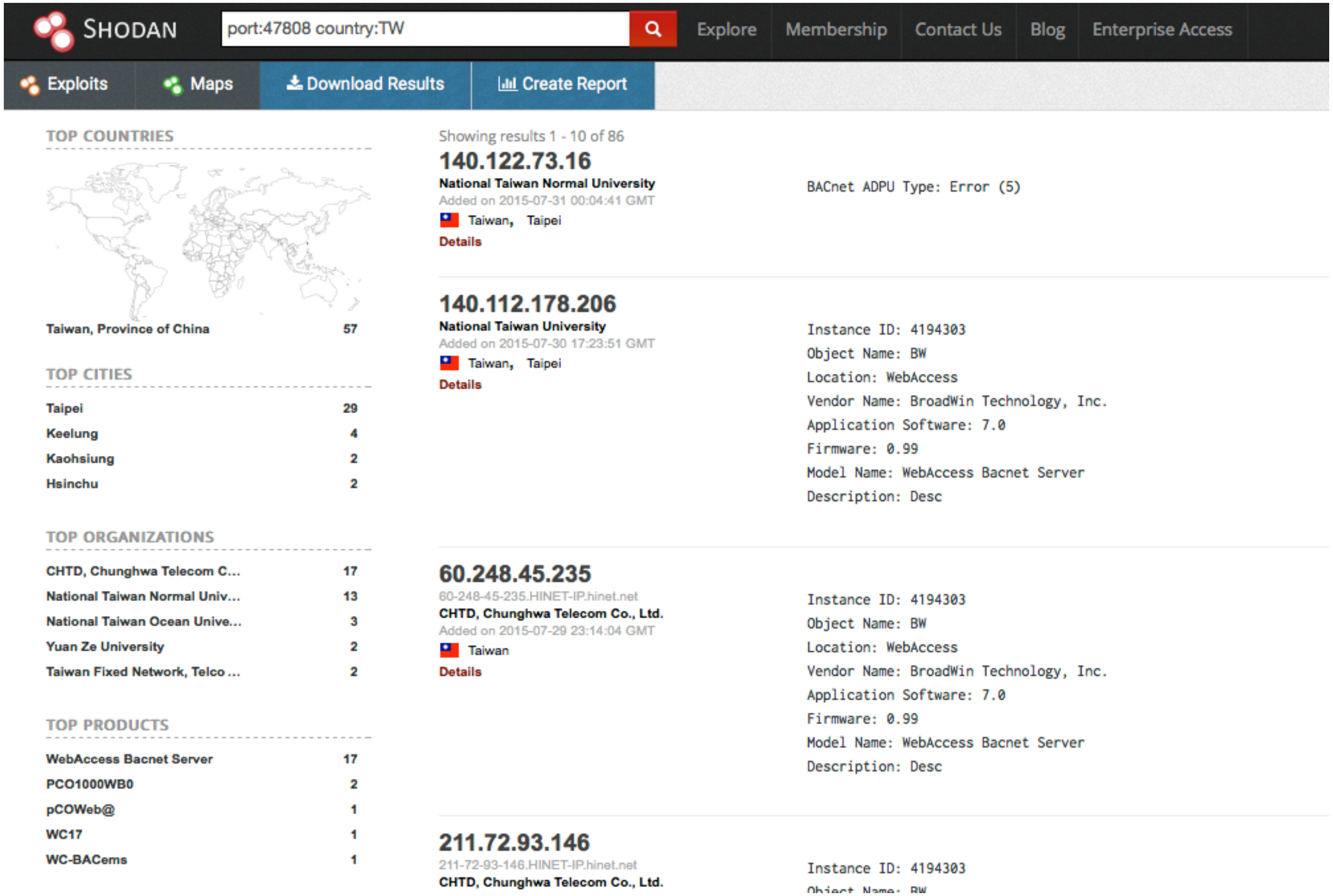


View Connected Inputs



Another day.
Today we look for BACnet devices.

Shodan + BACnet Discovery Tool



BACnet port = 0xBAC0 = port 47808

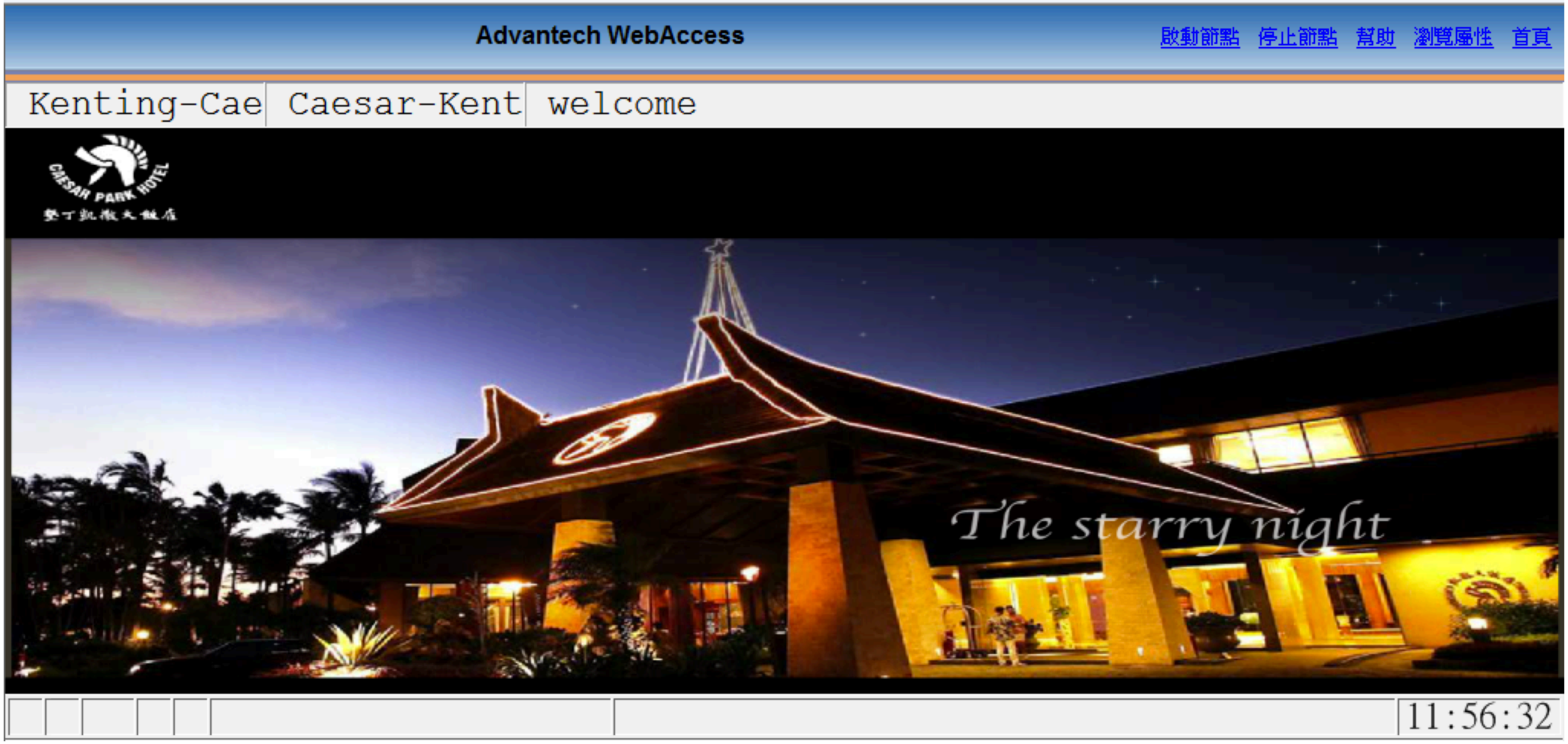
Country: TW

- As of July 29, 2015
- 48 BACnet devices
  - 14 Advantech / BroadWin WebAccess Bacnet Server 7.0
  - 4 Automated Logic LGR
  - 3 Carel S.p.A. pCOWeb
  - 2 TAC MNB-1000
  - 1 Siemens Insight
- 59 Ethernet/IP
- 23 Moxa Nport Ethernet-RS485 in N**U

14 Advantech/BroadWin WebAccess

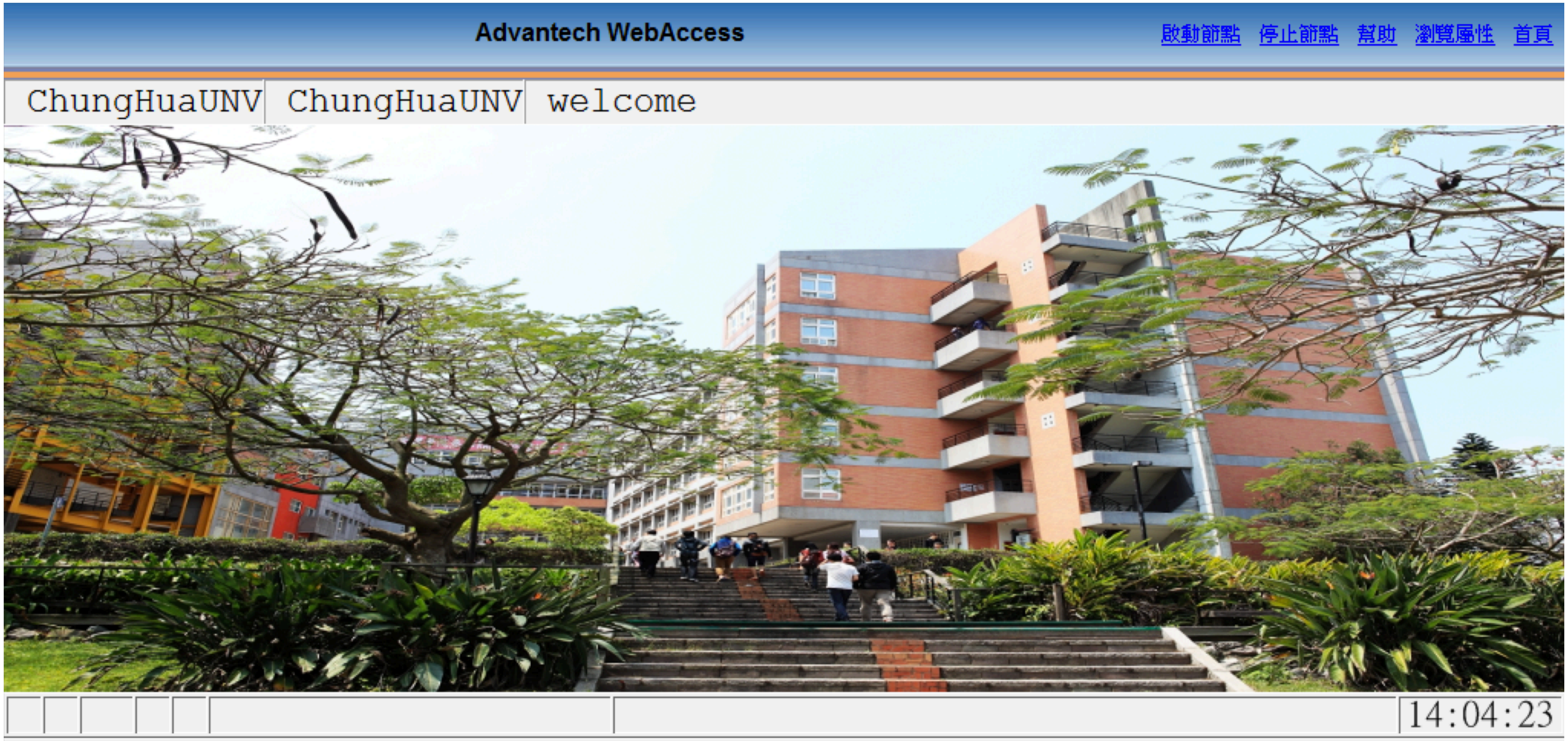
- CVE-2011-4522 XSS in bwerrdn.asp
- CVE-2011-4523 XSS in bwview.asp
- CVE-2011-4524 Long string REC
- CVE-2011-4526 ActiveX buffer overflow
- CVE-2012-0233 XSS of malformed URL
- CVE-2012-0234 SQL injection
- CVE-2012-0236 CSRF (Cross-site report forgery)
- CVE-2012-0237 Unauthorized modification
- CVE-2012-0238 opcImg.asp stack overflow REC
- **CVE-2012-0239 Authentication vulnerability (still in 7.0)**
- CVE-2012-0240 Authentication vulnerability in GbScriptAddUp.asp
- CVE-2012-0241 Arbitrary memory corruption
- CVE-2012-0242 Format string exploit
- CVE-2012-0243 ActiveX buffer overflow in bwocxrun.ocx
- CVE-2012-0244 SQL injection

11 Protected by Password



Kenting Caesar Park Hotel 墾丁凱撒大飯店

11 Protected by Password



Chung Hua University 中華大學

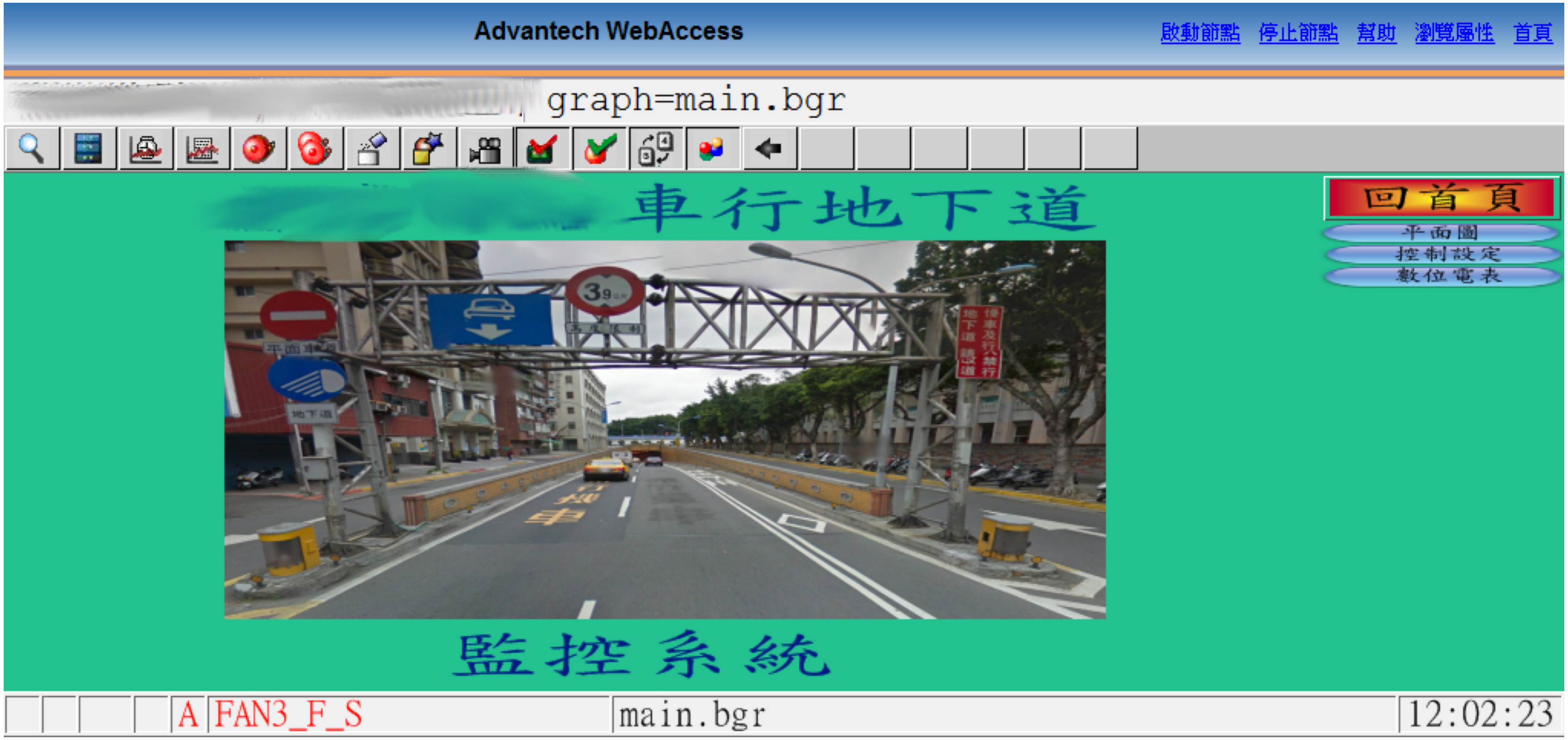
11 Protected by Password

Dorm, Chung Yuan Christian University 中原大學宿舍

11 Protected by Password

Hydean Biotechnology Co., Ltd. 瀚頂生物科技

3 No or Default Password

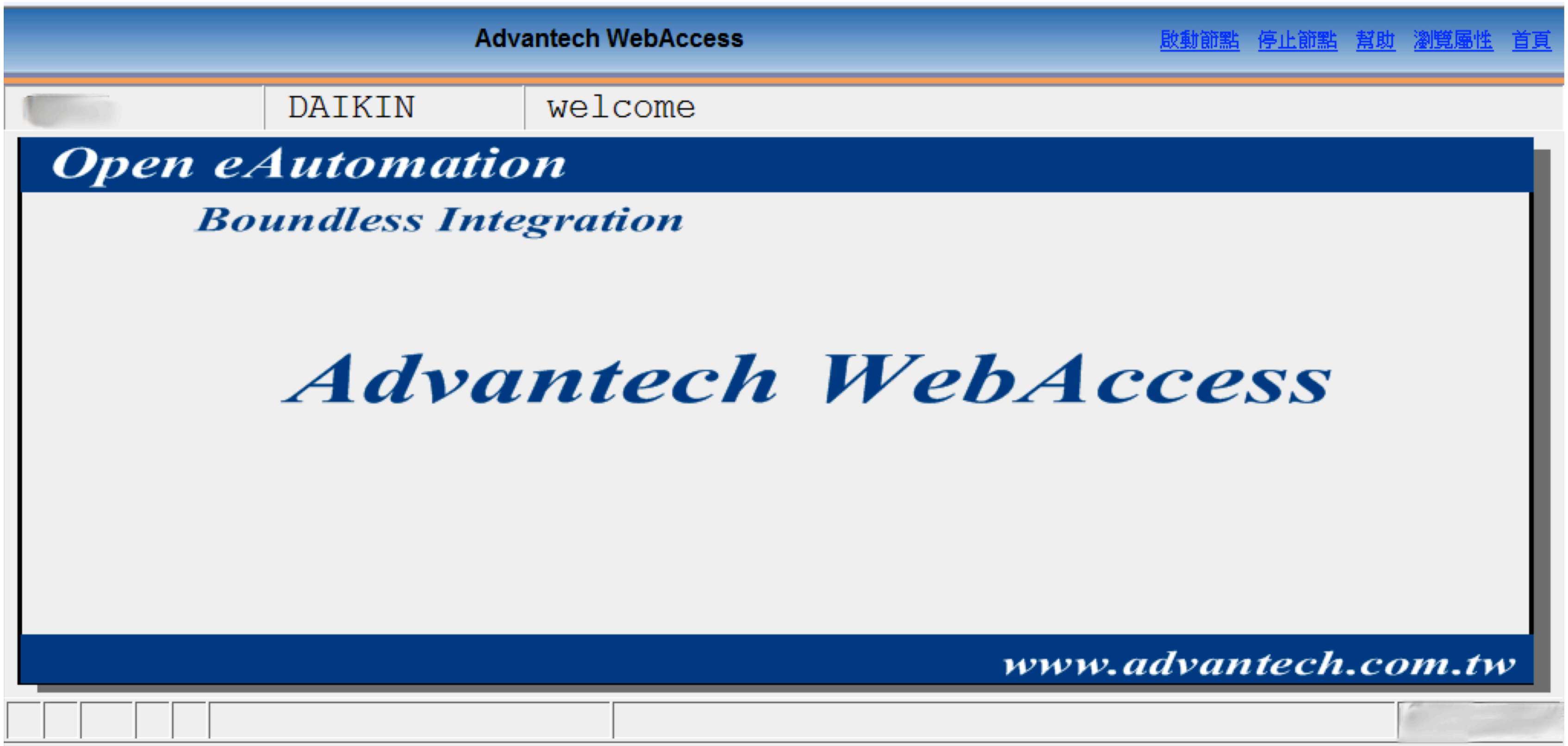


Underground Driveway, ** Road ***車行地下道

Unprotected HMI

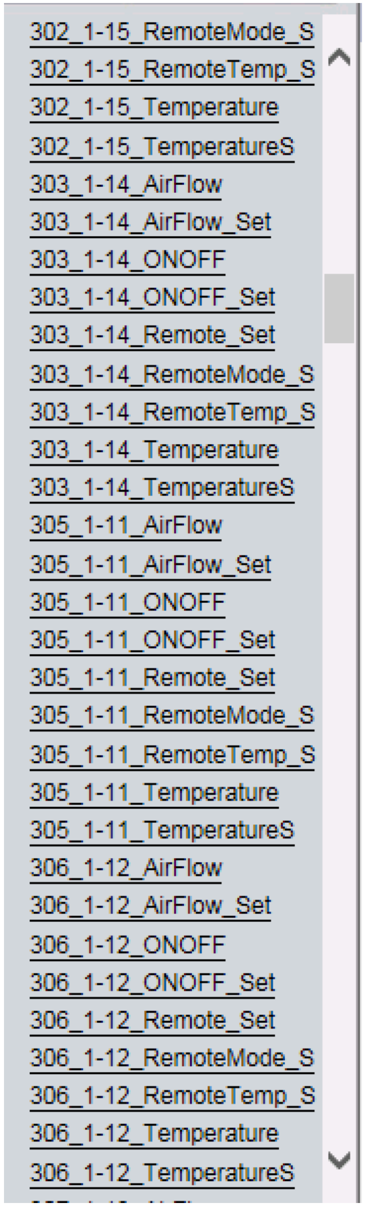
Unprotected HMI

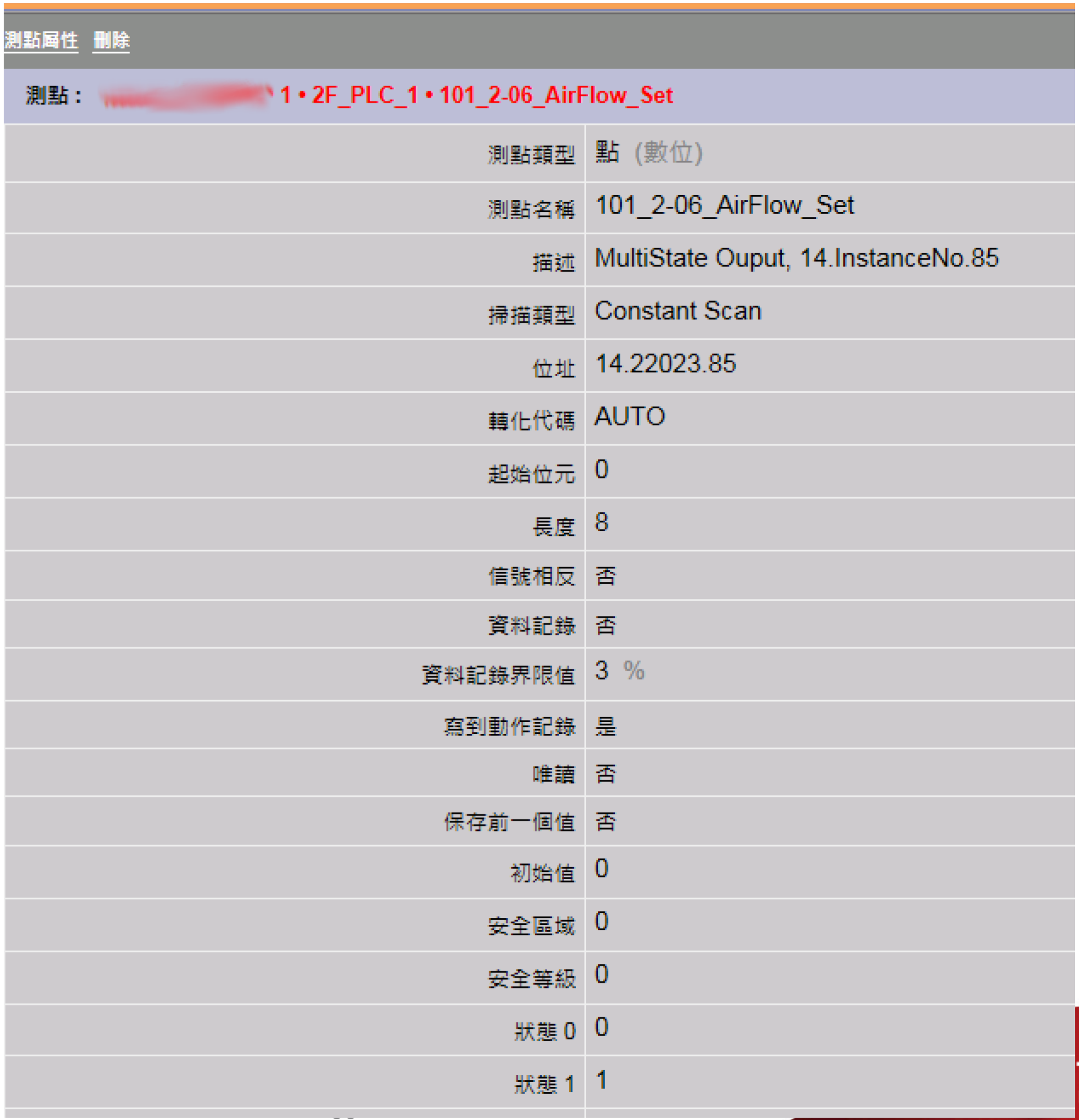
Unprotected HMI



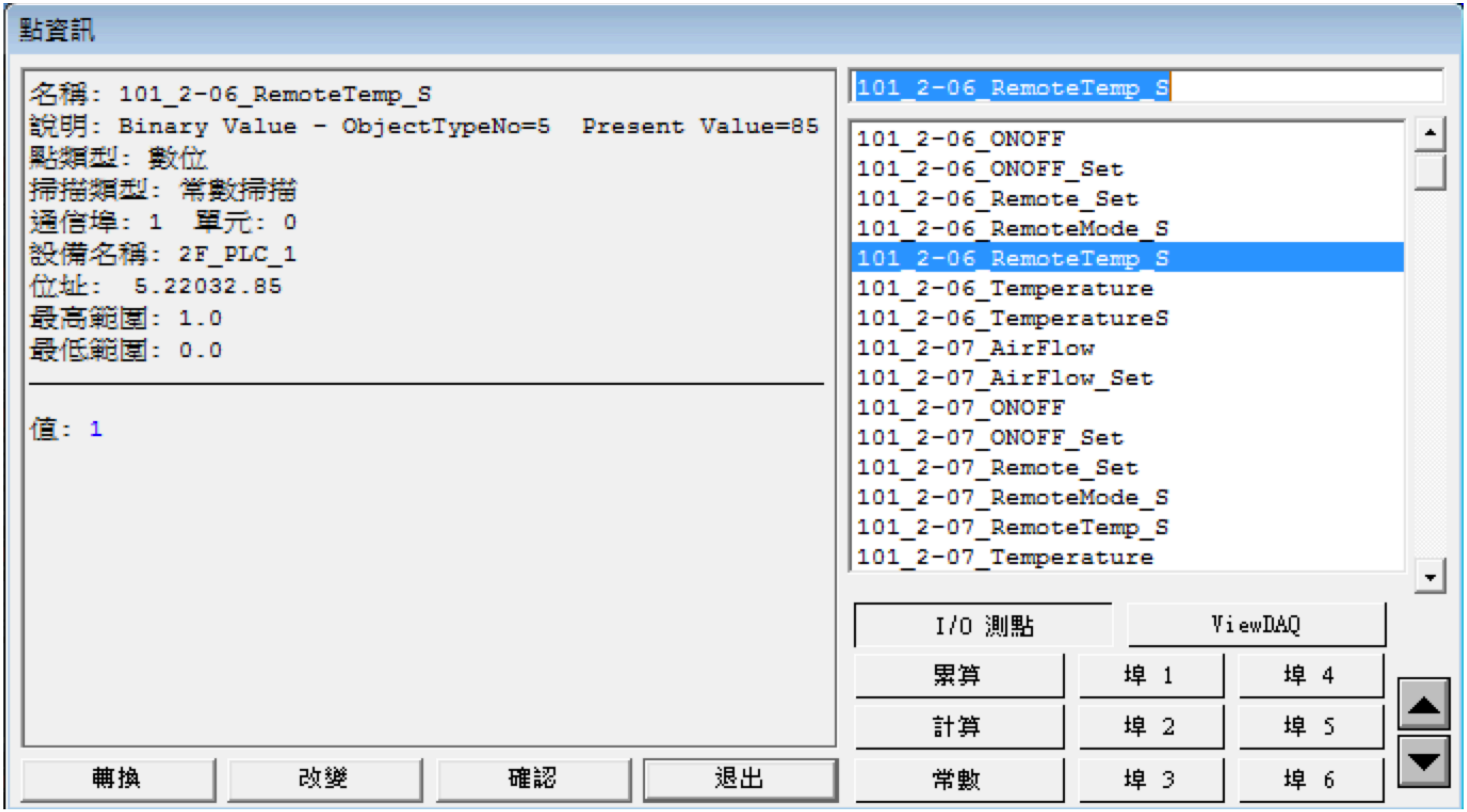
Project Management

Analog Input Parameters





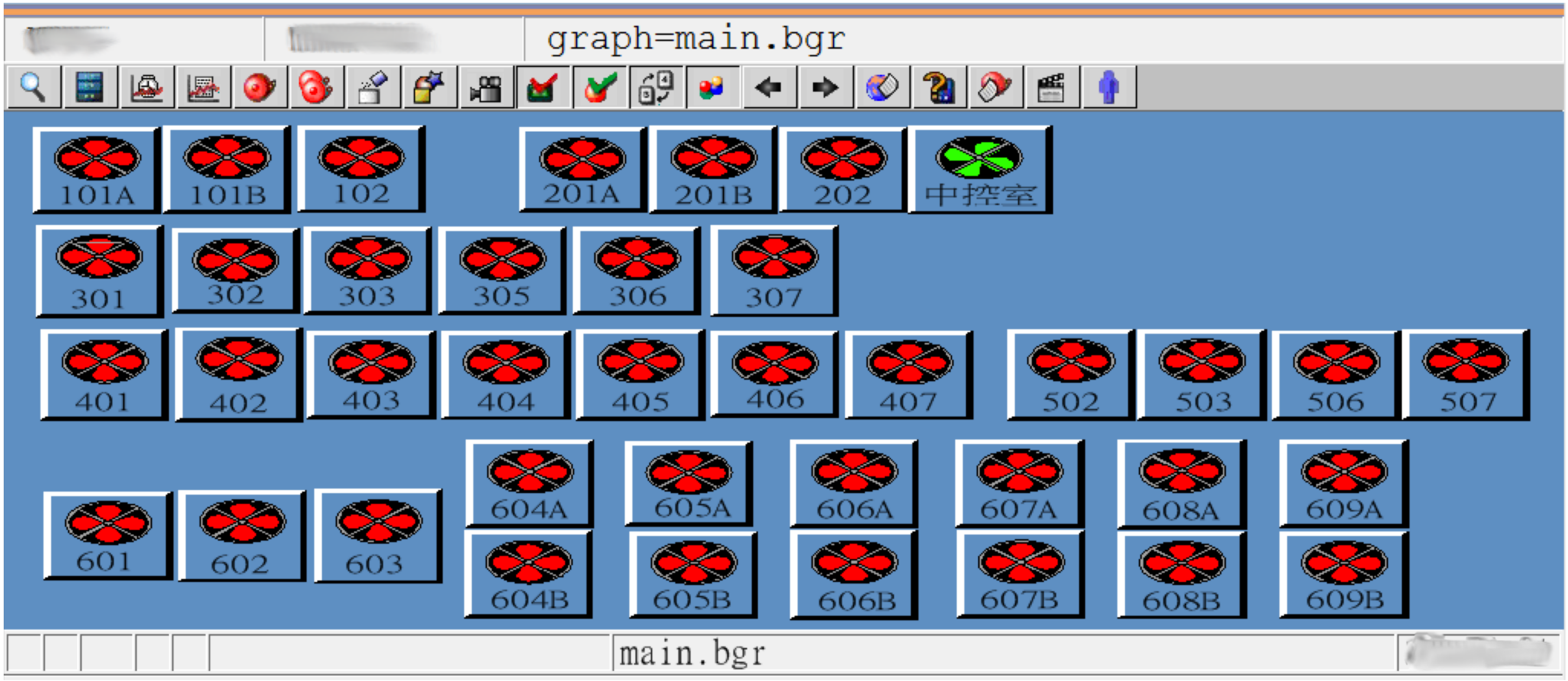
PLC Binary Value



Parameter Update

更新測點 [取消] 提供	
測點類型	點 (數位)
警報	沒有警報
測點名稱	101_2-06_AirFlow_Set
描述	MultiState Ouput, 14.InstanceNo.85
掃描類型	Constant Scan
位址	14.22023.85
轉化代碼	AUTO
起始位元	0
長度	8
信號相反	○是 ◉否
資料記錄	○是 ◉否
資料記錄界限值	3 %
寫到動作記錄	◉是 ○否
唯讀	○是 ◉否
保存前一個值	○是 ◉否
初始值	0
安全區域	0
安全等級	0
狀態 0	0
狀態 1	1
狀態 2	2
狀態 3	3
狀態 4	NotUsed

Main Graph

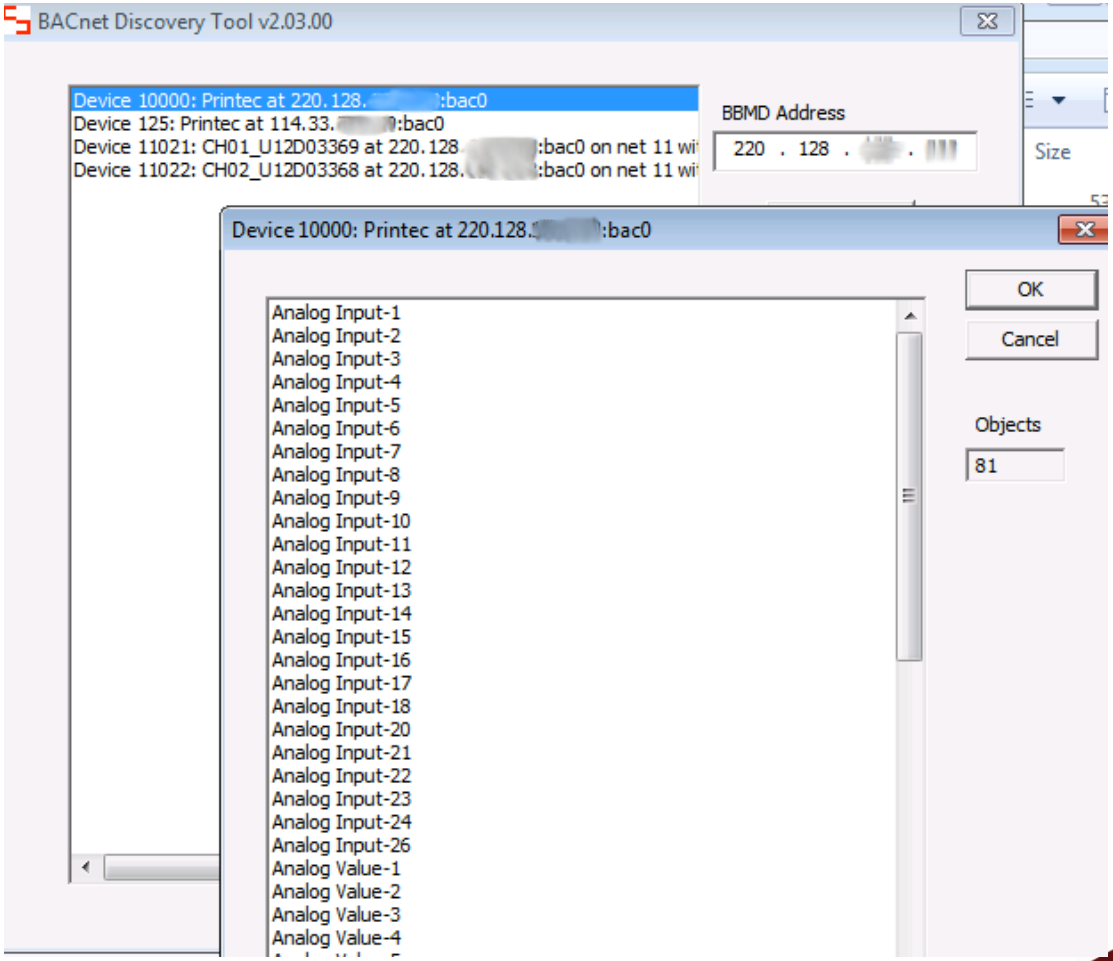


graph=main.bgr
101A
101B
102
201A
201B
202
中控室
301
302
303
305
306
307
401
402
403
404
405
406
407
502
503
506
507
601
602
603
604A
604B
605A
605B
606A
606B
607A
607B
608A
608B
609A
609B
main.bgr

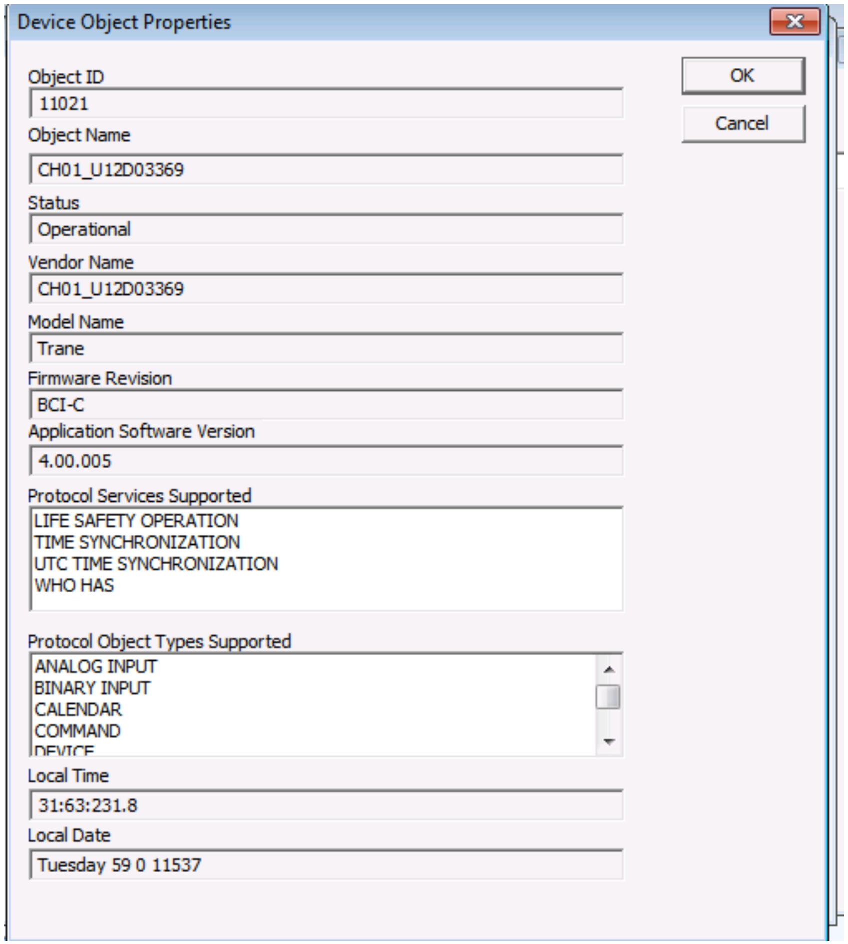
Turn Off the Aircon and Go Home?

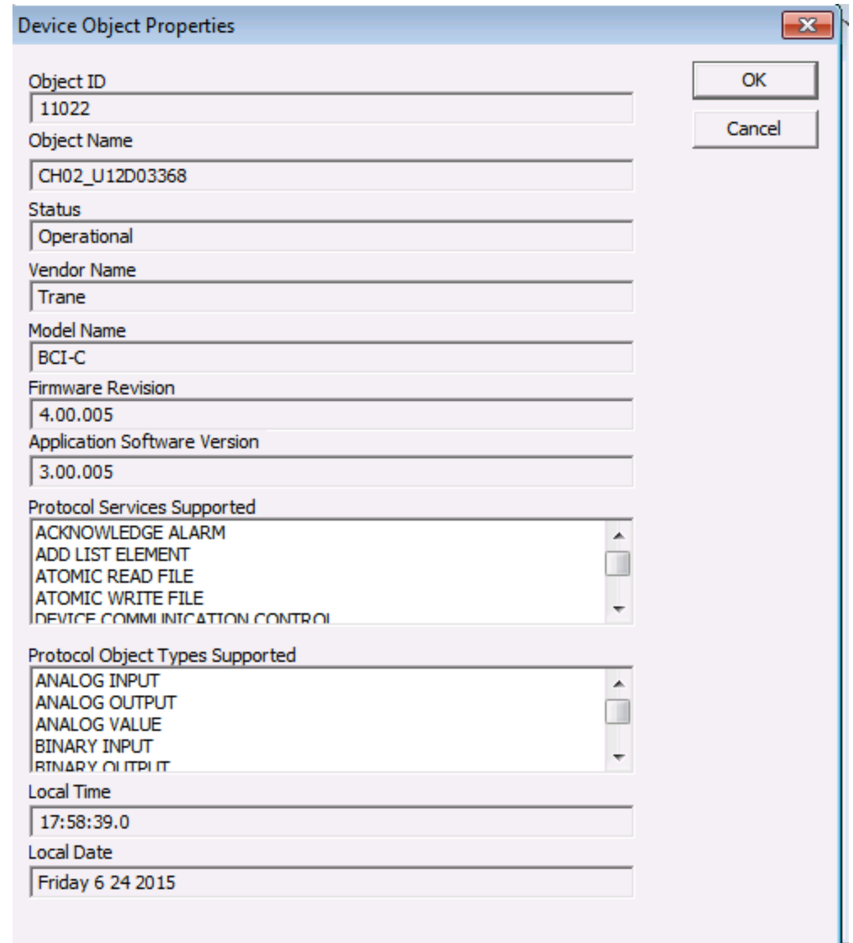
Life Is Harder without HMI, But ...

- Trane 2.6.30_HwVer12AB-hydra
- P******* Co., New Taipei City



Device 11021 / 11022





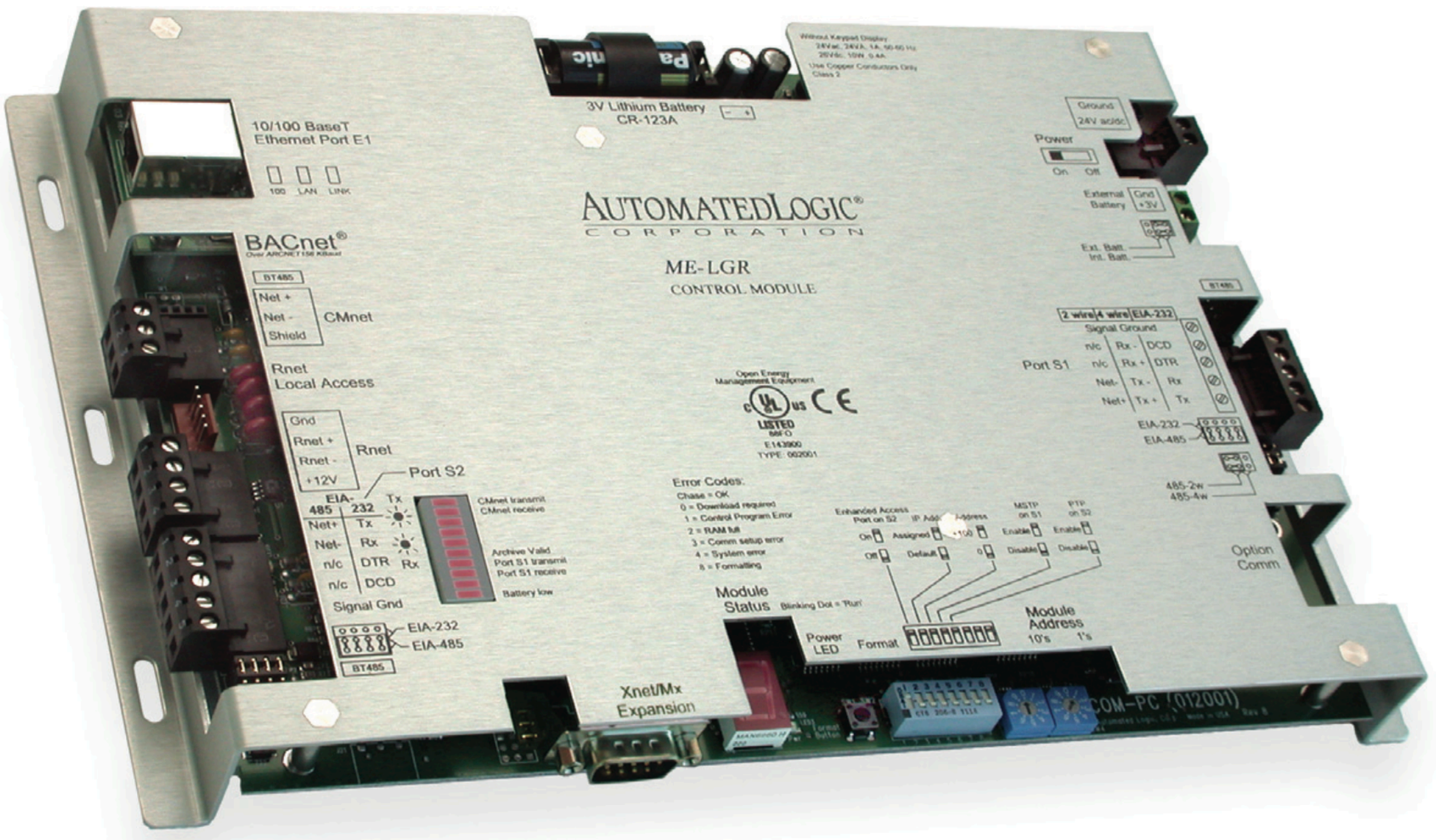
Analog Inputs

```
Analog Input-1 Facility Outdoor Air Temperature 0.000000
Analog Input-2 Facility Outdoor Air Humidity 0.000000
Analog Input-3 Condenser Approach Temperature Circuit 1|chlr-1 0.000000
Analog Input-4 Evaporator Approach Temperature Circuit 1|chlr-1 0.000000
Analog Input-5 Condenser Approach Temperature Circuit 1|chlr-2 6.319977
Analog Input-6 Evaporator Approach Temperature Circuit 1|chlr-2 1.299988
Analog Input-7 Ch01_Condenser Pressure 1057.900024
Analog Input-8 Ch02_Condenser Pressure 1029.300171
Analog Input-9 CH02_Cooling Entering Water Temperature 30.480011
Analog Input-10 CH01_Cooling Entering Water Temperature 30.610016
Analog Input-11 CH01_Discharge Temperature 53.519989
Analog Input-12 CH02_Discharge Temperature 0.000000
Analog Input-13 CH01_Current  Above 102% fro 1M 83.300003
Analog Input-14 CH02_Current  Above 102% fro 1M 75.199997
Analog Input-15 CH01_Voltage for 30seconds 373.000000
Analog Input-16 CH02_Voltage for 30second 376.000000
Analog Input-17 CH01_Eavp Refrig Pressure (Cooling Only) 371.200012
Analog Input-18 CH02_Low Eavp Refrig Pressure (Cooling Only) 361.299988
Analog Input-20 CH01_Condenser Leaving Water Temperaturee 34.339996
Analog Input-21 CH02_Condenser Leaving Water Temperaturee 33.899994
Analog Input-22 CH01_Condenser_Sat Refrig Temperature 40.389984
Analog Input-23 CH02_Condenser_Sat Refrig Temperature 39.989990
Analog Input-24 Ch01_Oil pressure_Compressor 983.400085
Analog Input-26 Ch02_Oil pressure_compressore 962.400085
Analog Value-1 CH01_Condenser Approach Temp 6.280029
Analog Value-2 CH02_Condenser Approach Temp 6.100006
Analog Value-3 CH01_Low Oil Flow 0.066524
Analog Value-4 CH02_Low Oil Flow 0.085340
Analog Value-5 Ch01_High Refrigerant Pressure Rate  2.780065
Analog Value-6 Ch02_High Refrigerant Pressure Rate  2.816593
Analog Value-7 Reference at chiller off = 0 0.000000
Binary Input-1 TIS Alarm Test 0
Binary Input-2 CH01_Chilled Water Flow Switch Trip 0
Binary Input-3 CH02_Chilled Water Flow Switch Trip 0
```

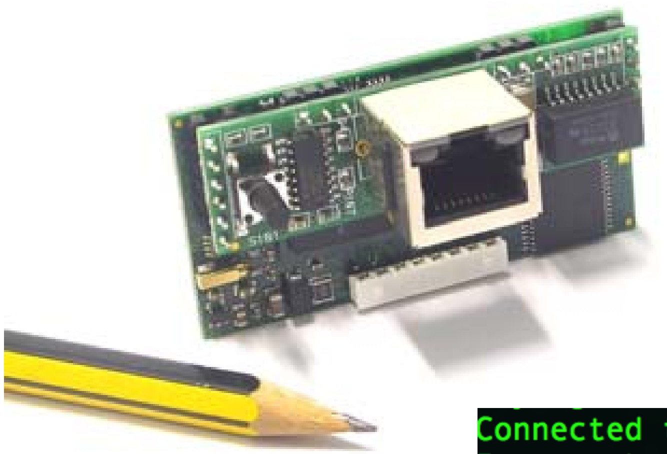
Output = Modifiable

```
Analog Input-98 Chiller Design Capacity 300.000000
Analog Output-1 Chilled Water Setpoint 44.603996
Analog Output-2 Current Limit Setpoint 100.000000
Binary Input-1 Run Enabled 1
Binary Input-2 Local Setpoint Control 1
Binary Input-3 Capacity Limited 0
Binary Input-4 Chiller Running State 1
Binary Input-5 Condenser Water Flow Status 1
Binary Input-7 Head Relief Request 0
Binary Input-9 Compressor 1A Running 1
Binary Input-17 Evaporator Water Pump Request 1
Binary Input-19 Condenser Water Pump Request 1
Binary Input-22 Evaporator Water Flow Status 1
Binary Input-23 Alarm Present 0
Binary Input-24 Shutdown Alarm Present 0
Binary Input-25 Last Diagnostic 0
Binary Output-1 Chiller Auto Stop Command 1
Binary Output-2 Remote Diagnostic Reset Command 0
Device-11021
Multi-State Input-1 Running Mode 3
Multi-State Input-2 Running Mode 1
Multi-State Input-3 MP Communication Status 1
Multi-State Input-4 Refrigerant Type 5
```

4 Automated Logic ME-LGR

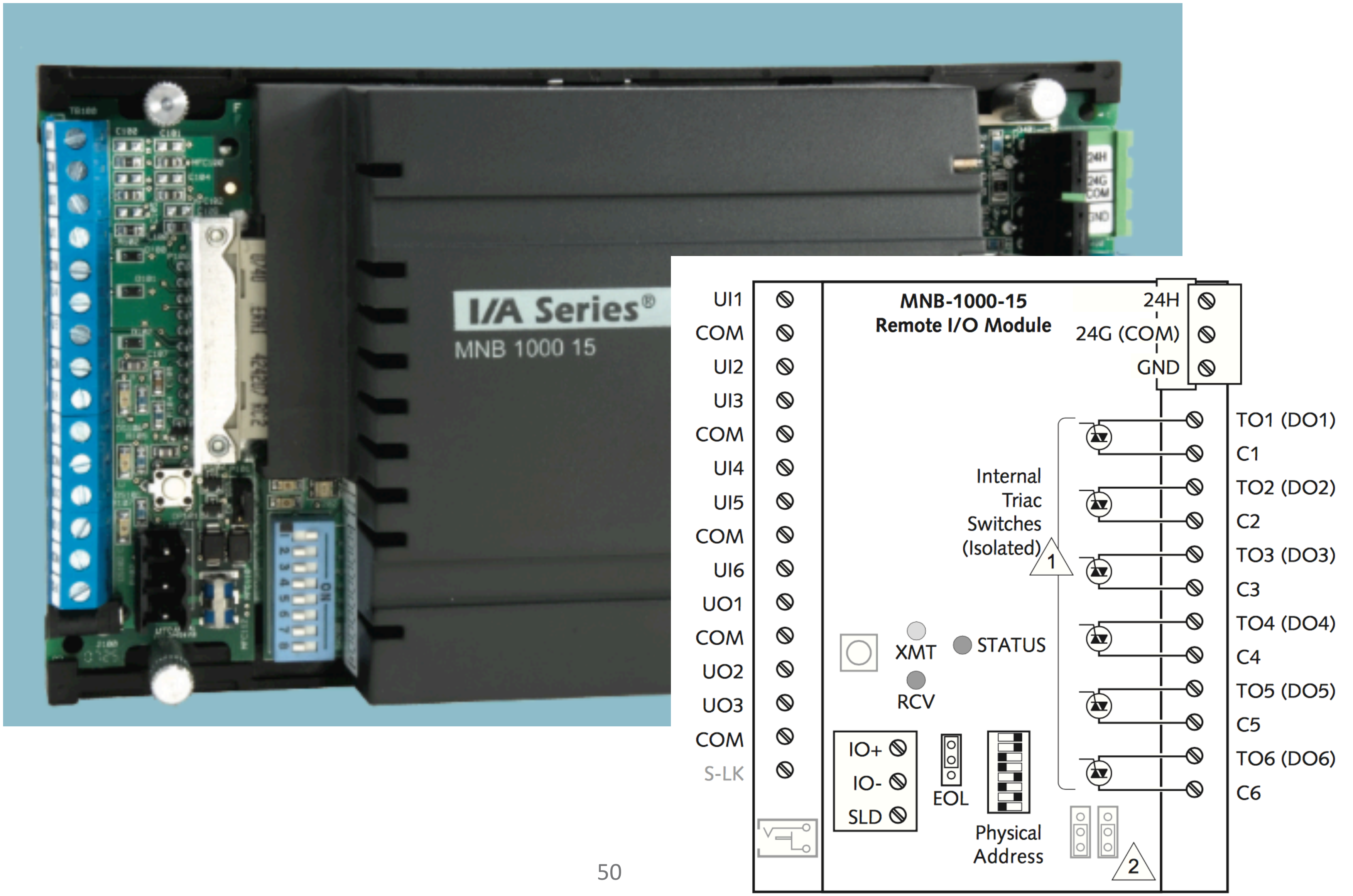


3 Carel pCOWeb



```
Connected to 203.68.
Escape character is '^]'.

Linux 2.4.21-rmk1 (pCOWeb) (ttya1)


pCOWeb login: root
Password:
Executing profile
/sbin:/bin:/usr/sbin:/usr/bin
[root@pCOWeb14:34:47 root]# ls /usr/local/root/
admin  apps_release  cbgtagfilt  config  defadmin  defindex.html
[root@pCOWeb14:34:57 root]#
```

2 TAC-MNB

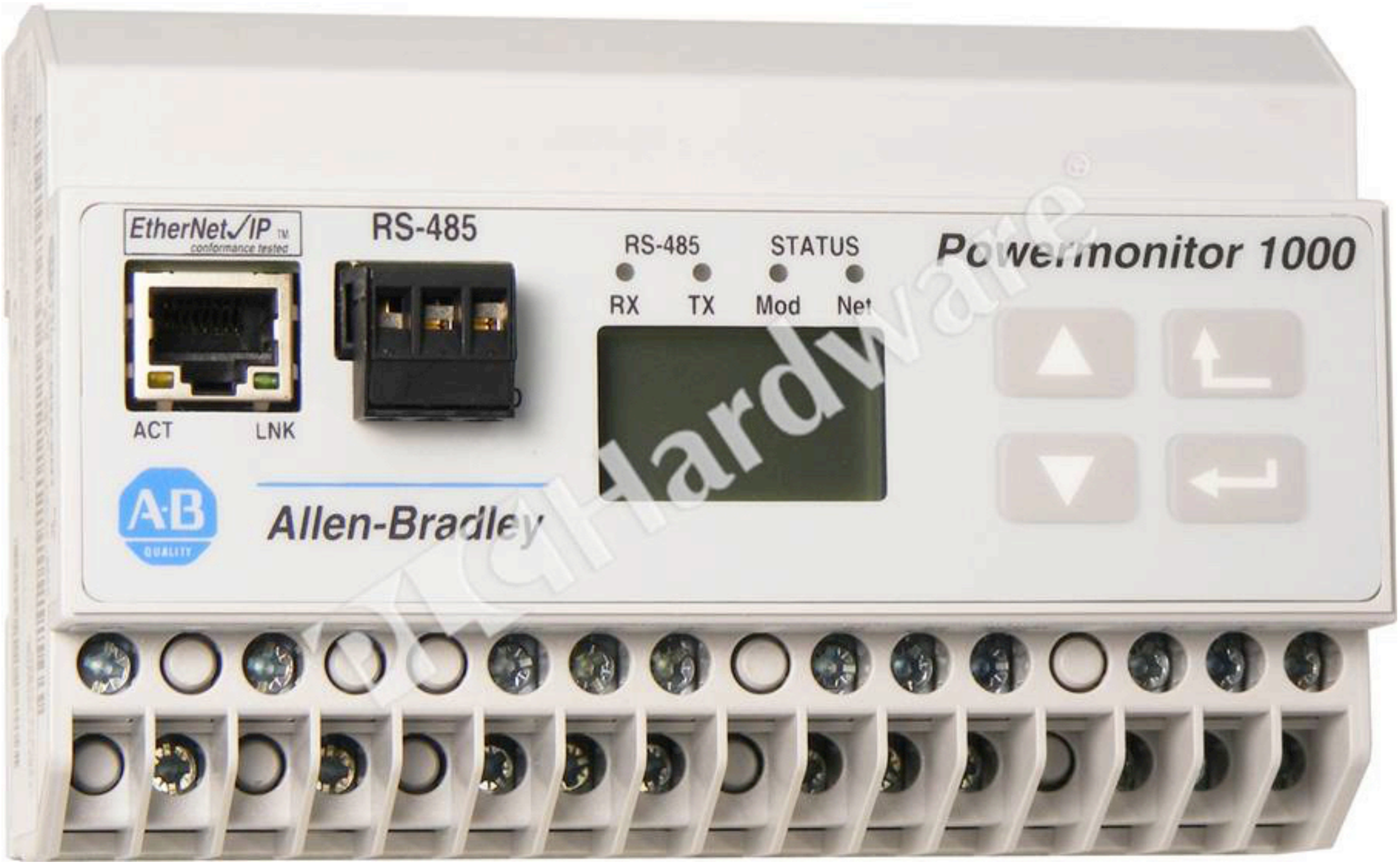

I/A Series®
MNB 1000 15
MNB-1000-15
Remote I/O Module
UI1
COM
UI2
UI3
COM
UI4
UI5
COM
UI6
UO1
COM
UO2
UO3
COM
S-LK
24H
24G (COM)
GND
TO1 (DO1)
C1
TO2 (DO2)
C2
TO3 (DO3)
C3
TO4 (DO4)
C4
TO5 (DO5)
C5
TO6 (DO6)
C6
Internal
Triac
Switches
(Isolated)
1
XMT
STATUS
RCV
IO+
IO-
SLD
EOL
Physical
Address
2

Siemens Insight

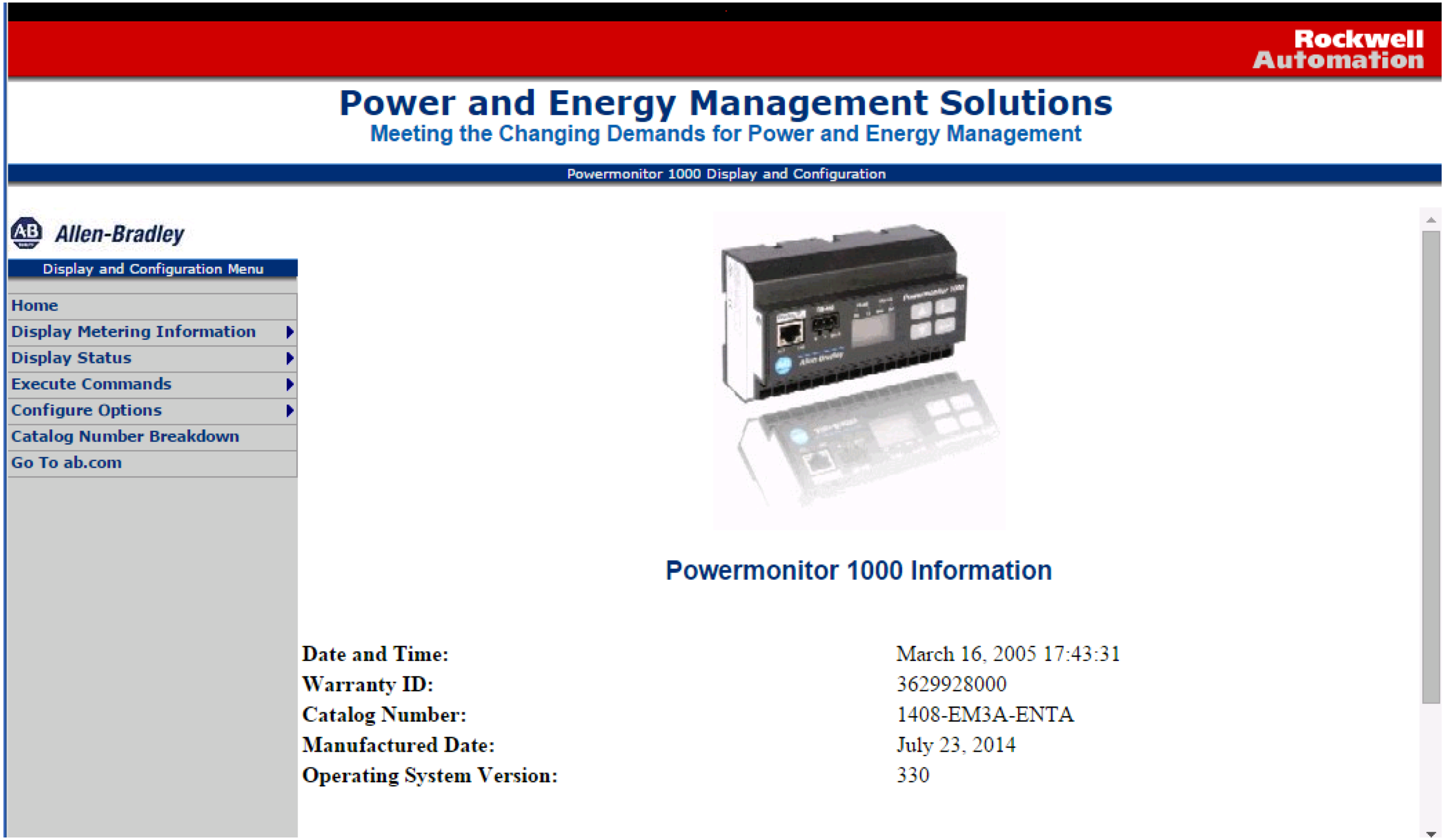
Other than BACnet

- 59 Ethernet/IP in TW
  - N**U Law Library
  - N**U Center of Biotechnology
  - N**U Men's Dormitory
  - N**U Precision Growth Chambers
  - N**U Grad. Inst. of National Development
  - N**U Grad. Inst. of Hydrotech Research
  - N**U Property Management Division
  - ... and so on
- ModBus/TCP
- Simple Ethernet-RS422/485 Adapters
  - 23 Moxa NPort in N**U

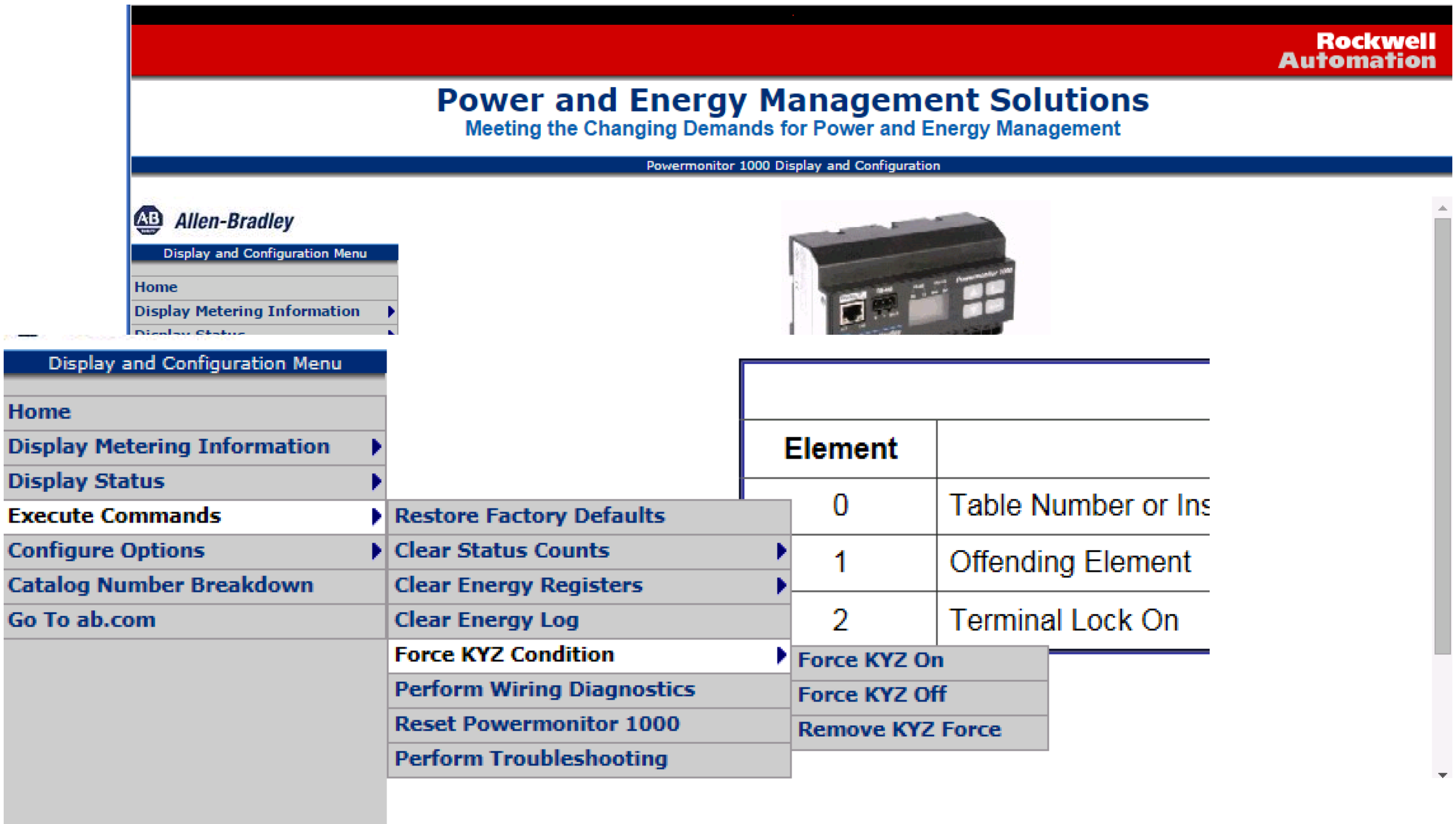
Allen-Bradley Powermonitor 1000



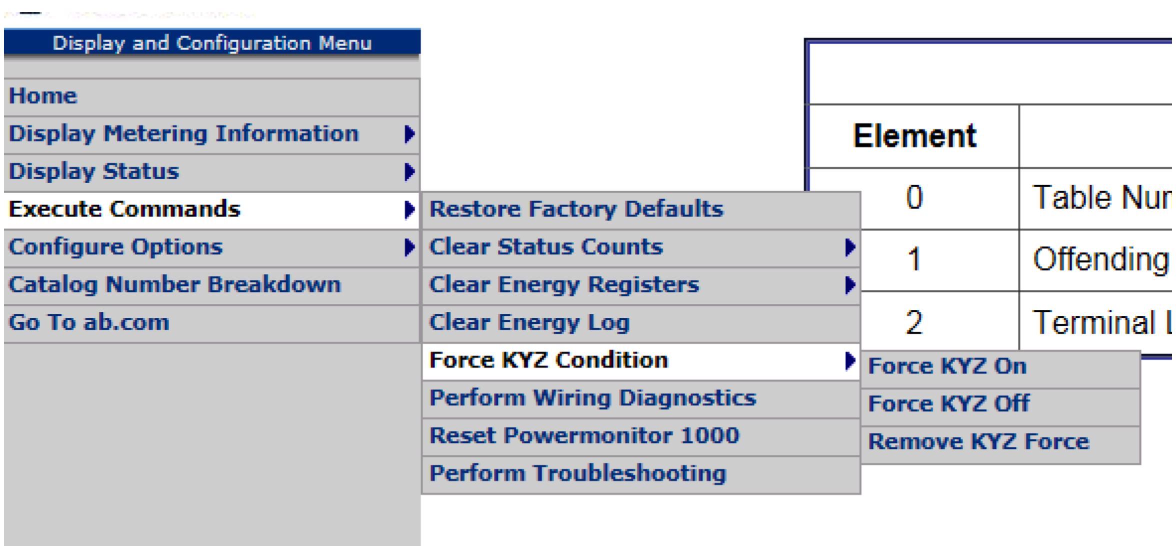
Unprotected HMI of Powermonitor 1000

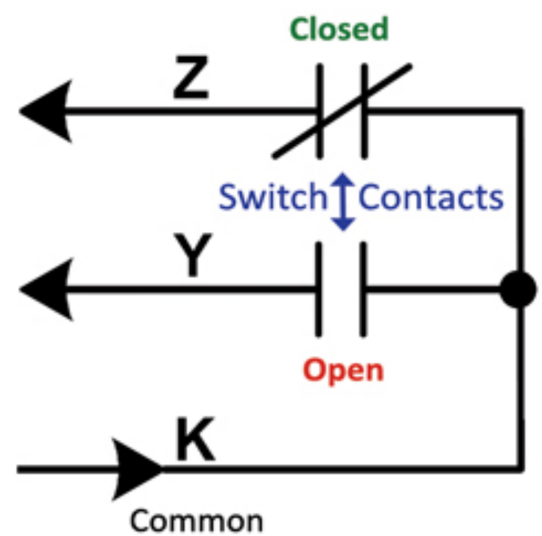


Force KYZ


Rockwell Automation
Power and Energy Management Solutions
Meeting the Changing Demands for Power and Energy Management
Powermonitor 1000 Display and Configuration
Allen-Bradley
Display and Configuration Menu
Home
Display Metering Information
Display Status
Execute Commands
Configure Options
Catalog Number Breakdown
Go To ab.com
Restore Factory Defaults
Clear Status Counts
Clear Energy Registers
Clear Energy Log
Force KYZ Condition
Perform Wiring Diagnostics
Reset Powermonitor 1000
Perform Troubleshooting
Force KYZ On
Force KYZ Off
Remove KYZ Force
Element
0
Table Number or Ins
1
Offending Element
2
Terminal Lock On

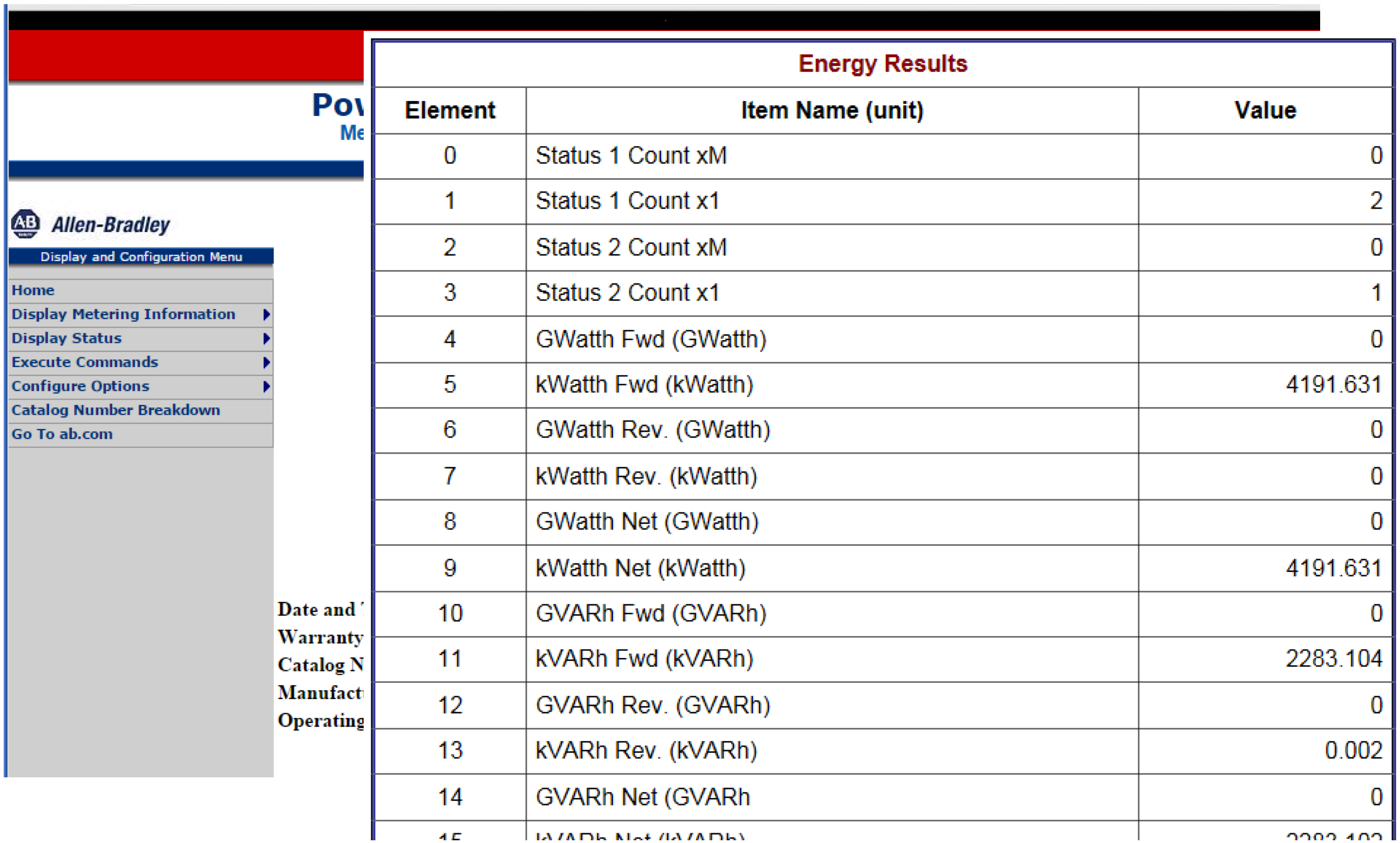
KYZ Pulse





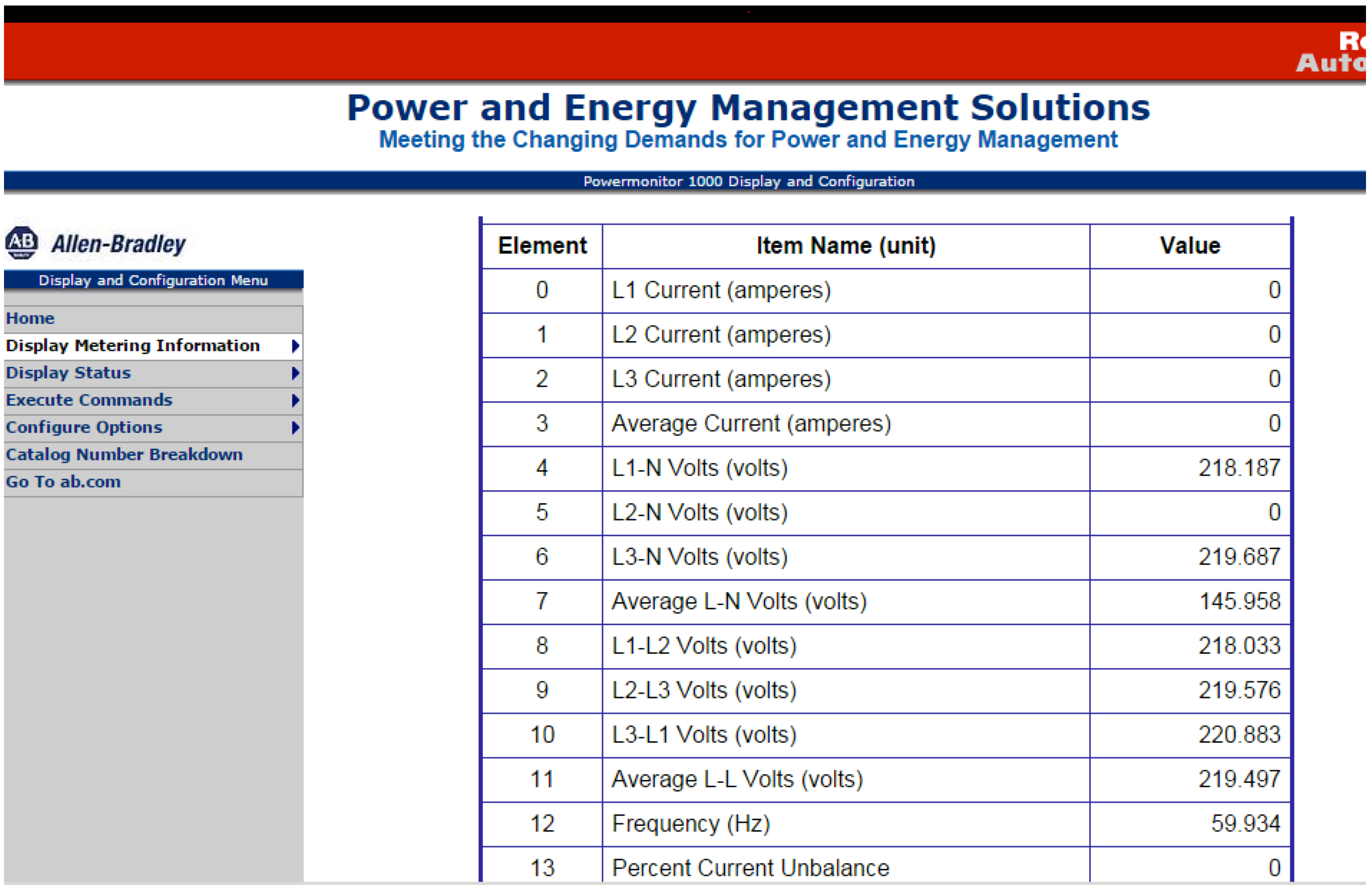
Circuit courtesy of http://solidstateinstruments.com/newsletters/kyz-pulses.php

Energy Results



Element	Item Name (unit)	Value
0	Status 1 Count xM	0
1	Status 1 Count x1	2
2	Status 2 Count xM	0
3	Status 2 Count x1	1
4	GWatth Fwd (GWatth)	0
5	kWatth Fwd (kWatth)	4191.631
6	GWatth Rev. (GWatth)	0
7	kWatth Rev. (kWatth)	0
8	GWatth Net (GWatth)	0
9	kWatth Net (kWatth)	4191.631
10	GVARh Fwd (GVARh)	0
11	kVARh Fwd (kVARh)	2283.104
12	GVARh Rev. (GVARh)	0
13	kVARh Rev. (kVARh)	0.002
14	GVARh Net (GVARh	0

Voltage Monitor



Element	Item Name (unit)	Value
0	L1 Current (amperes)	0
1	L2 Current (amperes)	0
2	L3 Current (amperes)	0
3	Average Current (amperes)	0
4	L1-N Volts (volts)	218.187
5	L2-N Volts (volts)	0
6	L3-N Volts (volts)	219.687
7	Average L-N Volts (volts)	145.958
8	L1-L2 Volts (volts)	218.033
9	L2-L3 Volts (volts)	219.576
10	L3-L1 Volts (volts)	220.883
11	Average L-L Volts (volts)	219.497
12	Frequency (Hz)	59.934
13	Percent Current Unbalance	0

23 Moxa Nport Ethernet-RS485 in N**U

NPort 5210/NPort 5230/NPort 5232 Series

2-port RS-232/422/485 serial device servers

- Datasheet
- Manual
- Drivers & Software
- Larger Image

Get a Quote

Evaluation units available for online purchase

>> Buy now (USA only)

Features	Details	Specs	Ordering

Unprotected NPort

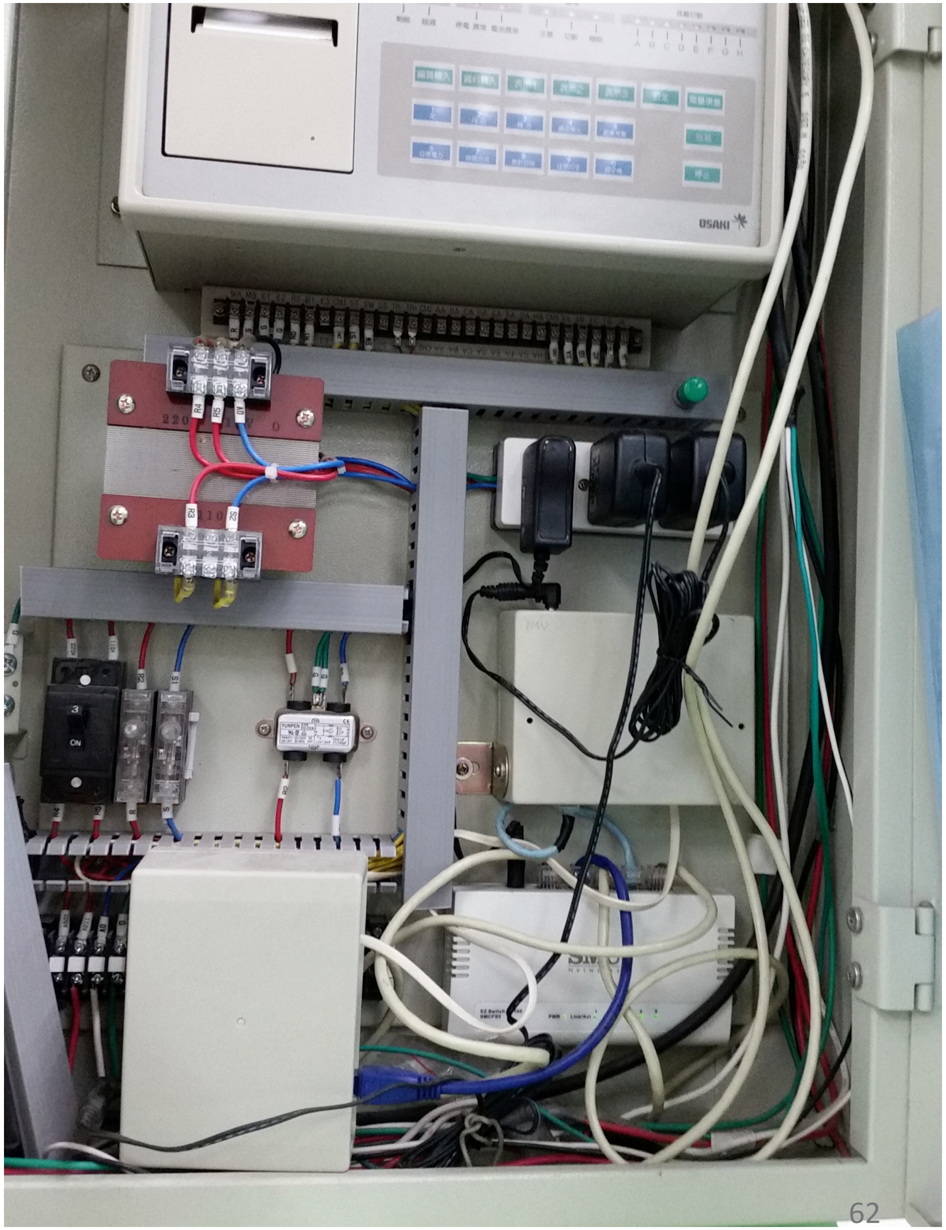
```
------------------------------------------------------------------------------
Model name       : NPort 5130
MAC address      : 00:90:E8:4A:65:69
Serial No.       : 547
Firmware version : 3.4 Build 11080114
System uptime    : 23 days, 03h:00m:55s
------------------------------------------------------------------------------
<< Main menu >>
  (1) Basic settings
  (2) Network settings
  (3) Serial settings
  (4) Operating settings
  (5) Accessible IP settings
  (6) Auto warning settings
  (7) Monitor
  (8) Ping
  (9) Change password
  (a) Load factory default
  (v) View settings
  (s) Save/Restart
  (q) Quit

Key in your selection: 3
------------------------------------------------------------------------------
<< Main menu->Serial settings >>
  (1) Port 1
  (m) Back to main menu
  (q) Quit

Key in your selection: 1
------------------------------------------------------------------------------
<< Main menu->Serial settings->Port 1 >>
  (1) Port alias
  (2) Baud rate
  (3) Data bits
  (4) Stop bits
  (5) Parity
  (6) Flow control
  (7) FIFO
  (8) Interface
  (v) View settings
  (m) Back to main menu
  (q) Quit
```

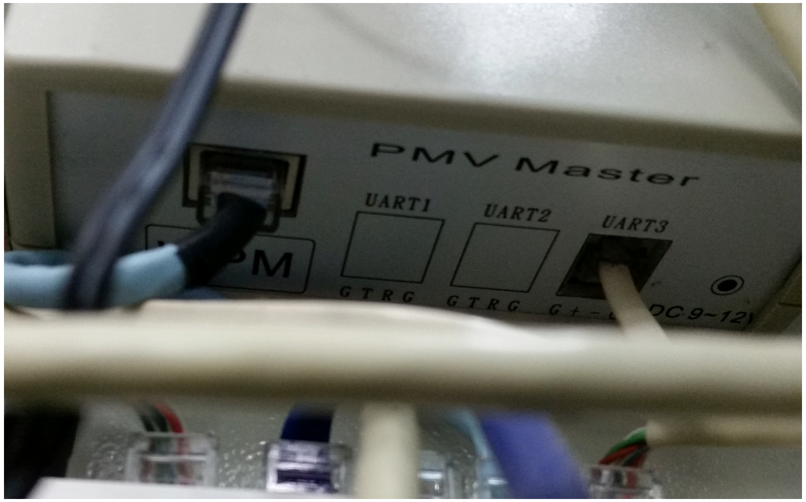
- 23 NPort in N**U
- 12 firewalled
- 2 password protected
- 9 no password

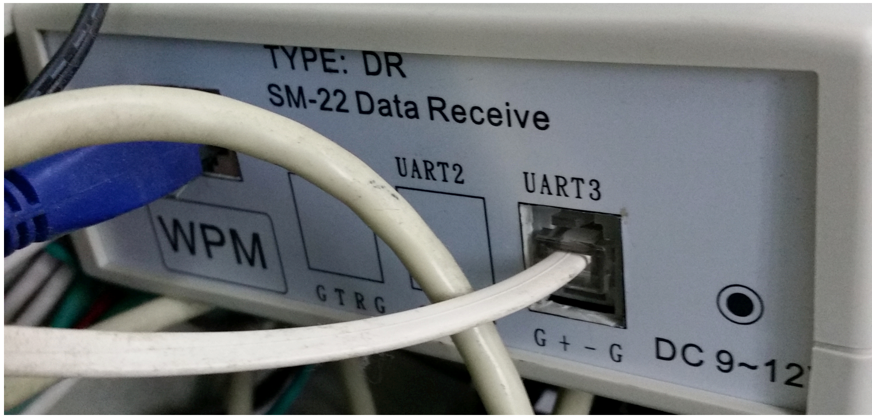
Dump and Have Fun

```
-------------------------------------------------------------------

Server name                      : NP5130_[redacted]
Web console                      : Enable
Telnet console                   : Enable
Reset button protect             : No

Press any key to continue...

-------------------------------------------------------------------

IP address                       : 192.168.[redacted]
Netmask                          : 255.255.255.0
Gateway                          :
IP configuration                 : Static
DNS server 1                     :
DNS server 2                     :
SNMP                             : Enable
SNMP community name              : public
SNMP contact                     :
SNMP location                    :
Auto IP report to IP             :
Auto IP report to UDP port       : 4002
Auto IP report period(seconds)   : 10

Press any key to continue...

-------------------------------------------------------------------

Port 1
Baud rate                        : 115200
Data bits                        : 8
Stop bits                        : 1
Parity                           : None
Flow control                     : RTS/CTS
FIFO                             : Enable
Interface                        : RS-485 2Wire
```

Legacy Devices (Osaki PowerMax 22)







Legacy Devices (Osaki PowerMax 22)

Special thanks to Chien Kuo Senior High School.

Subsidies from Ministry of Education

102 年度補助高級中等以上學校校園能資源管理及環境安全衛生計畫補助

表 **1-2** 能資源管理軟硬體設備(示範案)

項次	重點補助項目 **(80 萬元為原則)**	說明
1	校園電力需量控制系統	1.電力需量管理、紀錄、卸載、冷氣照明電源課表監控或其它等。 2.汰換電力變壓器(汰換為高效率之非晶質變壓器設備)。
2	建築物能源管理系統(BEMS)	集中監控各建築物（例如總表、教室、行政大樓、圖書館等）配電箱之供電需量、空調主機、照明設備等之運轉狀況，透過網路遠端連線操作，以有效管理或分析歷年運轉資料及控制電力負載狀況，防止尖峰用電超約罰款。
3	冷氣空調控制改善	1.冷氣機之最低溫限制、啟閉時間、開啟環境控制或其它。 2.空調主機、送風機、水泵、空調箱或其它設備裝設變頻控制。 3.冷氣計費儲值卡設備或冷氣用電計量電錶(冷氣計費、計量之儲值卡設備或冷氣用電計量電錶)。 4.換裝高效率之中央空調主機、冰水主機、空調附屬設備等。 5.熱泵、熱水空調系統。

MOE subsidies ~25,000 USD to schools for,

- Power consumption management system
- Building energies management system
- Improvement of air-condition controls

National Chia-Yi University

用電資料統計表 --- 資料來源請參閱 97-98 用電曲線圖 ---

<table>
<tr><td>用戶屬性</td><td colspan="3">高壓綜合用電戶(需量契約)</td><td colspan="2">經常契約容量</td><td>4,700KW</td></tr>
<tr><td>最高需量(尖峰) 月份</td><td colspan="2">5,392KW 97 年 9 月
5,216KW 98 年 9 月</td><td colspan="2">最低需量(尖峰) 月份</td><td colspan="2">2,752KW 97 年 2 月</td></tr>
<tr><td>年平均需量</td><td>4,331KW</td><td>高低差值</td><td>2,640KW</td><td colspan="2">尖峰負載因數/月</td><td></td></tr>
<tr><td>超約月份數</td><td>5</td><td>年超約容量</td><td>1,385KW</td><td colspan="2">月平均超約容量</td><td>115KW</td></tr>
<tr><td>年總超約罰款</td><td colspan="2">97 年 1,800,419 元
98 年 434,263 元(至 9 月)</td><td colspan="2"></td><td colspan="2"></td></tr>
</table>

Contract capacity: 4,700kW
Peak capacity: 5,216kW
Minimum capacity: 2,752 kW

NTU’s Discussion about BACnet

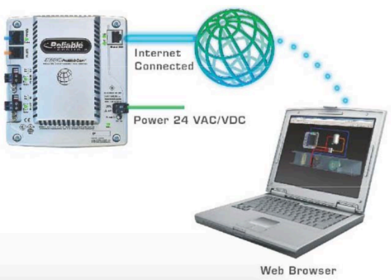
VRV空調監控及介面說明

VRV變頻設備，具有BACnet傳輸介面，如霖澤館，增加整合介面，提供空調管控，說明如下:

(1)介面控制器提供BACnet 網路連接VRV網路介面。

(2)介面控制器具有定時控制程式可提供瞬時及定時管控。

(3)介面控制器具有WEB網頁伺服器功能，可透過校園網路作監控管理。



103年3月10日 12

Shu-Zen Junior College

樹人醫護管理專科學校財物採購103036總務處教室節能監控招標須知

以下各項招標規定內容，由機關填寫，投標廠商不得填寫或塗改。

各項內含選項者，由機關擇符合本採購案者勾填。

一、 本採購適用政府採購法(以下簡稱採購法)及其主管機關所訂定之規定。

二、 本標案名稱：總務處教室節能監控

三、 採購標的為：

■財物；其性質為：■購買；□租賃；□定製；□兼具兩種以上性質者。

四、 本採購屬：

□ (1) 公告金額十分之一以下之採購。

□ (2) 逾公告金額十分之一未達公告金額之採購。

■ (3) 公告金額以上未達查核金額之採購。

□ (4) 查核金

□ (5) 巨額採

5. 具備 3 組 RS485 通信介面，2 個 10 / 100 Mbps Ethernet 供上下層資料通訊使用。

6. 支援 BACnet or Modbus TCP / IP or URL 等通訊定。

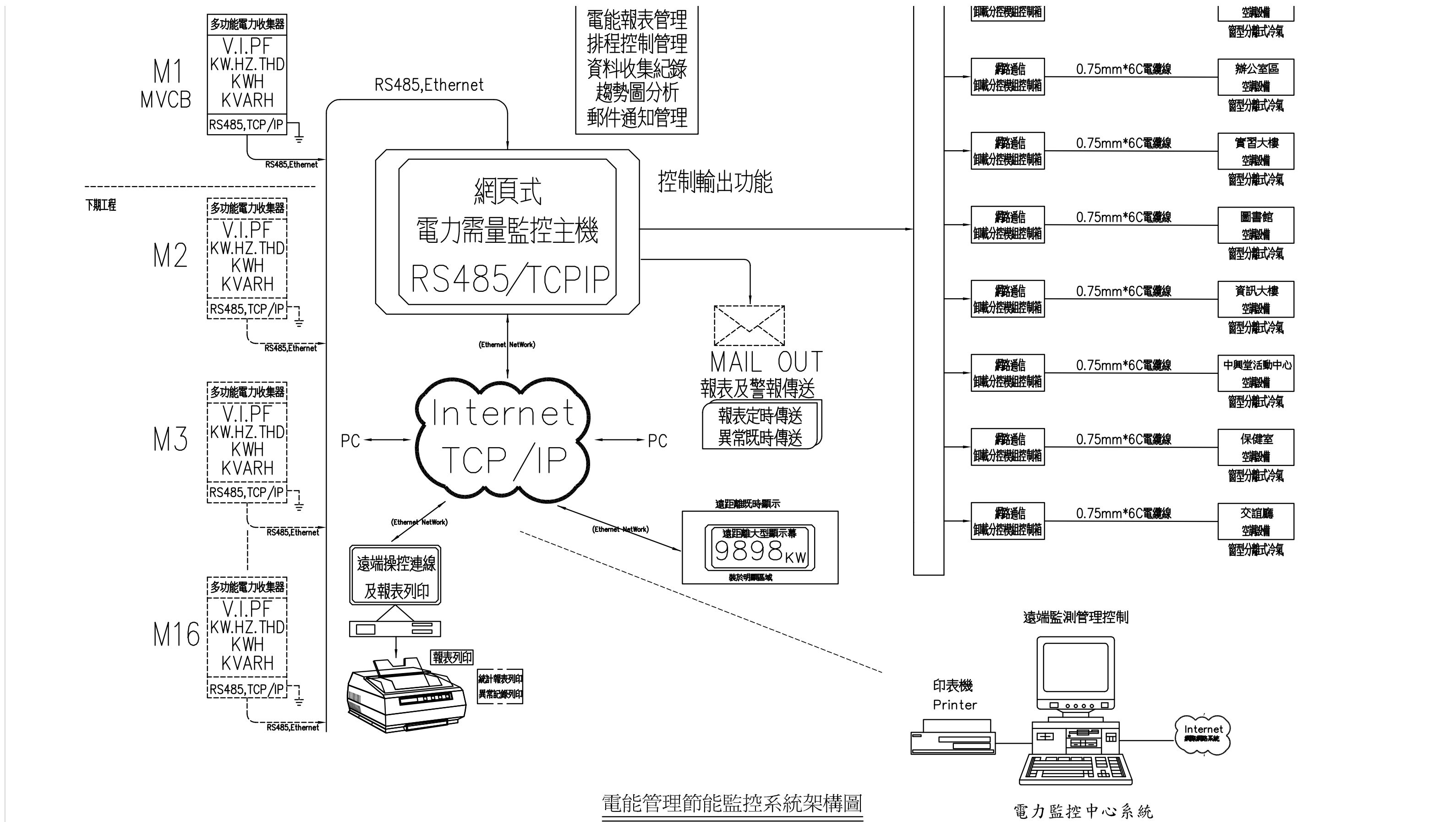
7. 可以透過 WEB 方式輕易管理及設定組態。

送風機控制器

1. 處理單元:8 位元。

2. 網路通訊:MODBUS RTU 標準格式 RS-485 通訊傳輸。

Taitung Senior Commercial Vocational School



St. Mary's Junior College of Medicine

103 學年度教育部補助-能源監控管理系統 建置規格書

項次	名稱	詳細規格	數量
一	能源監控管理系統	一.能源監控系統主機 (一) 能源監控系統主機 HP, DELL 或同等品(1 台)。	1 式

MODBUS 通訊之廠務設備通訊外，須具備有網路直接數位控制器 DDC 之功能。

11.可同時具有 MODBUS Ethernet TCP/IP 及 RS-485 RTU 之通訊能力。

12.每台整合通訊介面器至少可連接 8000 MODBUS 監控點。

13.提供 24 個可軟體配置的通用點，這些點包括:

(1) 18 個 UI/O:可使用軟體設定為 DI 或 Pulse Input 或 AI(0-10Vdc, 4-20mA, 1KRTD,10K,100K)，還可使用軟體設定為 AO(0-10Vdc)。

(2) 6 個超級泛用 Super IO:除了上述 UI/O 功能外, 還可使用軟體設定為 DO or AO(4~20mA)。

14.4 個數位輸入點(DI)。

(二) 15.8 個數位輸出點(DO)。

Points in Common

- Subsidized
- Public Tender
- Contracted

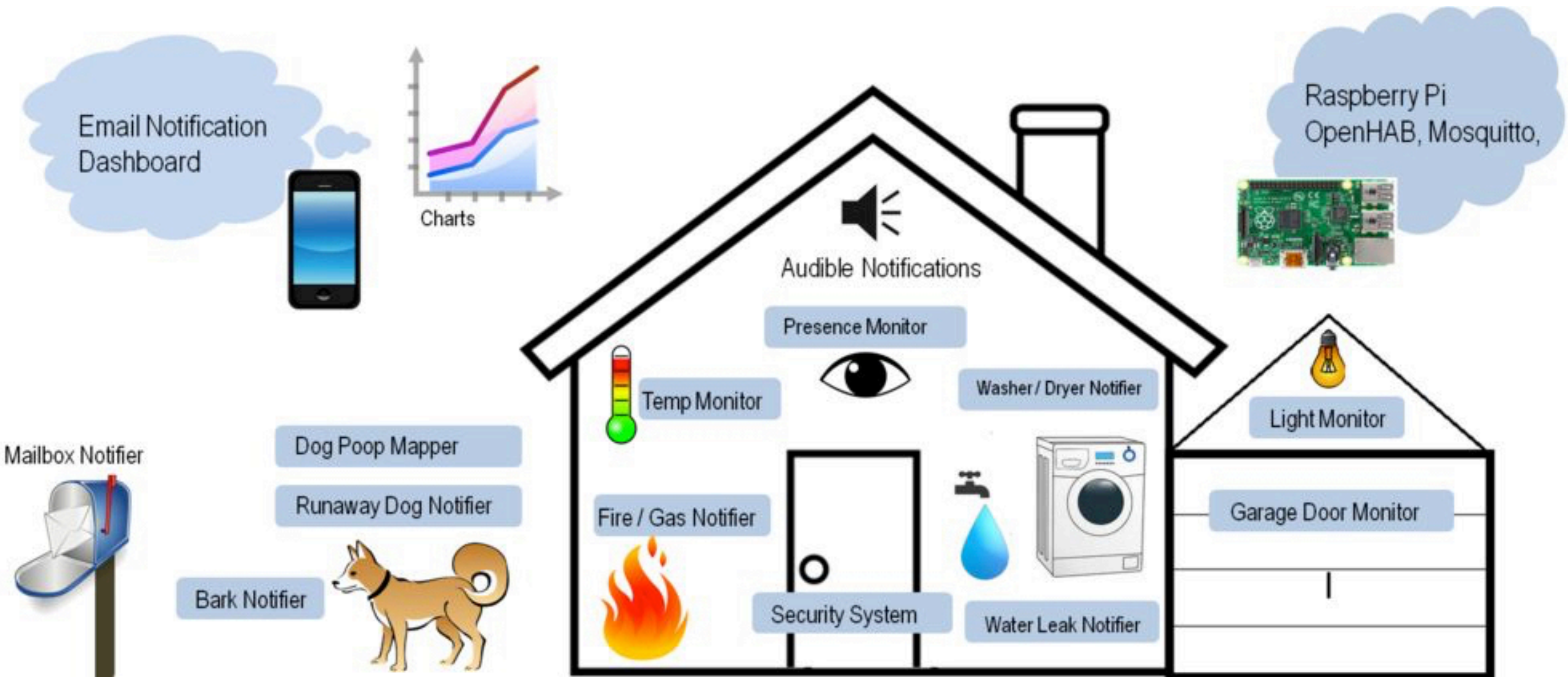
Note

You can find the papers on Google.
We did not probe / test their devices.

Suggestions

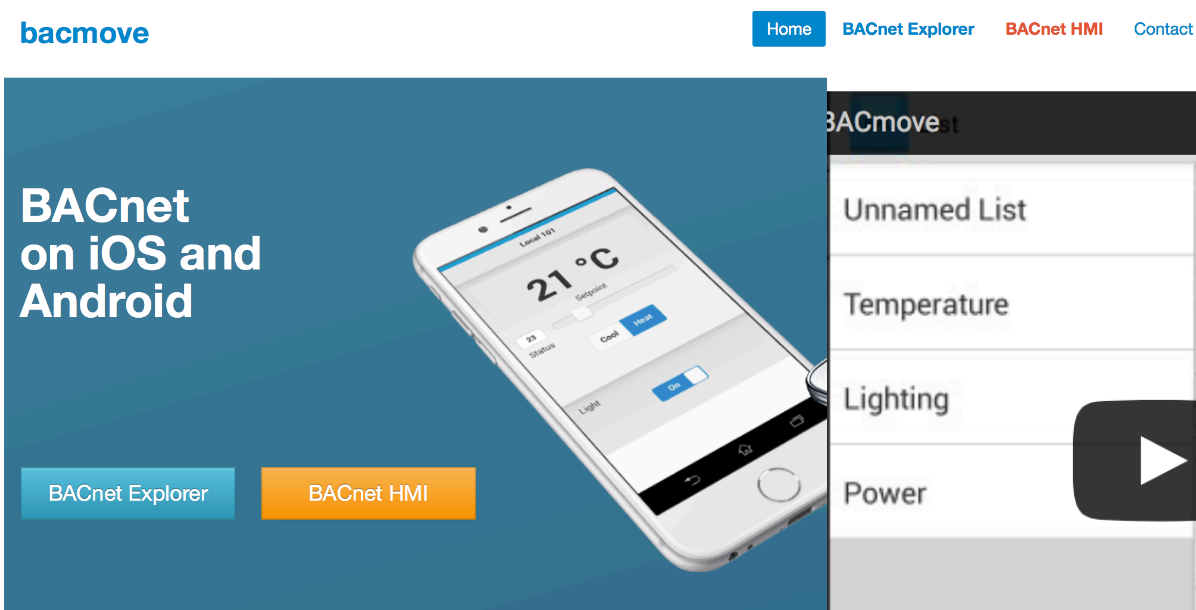
- Password
- Use private IP. No, not corporate LAN
- Firewall, SDN or tagged VLAN
- Upgrade / Patch
- Contract with a pentester

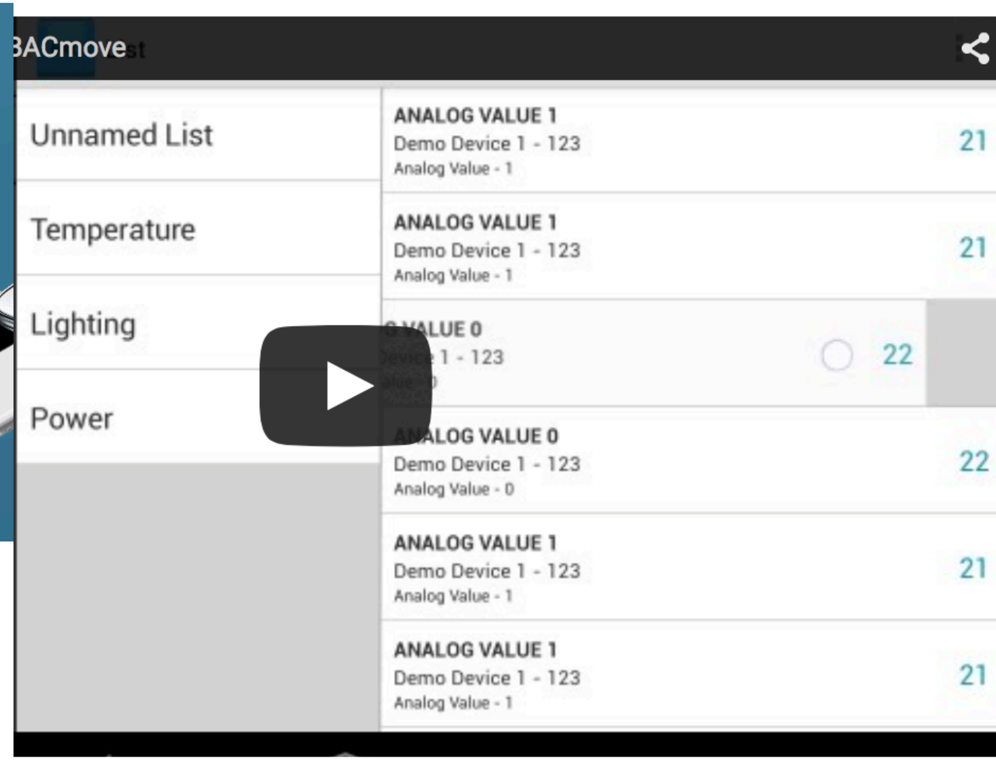
Home Automation with Arduino & RPi



Project at http://www.instructables.com/id/Uber-Home-Automation-w-Arduino-Pi/

Control System on Your Hand





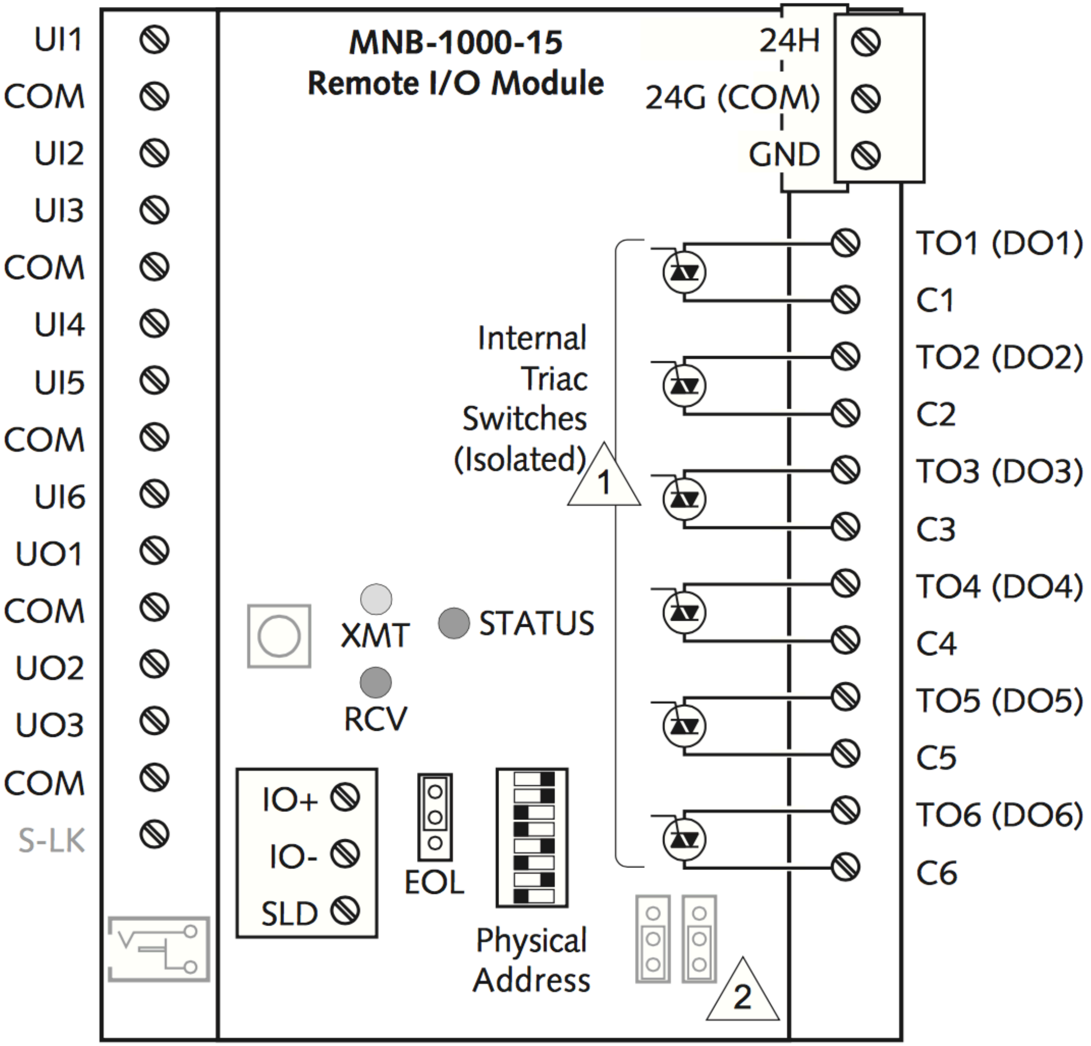
Homepage of http://bacmove.com

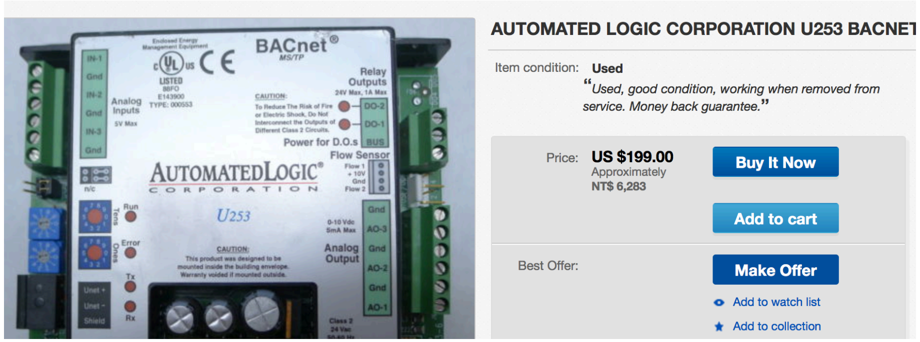
Our suggestion:
These things shouldn't even be on the internet, not on the corporate network.
It’s a control system and should be treated as such.

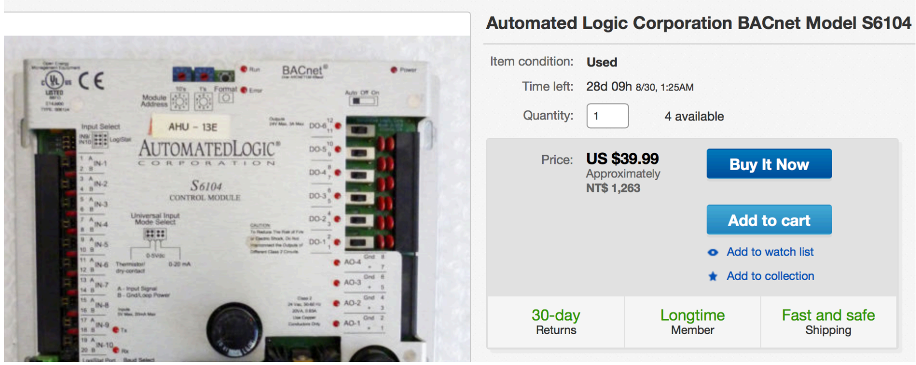
Securing Your Journey to the Cloud

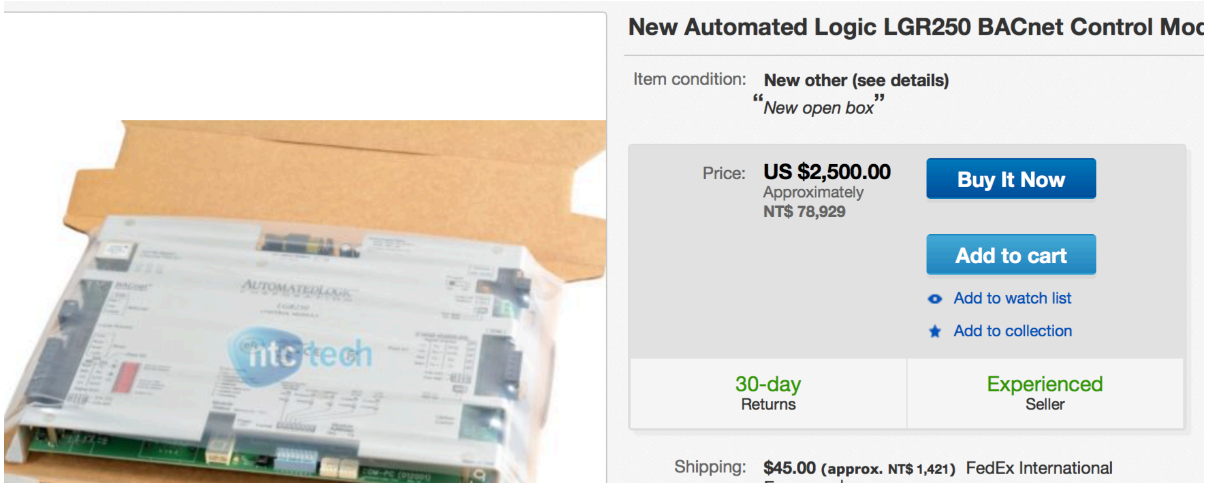
Questions?

TAC-MNB Module

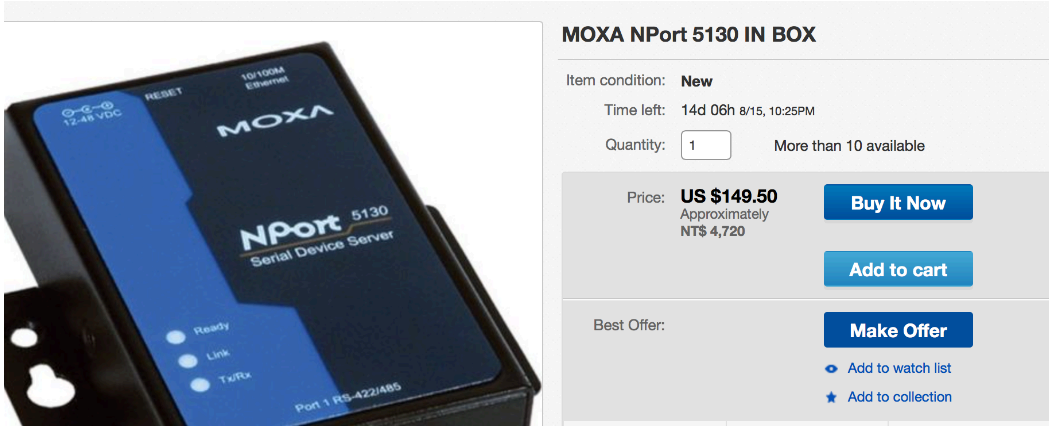




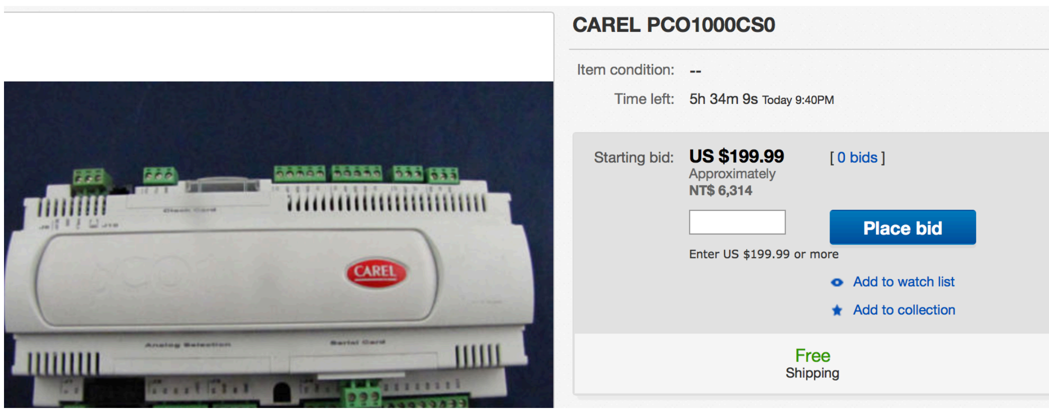




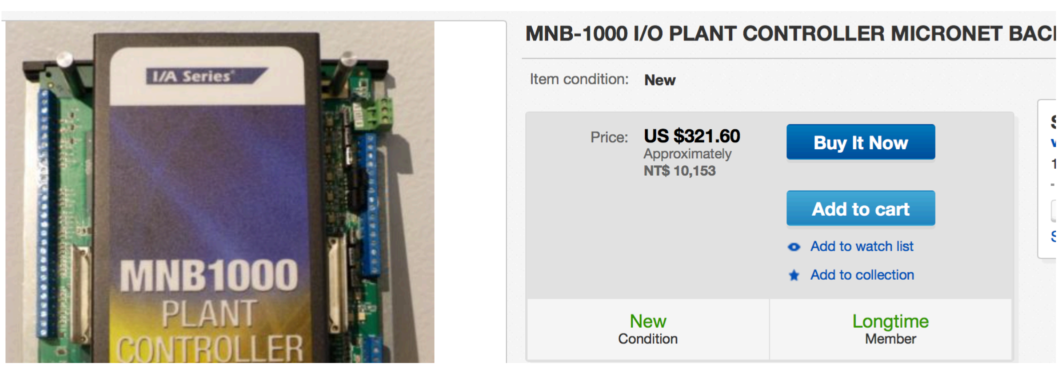
Automated Logic
US$40 (used)
|
US$2,500 (new)



MOXA NPort 5130
US$75 - 149 (new)

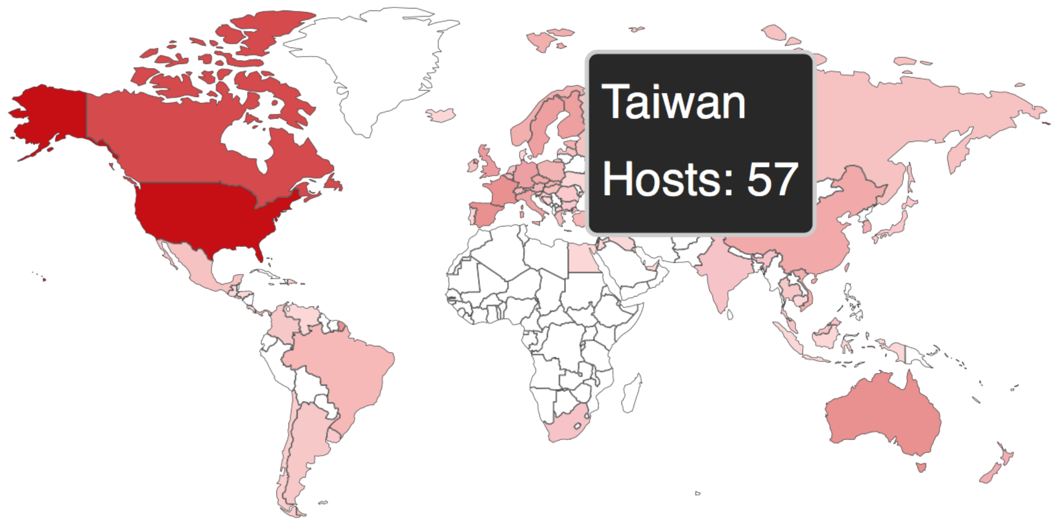


Carel pCO1000 US$200
pCOWEB, unknown



MNB-1000 US$321.60

Port 47808, TW: 57/12,358



United States	**4,869**
Canada	**1,260**
Spain	**123**
Australia	**122**
France	**121**