



Building Automation and Control – Hacking Subsidized Energy Saving System

Stephen Hilt, miaoski

2015/8/26-27



Securing Your Journey
to the Cloud

\$ whoami

- miaoski (@miaoski)
- Staff engineer in Trend Micro
- BACnet newbie



\$ whoami

- Stephen Hilt (@tothehilt)
- 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.



Public domain

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?

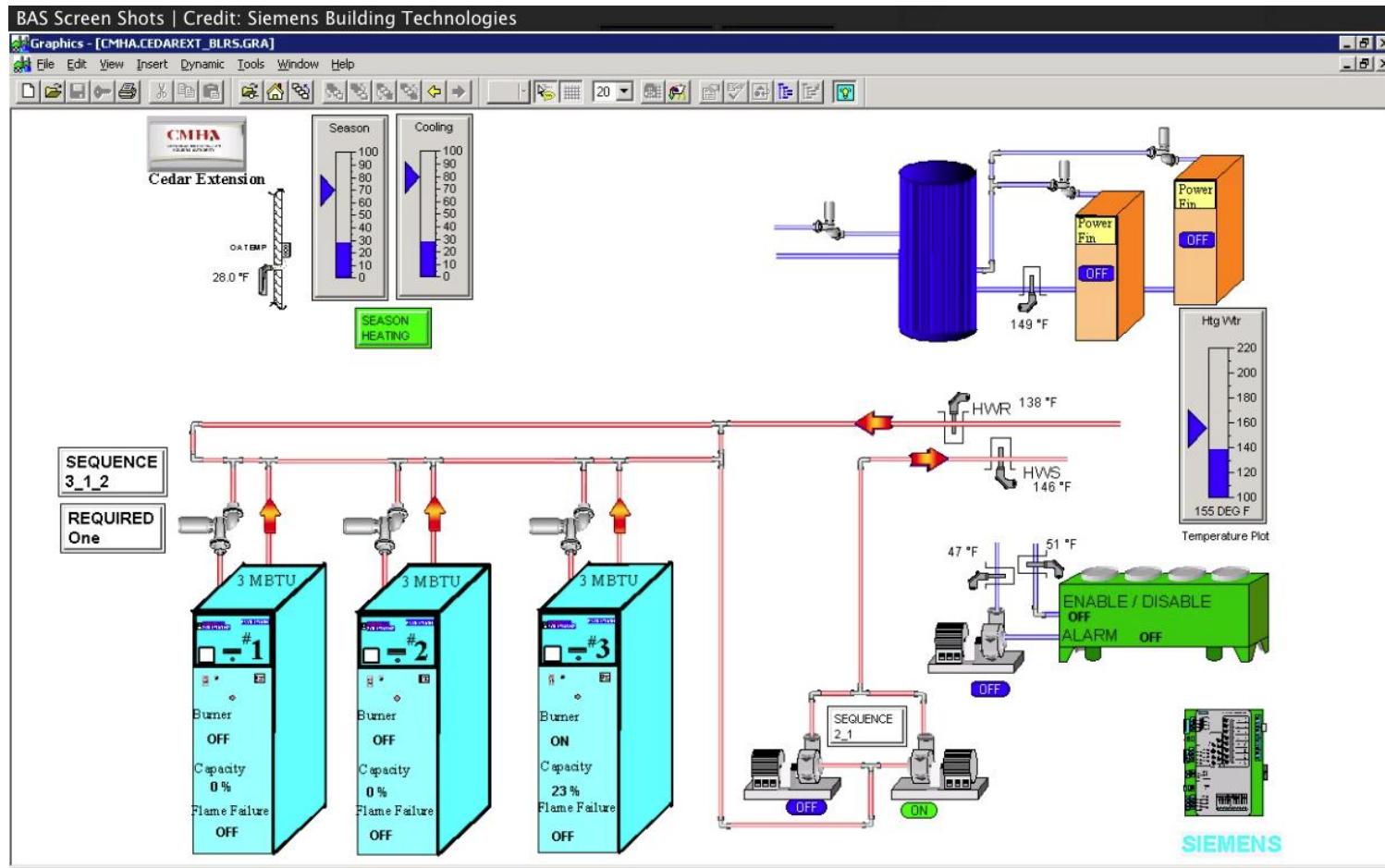


Image from <http://buildipedia.com/aec-pros/facilities-ops-maintenance/case-study-cuyahoga-metro-housing-authority-utilizes-bas>

Credit: Siemens Building Technologies

Building Automation!

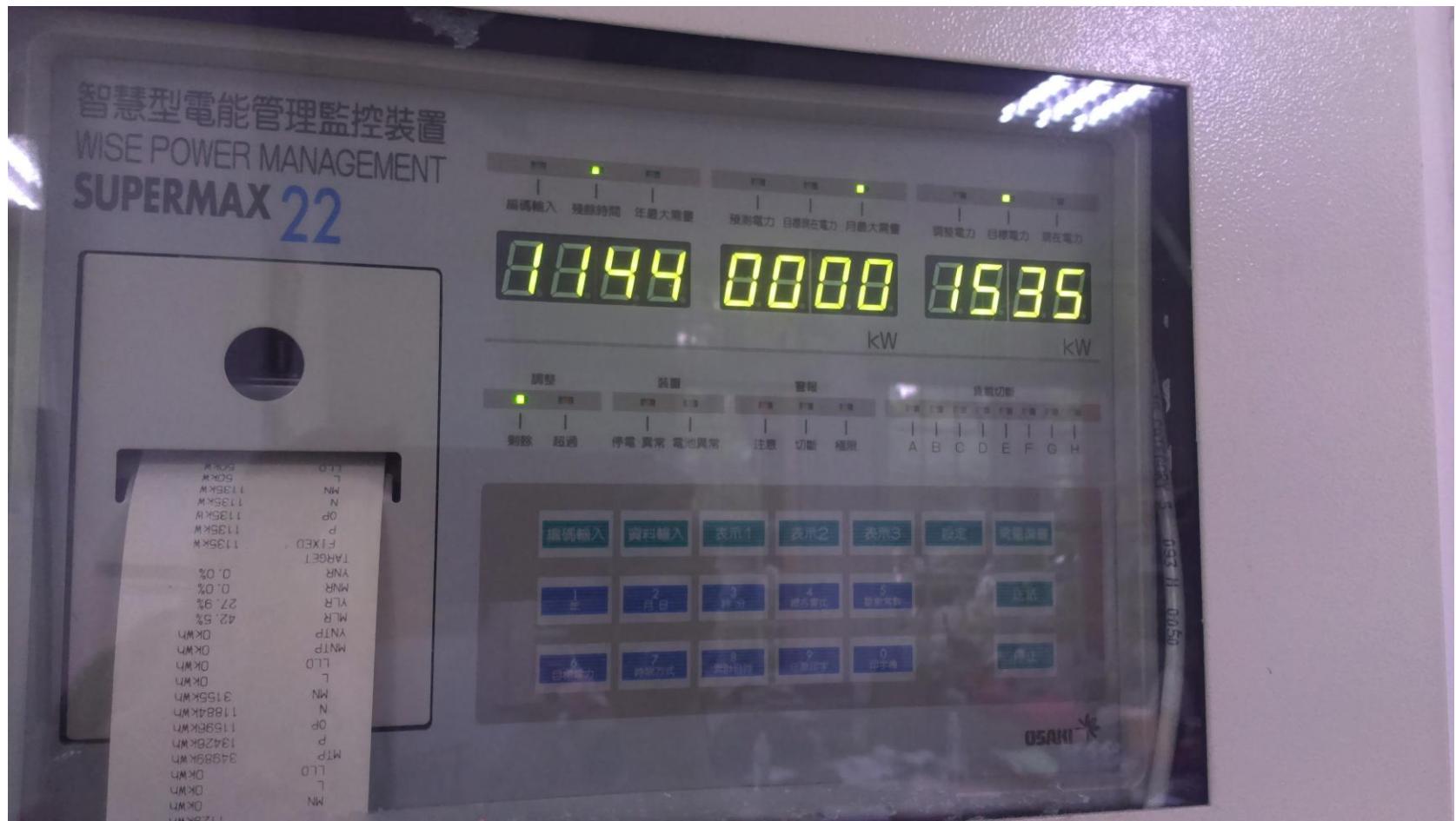


Photo courtesy of Chien Kuo Senior High School.

ANSI/ASHRAE 135-2001



ANSI/ASHRAE Standard 135-2001 (Including ANSI/ASHRAE Addenda 135a, 135b, 135c, 135d, and 135e)

ASHRAE[®] STANDARD

BACnet®—
A Data Communication
Protocol for Building
Automation and
Control Networks

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 BACnetVTSessions	O ²
Local_Time	Time	O ^{3,4}
Local_Date	Date	O ^{3,4}
UTC_Offset	INTEGER	O ⁴
Daylight_Savings_Status	BOOLEAN	O ¹
APDU_Segment_Timeout	Unsigned	R
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



- 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

BACnet Defined		BACnet Stack Layers				OSI Layers	
		BACnet Application Layer				Application (7)	
		BACnet Network Layer				Network (3)	
ISO 8802-2 (IEEE 802.2) Type 1	MS/TP	PTP	LonTalk	BVLL	BZLL	Data-Link (2)	
				UDP/IP	BP/GT	Physical (1)	
ISO 8802-3 Ethernet	ARCNET	EIA 485	EIA 232	IP Supporting Data link		Zigbee Stack	

Credit: icpdas.com

BACnet/IP

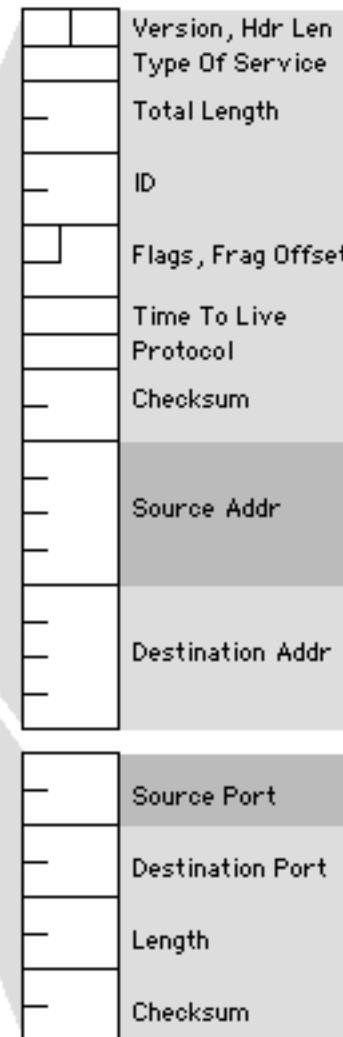
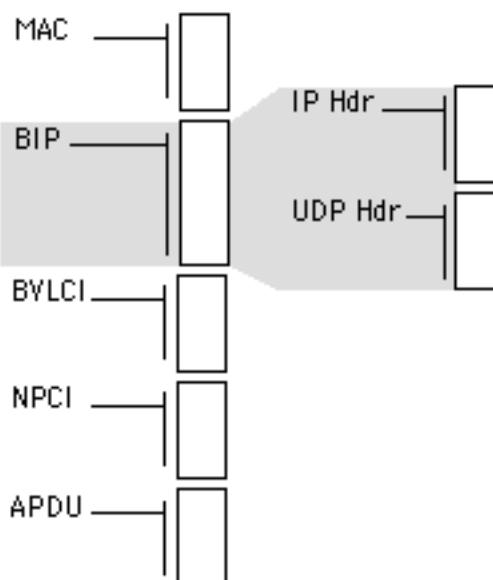
791 10:59:52.600060000 10.1.1.23	10.1.3.4	BVLC	48 BACnet Virtual Link Control
792 10:59:52.601602000 10.1.3.4	10.1.1.23	BVLC	60 BACnet Virtual Link Control
970 10:59:55.345765000 10.1.1.23	10.1.3.4	BACnet-APDU	54 Unconfirmed-REQ who-Is
972 10:59:55.348832000 10.1.3.4	10.1.1.23	BACnet-APDU	73 Unconfirmed-REQ 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)			
<hr/>			
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 + ...

791	10:59:52.600060000	10.1.1.23
792	10:59:52.601602000	10.1.3.4
970	10:59:55.345765000	10.1.1.23
972	10:59:55.348832000	10.1.3.4
1072	10:59:57.425856000	10.1.1.23
1073	10:59:57.425954000	10.1.1.23
1074	10:59:57.429561000	10.1.3.4
1075	10:59:57.430674000	10.1.3.4

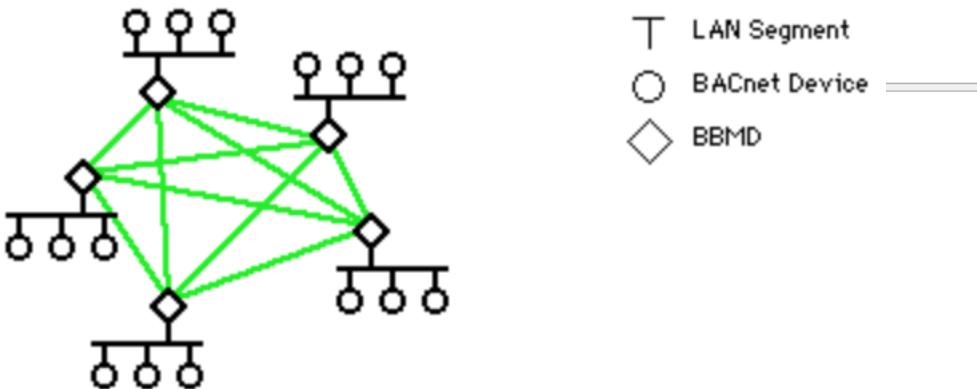
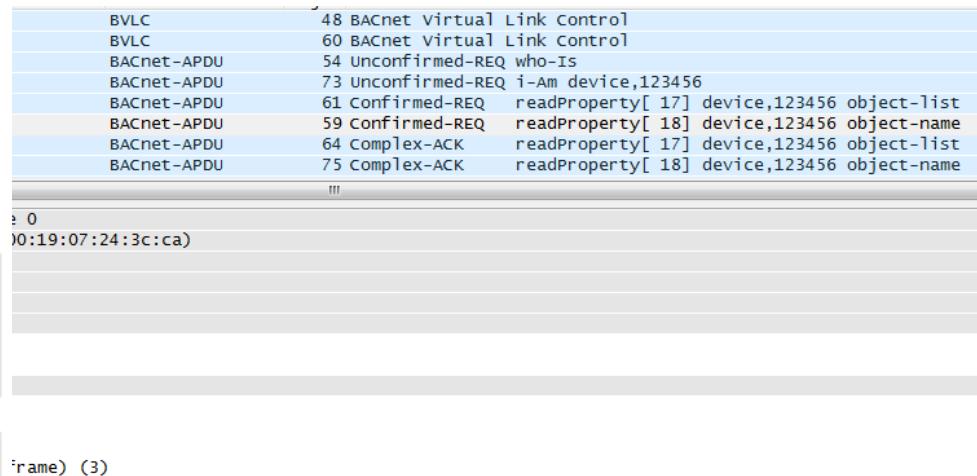
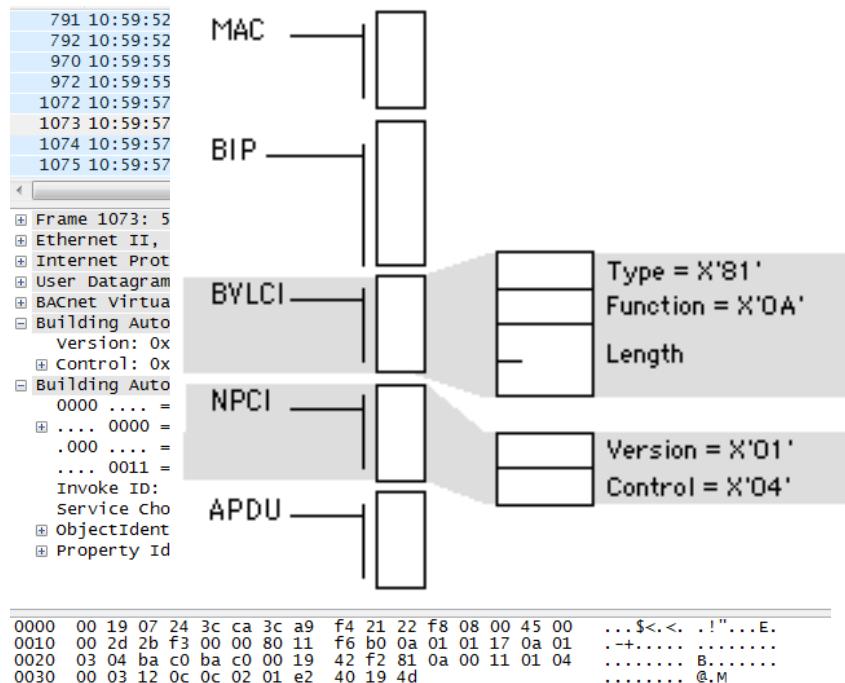
```
Frame 1073: 59 bytes on wire (472 bits)
Ethernet II, Src: 3c:a9:f4:21:22:f8
Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15)
User Datagram Protocol, Src Port: 47000, Dst Port: 47000
BACnet Virtual Link Control
Building Automation and Control Network
    Version: 0x01 (ASHRAE 135-1995)
    Control: 0x04
Building Automation and Control Network
    0000 .... = APDU Type: Confirmed-FR
    .... 0000 = PDU Flags: 0x00
    .000 .... = Max Response Segments
    .... 0011 = Size of Maximum ADPU
    Invoke ID: 18
    Service Choice: readProperty (12)
ObjectIdentifier: device, 123456
Property Identifier: object-name (
```

0000	00	19	07	24	3c	ca	3c	a9	f4	21	2
0010	00	2d	2b	f3	00	00	80	11	f6	b0	0
0020	03	04	ba	co	ba	c0	00	19	42	f2	8
0030	00	03	12	0c	0c	02	01	e2	40	19	4



```
ontrol
ontrol
s
device,123456
property[ 17] device,123456 object-list
property[ 18] device,123456 object-name
property[ 17] device,123456 object-list
property[ 18] device,123456 object-name
```

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



BBMD = BACnet broadcast management device

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

BACnet Objects

 Binary Input	 Multi-state Input	 File
 Binary Output	 Multi-state Output	 Program
 Binary Value	 Multi-state Value	 Schedule
 Analog Input	 Loop	 Trend Log
 Analog Output	 Calendar	 Group
 Analog Value	 Notification Class	 Event Enrollment
 Averaging	 Command	 Device
 LifeSafetyZone	 LifeSafetyPoint	

Credit: www.bacnet.org

BACnet-discover-enumerate.nse (1)

Object Name Packet Sent == 810a001101040005010c0c023FFFFF194d

-----	,
object-identifier	(75),
object-list	(76),
object-name	(77), → 77 == 0x4d
object-property-reference	(78),
object-type	(79),

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.xx.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-xxx-xxx-xxx.n**k.edu.tw (140.xxx.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.xxx.xxx.xxx:47808

| 140.xxx.xxx.xxx:47808

| 172.18.9.254:47808

|_ Foreign Device Table (FDT): Non-Acknowledgement (NAK)

FDT → NAK!

Nmap scan report for 140-xxx-xxx-xxx.n**k.edu.tw (140.xxx.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.xxx.xxx.xxx:47808

| 140.xxx.xxx.xxx:47808

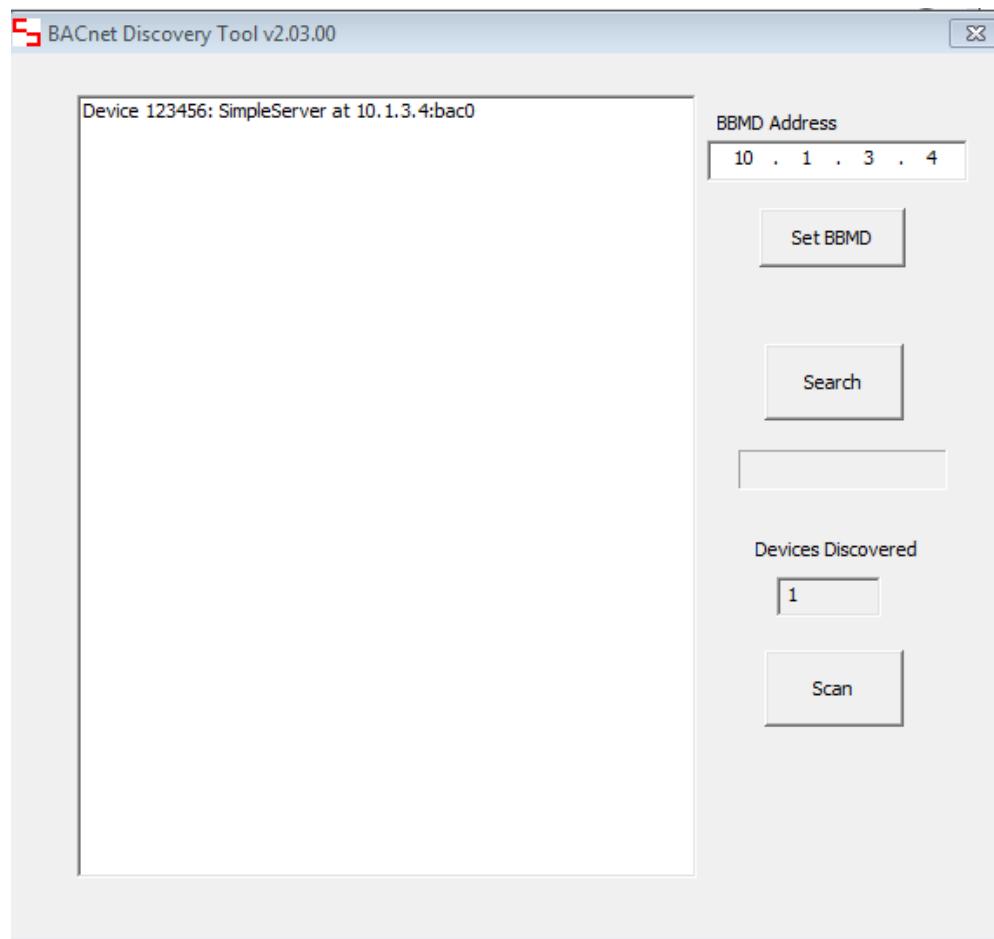
| 172.18.9.254:47808

|_ Foreign Device Table (FDT): Non-Acknowledgement (NAK)

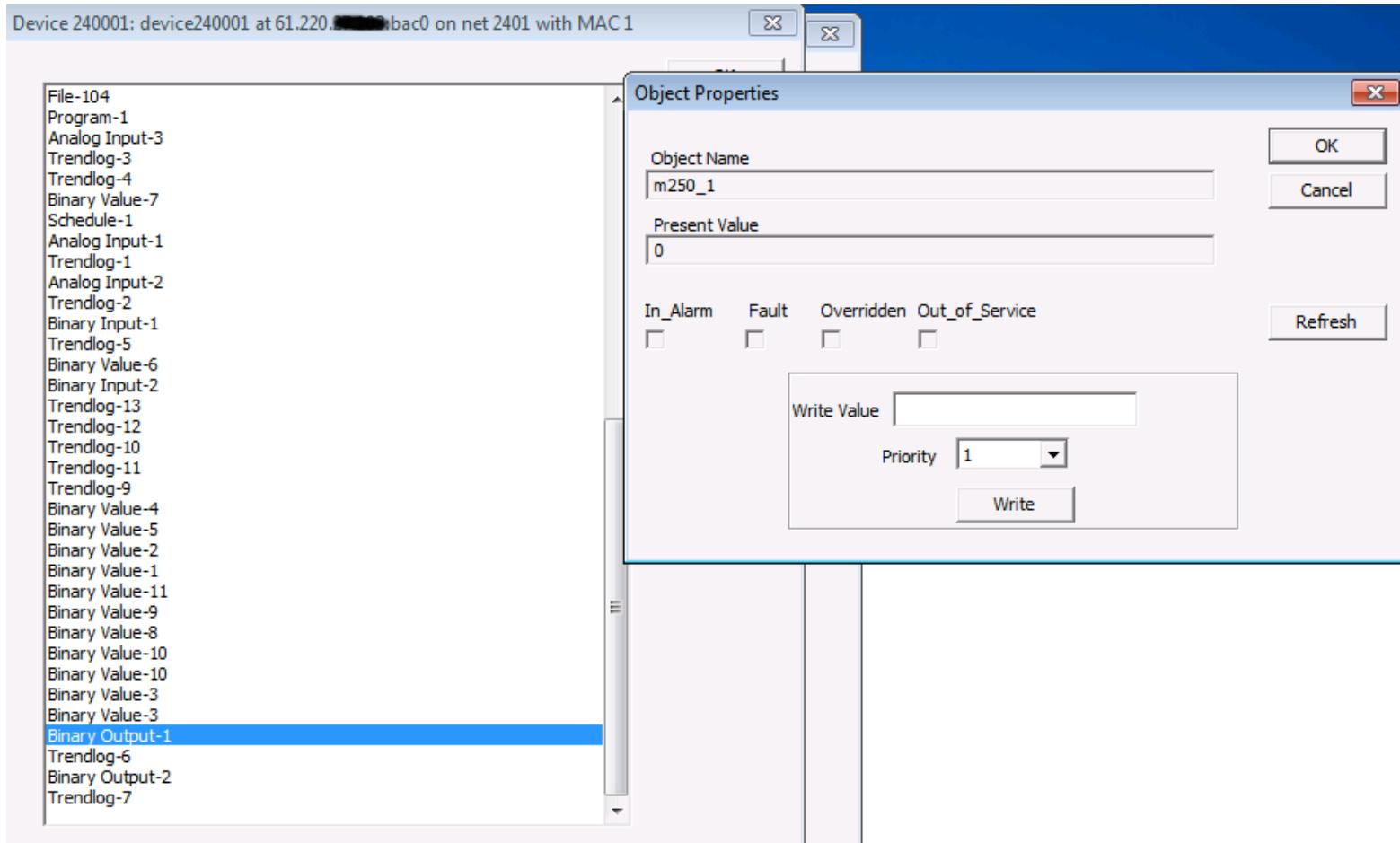
Let's Gather MORE Information

- 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





We're looking for a dentist....?

Another day.
Today we look for BACnet devices.

Shodan + BACnet Discovery Tool

SHODAN port:47808 country:TW

Exploits Maps Download Results Create Report

TOP COUNTRIES

Taiwan, Province of China 57

TOP CITIES

City	Count
Taipei	29
Keelung	4
Kaohsiung	2
Hsinchu	2

TOP ORGANIZATIONS

Organization	Count
CHTD, Chunghwa Telecom Co., Ltd.	17
National Taiwan Normal University	13
National Taiwan Ocean University	3
Yuan Ze University	2
Taiwan Fixed Network, Telco ...	2

TOP PRODUCTS

Product	Count
WebAccess Bacnet Server	17
PCO1000WB0	2
pCOWeb@	1
WC17	1
WC-BACems	1

Showing results 1 - 10 of 86

140.122.73.16
National Taiwan Normal University
Added on 2015-07-31 00:04:41 GMT
Taiwan, Taipei
Details

BACnet ADPU Type: Error (5)

140.112.178.206
National Taiwan University
Added on 2015-07-30 17:23:51 GMT
Taiwan, Taipei
Details

Instance ID: 4194303
Object Name: BW
Location: WebAccess
Vendor Name: BroadWin Technology, Inc.
Application Software: 7.0
Firmware: 0.99
Model Name: WebAccess Bacnet Server
Description: Desc

60.248.45.235
60-248-45-235.HINET-IP.hinet.net
CHTD, Chunghwa Telecom Co., Ltd.
Added on 2015-07-29 23:14:04 GMT
Taiwan
Details

Instance ID: 4194303
Object Name: BW
Location: WebAccess
Vendor Name: BroadWin Technology, Inc.
Application Software: 7.0
Firmware: 0.99
Model Name: WebAccess Bacnet Server
Description: Desc

211.72.93.146
211-72-93-146.HINET-IP.hinet.net
CHTD, Chunghwa Telecom Co., Ltd.

Instance ID: 4194303
Object Name: RW

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



Enabling an Intelligent Planet

- 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 opclImg.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

Advantech WebAccess

啟動節點 停止節點 幫助 瀏覽屬性 首頁

Kenting-Cae Caesar-Kent welcome

 墾丁凱撒大酒店



The starry night

11:56:32

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

Advantech WebAccess

啟動節點 停止節點 幫助 瀏覽屬性 首頁

ChungYuan | CYCU_Dormit| welcome

The screenshot shows a web-based interface for managing network nodes. At the top, it displays 'Advantech WebAccess' and navigation links in Chinese. Below this, the URL 'ChungYuan | CYCU_Dormit| welcome' is visible. The main content area features a collage of five images related to Chung Yuan Christian University (CYCU). The images include: a modern building facade with the text 'CHUNG YUAN CHRISTIAN UNIVERSITY' and '邀請您想像的中原大學'; a view of a building with a staircase and trees; a street scene with a white scooter; a night view of a modern building with illuminated windows; and a landscape image with a church spire and the text '愛是教育的主要力量' (Love is the main force of education) and '自然與人性的尊嚴 天人合一的和諧' (The dignity of nature and humanity, the harmonious unity of heaven and man).

12:12:55

Dorm, Chung Yuan Christian University 中原大學宿舍

11 Protected by Password

Advantech WebAccess

啟動節點 停止節點 幫助 瀏覽屬性 首頁

HYDEAN RAS welcome

主循環監控系統 MAIN

養殖槽溶氧監控 FRP

循環設備監控 PUMP

歷史驅勢折線圖 History

3 A E_MS_Salt 11:54:05

PURE DISE
瀚頂生物科技股份有限公司
Hydean Biotechnology Co., Ltd
循環水養殖監控系統

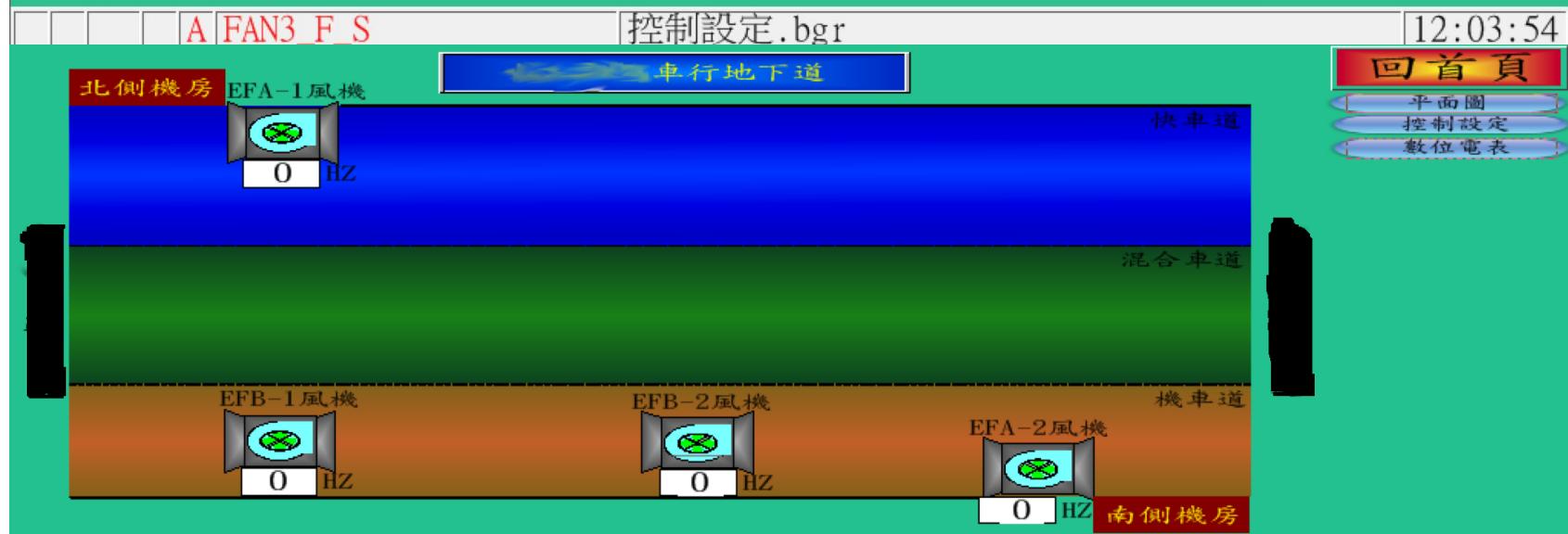
Hydean Biotechnology Co., Ltd. 瀚頂生物科技

3 No or Default Password



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

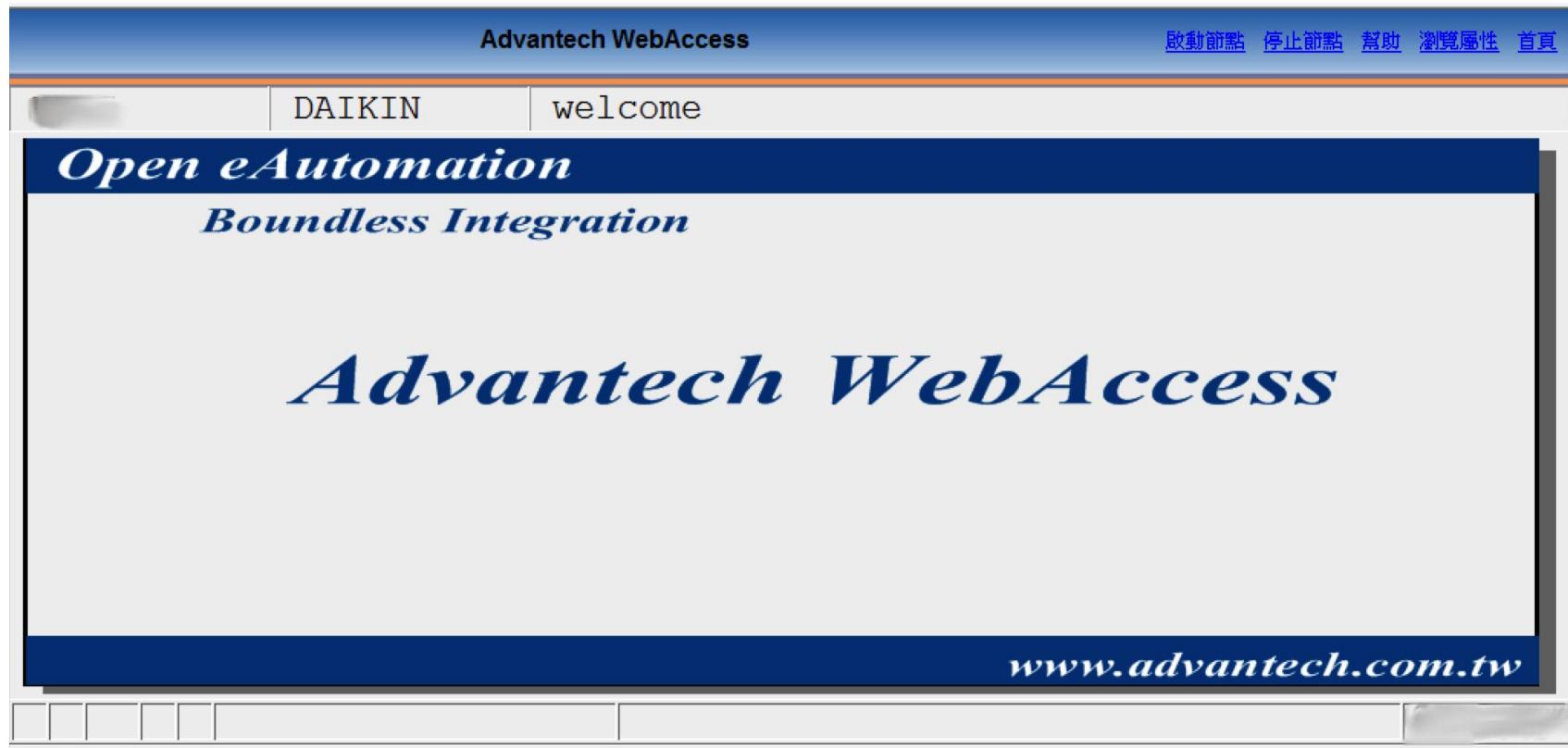
Unprotected HMI



Unprotected HMI



Unprotected HMI



Project Management

Advantech WebAccess 工程管理員

快速入門 幫助 首頁 登出

系統 事件記錄 按鍵轉換 導入外部數據 當量控制 BACNetServerConfig ModbusServerConfig 谷歌地圖 Excel 報表

節點屬性 刪除 增加通訊埠 累算點 計算點 常數點 系統點 面板 即時趨勢圖 資料記錄趨勢 告報群組 配方 影像 監控程序 管理員程式 資料傳送 輸入Excel 輸出Excel 報表 排程 課程排程 告報人員管理

工程/節點

通信埠1 (tcpip)
2F_PLU_1
101_2-06_AirFlow
101_2-06_AirFlow_Set
101_2-06_ONOFF
101_2-06_ONOFF_Set
101_2-06_Remote_Set
101_2-06_RemoteMode_S
101_2-06_RemoteTemp_S
101_2-06_Temperature
101_2-06_TemperatureS
101_2-07_AirFlow
101_2-07_AirFlow_Set
101_2-07_ONOFF
101_2-07_ONOFF_Set
101_2-07_Remote_Set
101_2-07_RemoteMode_S
101_2-07_RemoteTemp_S
101_2-07_Temperature
101_2-07_TemperatureS
102_2-05_AirFlow
102_2-05_AirFlow_Set
102_2-05_ONOFF
102_2-05_ONOFF_Set
102_2-05_Remote_Set
102_2-05_RemoteMode_S
102_2-05_RemoteTemp_S
102_2-05_Temperature
102_2-05_TemperatureS

節點： [redacted]

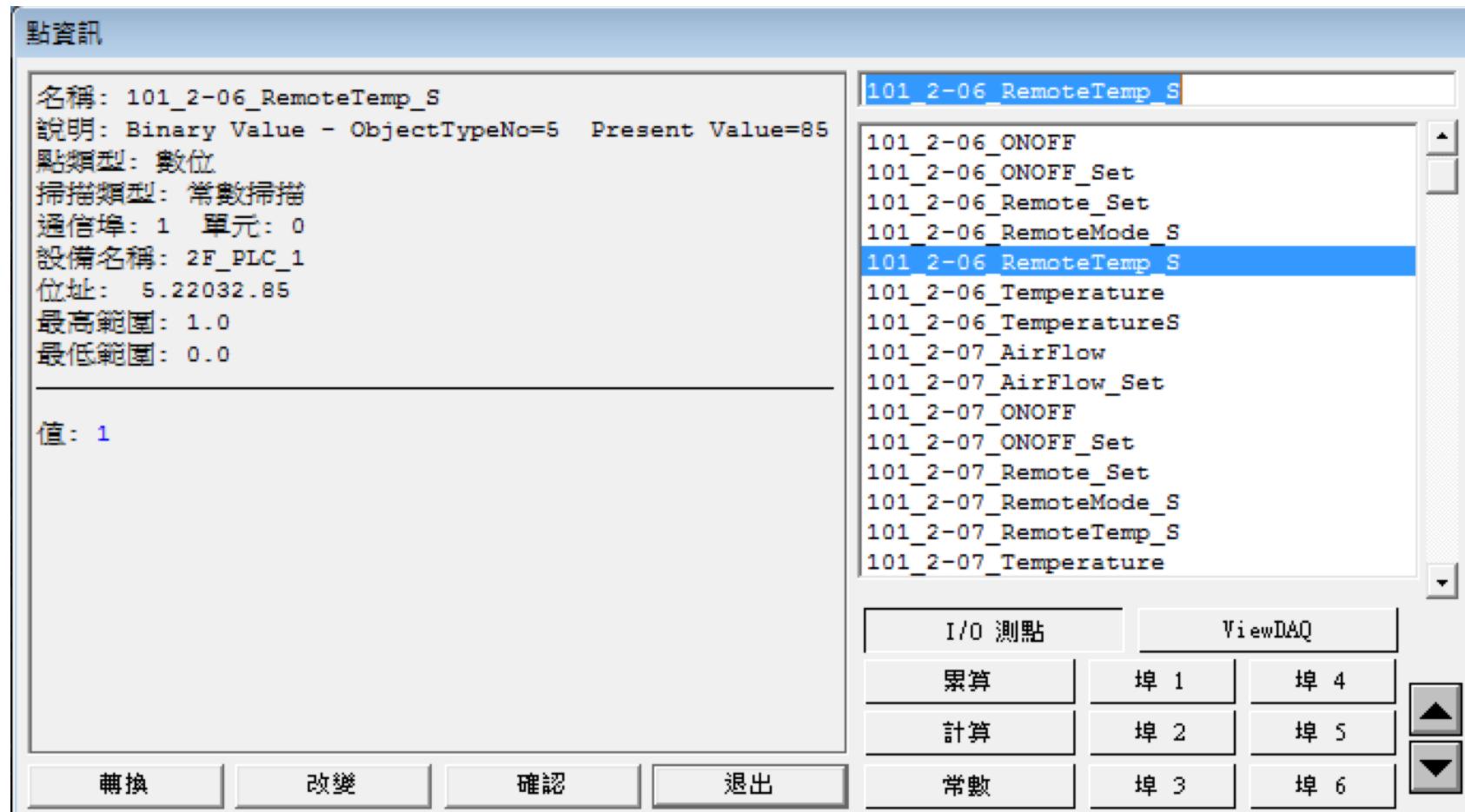
節點類型	專業版		
節點名稱	[redacted]		
節點描述	空調		
監控節點IP位址	140.111.111.111		
主要TCP埠	0	次要TCP埠	0
節點遠端	0		
遠端存取代碼			
外送郵件(SMTP)伺服器名稱	192.168.0.100	電子郵件通信埠	0
電子郵件地址			
電子郵件帳戶名稱			
電子郵件密碼			
電子郵件發件人			
報表電子郵件收件人			
報表電子郵件副本收件人			
警報電子郵件收件人			
警報電子郵件副本收件人			
回覆警報電子郵件為確認	否		
監控程序經由電子郵件	否		
監控程序安全代碼			
內送郵件伺服器(POP3)名稱		電子郵件通信埠	0

Analog Input Parameters

302_1-15_RemoteMode_S
302_1-15_RemoteTemp_S
302_1-15_Temperature
302_1-15_TemperatureS
303_1-14_AirFlow
303_1-14_AirFlow_Set
303_1-14_ONOFF
303_1-14_ONOFF_Set
303_1-14_Remote_Set
303_1-14_RemoteMode_S
303_1-14_RemoteTemp_S
303_1-14_Temperature
303_1-14_TemperatureS
305_1-11_AirFlow
305_1-11_AirFlow_Set
305_1-11_ONOFF
305_1-11_ONOFF_Set
305_1-11_Remote_Set
305_1-11_RemoteMode_S
305_1-11_RemoteTemp_S
305_1-11_Temperature
305_1-11_TemperatureS
306_1-12_AirFlow
306_1-12_AirFlow_Set
306_1-12_ONOFF
306_1-12_ONOFF_Set
306_1-12_Remote_Set
306_1-12_RemoteMode_S
306_1-12_RemoteTemp_S
306_1-12_Temperature
306_1-12_TemperatureS

測點屬性 刪除	
測點: 1•2F_PLC_1•101_2-06_AirFlow_Set	
測點類型	點 (數位)
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	否
資料記錄	否
資料記錄界限值	3 %
寫到動作記錄	是
唯讀	否
保存前一個值	否
初始值	0
安全區域	0
安全等級	0
狀態 0	0
狀態 1	1

PLC Binary Value

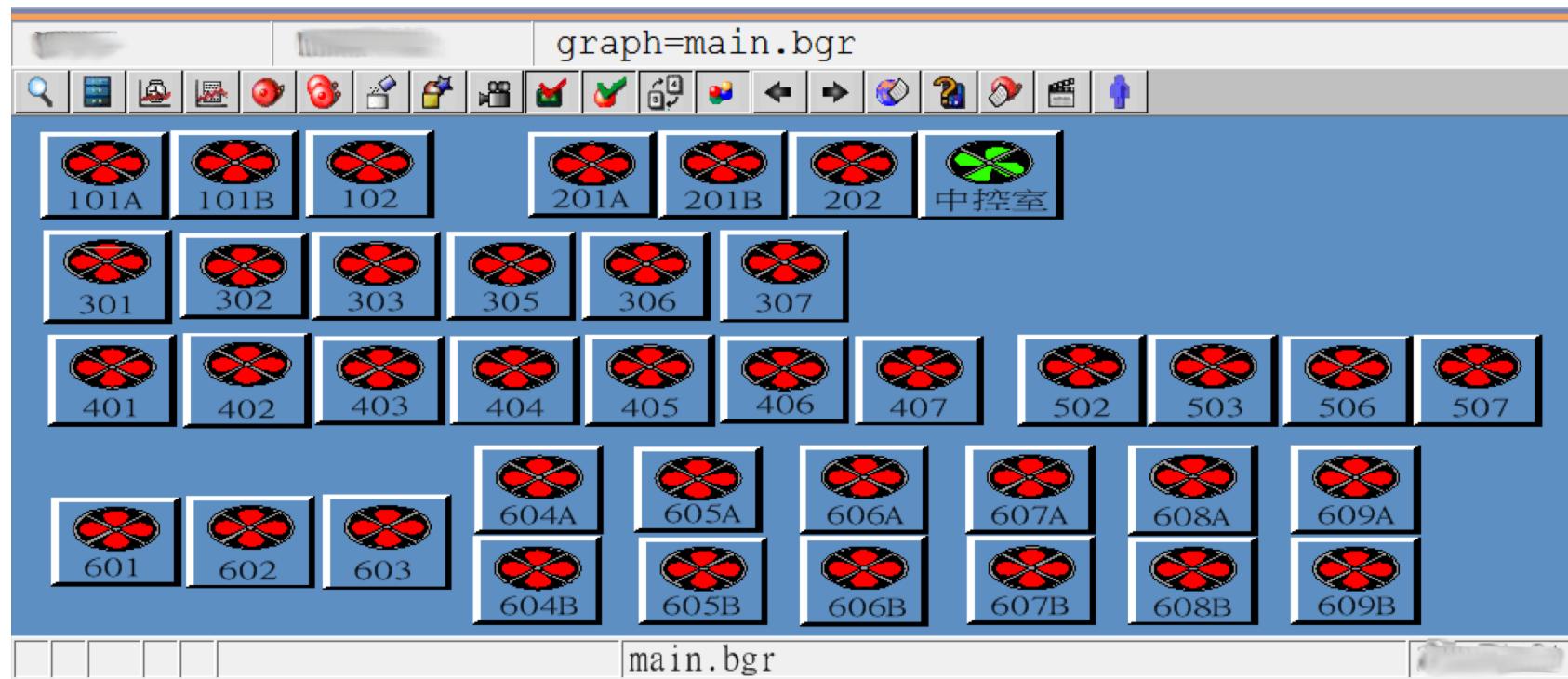


Parameter Update

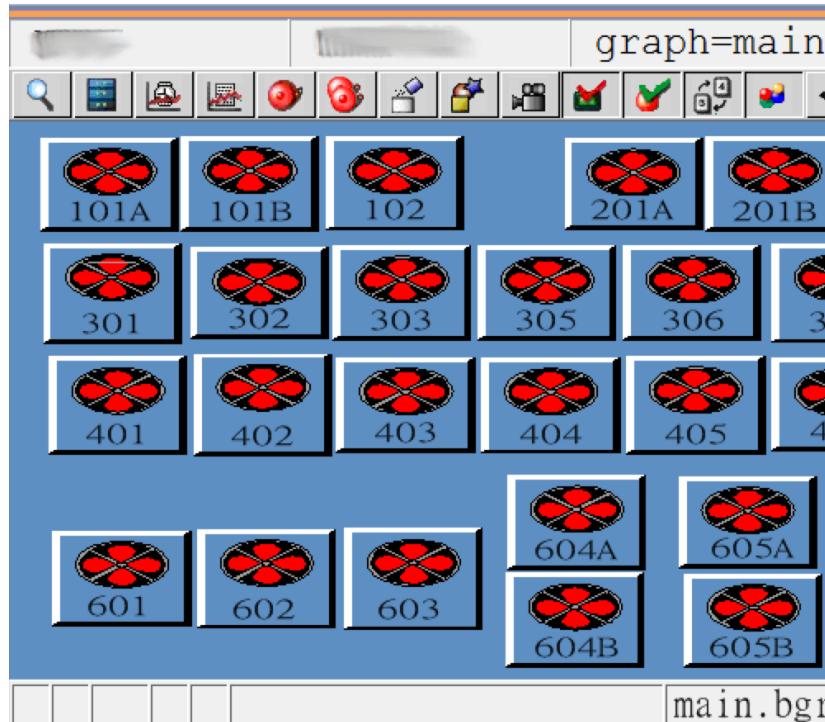
更新測點 [取消] 提供

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 Output, 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	<input type="radio"/> 是 <input checked="" type="radio"/> 否
資料記錄	<input type="radio"/> 是 <input checked="" type="radio"/> 否
資料記錄界限值	3 %
寫到動作記錄	<input checked="" type="radio"/> 是 <input type="radio"/> 否
唯讀	<input type="radio"/> 是 <input checked="" type="radio"/> 否
保存前一個值	<input type="radio"/> 是 <input checked="" type="radio"/> 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

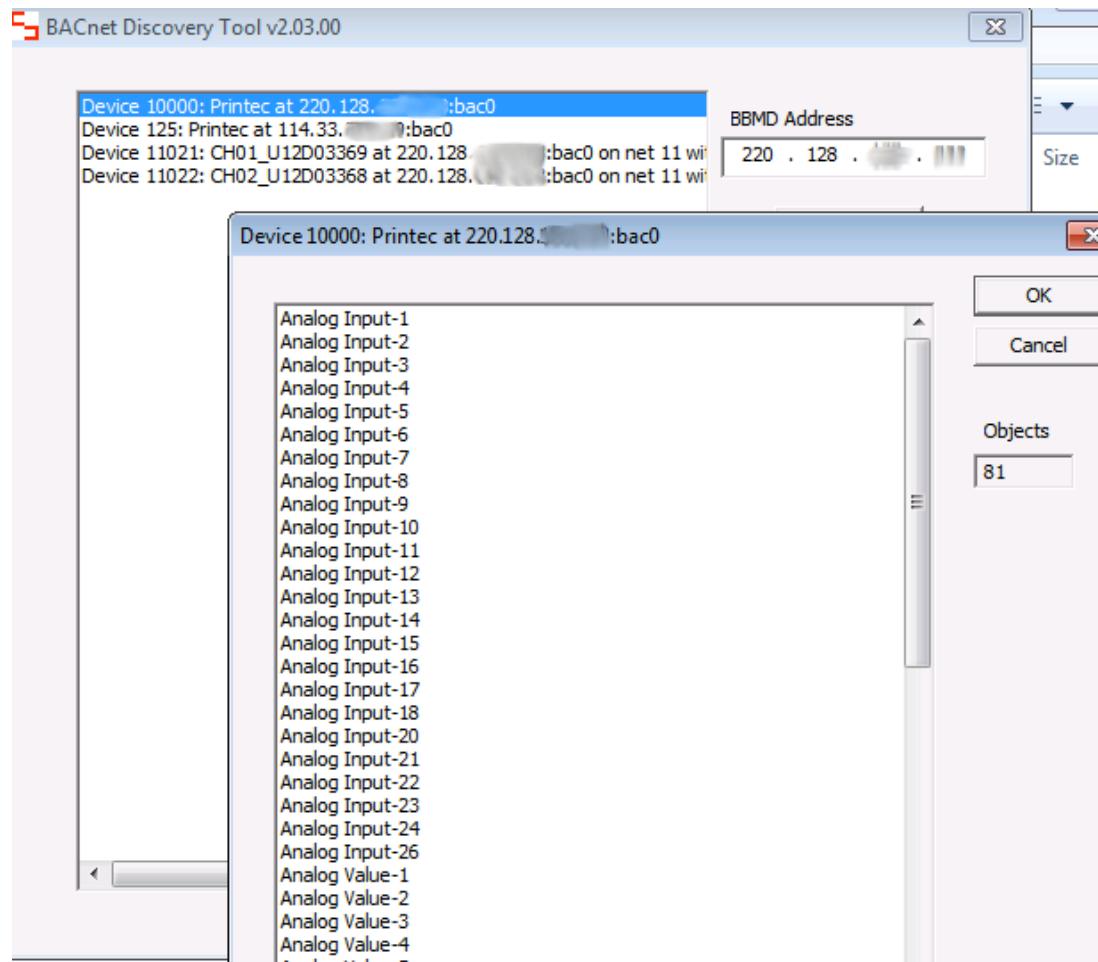


Turn Off the Aircon and Go Home?



Life Is Harder without HMI, But ...

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



Device 11021 / 11022

Device Object Properties

Object ID	11021
Object Name	CH01_U12D03369
Status	Operational
Vendor Name	Trane
Model Name	BCI-C
Firmware Revision	4.00.005
Application Software Version	4.00.005
Protocol Services Supported	LIFE SAFETY OPERATION TIME SYNCHRONIZATION UTC TIME SYNCHRONIZATION WHO HAS
Protocol Object Types Supported	ANALOG INPUT BINARY INPUT CALENDAR COMMAND DEVICE
Local Time	31:63:231.8
Local Date	Tuesday 59 0 11537

OK Cancel

Device Object Properties

Object ID	11022
Object Name	CH02_U12D03368
Status	Operational
Vendor Name	Trane
Model Name	BCI-C
Firmware Revision	4.00.005
Application Software Version	3.00.005
Protocol Services Supported	ACKNOWLEDGE ALARM ADD LIST ELEMENT ATOMIC READ FILE ATOMIC WRITE FILE DEVICE COMMUNICATION CONTROL
Protocol Object Types Supported	ANALOG INPUT ANALOG OUTPUT ANALOG VALUE BINARY INPUT BINARY OUTPUT
Local Time	17:58:39.0
Local Date	Friday 6 24 2015

OK Cancel

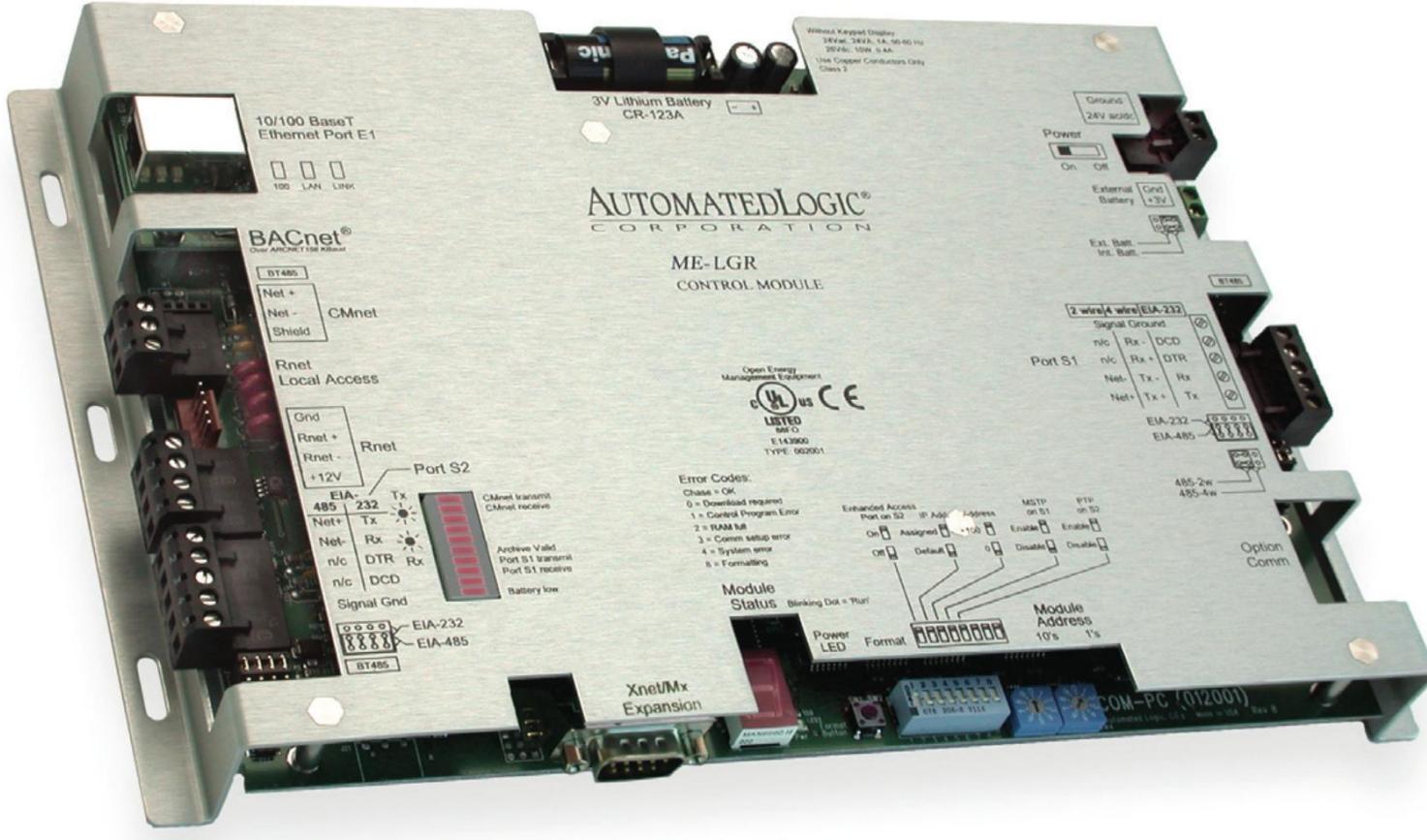
Analog Inputs

```
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|chlrv-1 0.000000
Analog Input-4 Evaporator Approach Temperature Circuit 1|chlrv-1 0.000000
Analog Input-5 Condenser Approach Temperature Circuit 1|chlrv-2 6.319977
Analog Input-6 Evaporator Approach Temperature Circuit 1|chlrv-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_compresso 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
```

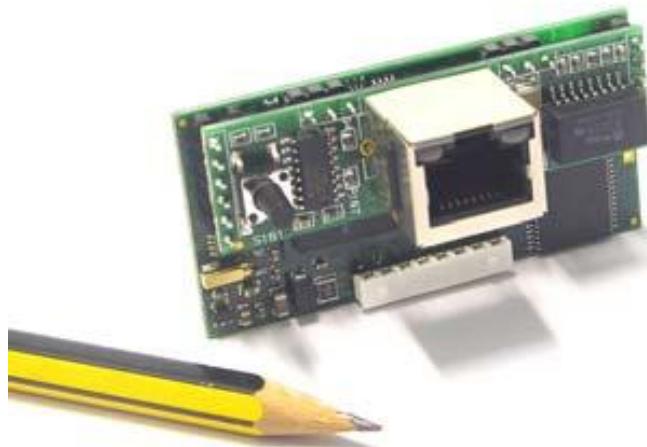
Output = Modifiable

```
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-ii021
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

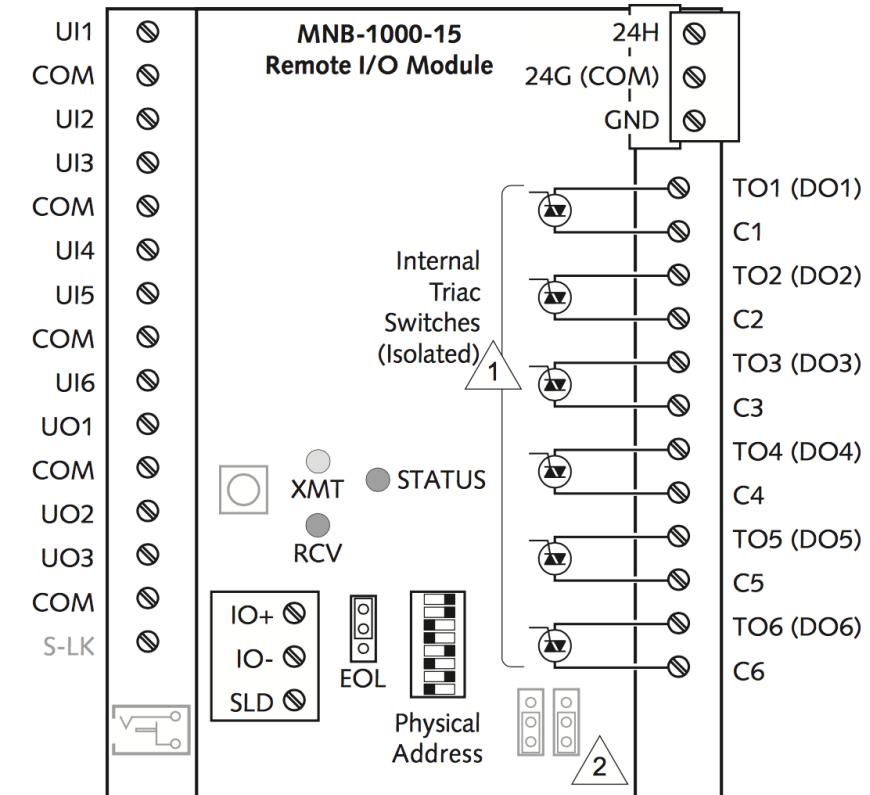
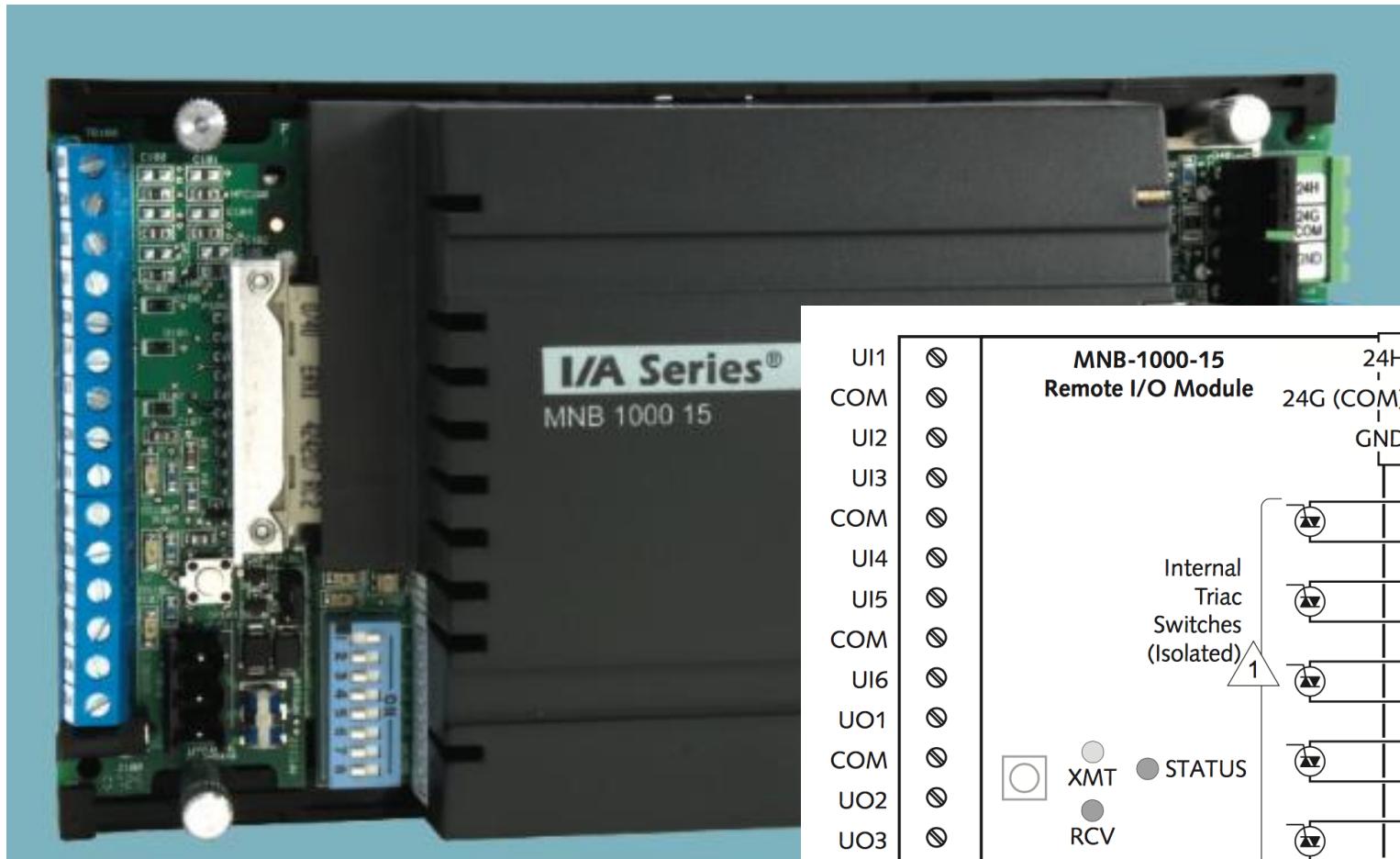


```
Connected to 203. [REDACTED]
Escape character is '^]'.

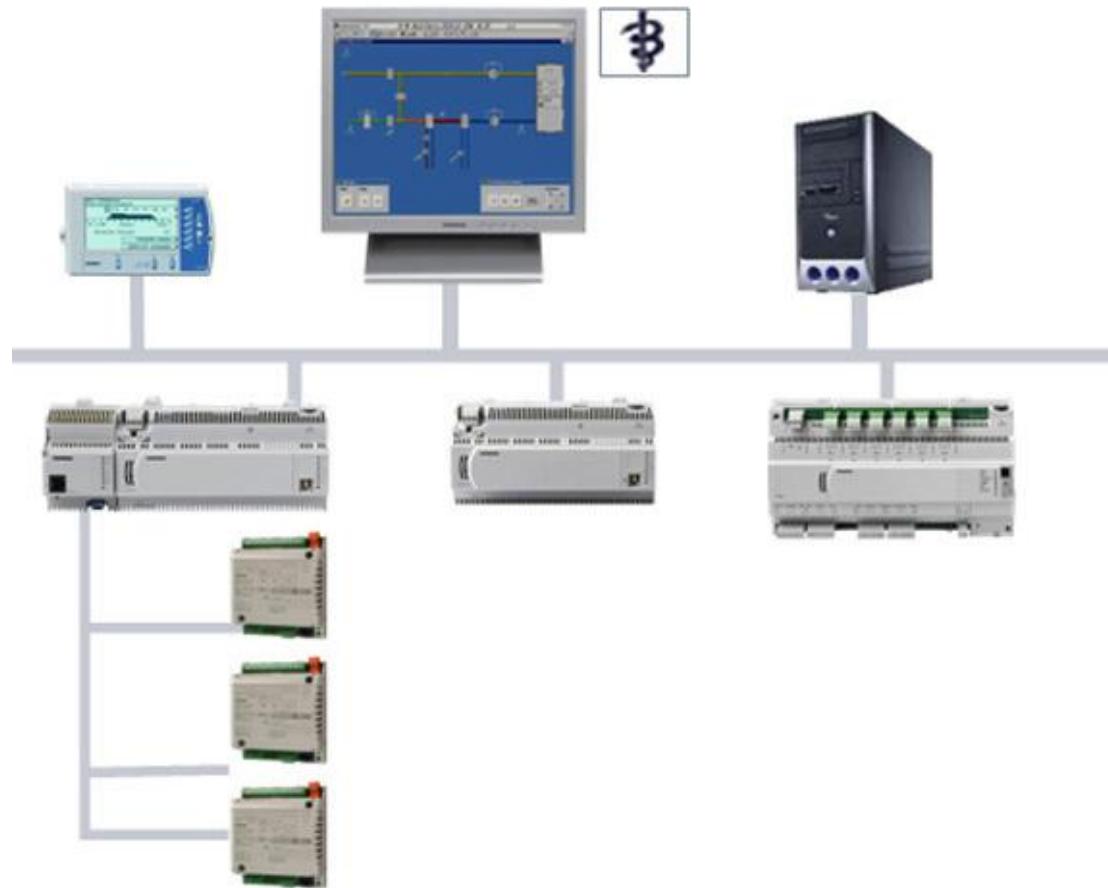
Linux 2.4.21-rmk1 (pCOWeb) (ttya1)

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



Siemens Insight



Other than BACnet

- 59 Ethernet/IP in TW
 - N**U Library
 - N**U Bio Center
 - N**U Men's Dormitory
 - N**U 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

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



Powermonitor 1000 Information

Date and Time:	March 16, 2005 17:43:31
Warranty ID:	3629928000
Catalog Number:	1408-EM3A-ENTA
Manufactured Date:	July 23, 2014
Operating System Version:	330

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

Display and Configuration Menu

- Home
- Display Metering Information
- Display Status
- Execute Commands
 - Restore Factory Defaults
 - Clear Status Counts
 - Clear Energy Registers
 - Clear Energy Log
- Configure Options
- Catalog Number Breakdown
- Go To ab.com

Force KYZ Condition

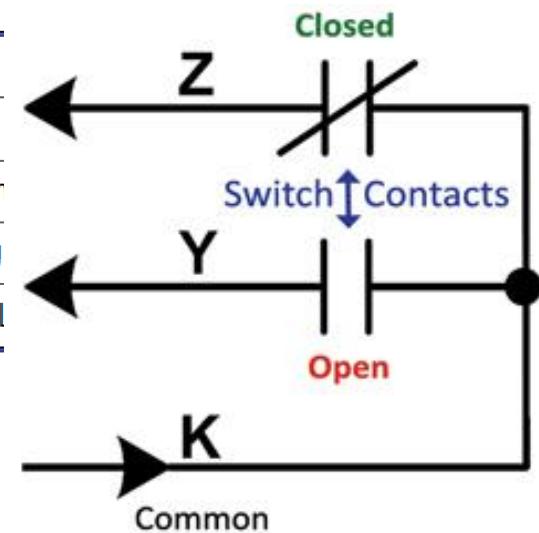
- Force KYZ On
- Force KYZ Off
- Remove KYZ Force



KYZ Pulse

Display and Configuration Menu

- Home
- Display Metering Information
- Display Status
- Execute Commands
 - Restore Factory Defaults
 - Clear Status Counts
 - Clear Energy Registers
 - Clear Energy Log
- Force KYZ Condition
 - Force KYZ On
 - Force KYZ Off
 - Remove KYZ Force
- Perform Wiring Diagnostics
- Reset Powermonitor 1000
- Perform Troubleshooting



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

Energy Results

The screenshot shows a software interface for managing powerline data. On the left, there's a vertical menu bar with sections like Home, Display Metering Information, Display Status, Execute Commands, Configure Options, Catalog Number Breakdown, and Go To ab.com. Below this is a section for Date and Warranty, Catalog Number, Manufacturer, and Operating. The main area has a red header bar with the text "Powerline Management". Below it, the title "Energy Results" is centered above a table.

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
15	VA/Wk Net (VA/Wk)	0000.100

Voltage Monitor

The screenshot shows a software interface for power monitoring. At the top, there's a red header bar with the text "Power and Energy Management Solutions" and "Meeting the Changing Demands for Power and Energy Management". Below this is a blue navigation bar with the text "Powermonitor 1000 Display and Configuration". On the left, there's a sidebar with the "Allen-Bradley" logo and a menu with options like "Display and Configuration Menu", "Home", "Display Metering Information", "Display Status", "Execute Commands", "Configure Options", "Catalog Number Breakdown", and "Go To ab.com". The main area contains a table with 14 rows, each representing a different power measurement. The columns are "Element", "Item Name (unit)", and "Value". The data is as follows:

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:████████
Serial No.     :
Firmware version : 3.4 Build 11080114
System uptime   : █████ 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

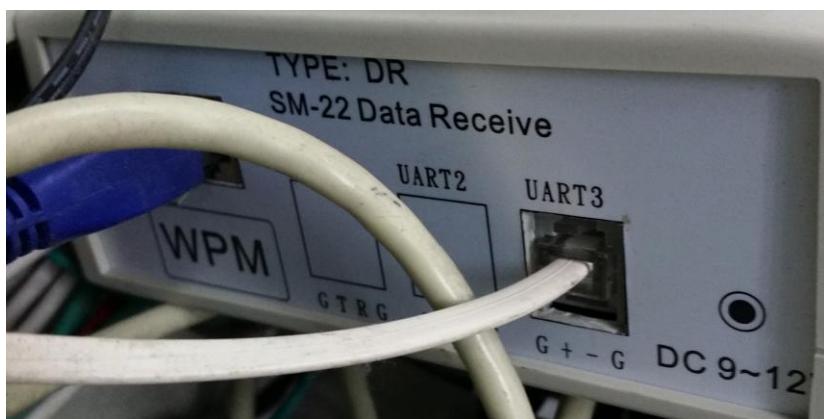
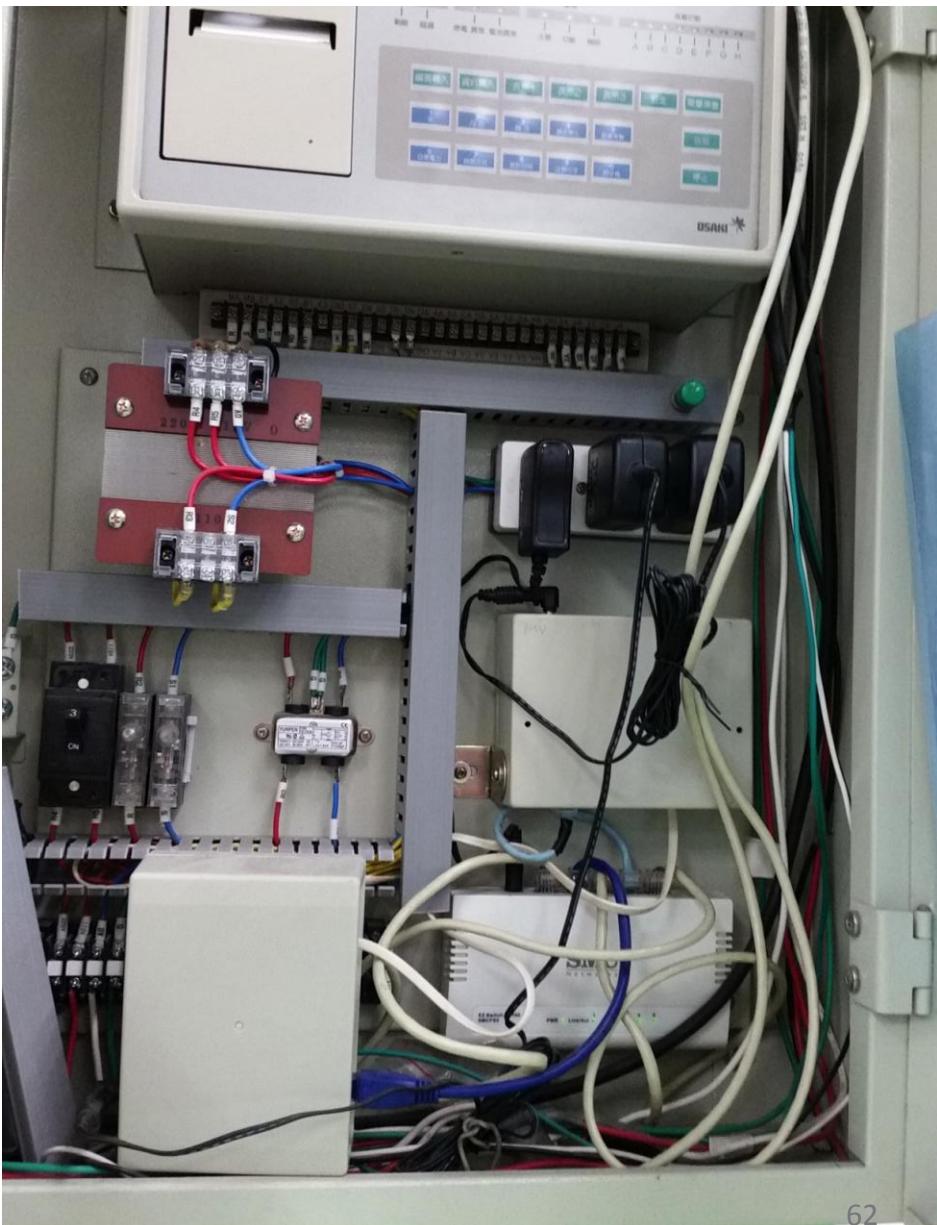
-->< Main menu->Serial settings->Port 1 ><
(1) Port alias
(2) Baud rate
(3) Data bits
(4) Stop bits
(5) Parity
(6) Flow control
(7) FIFO
(8) Interface
(v) View settings
(m) Back to main menu
(q) Quit
```

- 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 : 192.168.1.100  
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 ---

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

Contract capacity: 4,700kW

Peak capacity: 5,216kW

Minimum capacity: 2,752 kW



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. 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。

(5) 巨額採 6. 支援 BACnet or Modbus TCP / IP or URL 等通訊定。

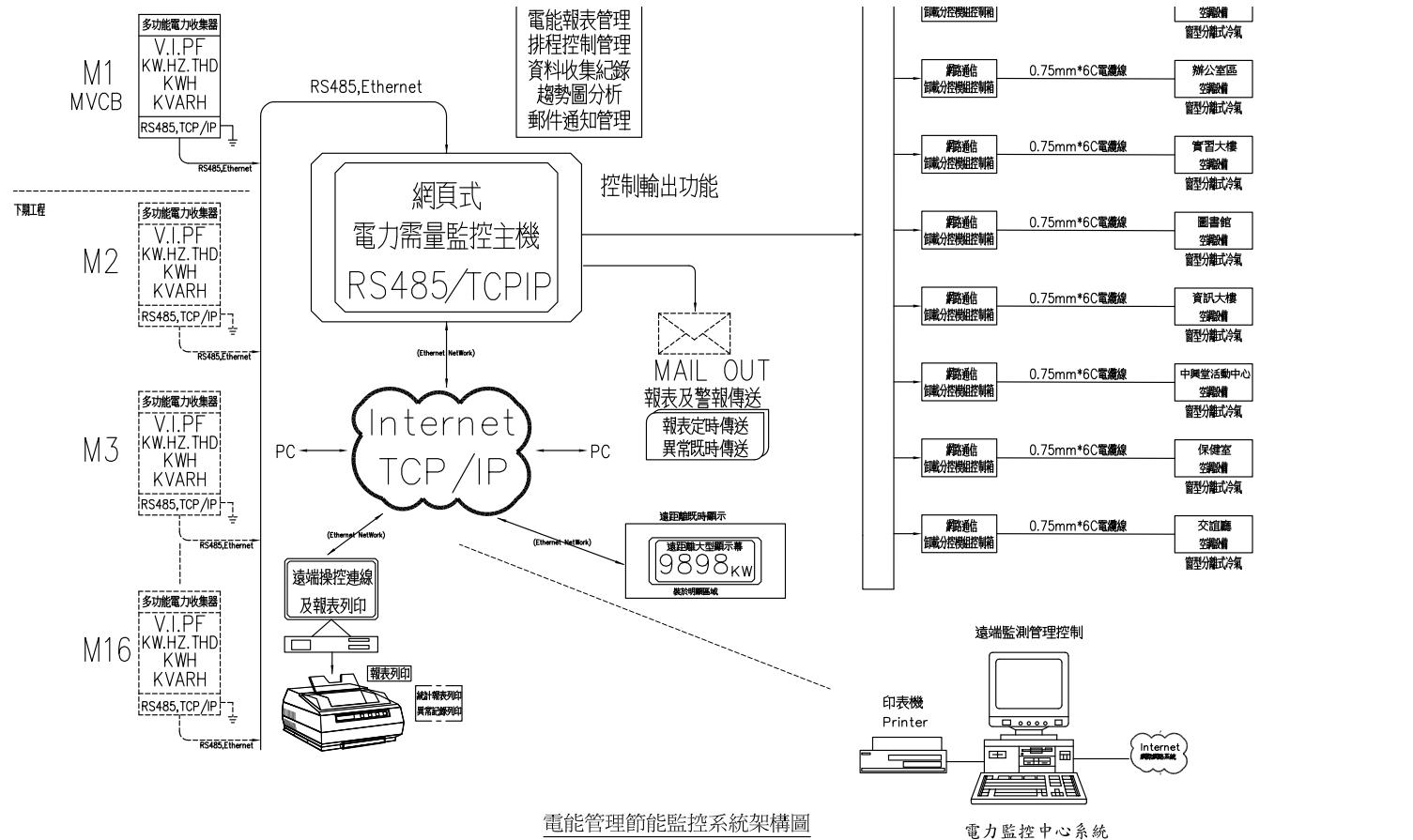
7. 可以透過 WEB 方式輕易管理及設定組態。

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	<p>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)。</p> <p>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。</p> <p>11.可同時具有 MODBUS Ethernet TCP/IP 及 RS-485 RTU 之通訊能力。</p> <p>12.每台整合通訊介面器至少可連接 8000 MODBUS 監控點。</p> <p>13.提供 24 個可軟體配置的通用點，這些點包括：</p> <p>(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)。</p> <p>(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)。</p> <p>14.4 個數位輸入點(DI)。</p> <p>(二) 15.8 個數位輸出點(DO)。</p>	1 式

Points in Common

- Subsidized
- Public Tender
- Contracted

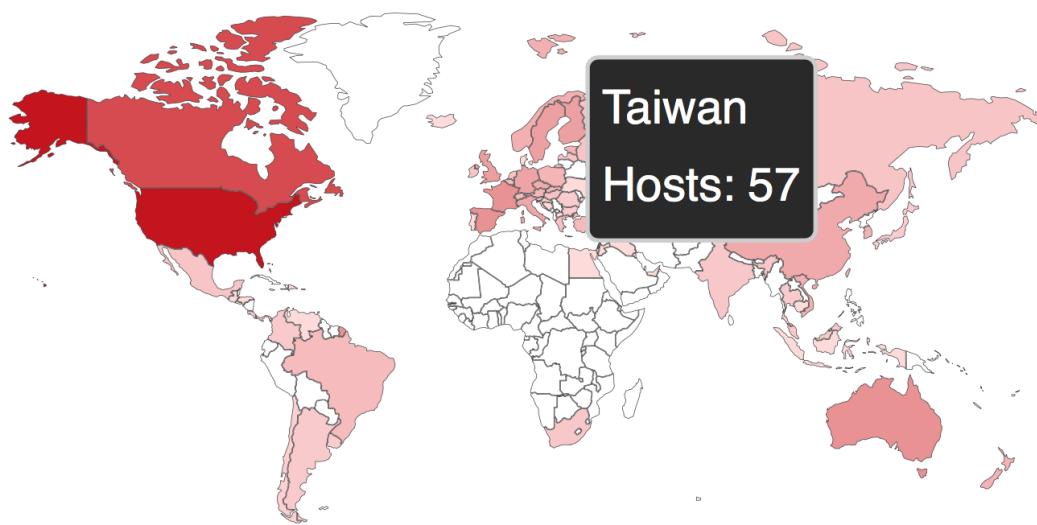
Note

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

Suggestions

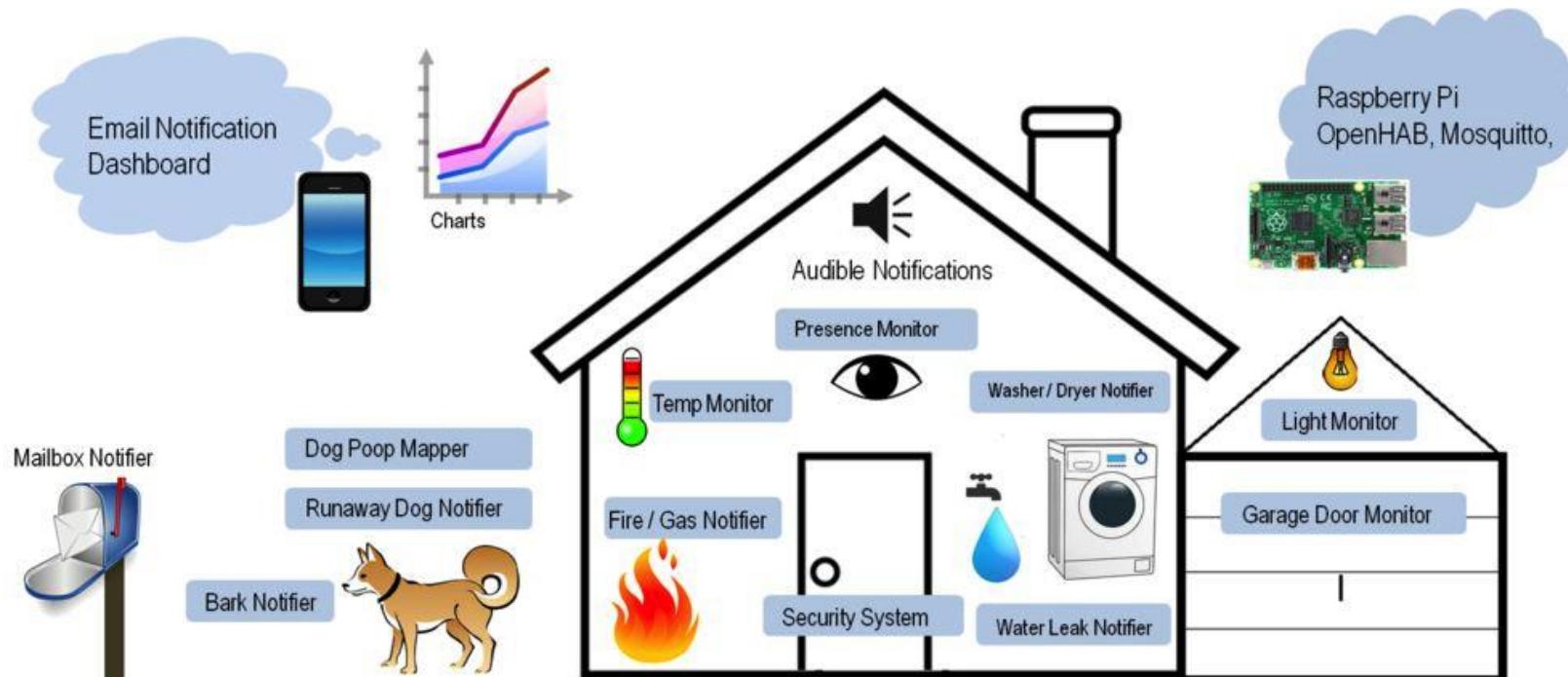
- Password
- Use private IP. No, not corporate LAN
- Firewall, SDN or tagged VLAN
- Upgrade / Patch
- Contract with a pentester

Port 47808, TW: 57/12,358



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

Home Automation with Arduino & RPi

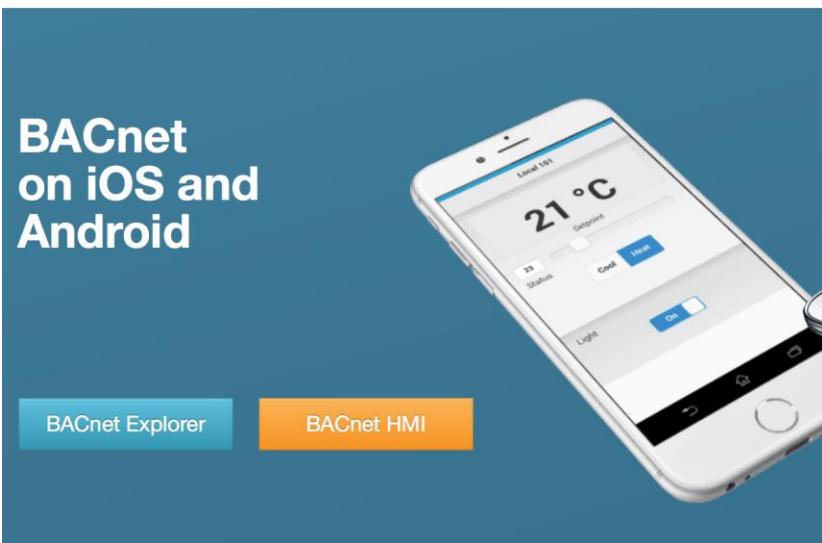


Project at <http://www.instructables.com/id/Uber-Home-Automation-w-Arduino-Pi/>

Control System on Your Hand

bacmove

Home BACnet Explorer BACnet HMI Contact



Homepage of <http://bacmove.com>

BACmove	
Unnamed List	ANALOG VALUE 1 Demo Device 1 - 123 Analog Value - 1 21
Temperature	ANALOG VALUE 1 Demo Device 1 - 123 Analog Value - 1 21
Lighting	G VALUE 0 Device 1 - 123 Value 10 22
Power	ANALOG VALUE 0 Demo Device 1 - 123 Analog Value - 0 22
	ANALOG VALUE 1 Demo Device 1 - 123 Analog Value - 1 21
	ANALOG VALUE 1 Demo Device 1 - 123 Analog Value - 1 21

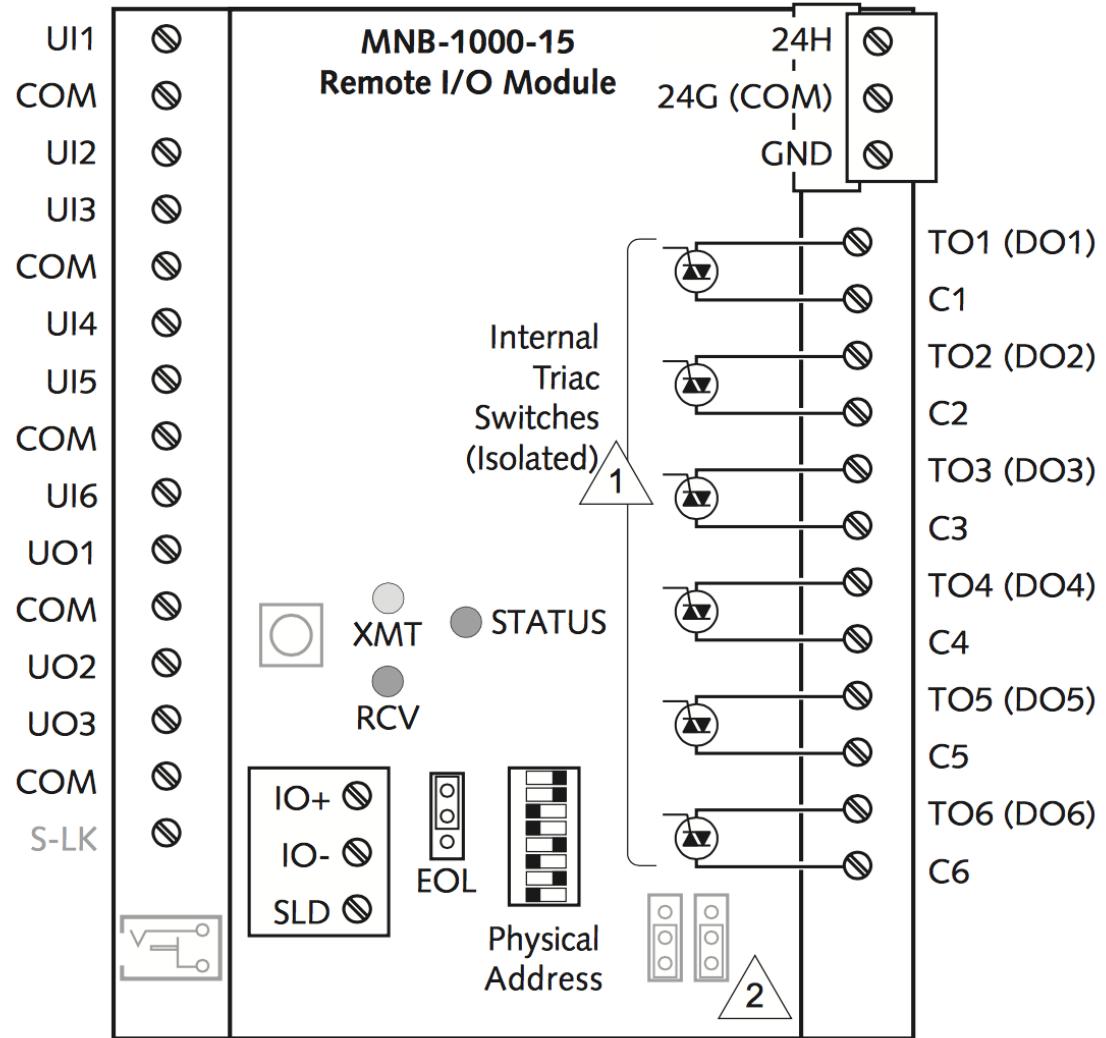
Our suggestion:

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.

Questions?



TAC-MNB Module





MOXA NPort 5130 IN BOX

Item condition: **New**

Time left: 14d 06h 8/15, 10:25PM

Quantity: 1 More than 10 available

Price: **US \$149.50**

Approximately
NT\$ 4,720

[Buy It Now](#)

[Add to cart](#)

[Make Offer](#)

[Add to watch list](#)

[Add to collection](#)



CAREL pCO1000CS0

Item condition: --

Time left: 5h 34m 9s Today 9:40PM

Starting bid: **US \$199.99**

Approximately
NT\$ 6,314

[0 bids]

[Place bid](#)

Enter US \$199.99 or more

[Add to watch list](#)

[Add to collection](#)

Free
Shipping



MNB-1000 I/O PLANT CONTROLLER MICRONET BACKPLANE

Item condition: **New**

Price: **US \$321.60**

Approximately
NT\$ 10,153

[Buy It Now](#)

[Add to cart](#)

[Add to watch list](#)

[Add to collection](#)

New
Condition

Longtime
Member

MOXA NPort 5130
US\$75 - 149 (new)

Carel pCO1000 US\$200
pCOWEB, unknown

MNB-1000 US\$321.60