context

Open Sesame – Bypassing Building Management Controls and Tradecraft

Dan Kennedy – Senior Consultant

BSIDES CANBERRA

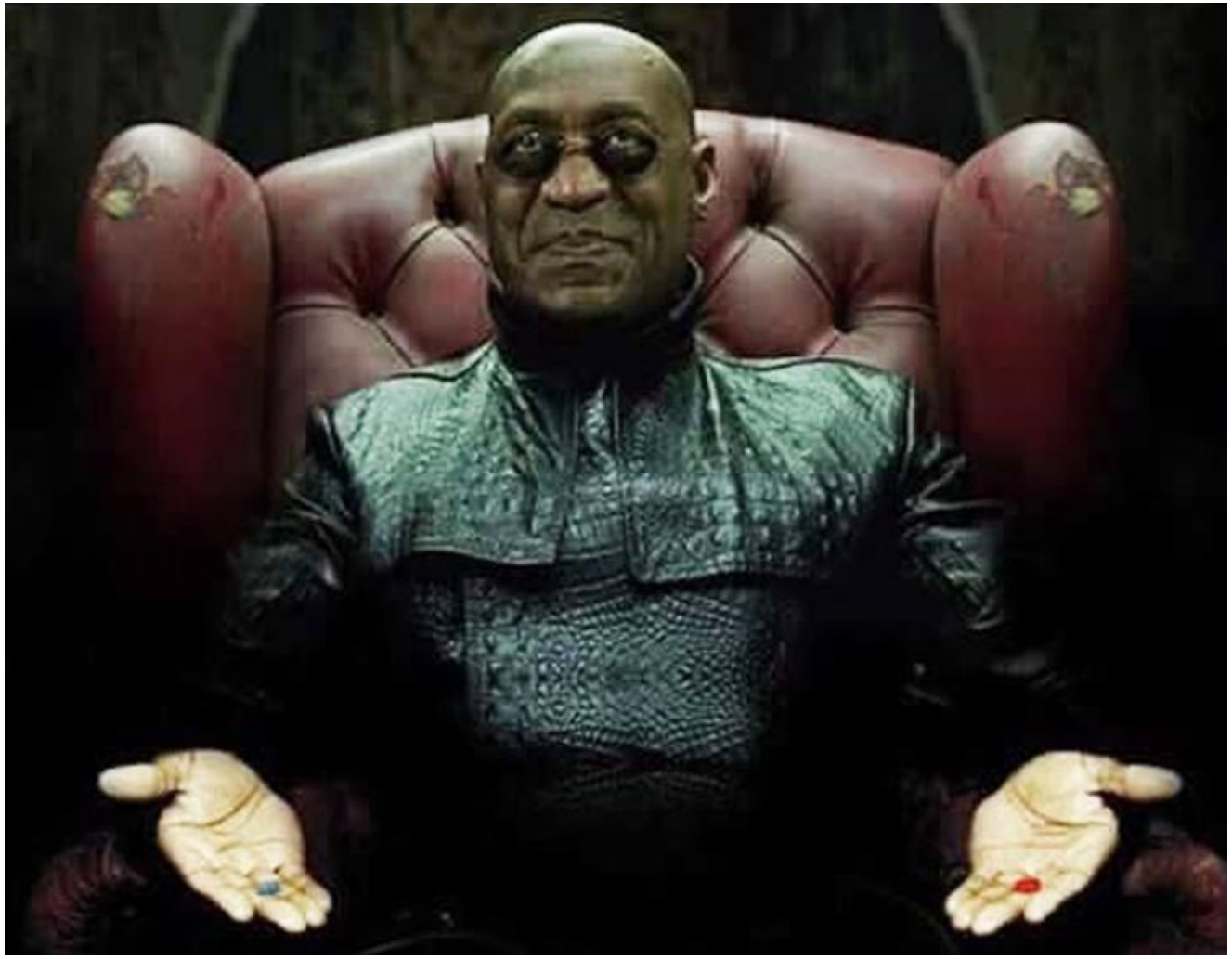
19/04/2016

context

Background Info

- Why this talk?
- Scope
- Where did our Vigilance go?
- </rant>

Blue?



Red?

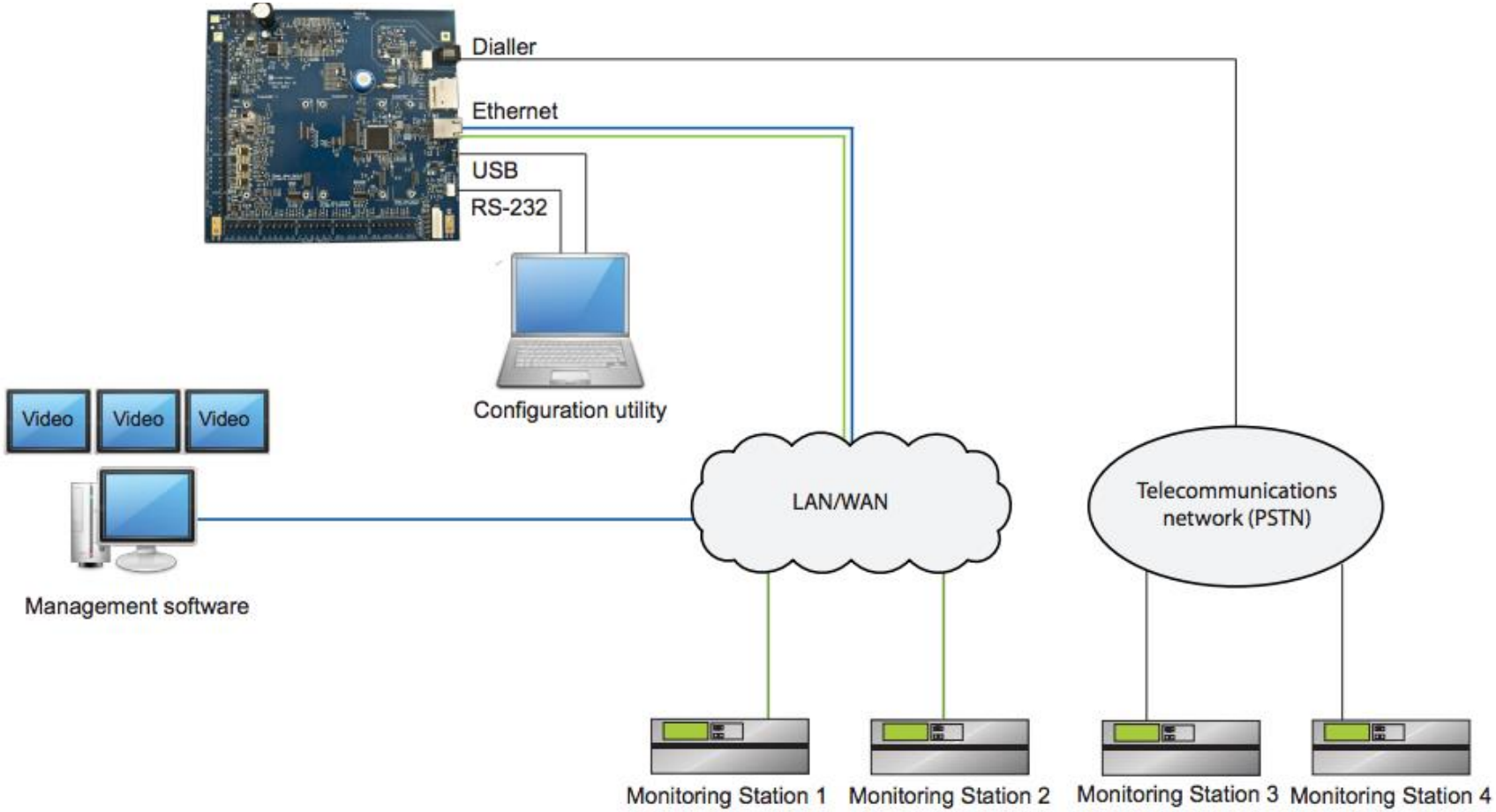
context

BMS environment

context

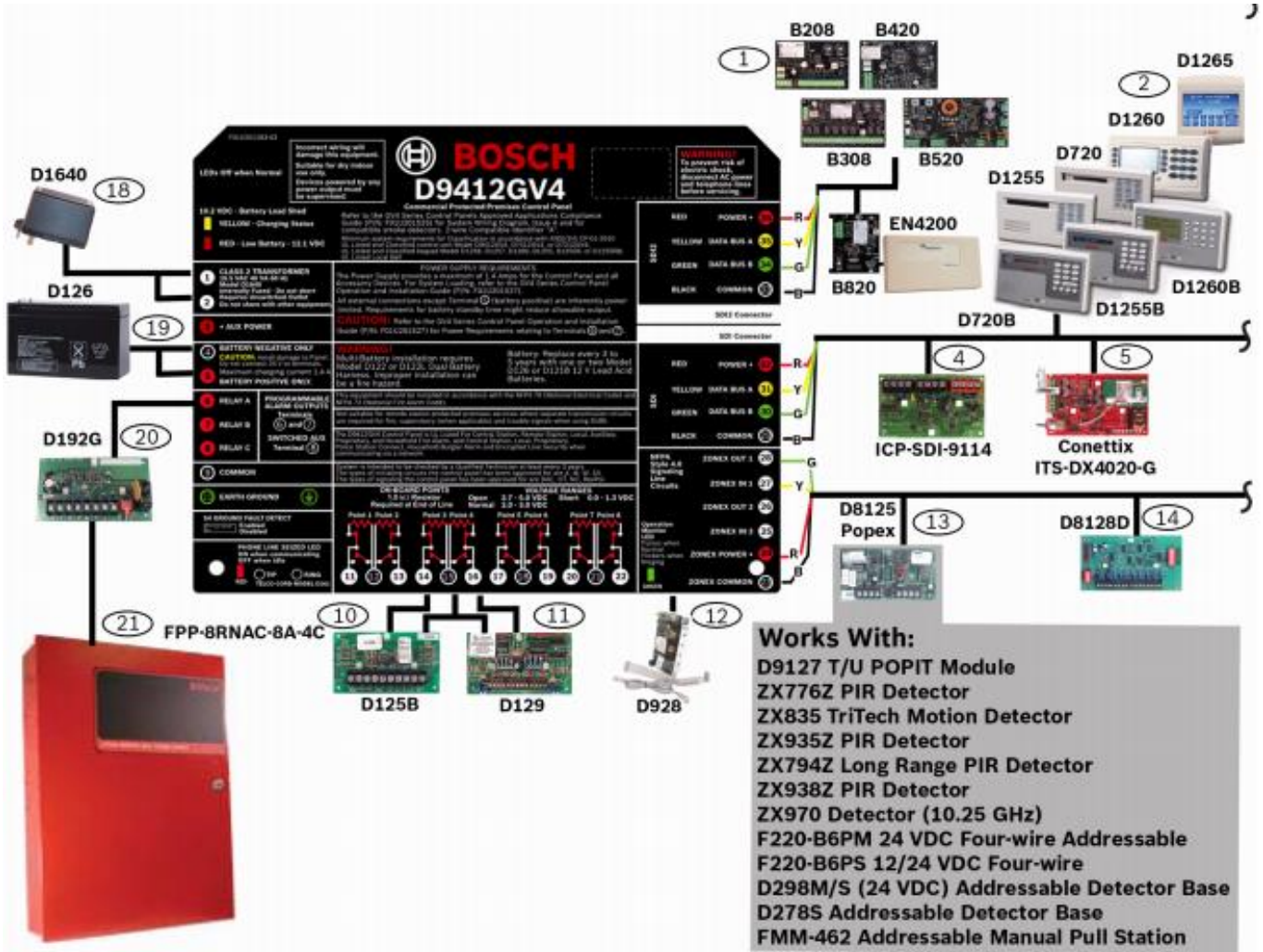
Physical Security Controls

Controller Systems Diagram



context

Component Diagram



Controller Enclosures

context

> D102 Replacement Key

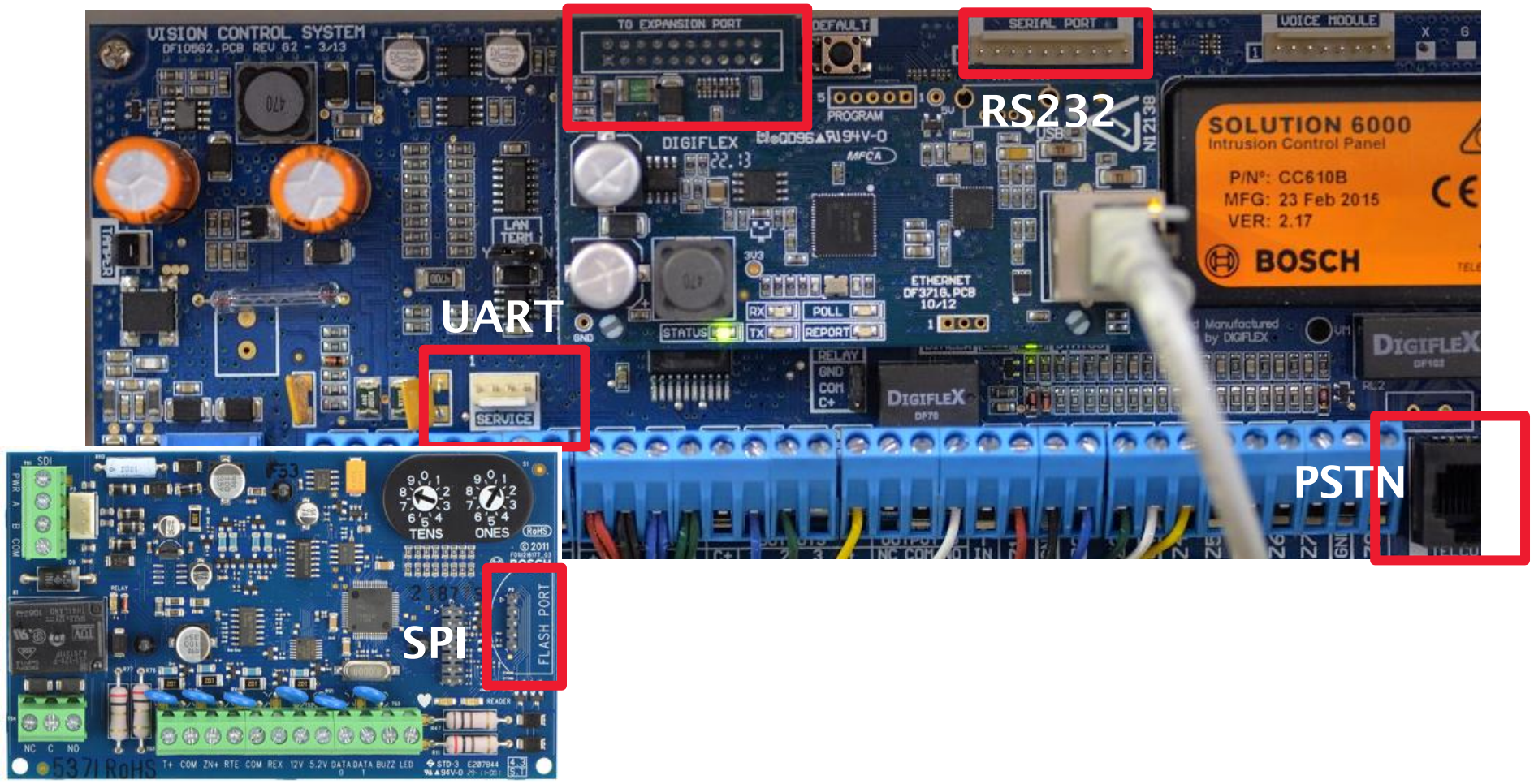
Product Page

context

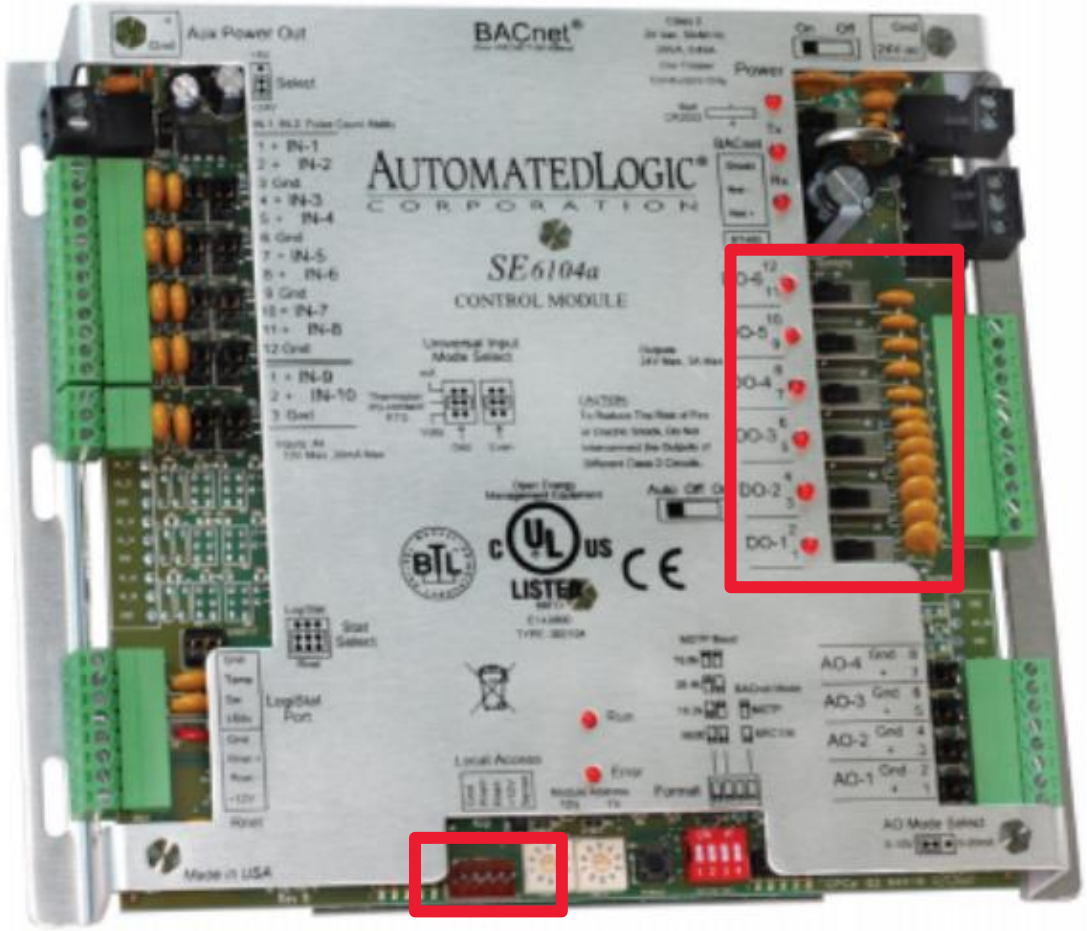
Enclosure Bypass

context

Control Panels



BacNet Native Controller



context

Building Control Protocols

- AS-Interface
- BACnet
- CANopen
- CC-Link
- ControlNet
- DeviceNet
- EtherNet/IP
- EtherCAT
- FIPIO
- FL-net
- Interbus
- Lonworks
- M-Bus
- Modbus Plus
- Modbus RTU & Modbus-TCP
- POWERLINK
- Profibus
- Profinet-IO
- Sercos

Net Enumeration

- Security Controller (BOSCH) **TCP/UDP Port 7700**
- Modbus: Master/Slave – **TCP Port 502**
- BACnet: Master/Slave – **UDP Port 47808**
- LonWorks/LonTalk: Peer to Peer - **Port 1679**
- DNP3: Master/Slave – **TCP Port 20000**
- Niagra Fox **TCP Port 1911**
- Zigbee – **TCP Port 17729-17756**
- Rockwell PLC **TCP/UDP Ports 2221 UDP 29402, 1434**
- FactoryTalk Port **TCP/UDP 1330-1332, 3060**

Tools

- Lots of proprietary ones
- BacNet Attack Framework
- ModBus SMOD Exploitation Framework

context

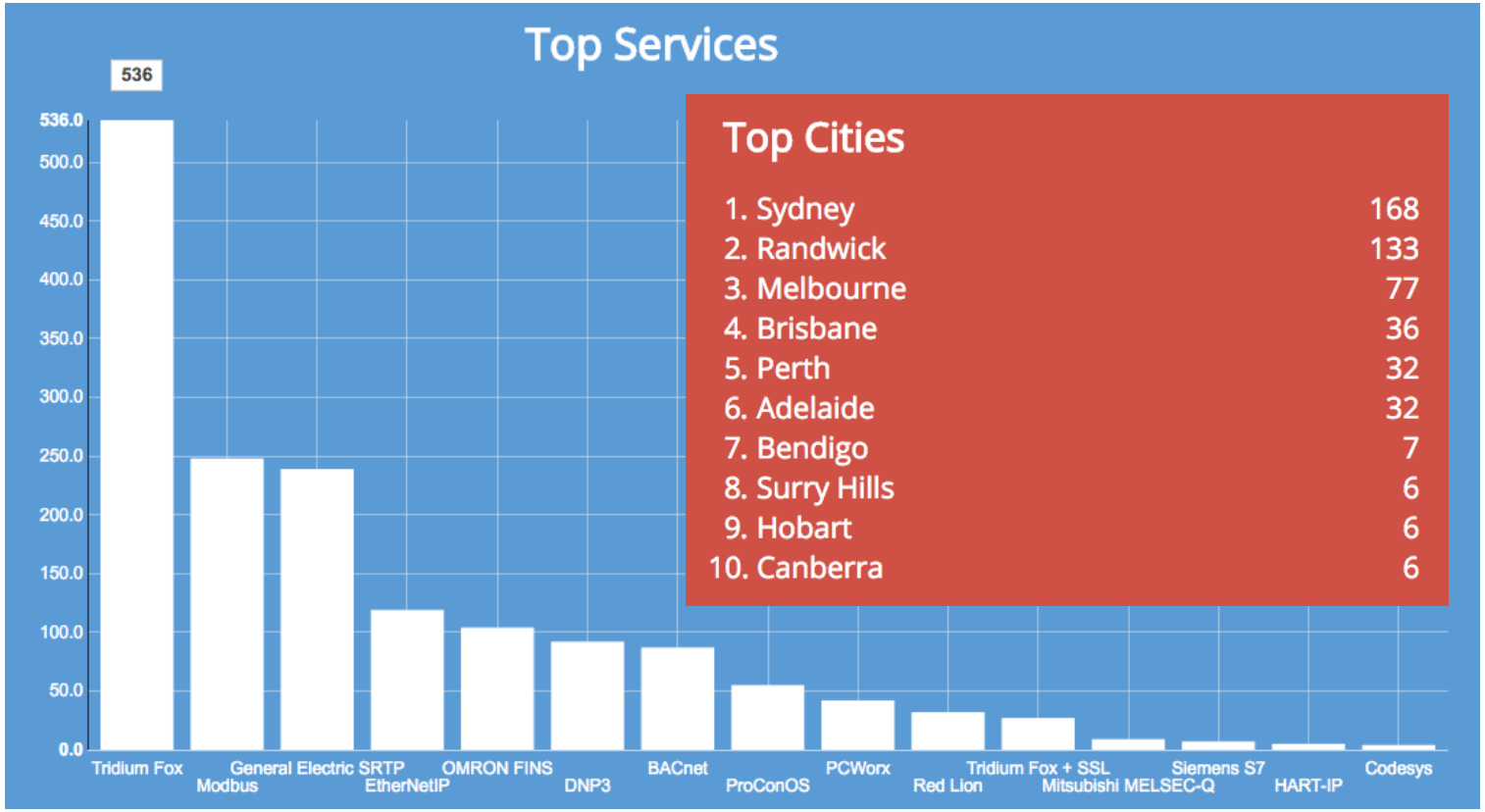
Exposures - Internet

Total Results: 2,436

Top Services	
DNP3	769
Tridium Fox	539
Modbus	248
General Electric SRTP	246
BACnet	181

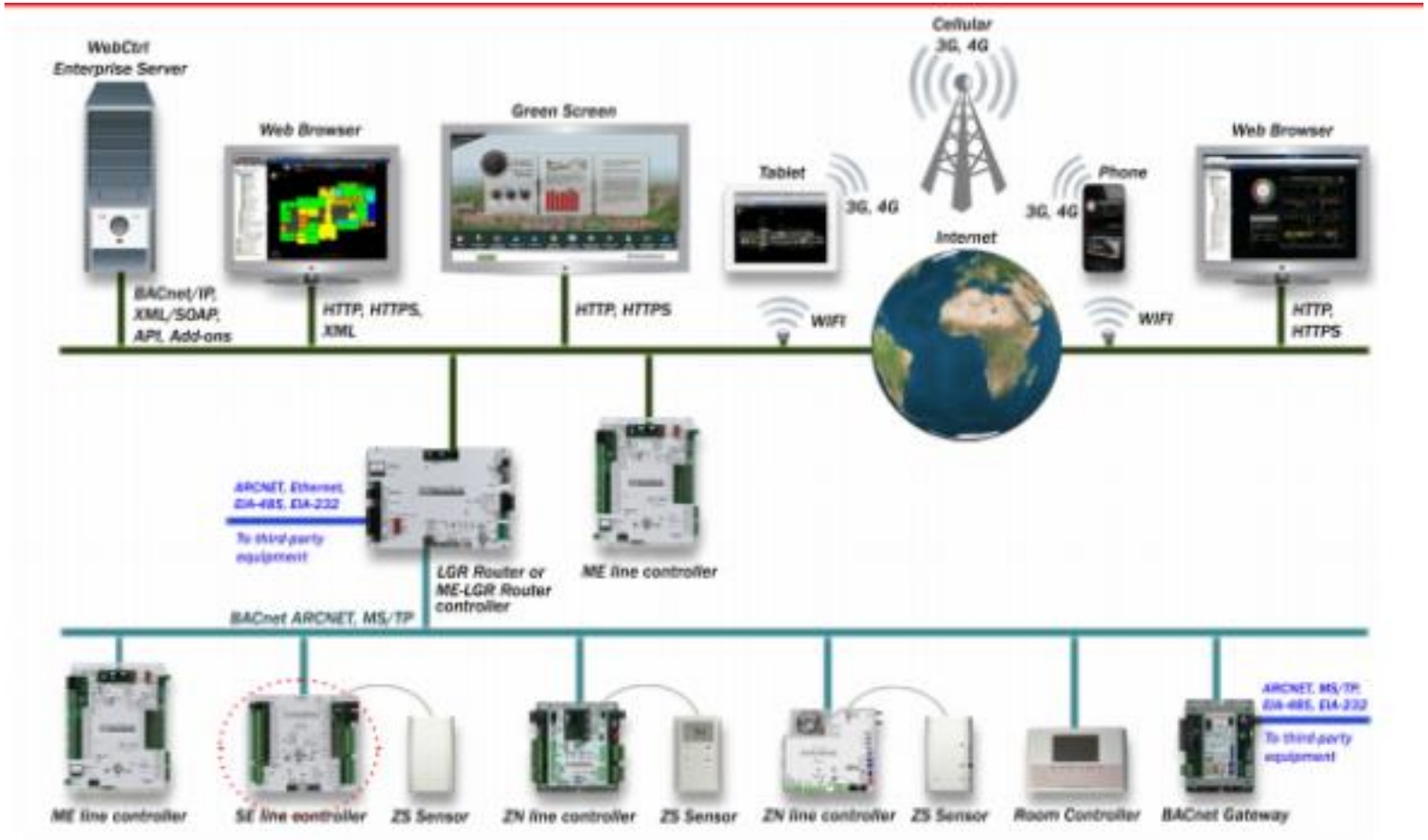
Top Organizations	
Telstra Internet	946
Pacific Internet (Australia...	172
iiNet Limited	141
Bucan Holdings Pty Ltd	73
TPG Internet	56

Exposure Stats - Current



context

Building Automation Control Architecture



http://www.automatedlogic.com/specsheets/se_cs.pdf

Bacnet Attacks

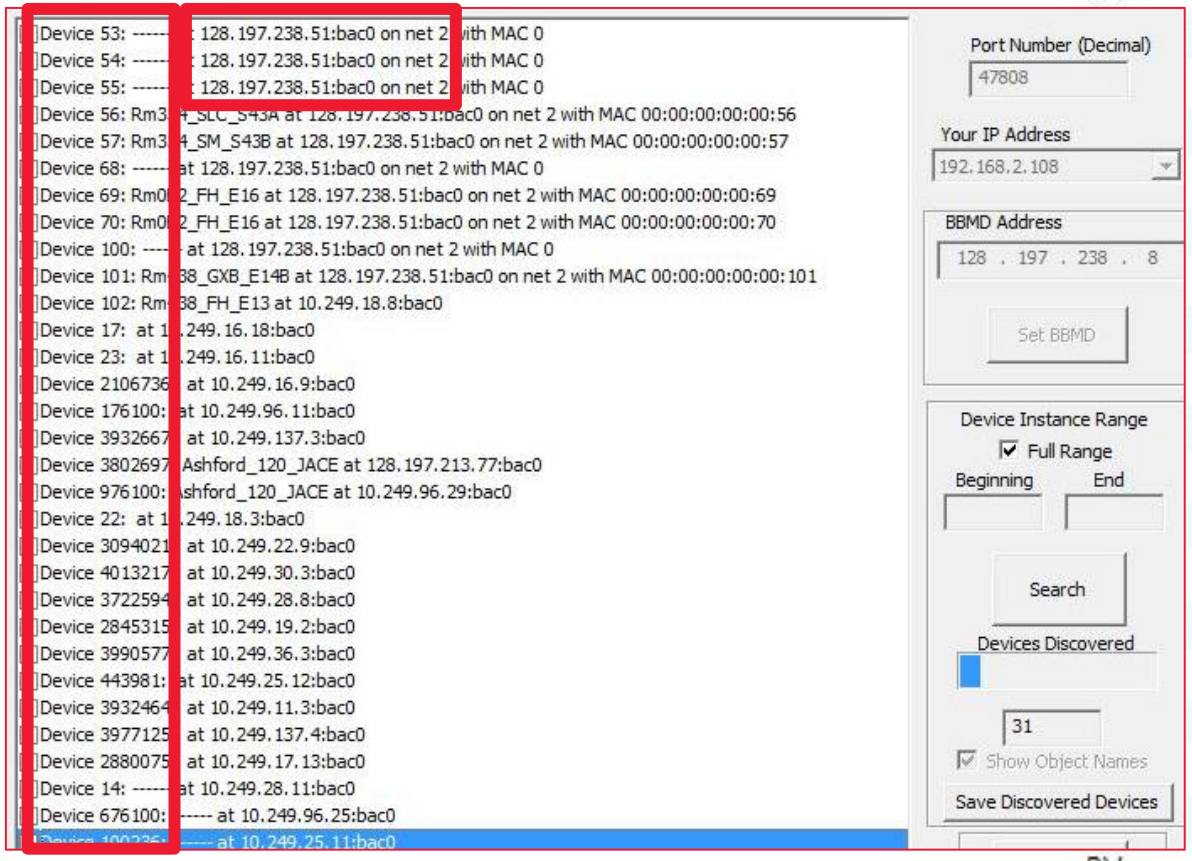
- Enumerate all the Devices
- Announce yourself as a trusted Bacnet Router
- Flood and Takedown entire net
- Arbitrary Command Execution

context

```
⊞ Frame 3: 59 bytes on wire (472 bits), 59 bytes captured (472 bits)
⊞ Ethernet II, Src: Netgear_86:79:23 (e8:fc:af:86:79:23), Dst: BelkinIn_8c:0e:4d (ec:1a:59:8c:0e:4d)
⊞ Internet Protocol Version 4, Src: 192.168.2.108 (192.168.2.108), Dst: 76.[redacted]
⊟ Building Automation and Control Network APDU
    0000 .... = APDU Type: Confirmed-REQ (0)
  ⊟ .... 0010 = PDU Flags: 0x02
      .... 0... = Segmented Request: Unsegmented Request
      .... .0.. = More Segments: No More Segments Follow
      .... ..1. = SA: Segmented Response accepted
    .100 .... = Max Response Segments accepted: 16 segments (4)
    .... 0101 = Size of Maximum ADPU accepted: Up to 1476 octets (fits in an ISO 8802-3 frame) (5)
    Invoke ID: 41
    Service Choice: readProperty (12)
  ⊟ ObjectIdentifier: device, 4194303
    ⊟ Context Tag: 0, Length/Value/Type: 4
        .... 1... = Tag Class: Context Specific Tag
        0000 .... = Context Tag Number: 0
        Length Value Type: 4
      0000 0010 00.. .... .... .... .... .... = Object Type: device (8)
      .... .... ..11 1111 1111 1111 1111 1111 = Instance Number: 4194303
  ⊟ Property Identifier: description (28)
    ⊟ Context Tag: 1, Length/Value/Type: 1
        .... 1... = Tag Class: Context Specific Tag
        0001 .... = Context Tag Number: 1
        Length Value Type: 1
      Property Identifier: description (28)
```


```
        0001 .... = Context Tag Number: 1
        Length Value Type: 1
      Property Identifier: description (28)
```

context



Obj. Type	Inst.-Nc	Present Value	Object Name	Description
DEV	2935851		Cumm_3_5_bCX	
FIL	1		ACCConfiguration	
PR	7007		Import.Prg	
BV	7028	[0, INACTIVE]	Be677BlrHWSAlarm	
BV	7029	[0, INACTIVE]	Be677BlrHWSP1Flt	
BV	7030	[0, INACTIVE]	Be677BlrHWSP2Flt	
BV	7037	[0, INACTIVE]	Be677BoilrComSta	InfNet Controller Comm Status
BV	7033	[0, INACTIVE]	Be677CHWSTempHi	
	7031	[0, INACTIVE]	Be677ExFACWC01A	
	7032	[0, INACTIVE]	Be677ExFACWC02A	
	7038	[0, INACTIVE]	Be677ExFanComSta	InfNet Controller Comm Status
	7039	[0, INACTIVE]	Be677Rm206ComSta	InfNet Controller Comm Status
	7034	[0, INACTIVE]	Be677Rm206LiebTr	
	7040	[0, INACTIVE]	Be677RTUComStat	InfNet Controller Comm Status
	7035	[0, INACTIVE]	Be677RTUFrzStat	
	70	[0, INACTIVE]	Be677RTURAS kDet	
	70 4	0.45	ChillerSpeed	Chiller VFD Speed
	70 1	1.00	ChillerStatus	Chiller Status
	72 2	1.00	ChlrPF	3-5 chlr power factor
	70 3	48.42	CHWStpt	Chiller Water Setpoint
	72 1	72.73	ChwSupTemp	3-5 chilled water sup temp
	71	[0, INACTIVE]	CMBChlr1CHWSuTmp	CMBChiller1 CHWSupplyTemp
	7135	[0, INACTIVE]	CMBChlr1DHWSuTmp	CMBChiller1 DHWSupplyTemp
	7133	[0, INACTIVE]	CMBChlr1FireAlm	CMBChiller1 FireAlarmPanel
	7143	[0, INACTIVE]	CMBHWSysBlr1Fail	CMBHWSystem Boiler1Failure
BV	7144	[0, INACTIVE]	CMBHWSysBlr2Fail	CMBHWSystem Boiler2Failure

context

Device 2935851 *Data loaded 11.04.2016 22:47:59*

BACnet ID: 2935851
Device Name: Cumm_3_5_bCX
BACnet MAC: 80C5EE08BAC0 => 128.1[redacted].8:47808

Description
Manufacturer: Schneider Electric

Objects

Search:

!	Obj. Type	Inst.-Nc	Present Value	Object Name	Description
	DEV	2935851		Cumm_3_5_bCX	
	FIL	1		ACCConfiguration	
	PR	7007		Import.Prg	
	BV	7028	[0, INACTIVE]	Be677BlrHWSAlarm	
	BV	7029	[0, INACTIVE]	Be677BlrHWSP1Flt	
	BV	7030	[0, INACTIVE]	Be677BlrHWSP2Flt	
	BV	7037	[0, INACTIVE]	Be677BoilrComSta	InfNet Controller Comm Status
	BV	7033	[0, INACTIVE]	Be677CHWSTempHi	
	BV	7031	[0, INACTIVE]	Be677ExFACWC01A	
	BV	7032	[0, INACTIVE]	Be677ExFACWC02A	
	BV	7038	[0, INACTIVE]	Be677ExFanComSta	InfNet Controller Comm Status
	BV	7039	[0, INACTIVE]	Be677Rm206ComSta	InfNet Controller Comm Status
	BV	7034	[0, INACTIVE]	Be677Rm206LiebTr	
	BV	7040	[0, INACTIVE]	Be677RTUComStat	InfNet Controller Comm Status
	BV	7035	[0, INACTIVE]	Be677RTUFrzStat	
	BV	7036	[0, INACTIVE]	Be677RTURASmkDet	
	AV	7004	0.45	ChillerSpeed	Chiller VFD Speed
	AV	7001	1.00	ChillerStatus	Chiller Status

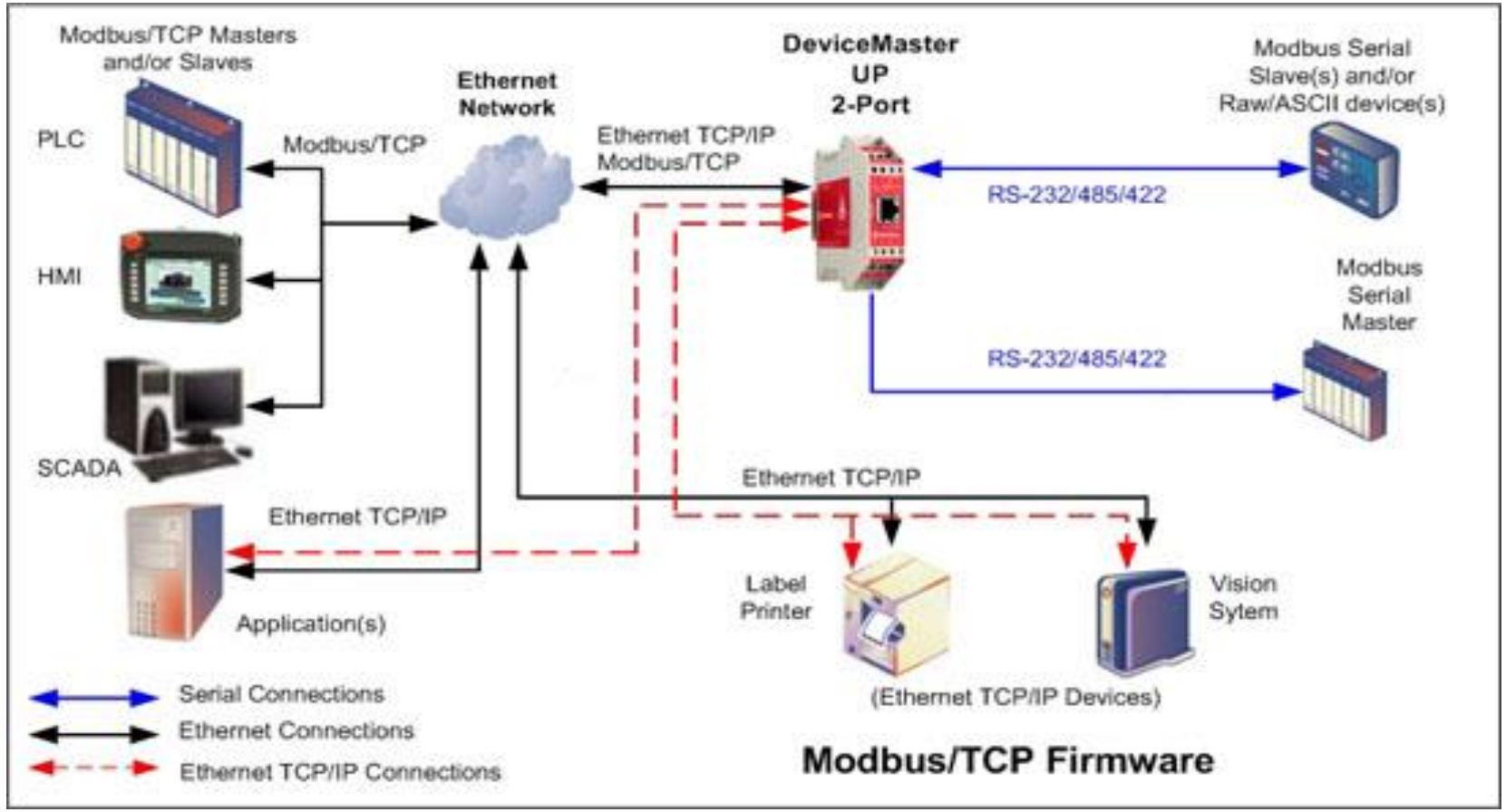
Analog Value

Standard | Proprietary

Object Identifier: AnalogValue
Object Name: BSides Chill
Object Type: AnalogValue

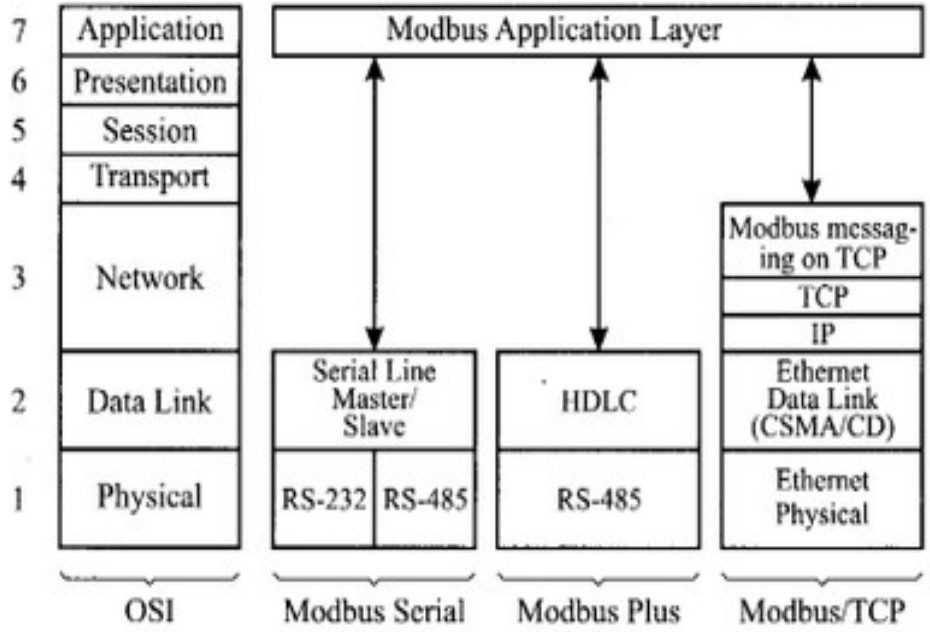
context

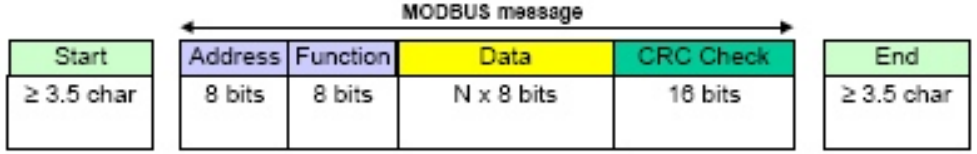
Modbus Component Architecture

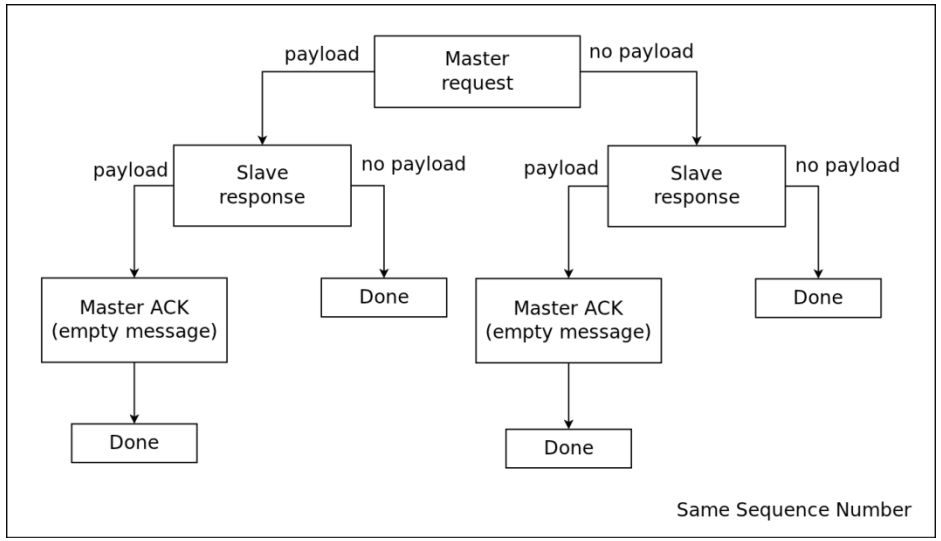


context

Modbus Protocol Design








```
Internet Protocol Version 4, Src: 10.21.22.10 (10.21.22.10), Dst: 10.21.22.24 (10.21.22.24)
Transmission Control Protocol, Src Port: 43972 (43972), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 15
Modbus/TCP
Modbus
   Function Code: Write Multiple Coils (15)
   Reference Number: 0
   Bit Count: 12
   Byte Count: 2
   Data: 6108

000  01011100 10000110 01001010 00000000 01101001 00000111 00000000 00001100   \.J.i...
008  00101001 11001111 01000110 10111010 00001000 00000000 01000101 00000000   ).F...E.
010  00000000 00110111 01000001 00011100 01000000 00000000 01000000 00000110   .7A.@.@.
018  10111001 01011001 00001010 00010101 00010110 00001010 00001010 00010101   .Y......
020  00010110 00011000 10101011 11000100 00000001 11110110 01101011 01011010   ......kZ
028  01011001 00000011 11010101 10101110 01011010 10100110 01010000 00011000   Y...Z.P.
030  00111001 00001000 00101111 11011110 00000000 00000000 01011001 10011001   9./...Y.
038  00000000 00000000 00000000 00001001 00000000 00001111 00000000 00000000   ........

Data (modbus.data), 2 bytes                                  Packets: 152 · Displayed: 152 · Marked: 0
```

context

Shells & More

- Documentation / Firmware
- Product Brief

External Device Server

- In minutes, securely connect factory floor devices to enterprise systems
- Access, monitor and control equipment over Ethernet
- Replace dedicated PCs and/or modem lines with fast and reliable Ethernet networking
- Supports RS-232, RS-422 and RS-485 communications
- Includes Modbus TCP, ASCII, RTU and DF1 protocols
- 15kV serial ESD protection
- Wide -40°– 70°C operating temperature range
- Environmentally-friendly RoHS and WEEE-compliant

Terminal — telnet [redacted]206 9999 — 80×24

telnet 2[redacted].206 9999 -zsh

```
Ethernet connection type: auto-negotiate

Change Setup:
  0 Server
  1 Channel 1
  5 Expert
  6 Security
  7 Defaults
  8 Exit without save
  9 Save and exit           Your choice ? 6

Disable SNMP (N) ? N

SNMP Community Name (public):

Disable Telnet Setup (N) ? N

Disable TFTP Firmware Update (N) ? N

Disable Port 77FEh (N) ? N

Disable Web Server (N) ? N

Disable Web Setup (N) ?
```

Terminal — telnet [redacted]137 — 80×24

```
pwny% telnet 201.[redacted]
Trying 201.[redacted]
Connected to tj-2[redacted].gtel.net.mx.
Escape character is '^]'.
Falcon Telnet (conn: 2) - Async port used by modbus or disabled
Connection Status:
1: Tcb: 1 Port: 23 Async: 0
2: Tcb: 2 Port: 23 Async: 0
3: Tcb: 0 Port: 0 Async: 0
4: Tcb: 0 Port: 0 Async: 0
```

Terminal — telnet [redacted].21 9999 — 80×24

```
Press Enter to go into Setup Mode

Model: Device Server Plus+! (Firmware Code:XA)

Modbus/TCP to RTU Bridge Setup
1) Network/IP Settings:
     IP Address ................. [redacted].76.21
     Default Gateway ............ 193.050.076.001
     Netmask .................... 255.255.255.224
2) Serial & Mode Settings:
     Protocol ................... Modbus/RTU,Slave(s) attached
     Serial Interface ........... 115200,8,N,1,RS232
3) Modem/Configurable Pin Settings:
     CP1 ...... Not Used
     CP2 ...... Not Used
     CP3 ...... Not Used
4) Advanced Modbus Protocol settings:
     Slave Addr/Unit Id Source .. Modbus/TCP header
     Modbus Serial Broadcasts ... Enabled (Id=0 used as broadcast)
     MB/TCP Exception Codes ..... No (no response if timeout or no slave)
     Char, Message Timeout ...... 00050msec, 05000msec

D)efault settings, S)ave, Q)uit without save
Select Command or parameter set (1..4) to change:
```

context

```
SMOD >use modbus/scanner/discover
SMOD modbus(discover) >set RHOSTS [redacted].171
SMOD modbus(discover) >exploit
[+] Module Modbus Discover Start
[+] Modbus is running on : [redacted]5.171
SMOD modbus(discover) >
```

```
[+] Module Brute Force UID Start
[+] Start Brute Force UID on : 1[redacted].171
[+] UID on 1[redacted].171 is : 10
```

```
[+] Module Read Input Registers Start
[+] Connecting to [redacted].171
[+] Response is :
###[ ModbusADU ]###
  transId   = 0x6
  protoId   = 0x0
  len       = 0x5
  unitId    = 0xa
###[ Read Input Registers Answer ]###
     funcCode  = 0x4
     byteCount = 2L
     registerVal= [1, 5]
```

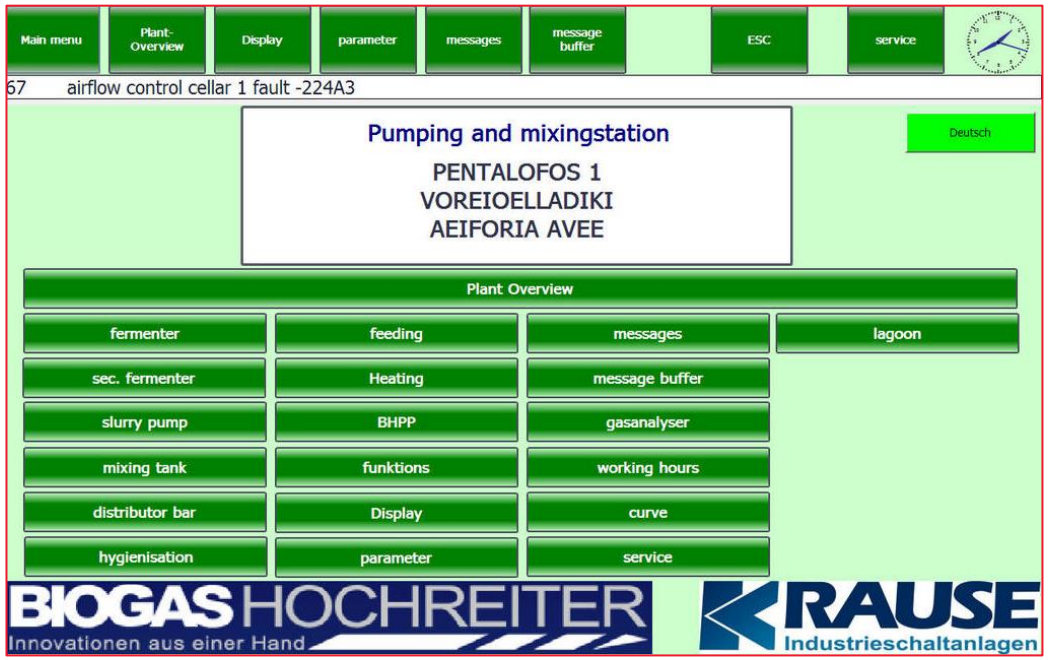
```
[+] Module Read Coils Function Start
[+] Connecting to 1[redacted]5.171
[+] Response is :
###[ ModbusADU ]###
  transId   = 0x7
  protoId   = 0x0
  len       = 0x4
  unitId    = 0xa
###[ Read Coils Answer ]###
     funcCode  = 0x1
     byteCount = 1L
     coilStatus= [0]
```

```
[+] Module Get Function Start
[+] Looking for supported function codes on [redacted]171
[+] 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 7(Read Exception Status) is supported.
[+] Function Code 8(Diagnostic) is
[+] Function Code 15(Write Multiple
[+] Function Code 16(Write Multiple
[+] Function Code 17(Report Slave I
```

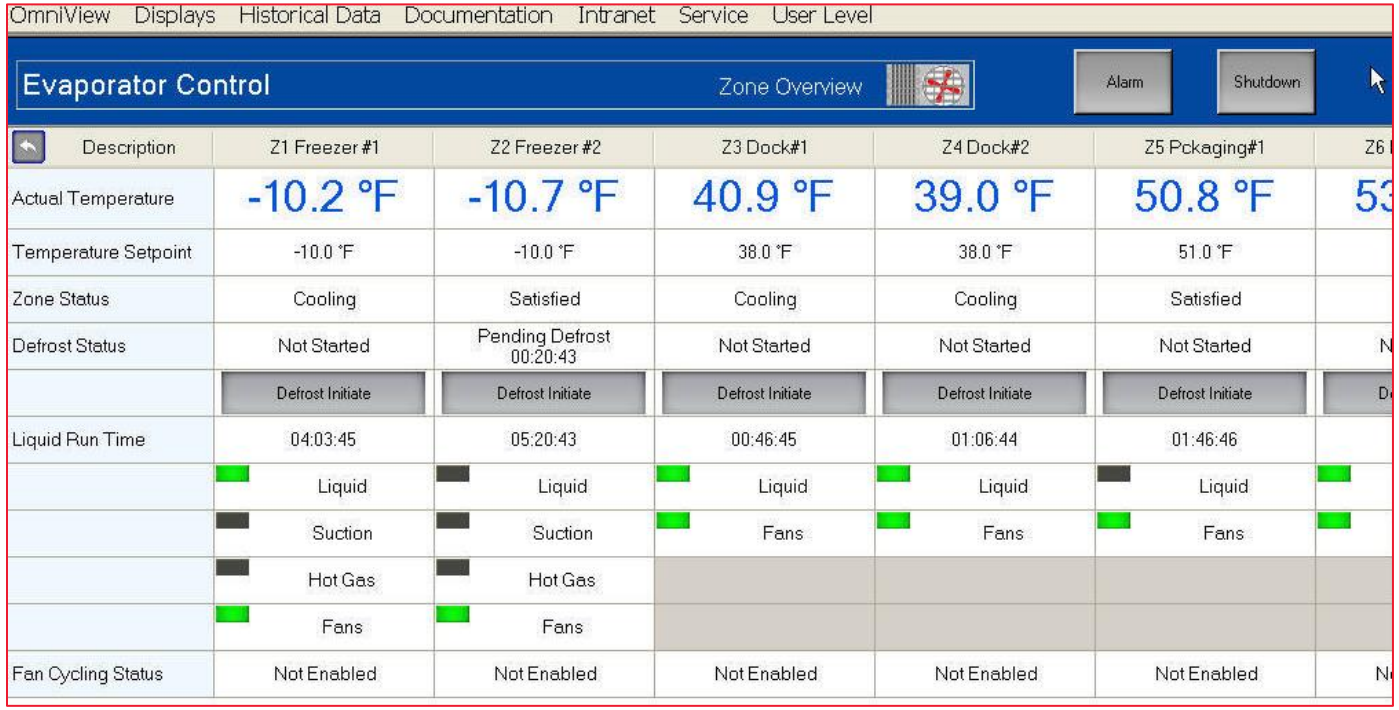
```
[+] Module Write Single Coil Start
[+] Connecting to [redacted].171
[+] Response is :
###[ ModbusADU ]###
  transId    = 0x8
  protoId    = 0x0
  len        = 0x6
  unitId     = 0xa
###[ Write Single Coil ]###
     funcCode   = 0x5
     outputAddr= 0x0
     outputValue= 0x1
```

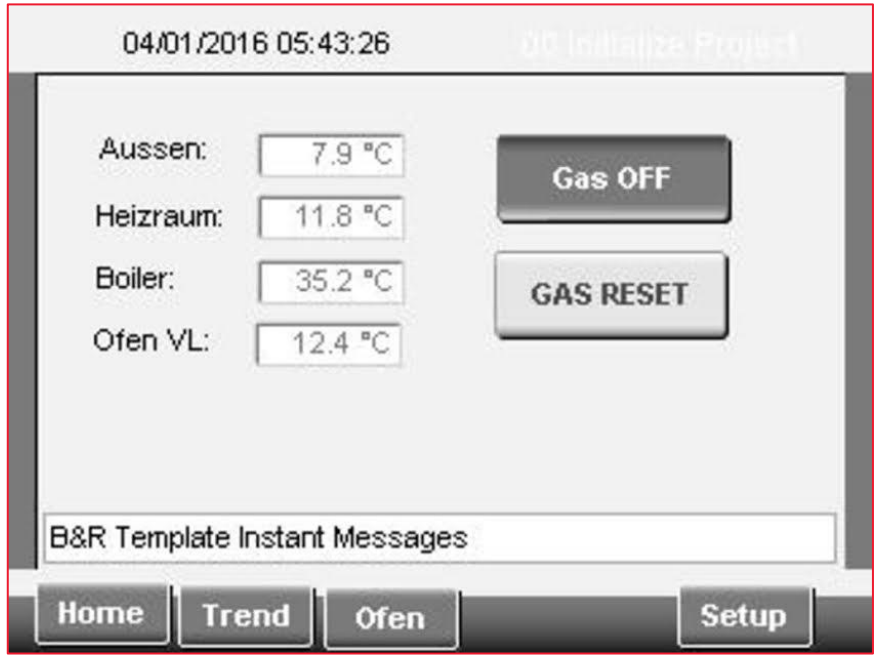
context


Owo 2H
Owo 1H
Berry 2H
Berry 1H
OVERVIEW Wells 5-8
Tanks
BMS
Tubing Press 0.0 0.0 0.0 0.0 PSI
Casing Press 0.0 0.0 0.0 0.0 PSI
Wellhead SDV CLOSE CLOSE CLOSE OPEN
GPU Pressure -0.6 -1.7 -1.7 345.5 PSI
GPU Temperature 47.5 47.5 51.1 68.7 *F
GPU Gas Flow Rate 0.0 0.0 0.0 11991.8 MCFD
Gas Diff Press 0.05 0.11 0.11 46.77 inH2O
Gas Static Press -0.4 0.0 -0.3 342.1 PSI
Gas Temp 41.7 41.5 41.8 66.4 *F
Gas Today 0 0 0 3970 MCF
Gas Yesterday 0 0 0 3412 MCF
Gas Accum 0 0 0 7382 MCF
Oil Today 0.0 0.0 0.0 0.0 BBL
Oil Yesterday 0.0 0.0 0.0 0.0 BBL

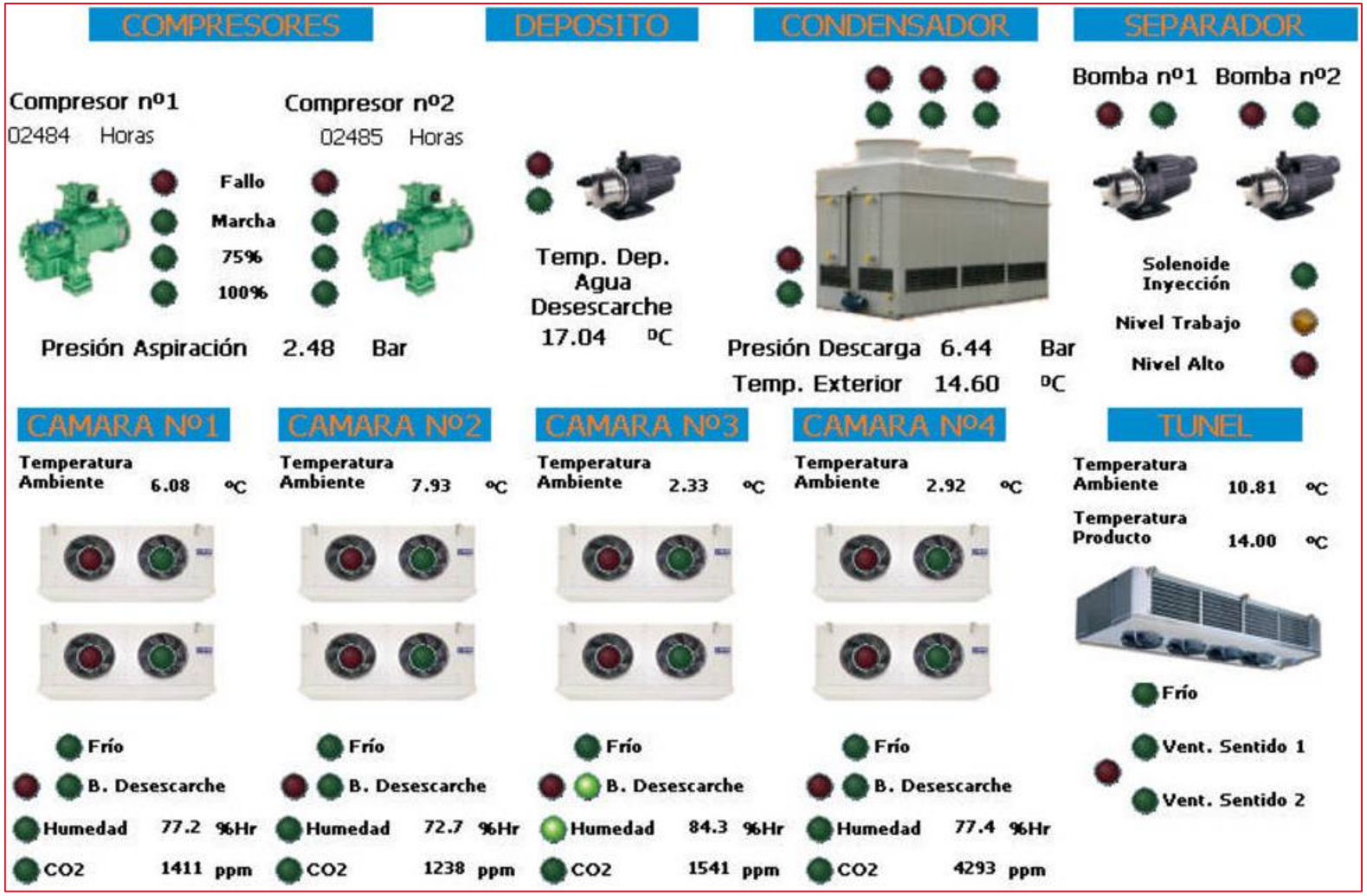

Main menu
Plant-Overview
Display
parameter
messages
message buffer
ESC
service
67 airflow control cellar 1 fault -224A3
Pumping and mixingstation
PENTALOFOS 1
VOREIOELLADIKI
AEIFORIA AVEE
Deutsch
Plant Overview
fermenter
feeding
messages
lagoon
sec. fermenter
Heating
message buffer
slurry pump
BHPP
gasanalyser
mixing tank
funktions
working hours
distributor bar
Display
curve
hygienisation
parameter
service
BIOGAS HOCHREITER
Innovationen aus einer Hand
KRAUSE
Industrieschaltanlagen

context

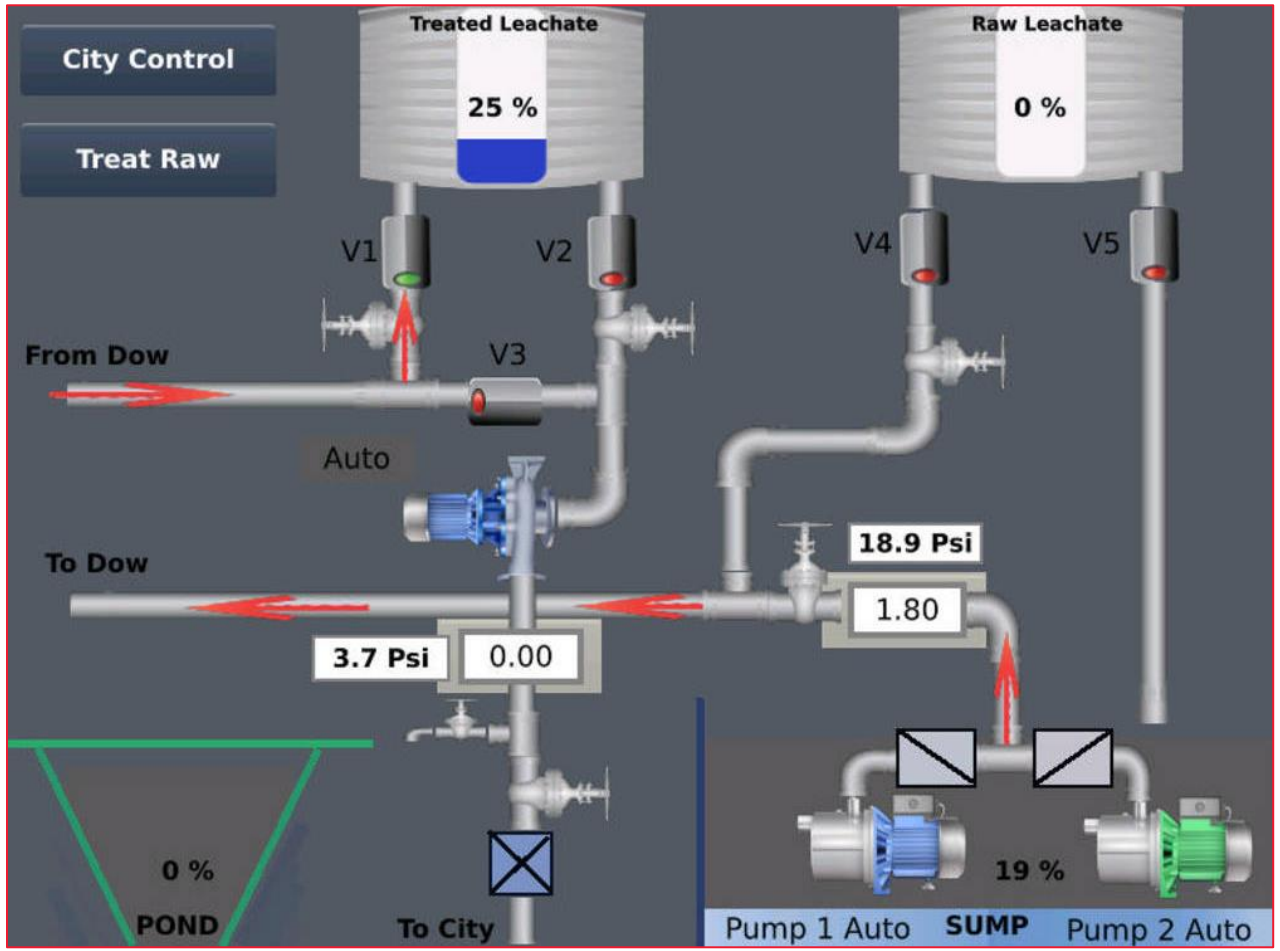

OmniView Displays Historical Data Documentation Intranet Service User Level
Evaporator Control
Zone Overview
Alarm
Shutdown
Description
Z1 Freezer #1
Z2 Freezer #2
Z3 Dock#1
Z4 Dock#2
Z5 Pckaging#1
Actual Temperature
-10.2 °F
-10.7 °F
40.9 °F
39.0 °F
50.8 °F
Temperature Setpoint
-10.0 °F
-10.0 °F
38.0 °F
38.0 °F
51.0 °F
Zone Status
Cooling
Satisfied
Cooling
Cooling
Satisfied
Defrost Status
Not Started
Pending Defrost 00:20:43
Not Started
Not Started
Not Started
Defrost Initiate
Liquid Run Time
04:03:45
05:20:43
00:46:45
01:06:44
01:46:46
Liquid
Suction
Fans
Hot Gas
Fan Cycling Status
Not Enabled

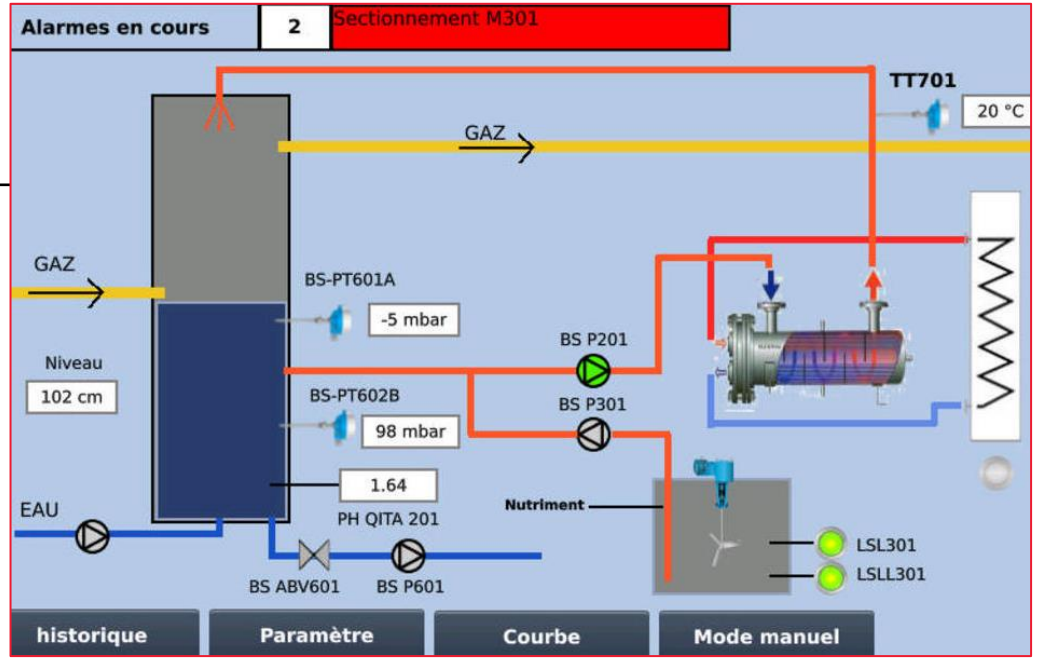

04/01/2016 05:43:26
Aussen: 7.9 °C
Heizraum: 11.8 °C
Boiler: 35.2 °C
Ofen VL: 12.4 °C
Gas OFF
GAS RESET
B&R Template Instant Messages
Home
Trend
Ofen
Setup

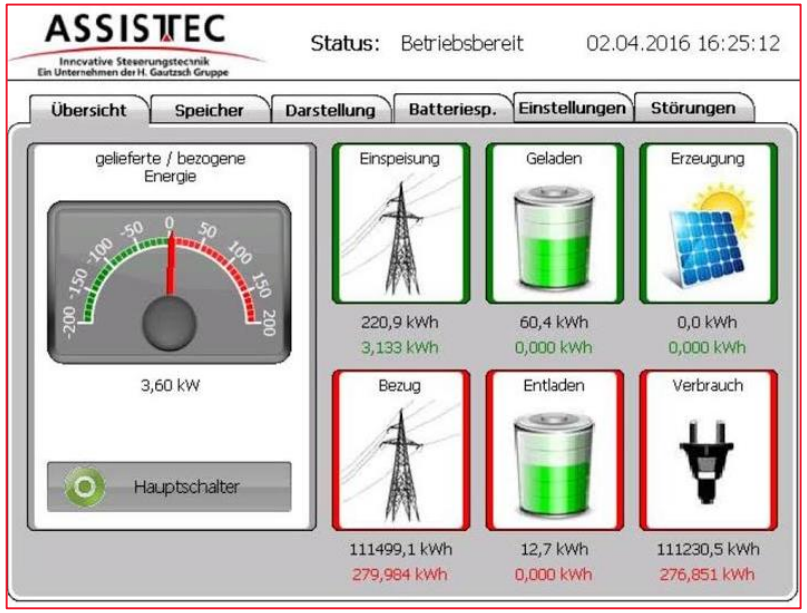
context


COMPRESORES
DEPOSITO
CONDENSADOR
SEPARADOR
Compresor nº1
02484 Horas
Compresor nº2
02485 Horas
Fallo
Marcha
75%
100%
Presión Aspiración 2.48 Bar
Temp. Dep. Agua Desescarche
17.04 ºC
Presión Descarga 6.44 Bar
Temp. Exterior 14.60 ºC
Bomba nº1
Bomba nº2
Solenoide Inyección
Nivel Trabajo
Nivel Alto
CAMARA Nº1
Temperatura Ambiente 6.08 ºC
Frío
B. Desescarche
Humedad 77.2 %Hr
CO2 1411 ppm
CAMARA Nº2
Temperatura Ambiente 7.93 ºC
Frío
B. Desescarche
Humedad 72.7 %Hr
CO2 1238 ppm
CAMARA Nº3
Temperatura Ambiente 2.33 ºC
Frío
B. Desescarche
Humedad 84.3 %Hr
CO2 1541 ppm
CAMARA Nº4
Temperatura Ambiente 2.92 ºC
Frío
B. Desescarche
Humedad 77.4 %Hr
CO2 4293 ppm
TUNEL
Temperatura Ambiente 10.81 ºC
Temperatura Producto 14.00 ºC
Frío
Vent. Sentido 1
Vent. Sentido 2

context


City Control
Treat Raw
Treated Leachate
25 %
Raw Leachate
0 %
V1
V2
V3
V4
V5
From Dow
Auto
To Dow
18.9 Psi
1.80
3.7 Psi
0.00
0 %
POND
To City
19 %
Pump 1 Auto
SUMP
Pump 2 Auto


Alarmes en cours
2
Sectionnement M301
TT701
20 °C
GAZ
GAZ
BS-PT601A
-5 mbar
Niveau
102 cm
BS P201
BS-PT602B
98 mbar
BS P301
1.64
PH QITA 201
Nutriment
EAU
LSL301
LSLL301
BS ABV601
BS P601
historique
Paramètre
Courbe
Mode manuel


ASSISTEC
Innovative Steuerungstecnik
Ein Unternehmen der H. Gautzsch Gruppe
Status: Betriebsbereit
02.04.2016 16:25:12
Übersicht
Speicher
Darstellung
Batteriesp.
Einstellungen
Störungen
gelieferte / bezogene Energie
3,60 kW
Hauptschalter
Einspeisung
220,9 kWh
3,133 kWh
Geladen
60,4 kWh
0,000 kWh
Erzeugung
0,0 kWh
0,000 kWh
Bezug
111499,1 kWh
279,984 kWh
Entladen
12,7 kWh
0,000 kWh
Verbrauch
111230,5 kWh
276,851 kWh

context

Schneider Electric

PowerLogic ION7650

Home

Monitoring | Control | Diagnostic | Maintenance | Setup

Setup
Network Setup

Setup

Power Meter			
Volts Mode	4W-WYE	Va Polarity	Normal
PT Primary	31500.00	Vb Polarity	Normal
PT Secondary	100.00	Vc Polarity	Normal
CT Primary	600.00	V4 Polarity	Normal
CT Secondary	5.00	Ia Polarity	Normal
V4 Primary	120.00	Ib Polarity	Normal
V4 Secondary	120.00	Ic Polarity	Normal
I4 Primary	5.00	I4 Polarity	Normal
I4 Secondary	5.00	I5 Polarity	Normal
I5 Primary	5.00	**Power Quality**	
I5 Secondary	5.00	Nominal Voltage	18187.00
Nameplate Information		**Sliding Window Deman**	
Owner		Sub Interval	900.00
Tag1		# Sub Intervals	1.00
Tag2		Predicted Response	70.00

Owner		Meter Type	7650
Tag 1		Firmware Version	7650V371s
Tag 2		Template	7650_FAC-PQ_V3.6.0.0.0
Device Time	2016-03-27 04:41:06 GMT +02:00	Serial Number	MJ-1407B153-04

EMERSON Network Power

Liebert

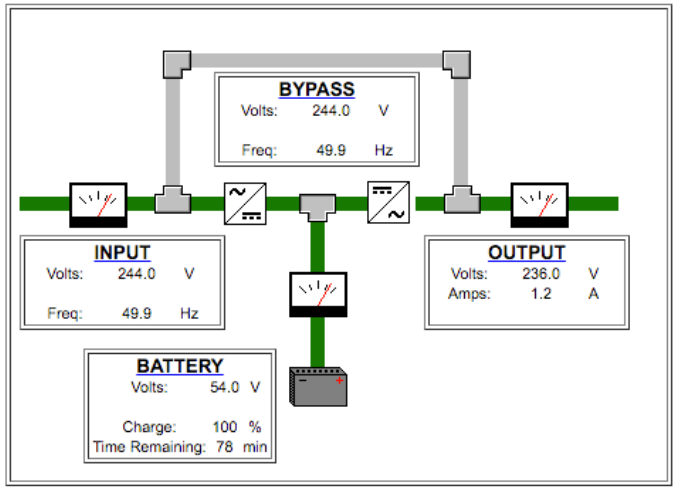
monitor | control | configure | event log | support

Agent Information:
URB Cleveland
Comms Room
Big Dusty room with no...

Device Status:
Load Protected:
No Alarms Present

Monitor Categories:
- GXT
  - Summary
  - Active Alarms
  - Battery
  - Bypass
  - Input
  - Inverter
  - Output
  - Hardware Configuration
  - Other

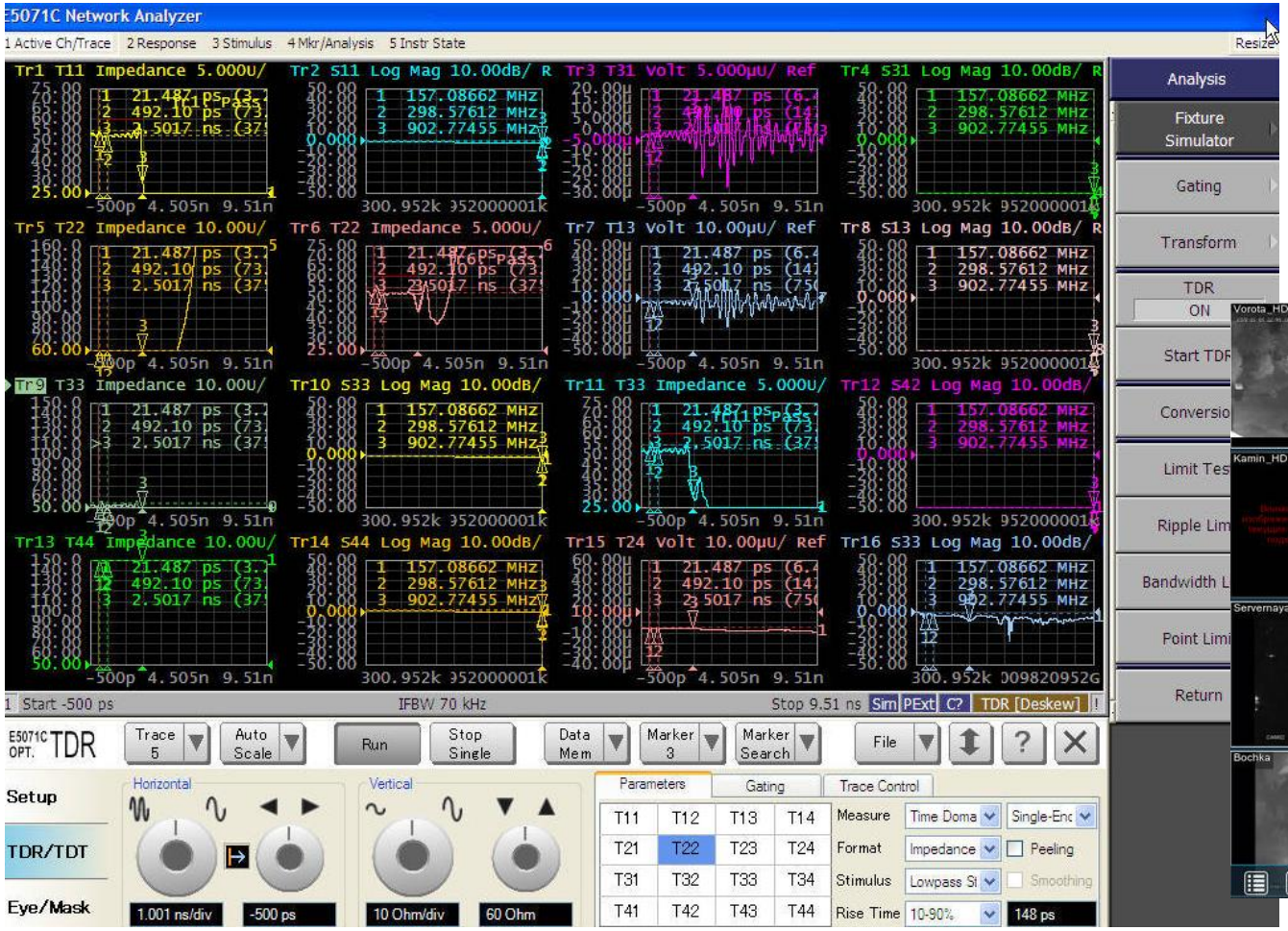
Summary: Updated: March 27, 2016 12:54:19PM



Active Alarms:

No Alarms Present

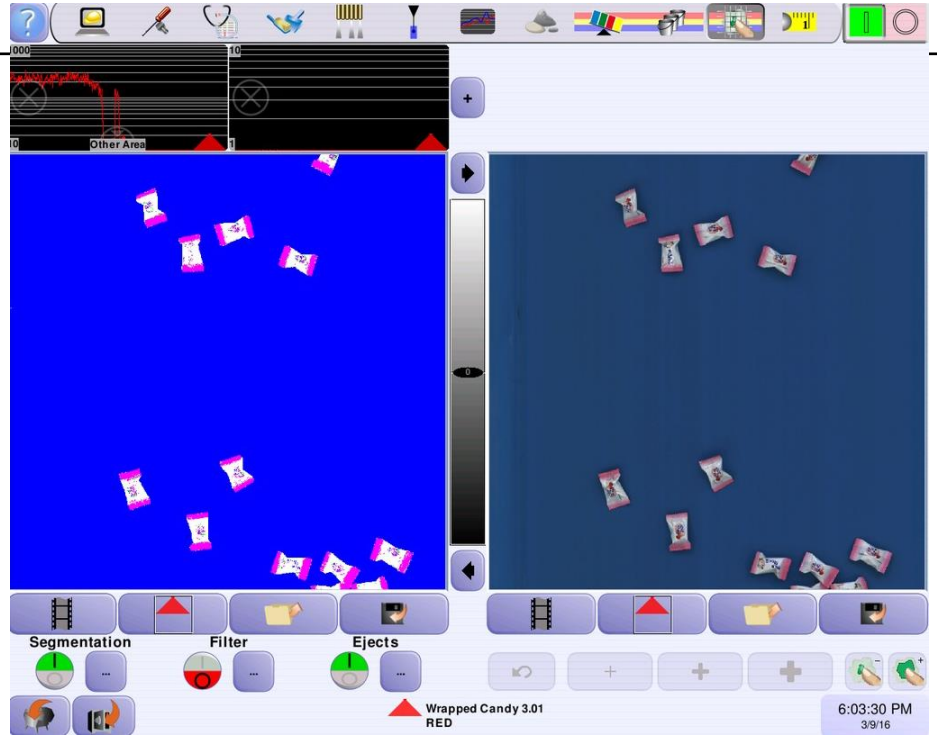
context


E5071C Network Analyzer
1 Active Ch/Trace 2 Response 3 Stimulus 4 Mkr/Analysis 5 Instr State
Resize
Tr1 T11 Impedance 5.000U/
Tr2 S11 Log Mag 10.00dB/ R
Tr3 T31 Volt 5.000µU/ Ref
Tr4 S31 Log Mag 10.00dB/ R
Tr5 T22 Impedance 10.00U/
Tr6 T22 Impedance 5.000U/
Tr7 T13 Volt 10.00µU/ Ref
Tr8 S13 Log Mag 10.00dB/ R
Tr9 T33 Impedance 10.00U/
Tr10 S33 Log Mag 10.00dB/
Tr11 T33 Impedance 5.000U/
Tr12 S42 Log Mag 10.00dB/
Tr13 T44 Impedance 10.00U/
Tr14 S44 Log Mag 10.00dB/
Tr15 T24 Volt 10.00µU/ Ref
Tr16 S33 Log Mag 10.00dB/
Start -500 ps
IFBW 70 kHz
Stop 9.51 ns
Sim PExt C? TDR [Deskew]
Analysis
Fixture Simulator
Gating
Transform
TDR
ON
Start TDR
Conversio
Limit Tes
Ripple Lim
Bandwidth L
Point Limi
Return
E5071C OPT. TDR
Trace 5
Auto Scale
Run
Stop Single
Data Mem
Marker 3
Marker Search
File
Setup
TDR/TDT
Eye/Mask
Horizontal
Vertical
1.001 ns/div
-500 ps
10 Ohm/div
60 Ohm
Parameters
Gating
Trace Control
T11 T12 T13 T14
T21 T22 T23 T24
T31 T32 T33 T34
T41 T42 T43 T44
Measure Time Doma
Single-Enc
Format Impedance
Peeling
Stimulus Lowpass St
Smoothing
Rise Time 10-90%
148 ps


Vorota_HD
Mashiny_Hd
UgolDoma_HD
UgolGaraz_HD
Garaz_HD
Kamin_HD
Podval_HD
zaborLes
dvorAnalog
BeliyDigitus
Servernaya
VorotaAnalog
DvorElka
2eraz_doroga
dvor2Analog
Bochka
DvorMashiny
Barbeku_HD

context


18:56:32
UTAL LICENSE PLATES SOLUTIONS
Ogólny
POD. TABL. ZAŁĄCZONE
PRASA ZAŁĄCZONA
FOLIARKA A ZAŁĄCZONA
FOLIARKA B ZAŁĄCZONA
ZDAWANIE TABL. ZAŁĄCZONA
TRYB AUTOMATYCZNY
STOP
TYP PRODUKCJI
WYDAJNOŚĆ [10 - 100%]
PL
DE
Cykl [s]: 5.2
Cykl Średni [s]: 5.7
Cykle dzisiaj 4669
Cykle ogółem 1385629
t szafy [°C]: 26.0
PL
100

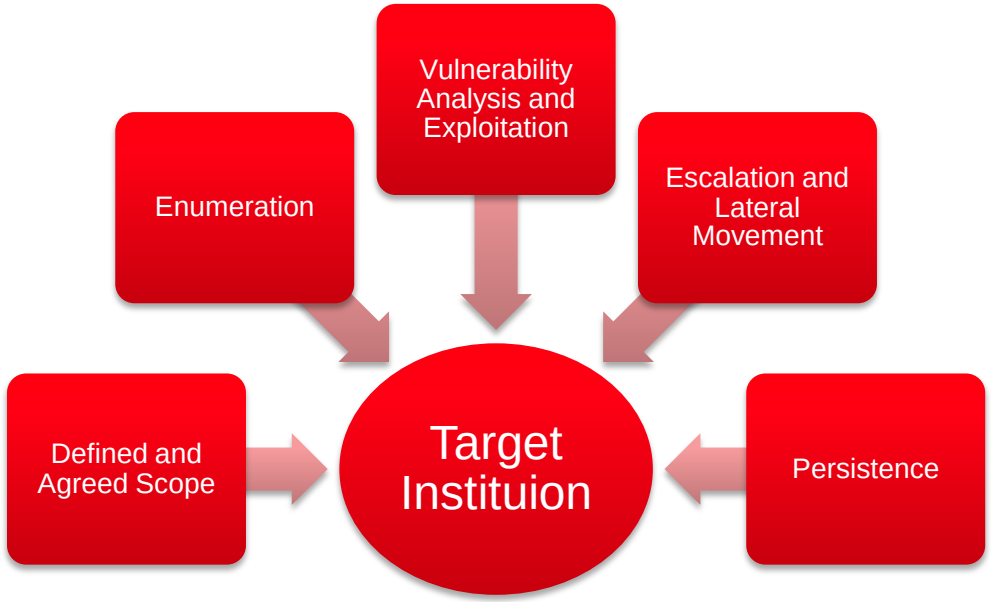

Other Area
Segmentation
Filter
Ejects
Wrapped Candy 3.01
RED
6:03:30 PM
3/9/16

context

An approach to alternative analysis of Building Management Control Environments

Checkpoint 1

Checkpoint 9



context

Intel Gathering

OSINT

//www.onegov.nsw.gov.au/publicregister/#/publicregisterdetails/1-131WA59

Property - Corporation

CURRENT

151 PROPERTY SERVICES PTY LTD

No. 10021417

START: 17/04/2014 » END: 16/04/2017

a810-bisweb.nyc.gov/bisweb/bispi00.jsp

BIS Menu | Bldg Info Search

NYC Buildings

NYC Department of Buildings

Building Information Search

Property Search | Complaints / Violations | Applications | Boiler Search | Gas Service | Power Authorizations | Elevator Devices | Cranes & Derricks

Search by Property

1 Bronx House No: Street: GO

2 Pick a Borough Block: Lot: GO

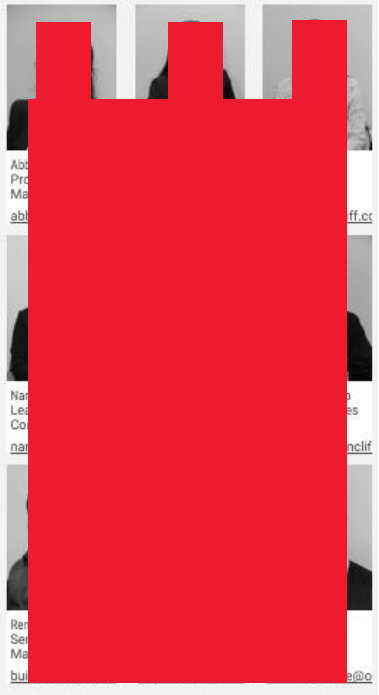
3 Building Identification Number (BIN): GO

Browse Block and Lot

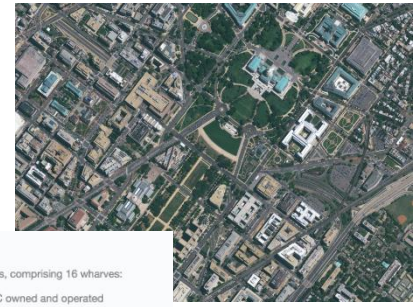
4 Pick a Borough Block: Lot (optional): GO

Back to top

VALAD COMMERCIAL MANAGEMENT LIMITED
76 101 802 046
Level 6 Suite 602 151 Castlereagh Street Sydney NSW 2000
30/10/2002
Current



GEOINT



Leverage public databases/records of Building facility management

Use Social Networks to determine People, Roles, Skill sets and behavioural traits

HUMINT

Physical Location Co-ordinates, Landscapes, Geospatial Info

Analyse building tenant documentation for any sensitive or usefull info, such as names, phone numbers, roles

Assess Signals Spectrum

Obtain protocol and procedures for contractors/3rd party suppliers

Facilities

The Port of Gladstone has six main wharf centres, comprising 16 wharves:

- RG Tanna Coal Terminal – four wharves GPC owned and operated
- Barney Point Coal Terminal – one wharf GPC owned and operated
- Auckland Point – four wharves GPC owned and operated by others
- Fisherman's Landing – four wharves operated by multiple companies
- South Trees – two wharves operated by Queensland Alumina Limited
- Boyne Wharf – one wharf operated by Boyne Smelters

The Port of Gladstone Information Handbook provides a detailed overview of the port's facilities and services for ship's masters, agents and owners.

SIGINT

Port of Gladstone

Gladstone Ports Corporation
Request for Contractor to Enter a Maritime Security Zone

Date of Entry	/ /	To / /	Reason for Entry	
LRZ Access (Please indicate by ✓)	☐ RG Tanna Coal Wharf	☐ Barney Point Coal Wharf	☐ Port of Rockhampton	
	☐ Auckland Point Facility	☐ Fisherman's Landing No. 5		
WRZ Access (Please indicate by ✓)	☐ WRZ	WRZ Location:		

INDUCTION

ION

etails to allow us to record your induction results.

Please enter your name: Dan

Please enter your email address: root@127.0.0.1

Your course completion transcript will be emailed to this address at the end of this induction, so please ensure you enter a valid email address. This transcript will need to be printed and presented to our Security Department to confirm your induction and get your site ID card. Without it, your induction will not be processed.

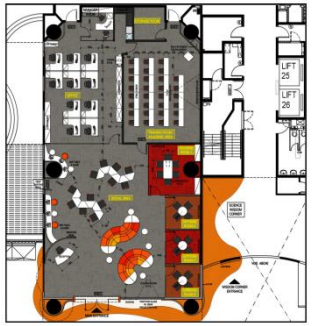
Please enter your company name: Bsides

SUBMIT

OSINT

Security forms

- Application for GPC site identification car
- Application for permanent site vehicle pas
- Notification of scheduled delivery of ship stores
- Request for contractor to enter a Maritime Security Zone



Facilities

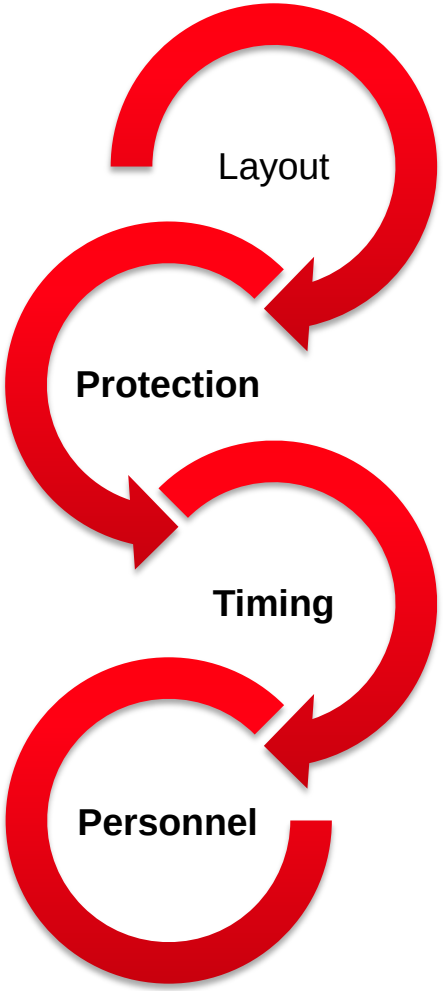
The Port of Gladstone has six main wharf centres, comprising 16 wharves:

- RG Tanna Coal Terminal – four wharves GPC owned and operated
- Barney Point Coal Terminal – one wharf GPC owned and operated
- Auckland Point – four wharves GPC owned and operated by others
- Fisherman's Landing – four wharves operated by multiple companies
- South Trees – two wharves operated by Queensland Alumina Limited
- Boyne Wharf – one wharf operated by Boyne Smelters

he Port of Gladstone Information Handbook provides a detailed overview of the ort's facilities and services for ship's masters, agents and owners.

context

Recon



Both ordinary and emergency exits, hallways, stairways ,windows, rooftops and even sewers
Observe and map all Entry/Exit points for public and staff
Location of important offices and rooms

Observe Guards and Patrol routes
Observe the type and placement of Perimeter security devices
Identify access methods

Observe Busy times where “reception/door access” is heavily utilised

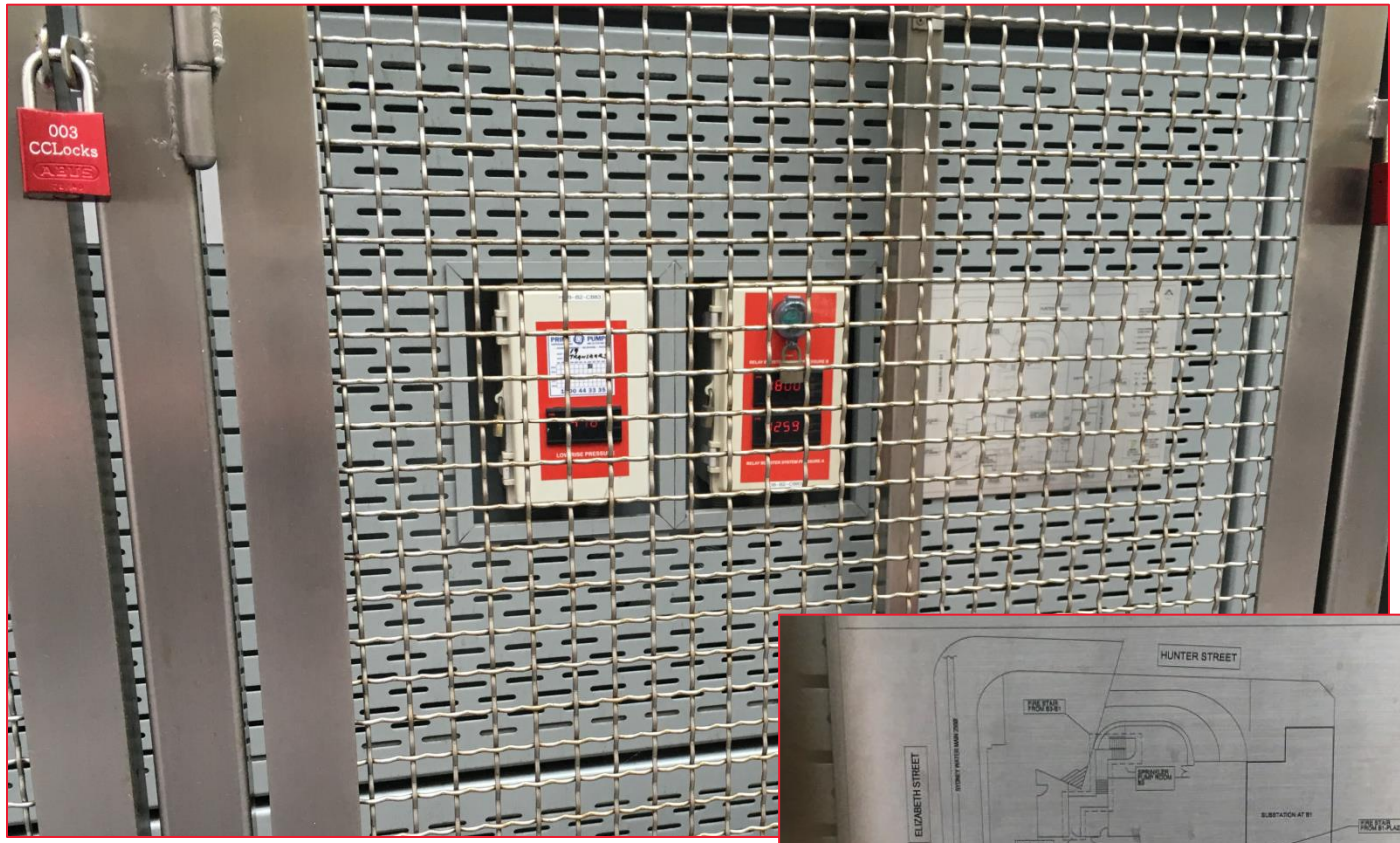
Map staff congregation and mustering areas
Observe type of Lanyard and Access Pass/Card technology used

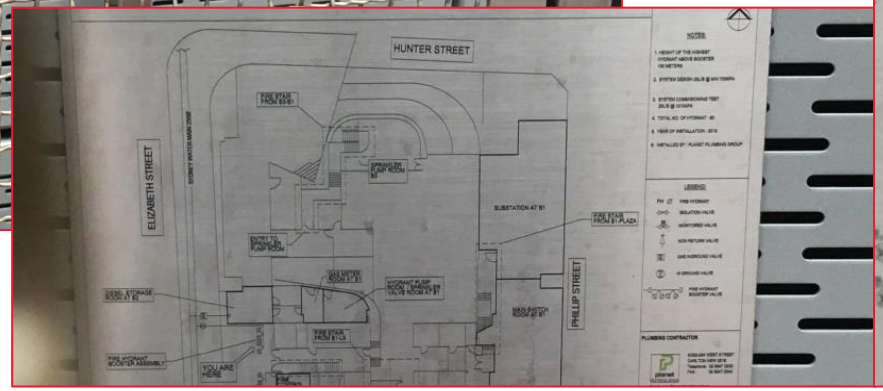
context

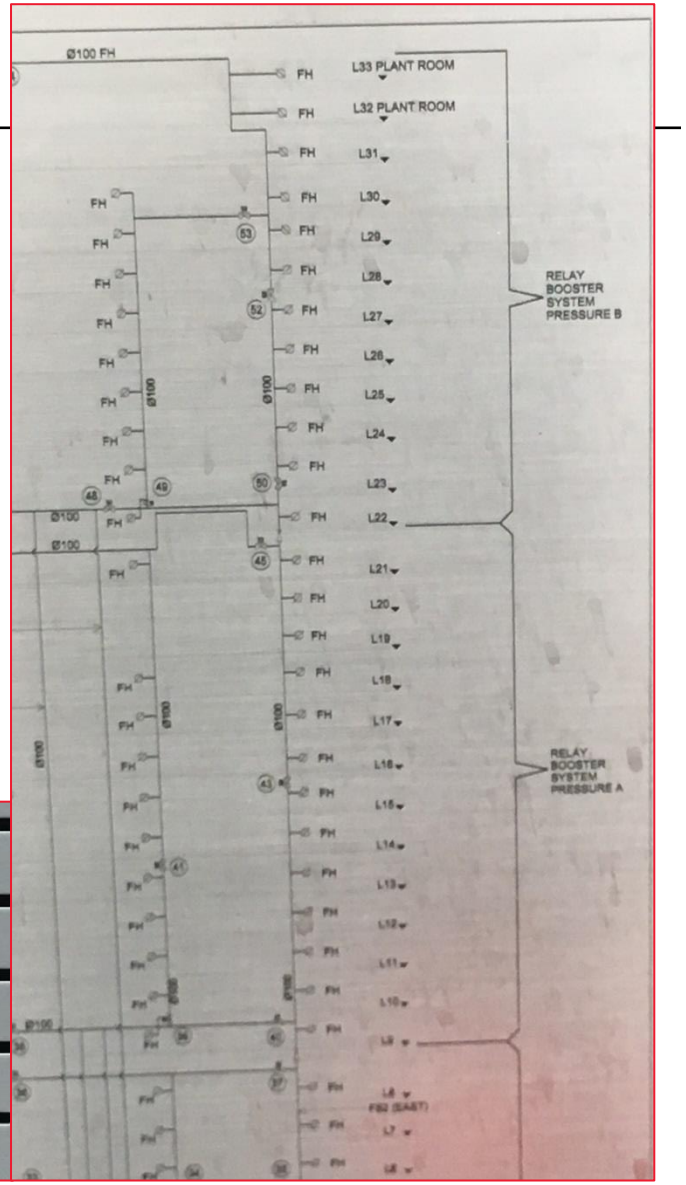
High Value Targets

- MDF Room
- Building Facilities Management Office
- Security Controller
- Plant Room
- Electrical Communications

context


003
CCLocks


HUNTER STREET
ELIZABETH STREET
PHILLIP STREET
SUBSTATION AT B1
NOTES
LEGEND
PLUMBING CONTRACTOR


Ø100 FH
L33 PLANT ROOM
L32 PLANT ROOM
RELAY BOOSTER SYSTEM PRESSURE B
RELAY BOOSTER SYSTEM PRESSURE A

context


FIRE DOOR
KEEP CLEAR
AT ALL TIMES
MAXIMUM
VEHICLE
LENGTH
6 METRES

context

Vulnerability Probing

i. **Human:** Employee Protocols, Procedures and Behaviours

ii. **Human**: Building Management Personel Reachability

iii. **Technology:** Perimeter and Internal Intrusion Monitoring Controls and Countermeasures

iv. **Technology**: Gate/Door/Elevator Access controls

v. **Technology:** Signals emanation & manipulation, BCS Exposures

vi. **Technology**: Door Controls

vii. **Processes**: Building Automation (Elevators), Security Gates, Service Entry Carpark,

viii. **Processes**: Identity Validation

context

context

Identity Validation

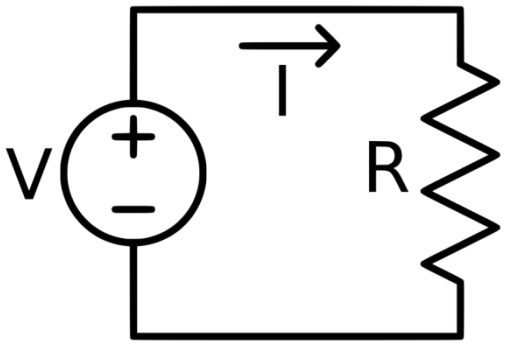
context

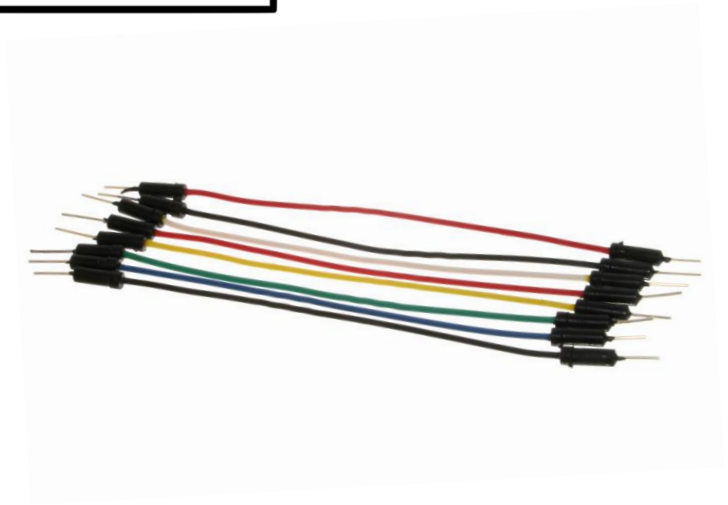
HMI RFID Cards & KeyPads

- RFID Cloning
- Circuit Jumper | Splicing
- Ultra Violet Ink
- Earth Magnets

Circuit Jumping

- Most alarm/sensors are protective circuits
- The notion of “open” and “closed” circuit is important
- locate the wires to and from the circuit and jumper them to bypass the entire system.
- Door Proximity Controllers usually 12v
- Watch for Anti-Tampering Measures (opened circuits) :-)





Magnetic Contact Switch Doors

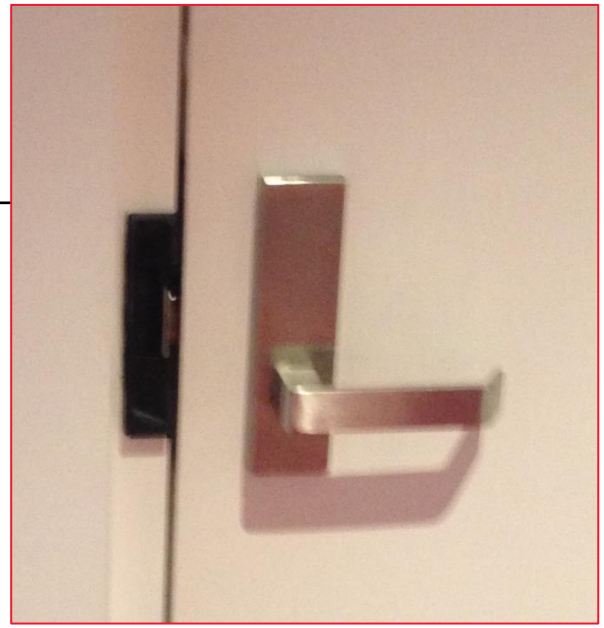
- Magnetic switch most common of hardwired components
- Two individual pieces, the switch and the companion magnet

Service Elevators

- Fire Emergency Services Elevator Key
- Security Key override
- Lift Surfing

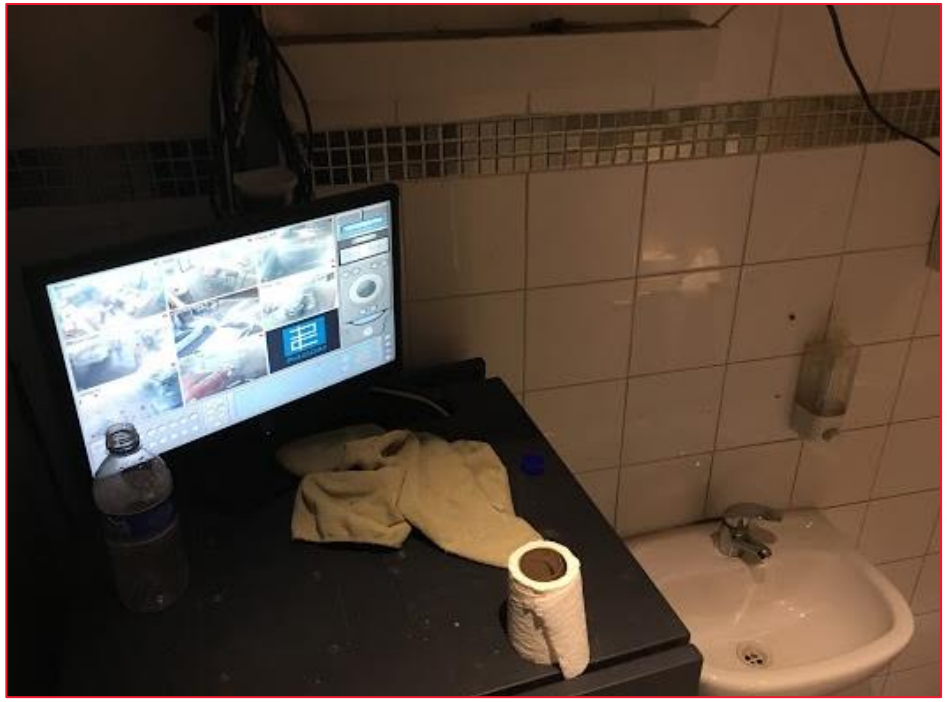
context

Lever Doors



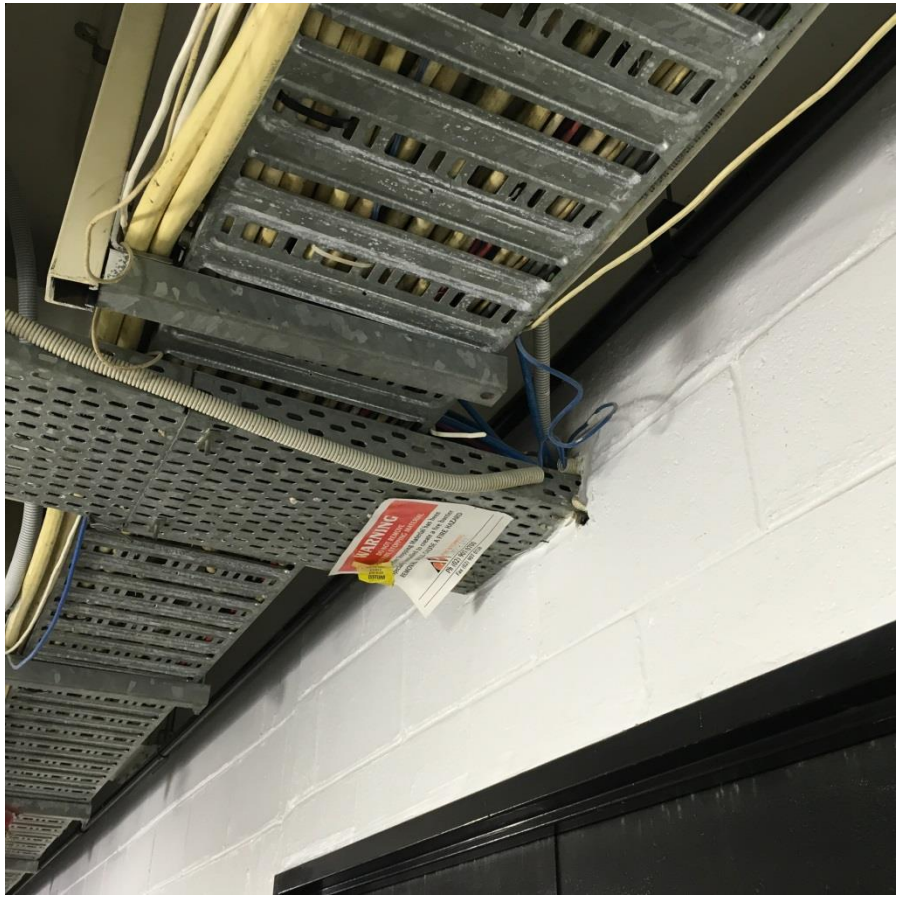
context

And some ftw moments



context

Exposed Wiring



Any Questions? Dan.kennedy@contextis.com

Greetz bsides team, rich, context, gio, david, petr, kurt, andrew and chris :-)