RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Is Your Fridge Conspiring Against You? IoT Attacks and Embedded Defenses

SESSION ID: SEC-T08

Wolfgang Kandek

Chief Technical Officer
Qualys
@wkandek

About:Me @WKANDEK

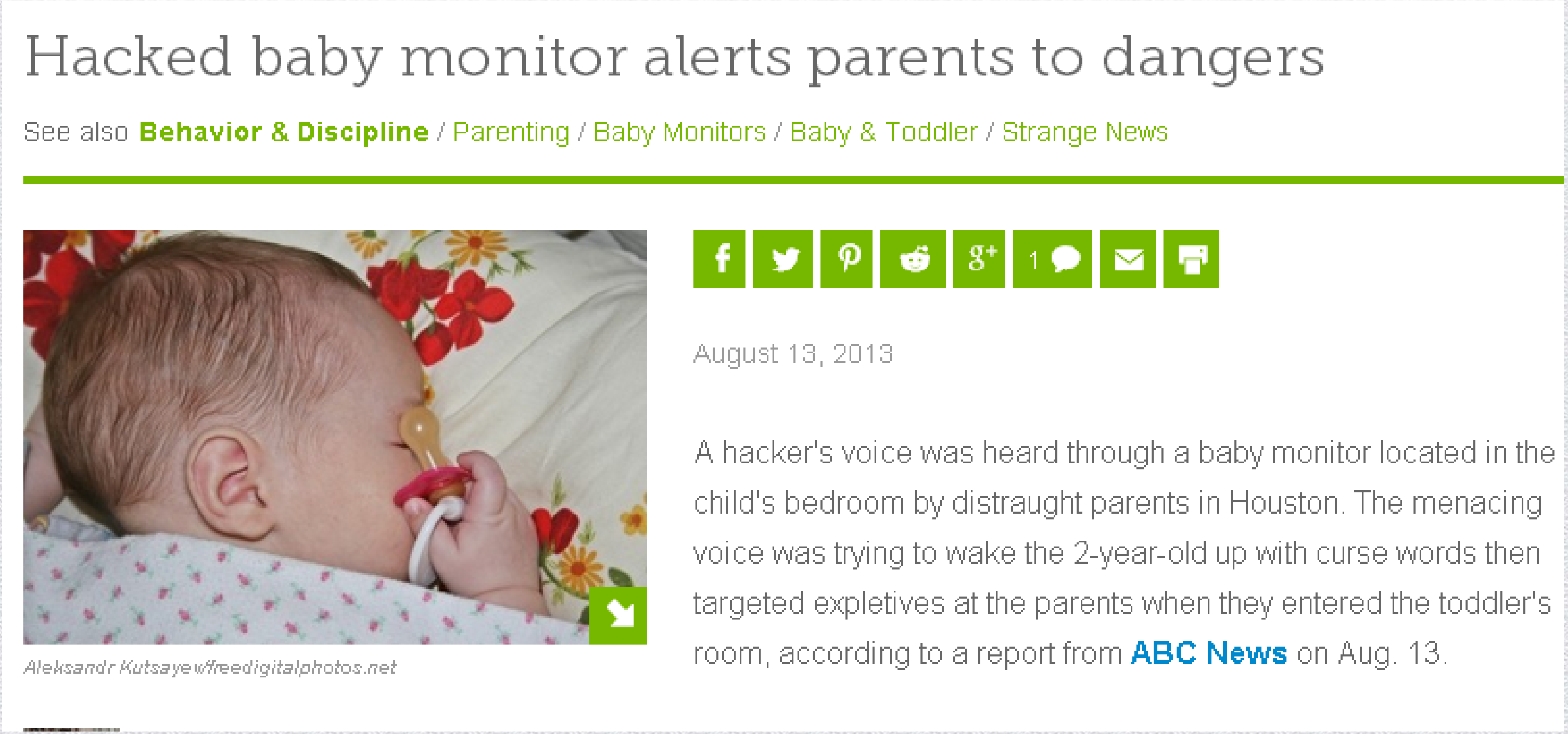
- Qualys – CTO
  - Responsible for Research and Outreach
  - Laws of Vulnerabilities
    - Half-life, Prevalence, Persistence, Exploitation
- Blog: Laws of Vulnerabilities
  - https://laws.qualys.com
- Twitter: @wkandek

About:Me - @XSSNIPER

- Qualys - Director of Research and Threat Intelligence
- Google - Technical Lead and Security for Google Plus
- Microsoft - Technical Lead in Security
- Books:
  - Hacking: The Next Generation – O'Reilly
  - Inside Cyber Warfare – O'Reilly
  - The Virtual Battlefield – IOS Press
- ICS Vulnerability Research:
  - 30 publically credited in ICS-CERT advisories
  - Over 1000 individual issues reported to DHS

Let’s Review 2013 and IoT Security

“The large-scale attack, which occurred between Dec. 23, 2013, and Jan. 6, 2014, involved more than 750,000 malicious email communications”



Hacked baby monitor alerts parents to dangers

See also **Behavior & Discipline** / Parenting / Baby Monitors / Baby & Toddler / Strange News

Aleksandr Kutsayev/freedigitalphotos.net

August 13, 2013

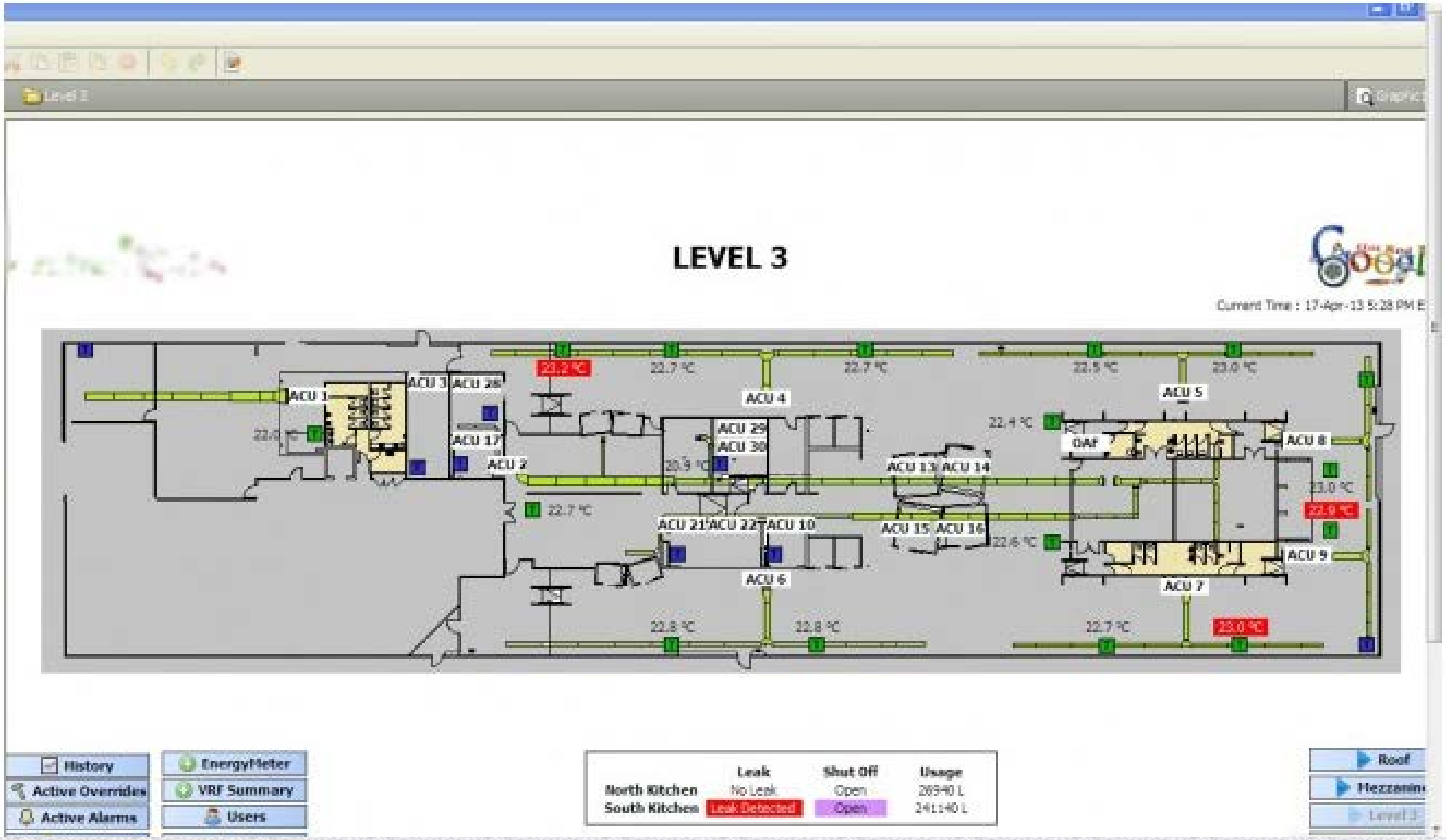
A hacker's voice was heard through a baby monitor located in the child's bedroom by distraught parents in Houston. The menacing voice was trying to wake the 2-year-old up with curse words then targeted expletives at the parents when they entered the toddler's room, according to a report from **ABC News** on Aug. 13.

“they woke up at midnight to the sounds of a man yelling at their daughter, Emma, and were surprised to find their Internet-enabled baby monitor moving -- even though they were not the ones moving it.”

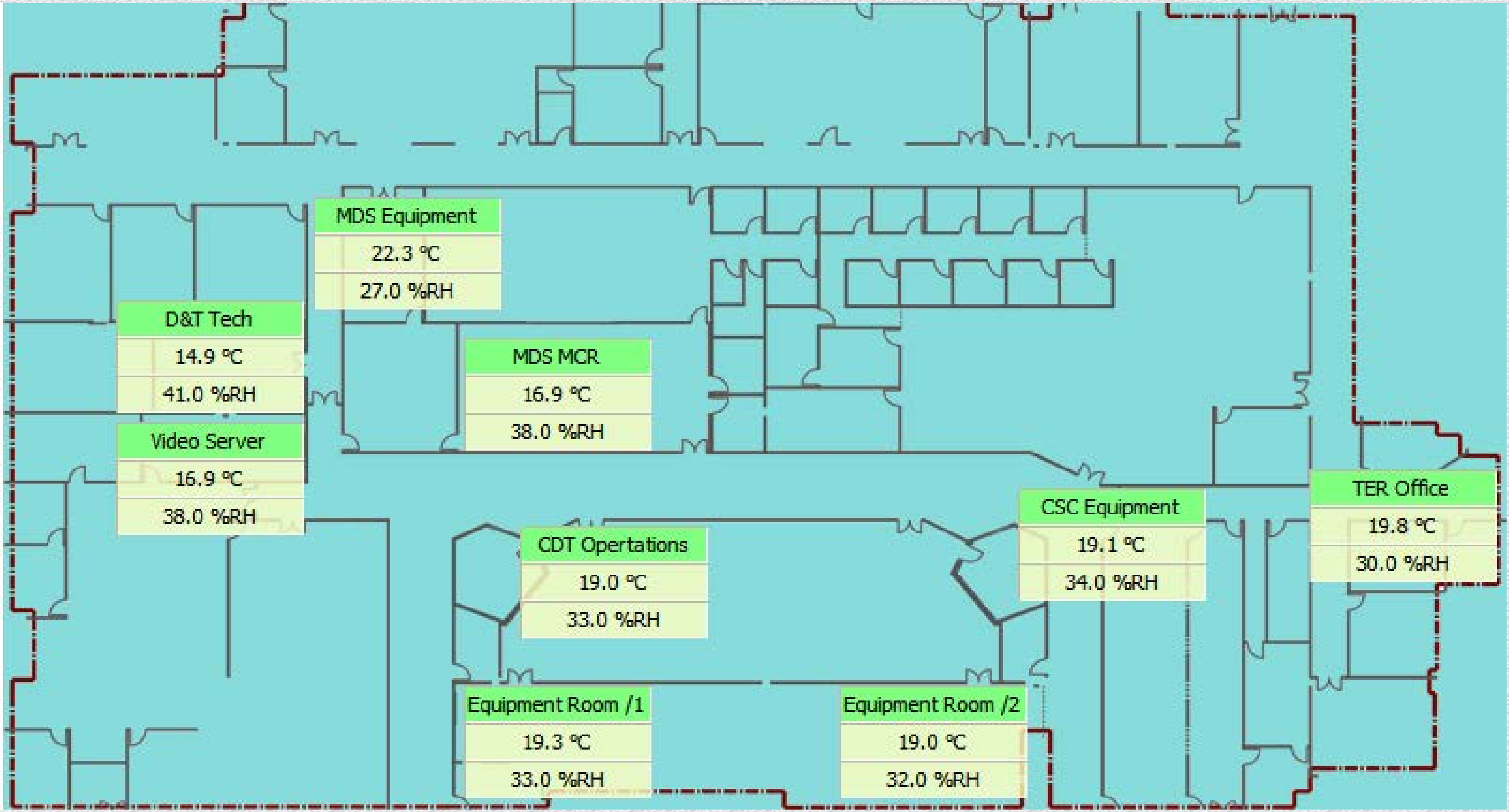
Researchers Hack Building Control System at Google Australia Office

BY KIM ZETTER 05.06.13 | 6:30 AM | PERMALINK

Share 0 Tweet 1 +1 85 Share Pin it



	Leak	Shut Off	Usage
North Kitchen	No Leak	Open	28940 L
South Kitchen	Leak Detected	Open	241140 L



MDS Equipment
22.3 ºC
27.0 %RH

D&T Tech
14.9 ºC
41.0 %RH

MDS MCR
16.9 ºC
38.0 %RH

Video Server
16.9 ºC
38.0 %RH

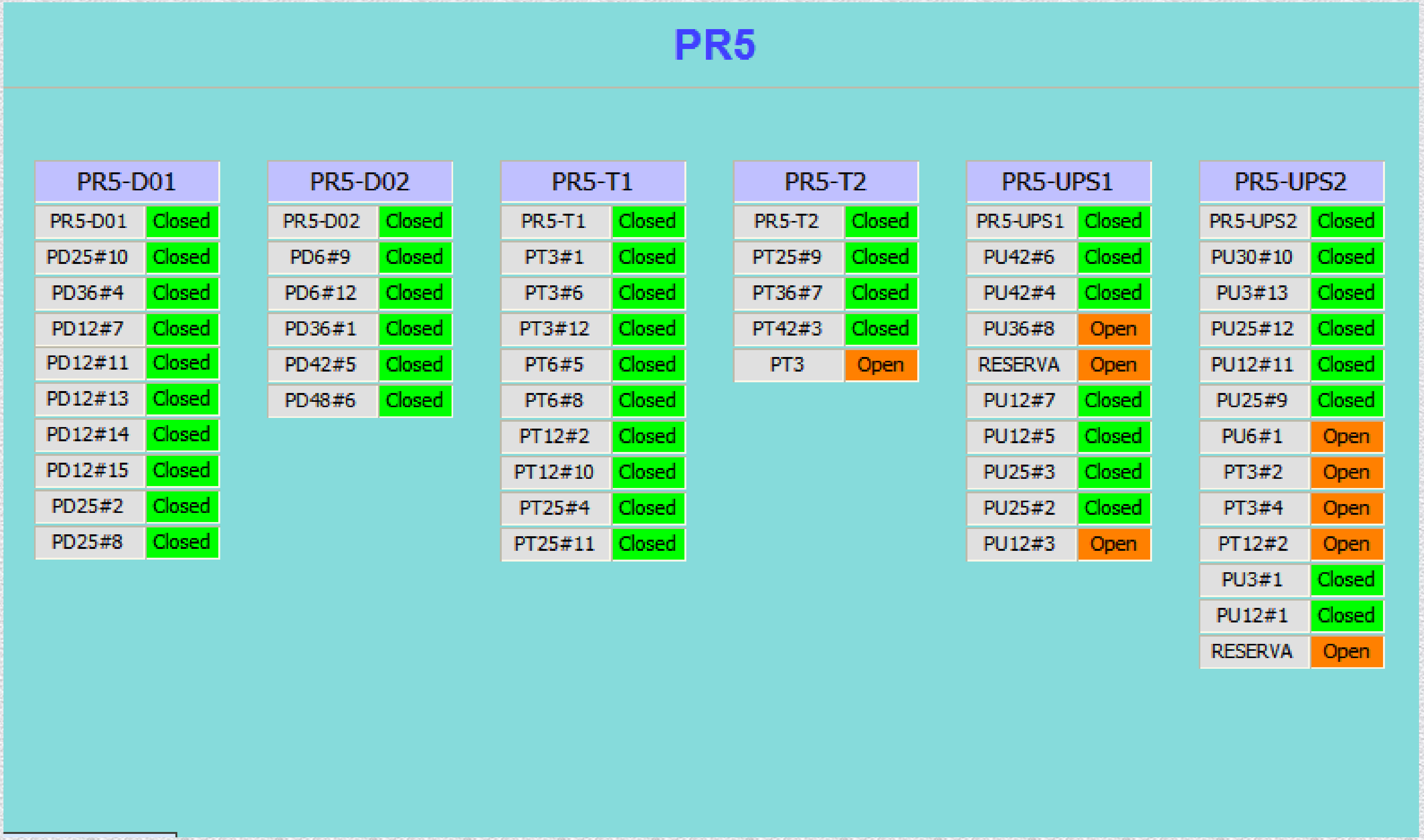
CDT Opertations
19.0 ºC
33.0 %RH

CSC Equipment
19.1 ºC
34.0 %RH

TER Office
19.8 ºC
30.0 %RH

Equipment Room /1
19.3 ºC
33.0 %RH

Equipment Room /2
19.0 ºC
32.0 %RH



PR5

PR5-D01	
PR5-D01	Closed
PD25#10	Closed
PD36#4	Closed
PD12#7	Closed
PD12#11	Closed
PD12#13	Closed
PD12#14	Closed
PD12#15	Closed
PD25#2	Closed
PD25#8	Closed

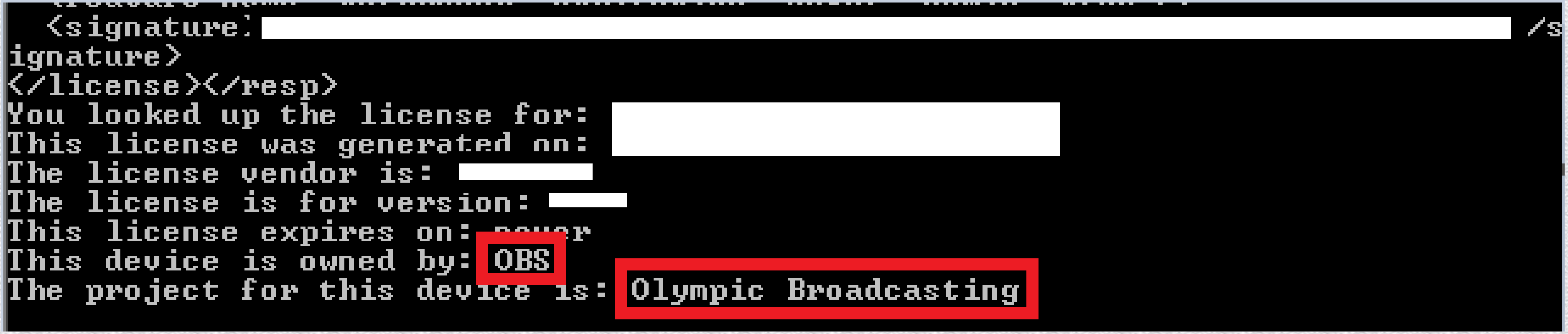
PR5-D02	
PR5-D02	Closed
PD6#9	Closed
PD6#12	Closed
PD36#1	Closed
PD42#5	Closed
PD48#6	Closed

PR5-T1	
PR5-T1	Closed
PT3#1	Closed
PT3#6	Closed
PT3#12	Closed
PT6#5	Closed
PT6#8	Closed
PT12#2	Closed
PT12#10	Closed
PT25#4	Closed
PT25#11	Closed

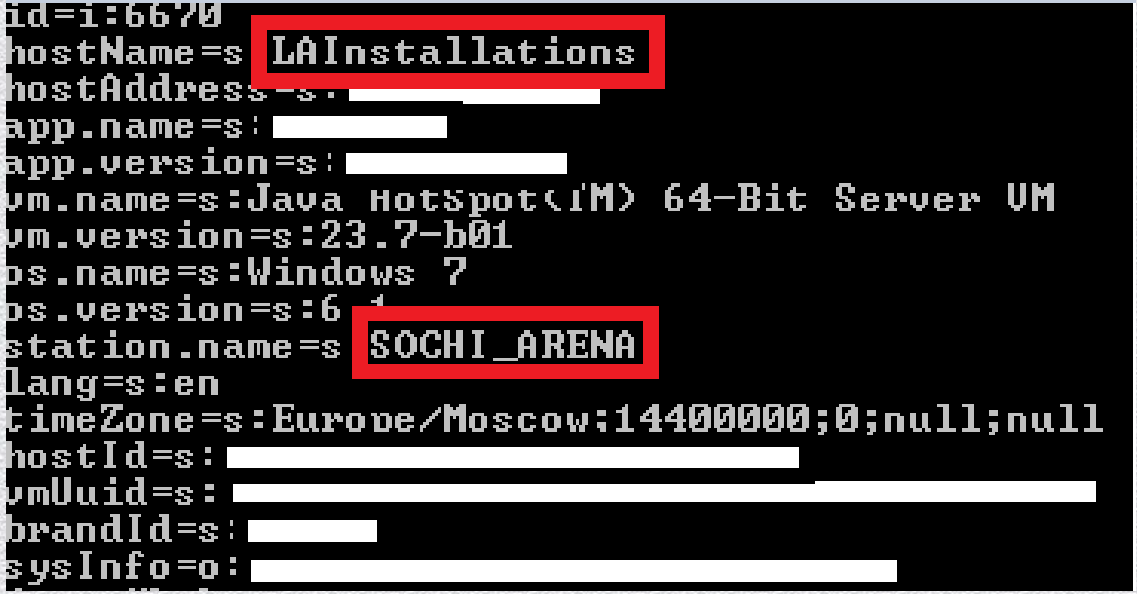
PR5-T2	
PR5-T2	Closed
PT25#9	Closed
PT36#7	Closed
PT42#3	Closed
PT3	Open

PR5-UPS1	
PR5-UPS1	Closed
PU42#6	Closed
PU42#4	Closed
PU36#8	Open
RESERVA	Open
PU12#7	Closed
PU12#5	Closed
PU25#3	Closed
PU25#2	Closed
PU12#3	Open

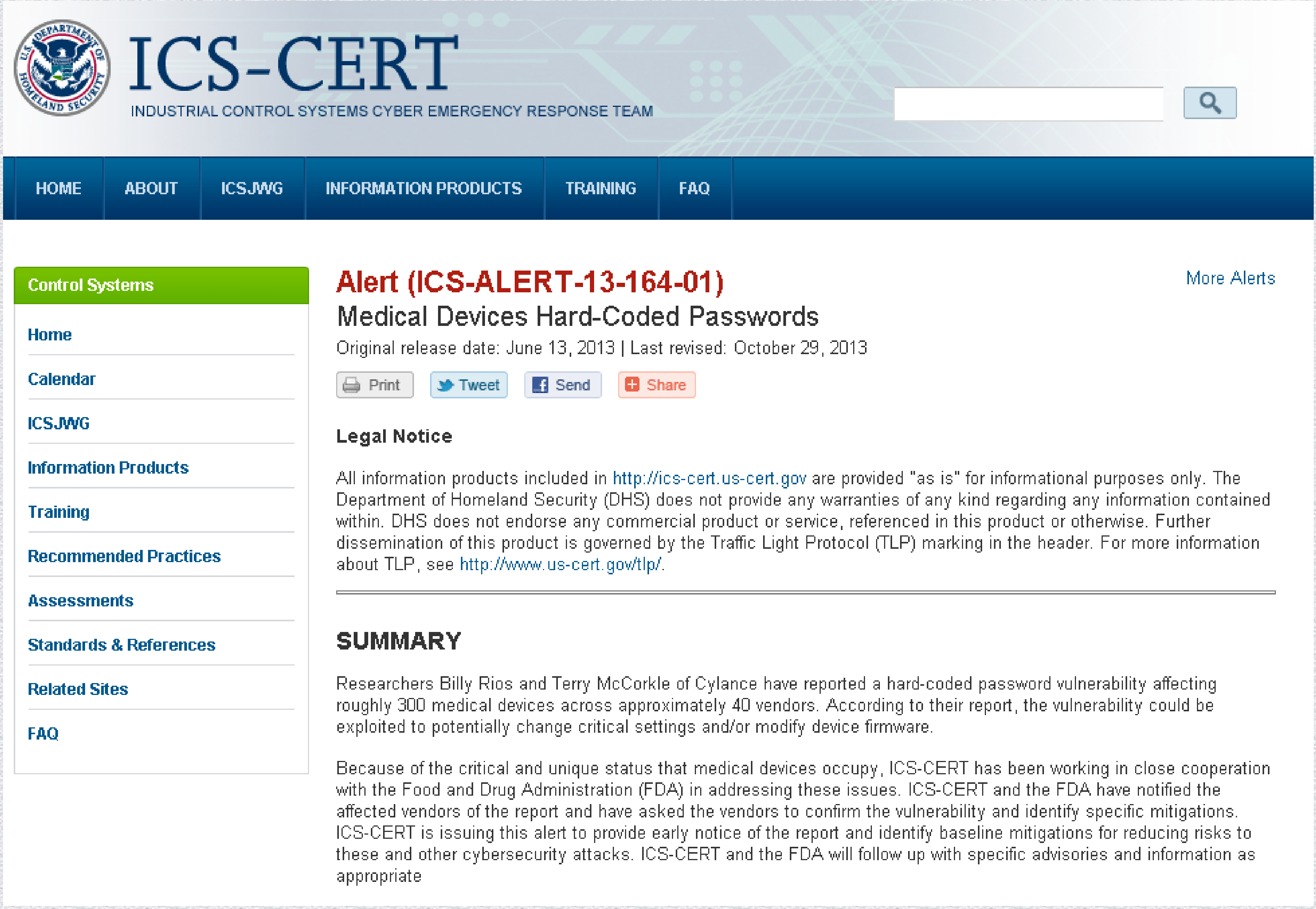
PR5-UPS2	
PR5-UPS2	Closed
PU30#10	Closed
PU3#13	Closed
PU25#12	Closed
PU12#11	Closed
PU25#9	Closed
PU6#1	Open
PT3#2	Open
PT3#4	Open
PT12#2	Open
PU3#1	Closed
PU12#1	Closed
RESERVA	Open



```
  <signature>[redacted] /s
ignature>
</license></resp>
You looked up the license for: [redacted]
This license was generated on: [redacted]
The license vendor is: [redacted]
The license is for version: [redacted]
This license expires on: never
This device is owned by: OBS
The project for this device is: Olympic Broadcasting
```



```
id=i:6670
hostName=s LAInstallations
hostAddress=s:[redacted]
app.name=s:[redacted]
app.version=s:[redacted]
vm.name=s:Java HotSpot(TM) 64-Bit Server VM
vm.version=s:23.7-b01
os.name=s:Windows 7
os.version=s:6.1
station.name=s SOCHI_ARENA
lang=s:en
timeZone=s:Europe/Moscow:14400000;0;null;null
hostId=s:[redacted]
vmUuid=s:[redacted]
brandId=s:[redacted]
sysInfo=o:[redacted]
```



Alert (ICS-ALERT-13-164-01)

Medical Devices Hard-Coded Passwords

Original release date: June 13, 2013 | Last revised: October 29, 2013

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

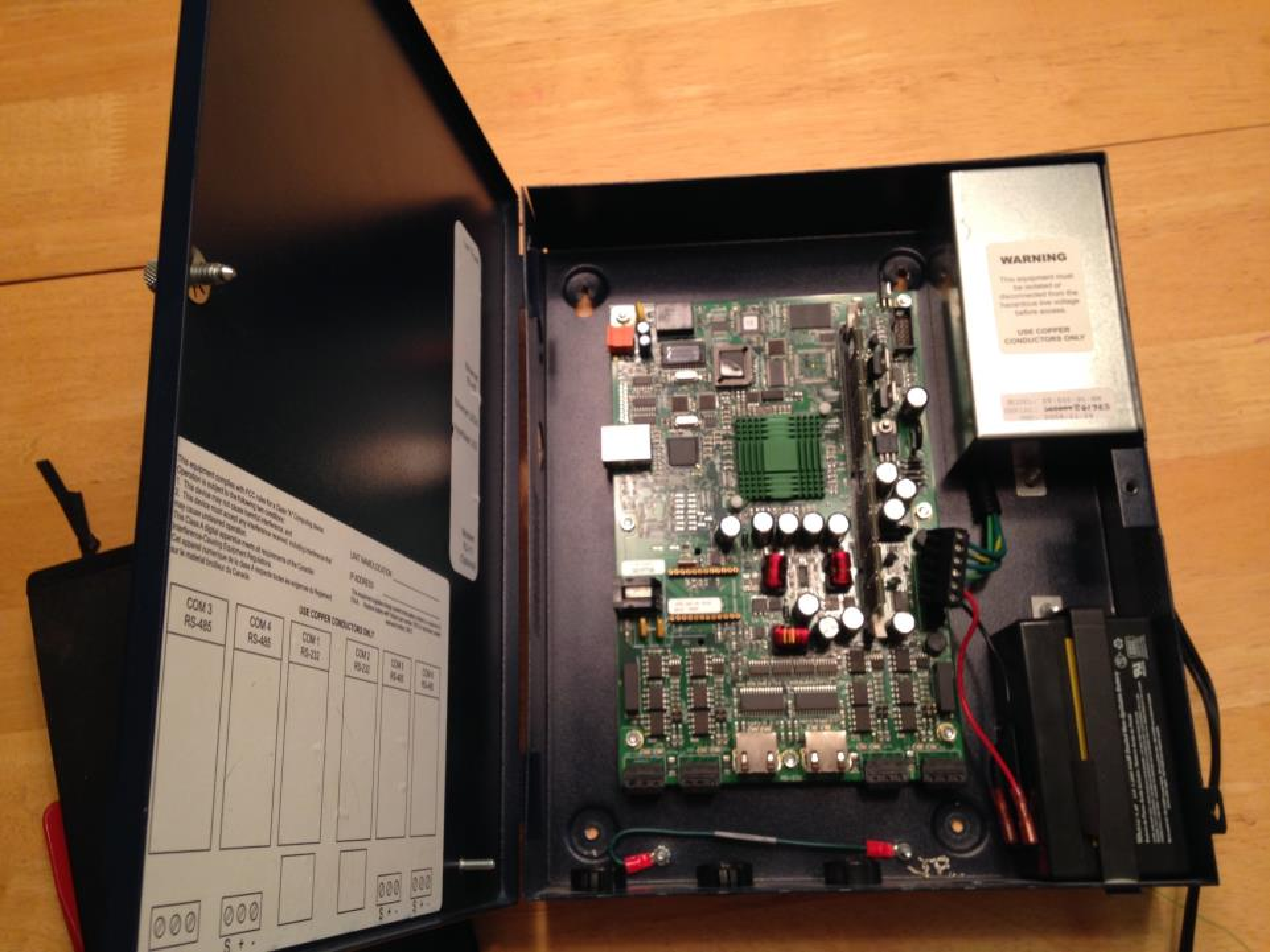
SUMMARY

Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware.

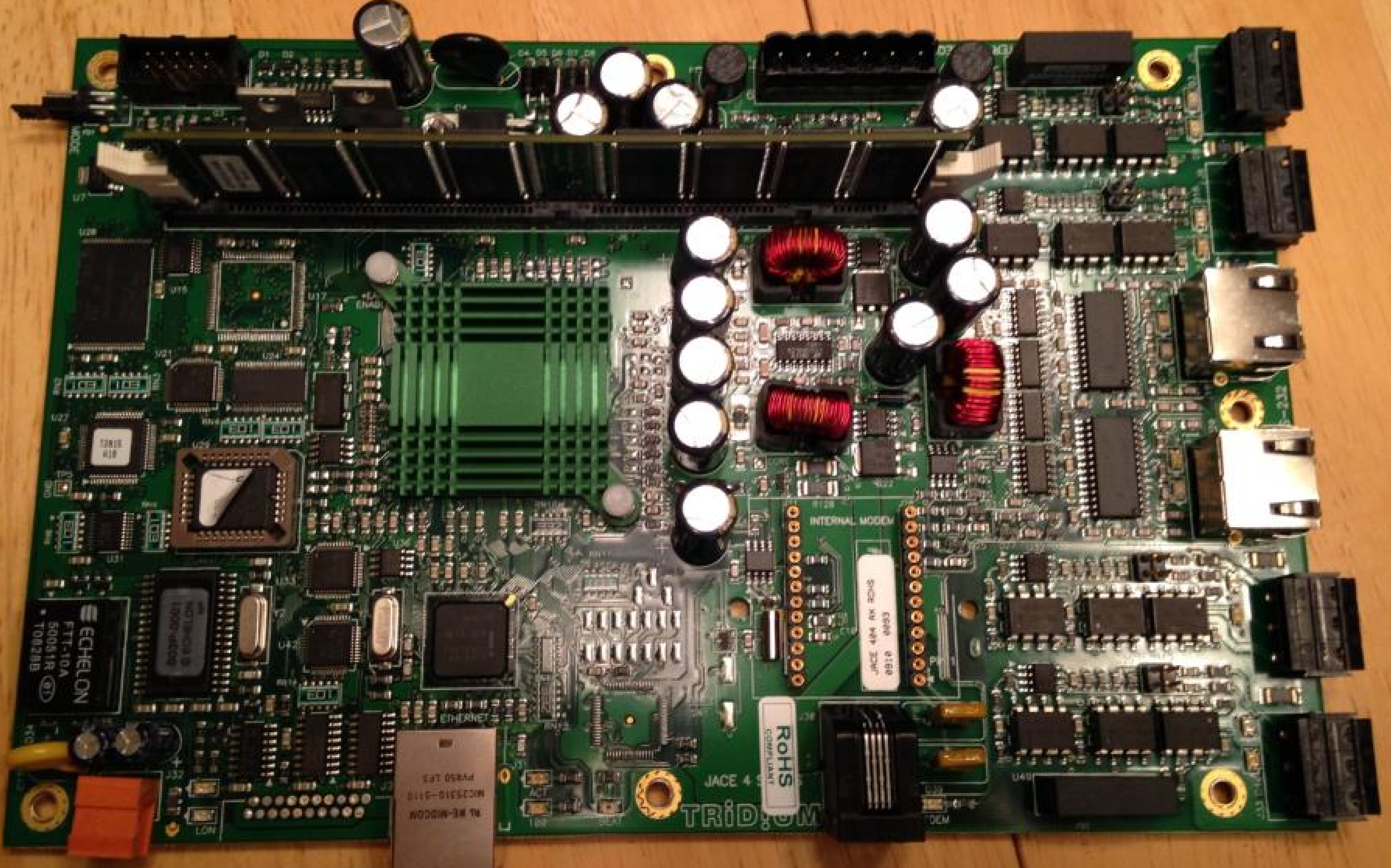
Because of the critical and unique status that medical devices occupy, ICS-CERT has been working in close cooperation with the Food and Drug Administration (FDA) in addressing these issues. ICS-CERT and the FDA have notified the affected vendors of the report and have asked the vendors to confirm the vulnerability and identify specific mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks. ICS-CERT and the FDA will follow up with specific advisories and information as appropriate “hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors”

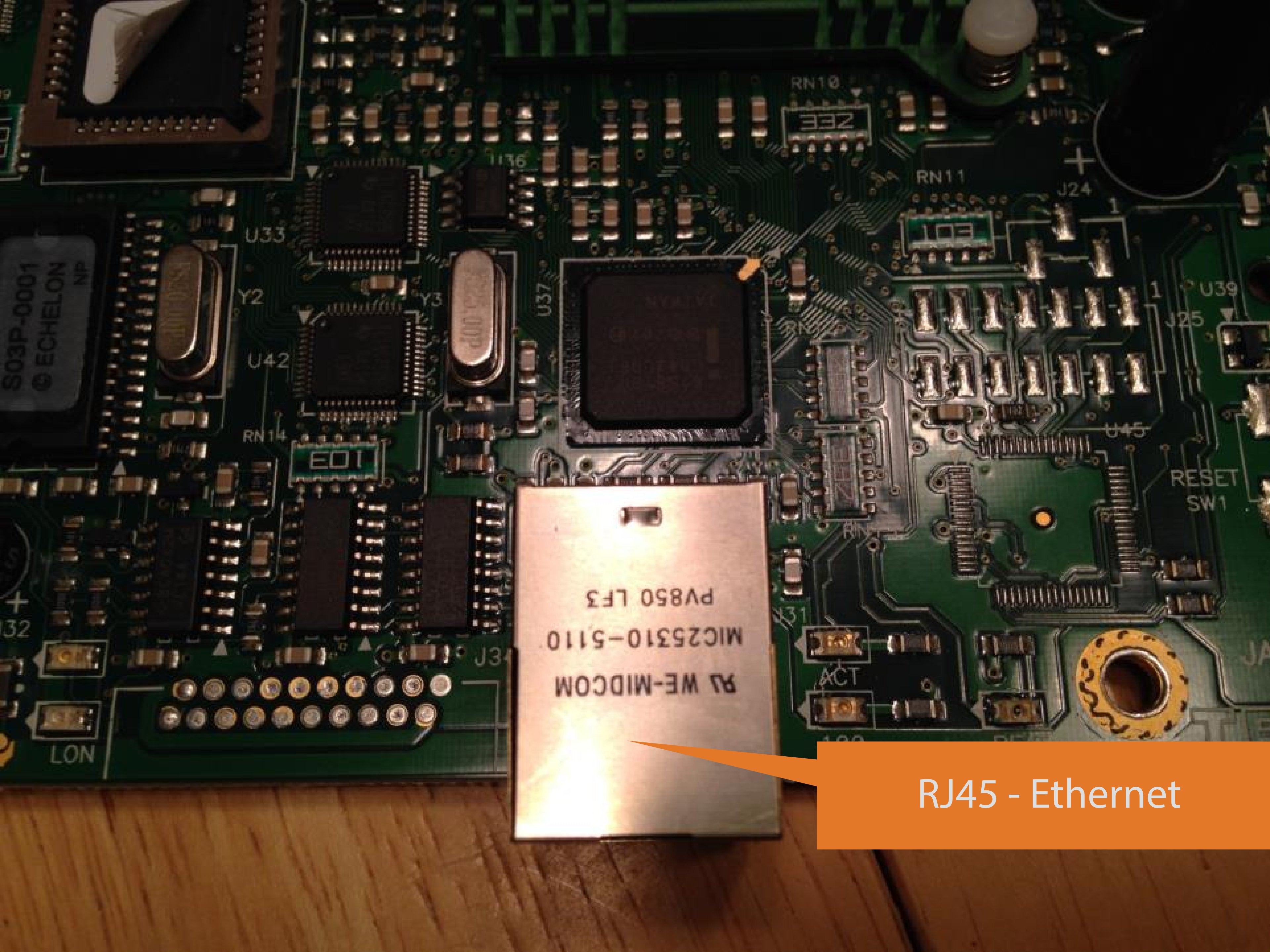
Niagara AX
INTEGRA™
AMERICAN AUTO-MATRIX®
SMART BUILDING SOLUTIONS®

AMERICAN
AUTO-MATRIX®
SMART BUILDING SOLUTIONS®

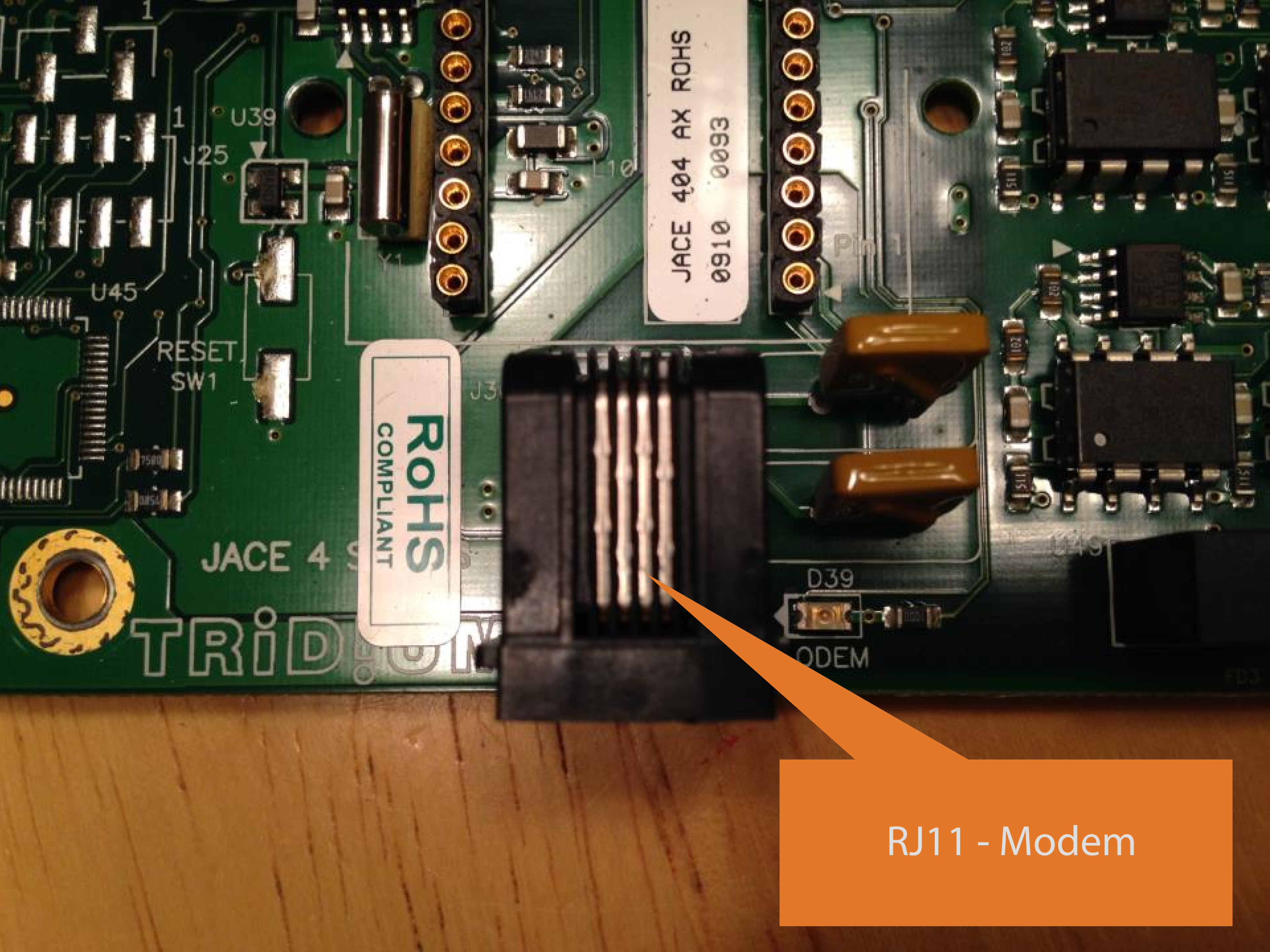


WARNING
This equipment must be isolated or disconnected from the hazardous line voltage before access.
USE COPPER CONDUCTORS ONLY
UNIT NAME/LOCATION
IP ADDRESS
USE COPPER CONDUCTORS ONLY
COM 3 RS-485
COM 4 RS-485
COM 1 RS-232
COM 2 RS-232
S + -
S + -
S + -


INTERNAL MODEM
RoHS
COMPLIANT
JACE 4
TRiD!UM
ETHERNET
ECHELON
FTT-10A
ACT
LON

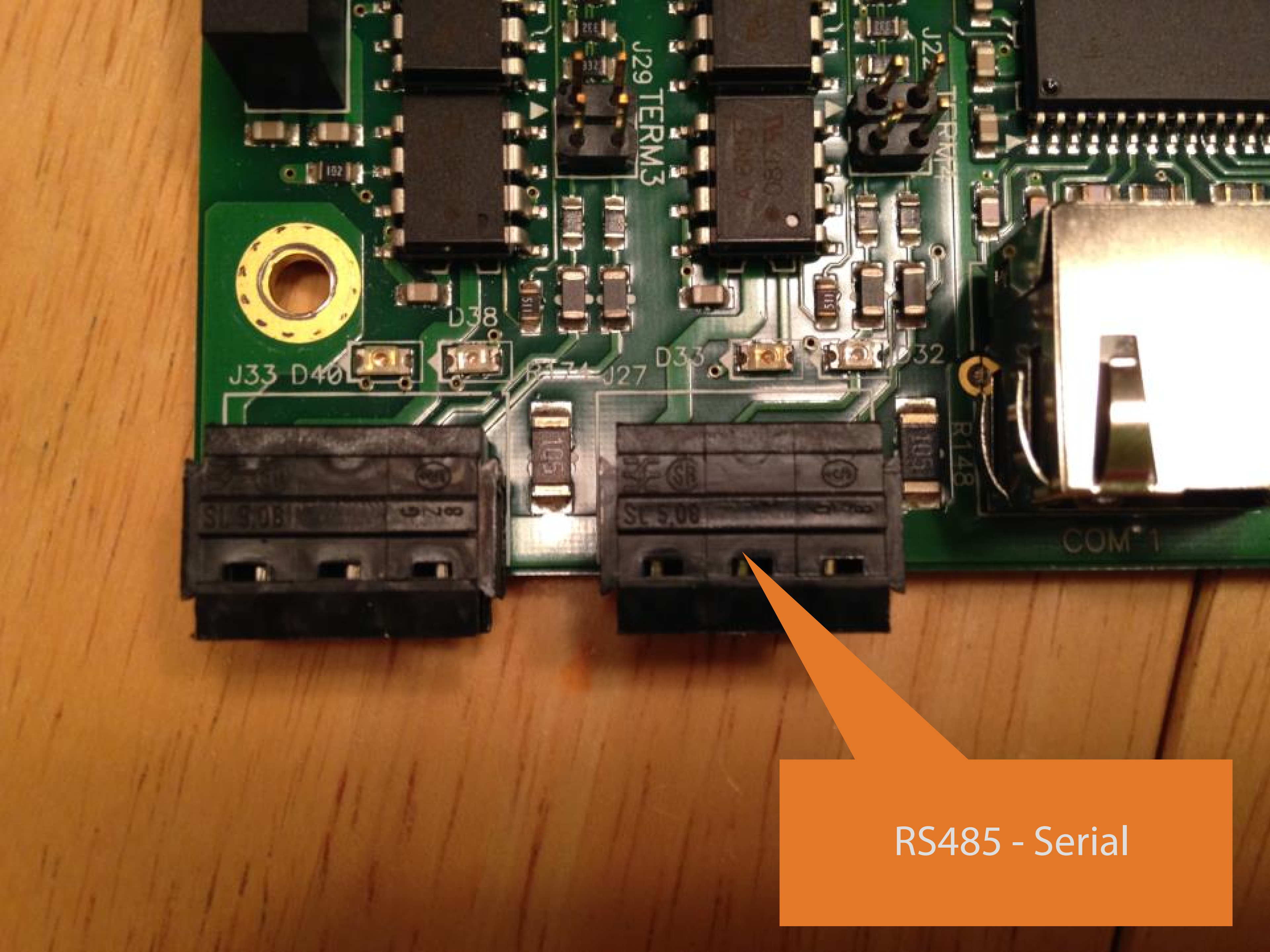


RJ45 - Ethernet

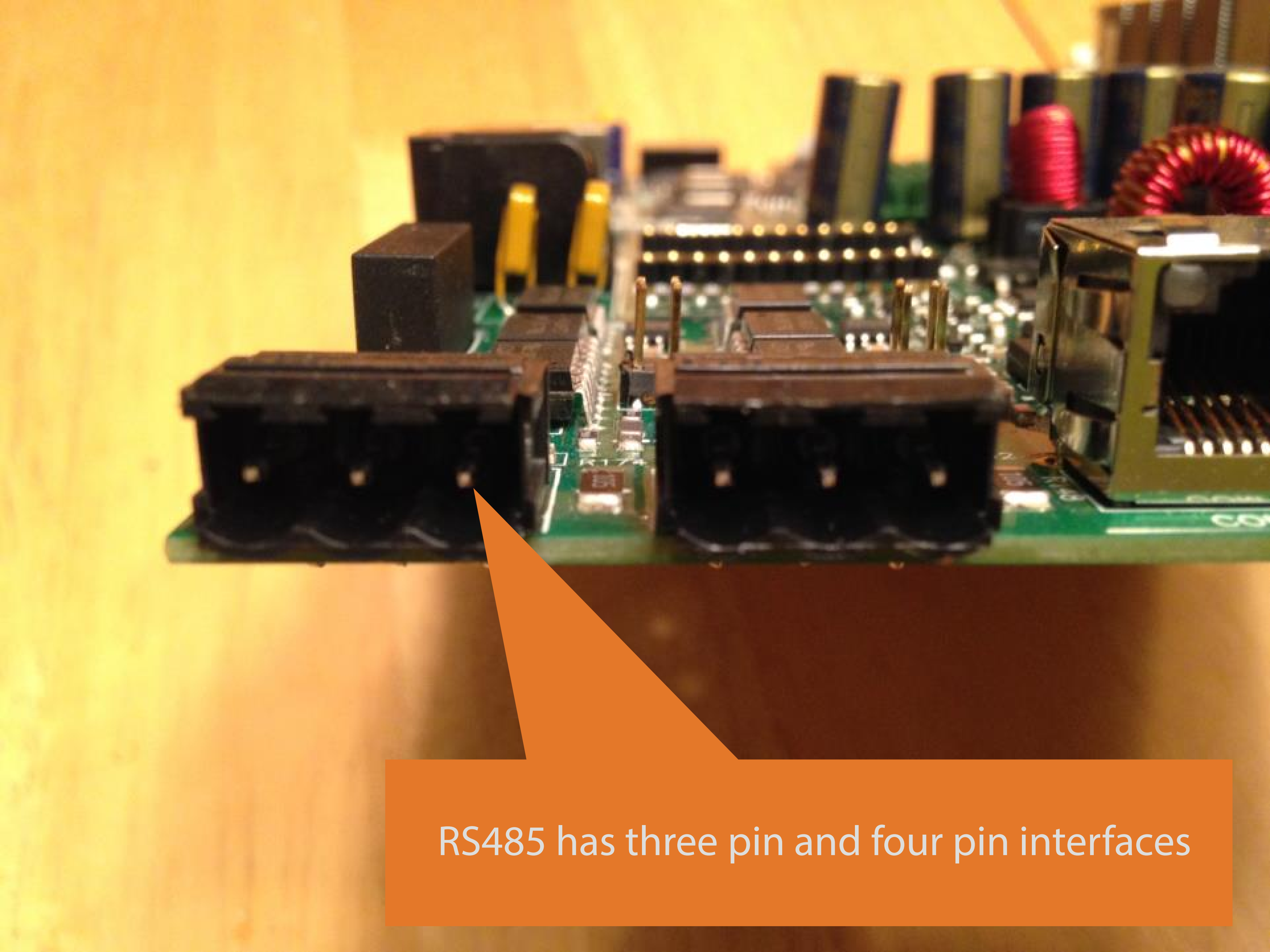


JACE 404 AX ROHS
0910 0093
RoHS
COMPLIANT
U39
J25
U45
RESET
SW1
Y1
L10
Pin 1
D39
MODEM
JACE 4
TRIDIUM

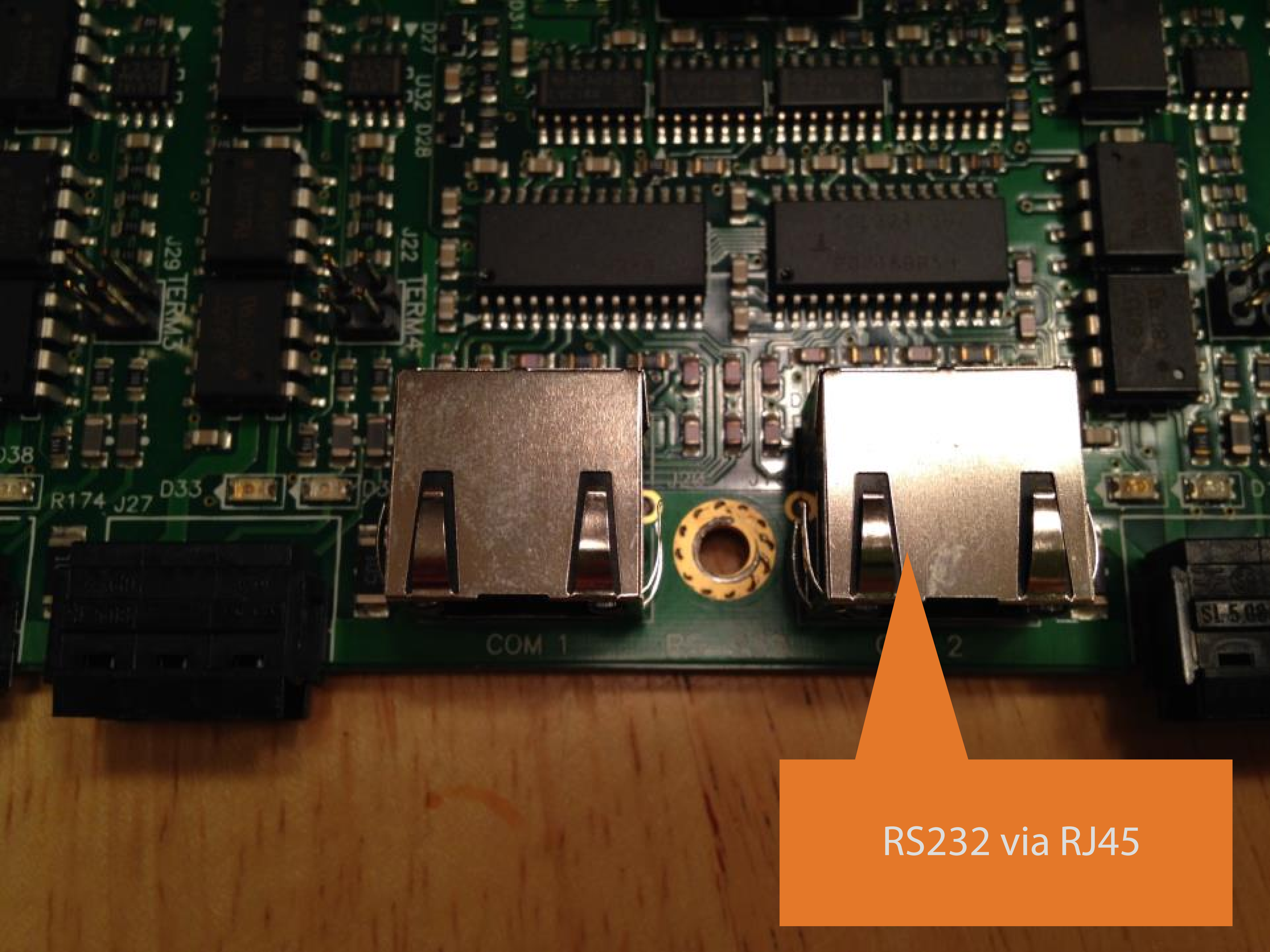
RJ11 - Modem



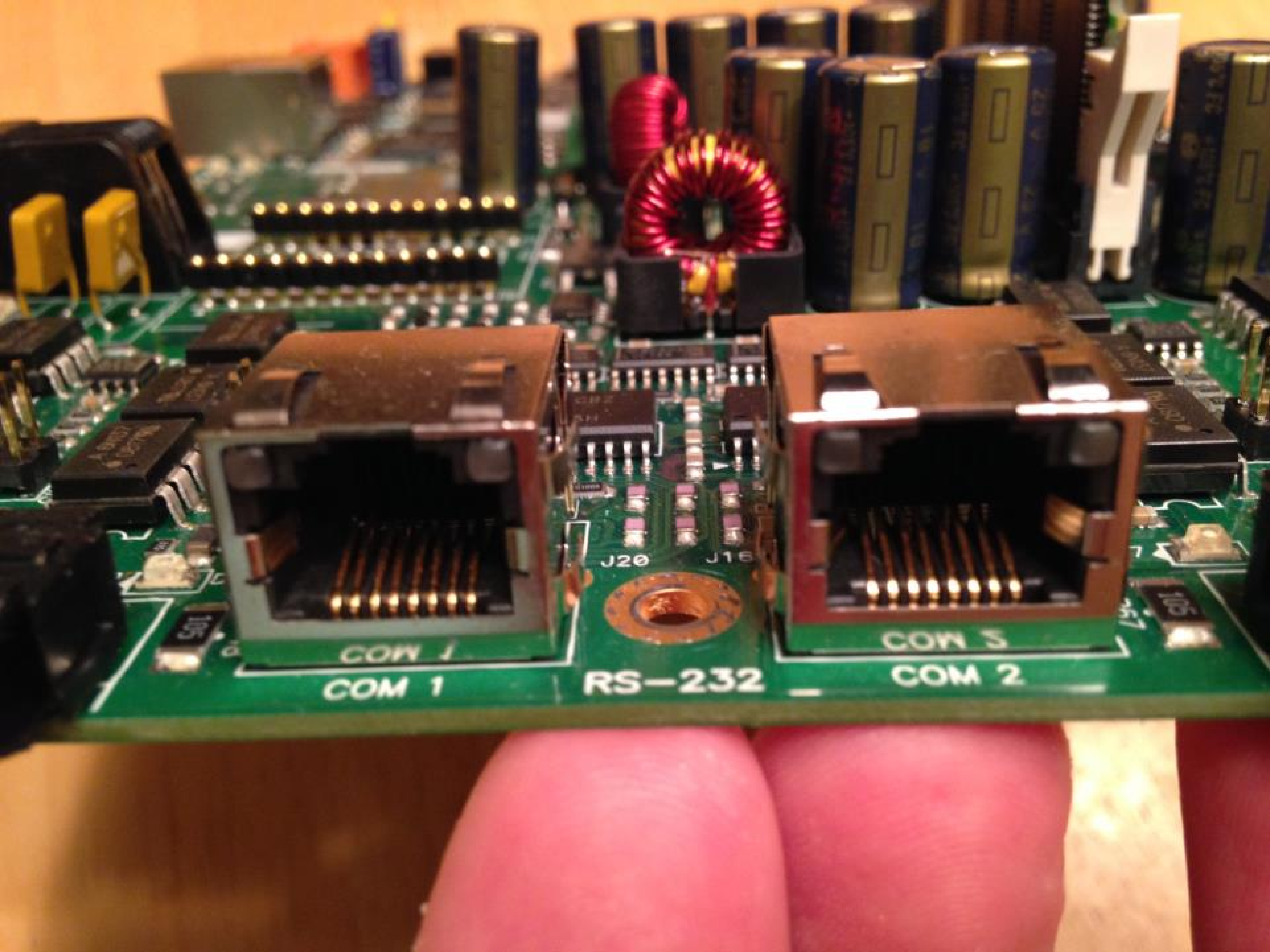
RS485 - Serial

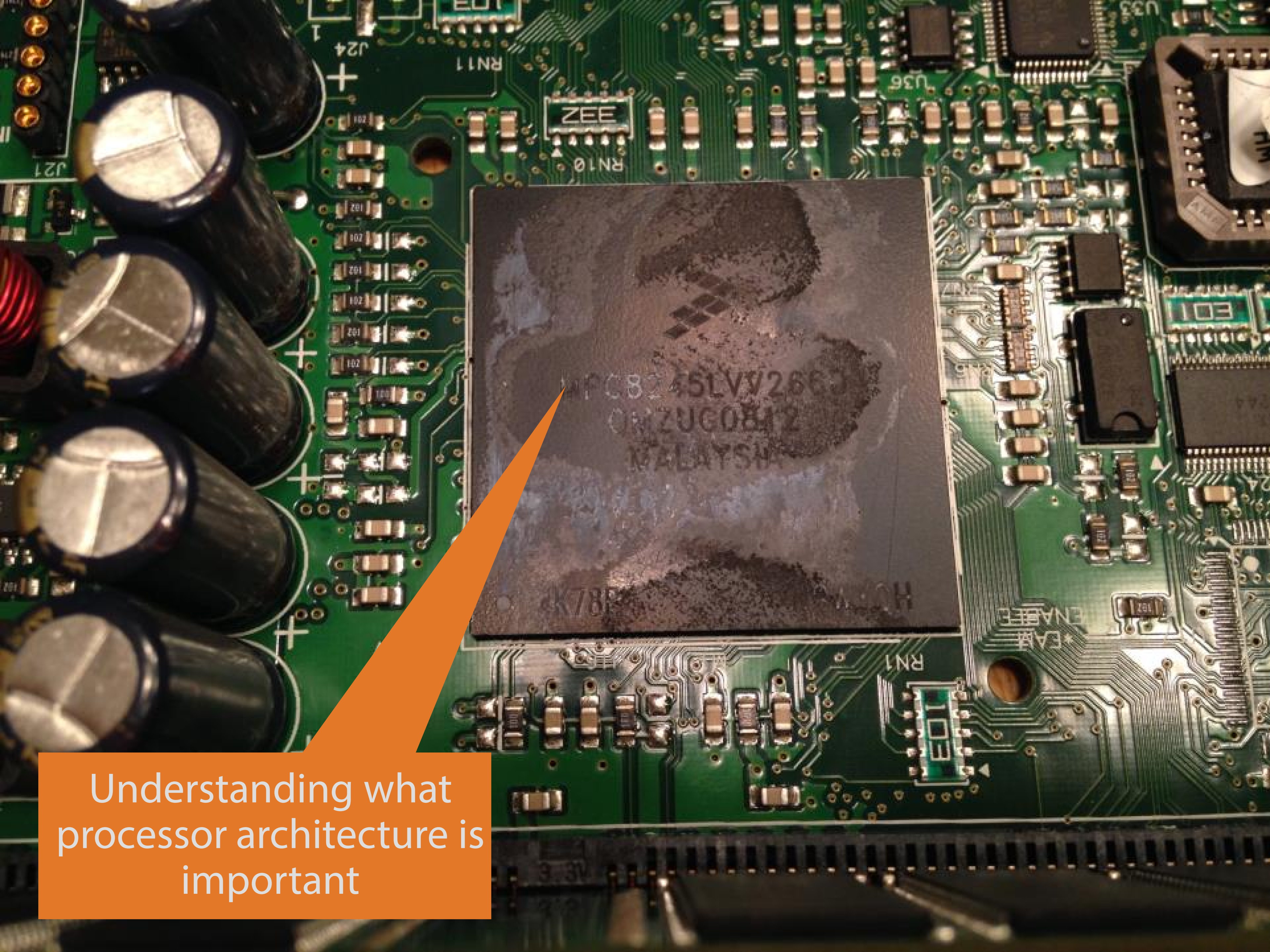


RS485 has three pin and four pin interfaces



RS232 via RJ45


J20
J16
COM 1
COM 2
COM 1
RS-232
COM 2
105
105

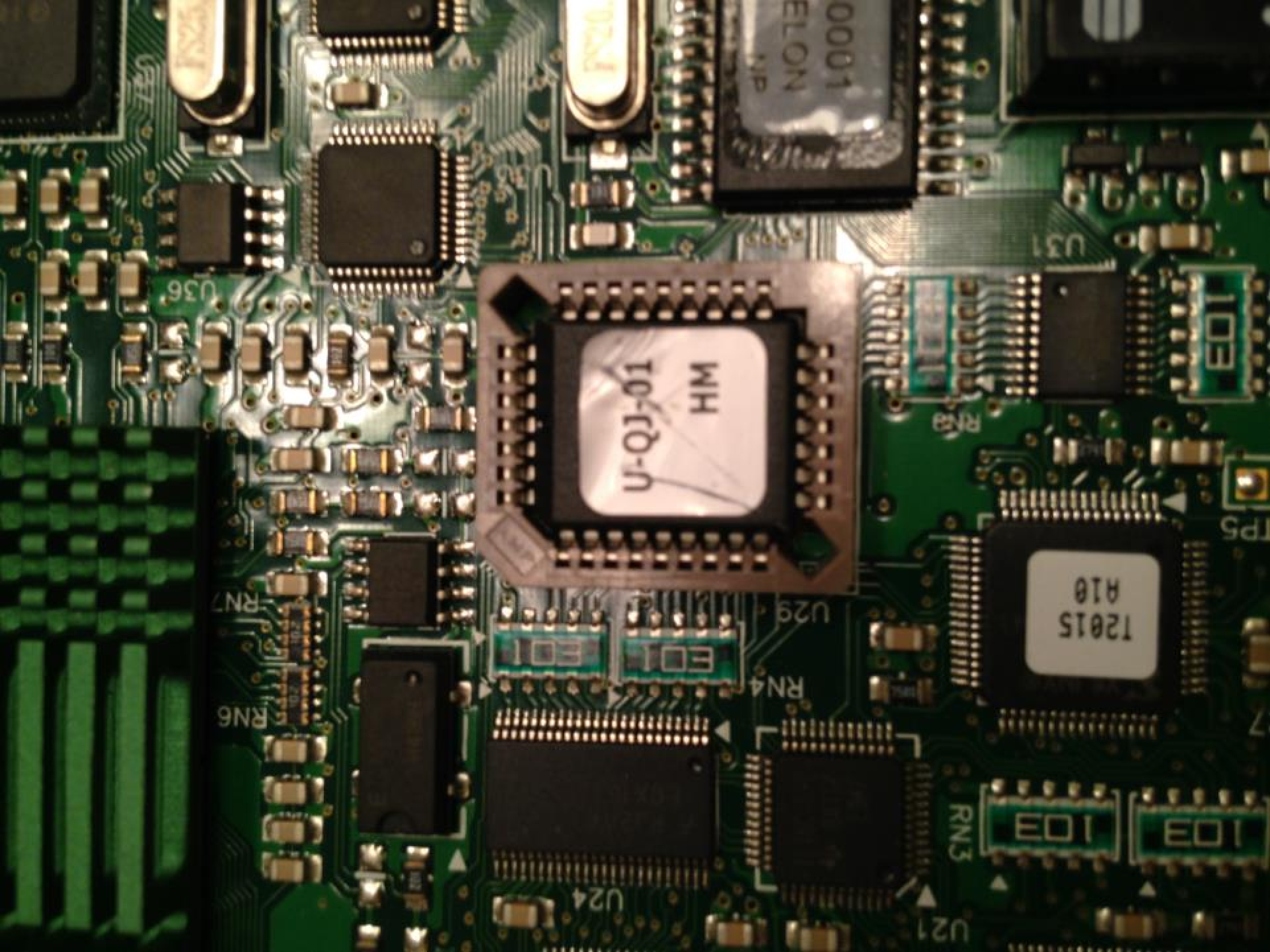


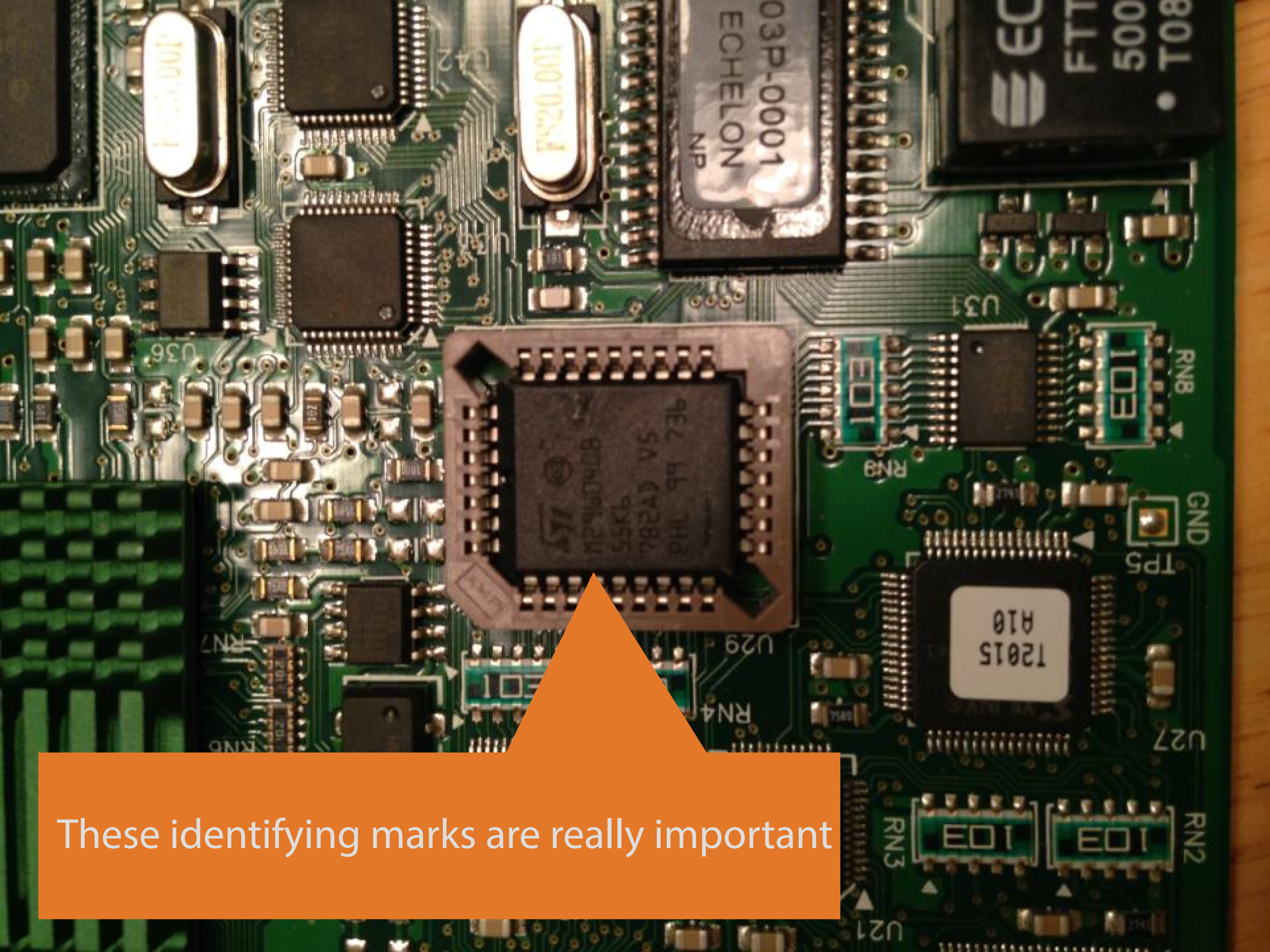
Understanding what processor architecture is important

Common Embedded Architectures

- Processors
  - X86
  - ARM
  - Motorola PowerPC

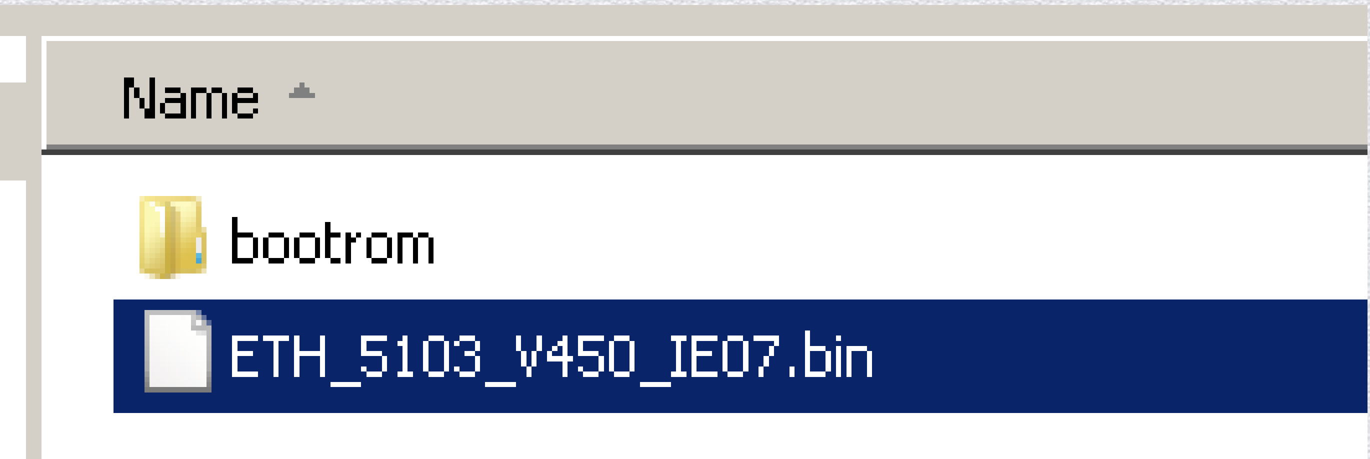
- Operating Systems
  - Windows CE/Embedded
  - VxWorks
  - BusyBox
  - QNX


U36
U31
U29
RN4
RN3
RN6
RN7
RN8
U24
U21
TP5
103



These identifying marks are really important

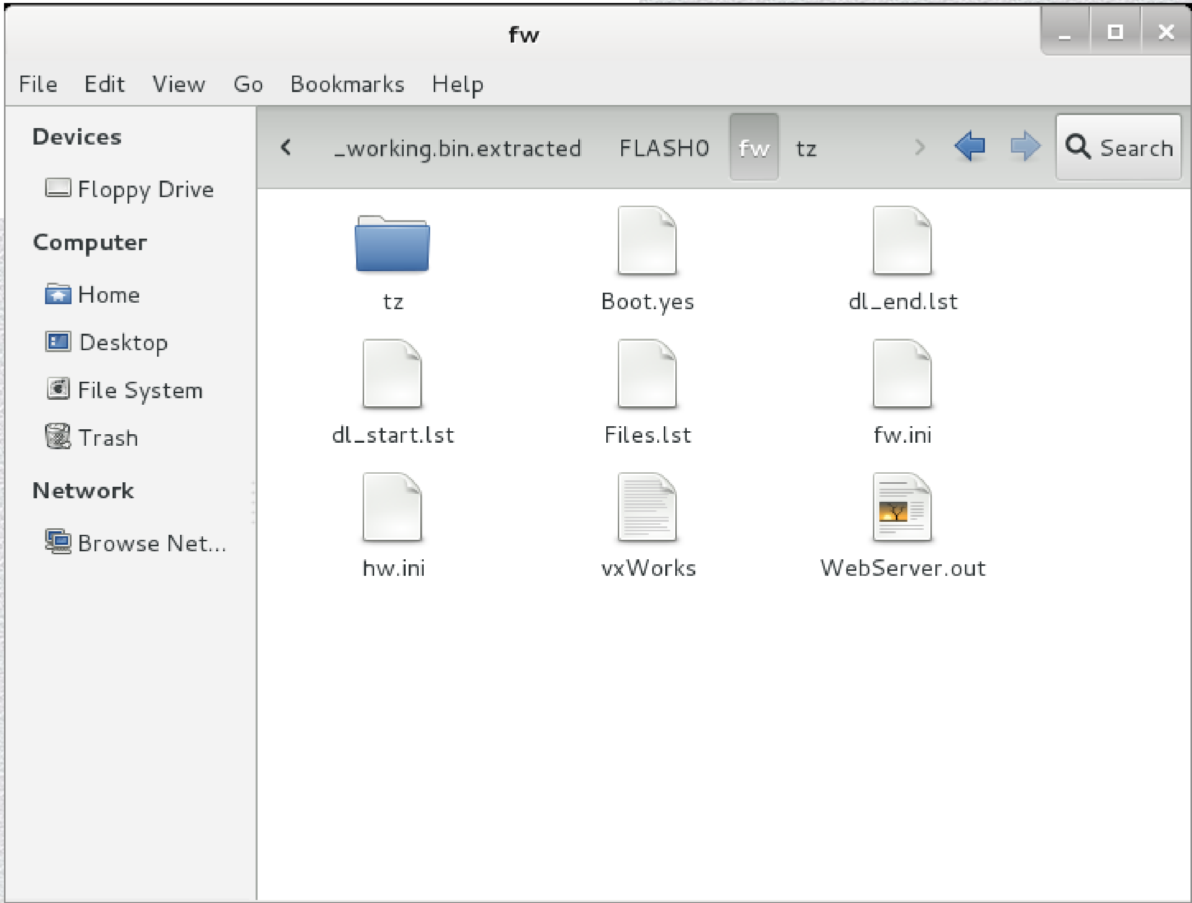
GQ-4X
True USB Universal Programmer
VCC ON VPP
3M



Name

bootrom

ETH_5103_V450_IE07.bin



tz

Boot.yes

dl_end.lst

dl_start.lst

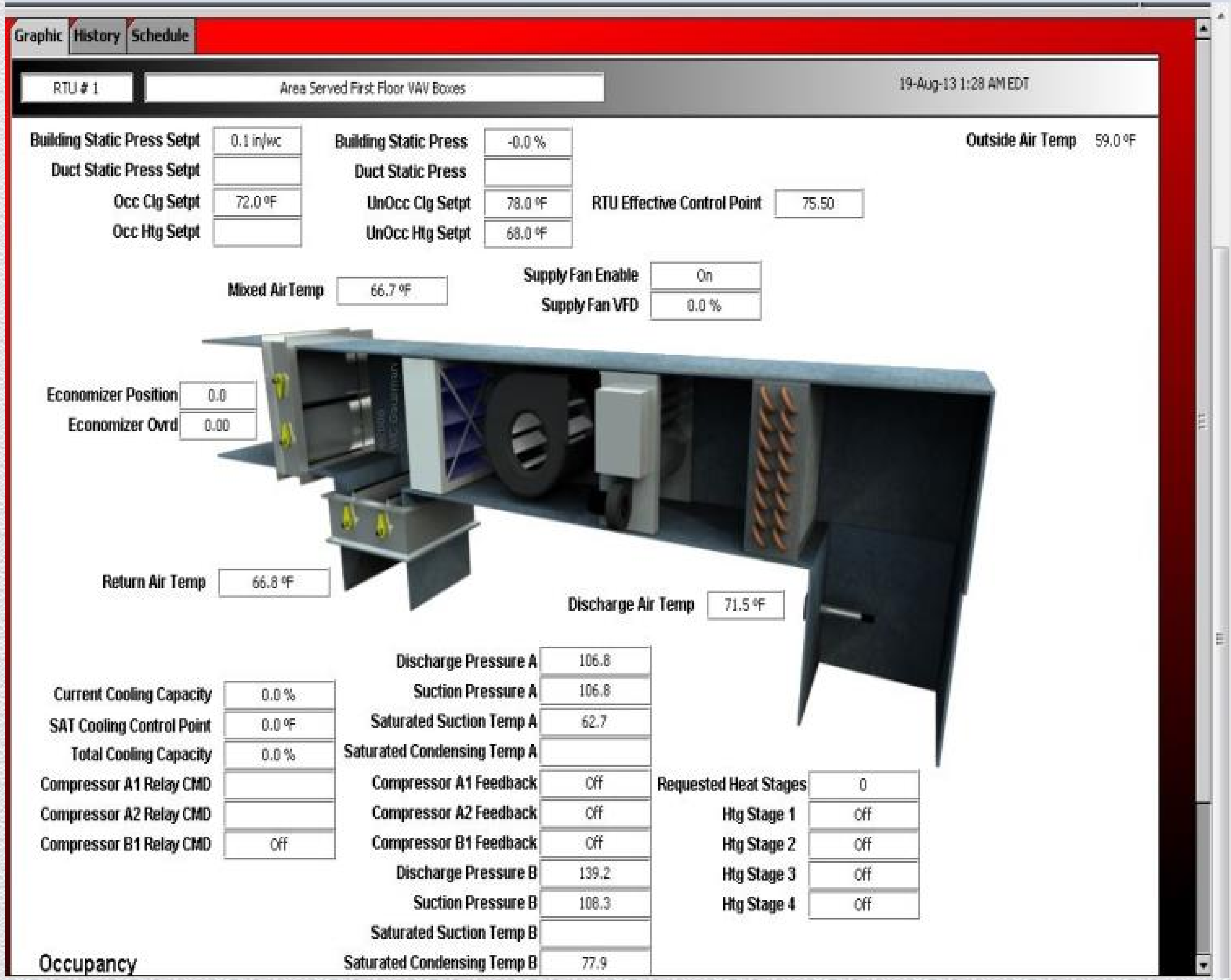
Files.lst

fw.ini

hw.ini

vxWorks

WebServer.out



RTU # 1

Area Served First Floor VAV Boxes

19-Aug-13 1:28 AM EDT

Building Static Press Setpt: 0.1 in/wc

Duct Static Press Setpt:

Occ Clg Setpt: 72.0 °F

Occ Htg Setpt:

Building Static Press: -0.0 %

Duct Static Press:

UnOcc Clg Setpt: 78.0 °F

UnOcc Htg Setpt: 68.0 °F

RTU Effective Control Point: 75.50

Outside Air Temp: 59.0 °F

Mixed Air Temp: 66.7 °F

Supply Fan Enable: On

Supply Fan VFD: 0.0 %

Economizer Position: 0.0

Economizer Ovrd: 0.00

Return Air Temp: 66.8 °F

Discharge Air Temp: 71.5 °F

Current Cooling Capacity: 0.0 %

SAT Cooling Control Point: 0.0 °F

Total Cooling Capacity: 0.0 %

Compressor A1 Relay CMD:

Compressor A2 Relay CMD:

Compressor B1 Relay CMD: Off

Discharge Pressure A: 106.8

Suction Pressure A: 106.8

Saturated Suction Temp A: 62.7

Saturated Condensing Temp A:

Compressor A1 Feedback: Off

Compressor A2 Feedback: Off

Compressor B1 Feedback: Off

Discharge Pressure B: 139.2

Suction Pressure B: 108.3

Saturated Suction Temp B:

Saturated Condensing Temp B: 77.9

Requested Heat Stages: 0

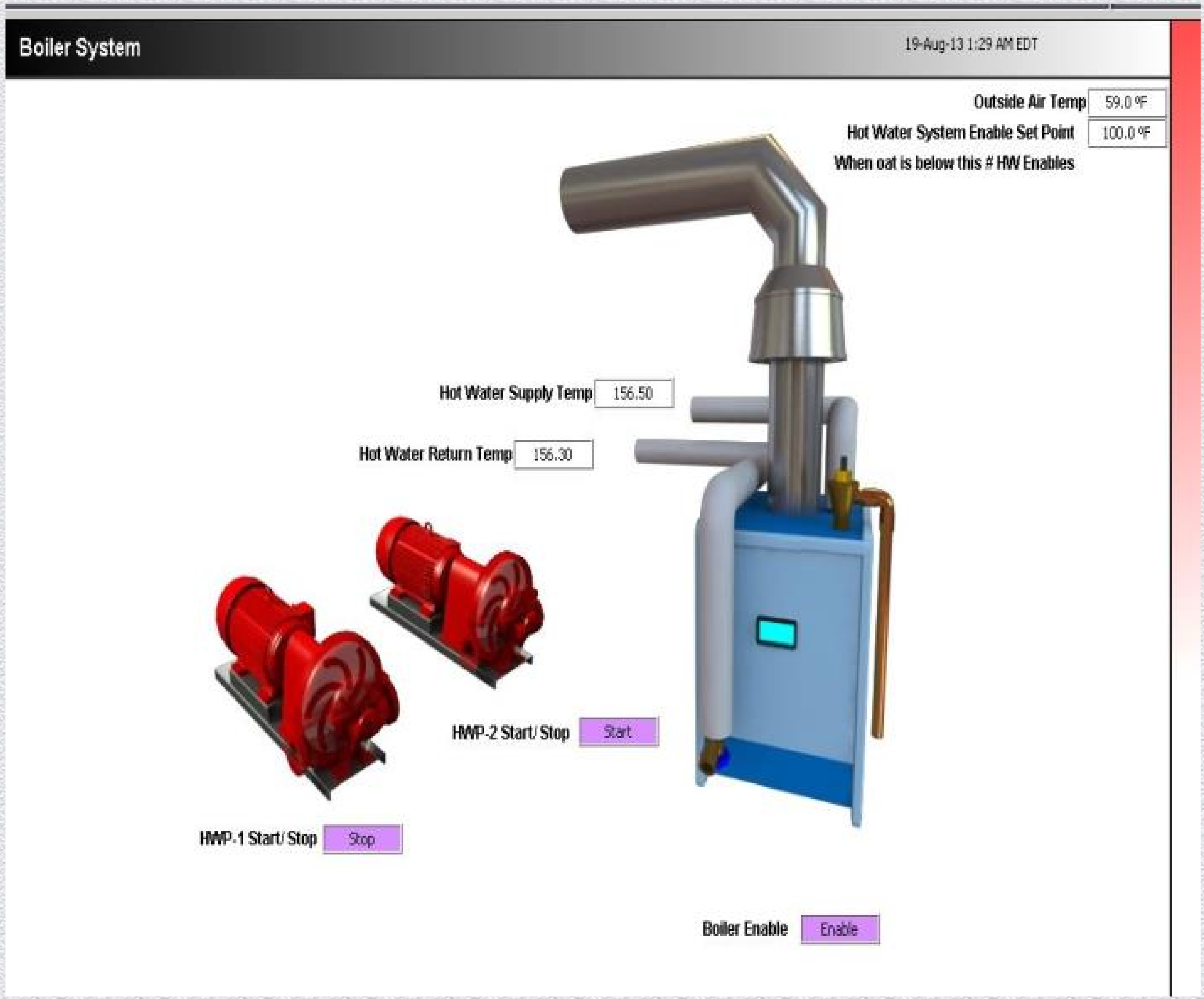
Htg Stage 1: Off

Htg Stage 2: Off

Htg Stage 3: Off

Htg Stage 4: Off

Occupancy



Boiler System

19-Aug-13 1:29 AM EDT

Outside Air Temp 59.0 °F

Hot Water System Enable Set Point 100.0 °F

When oat is below this # HW Enables

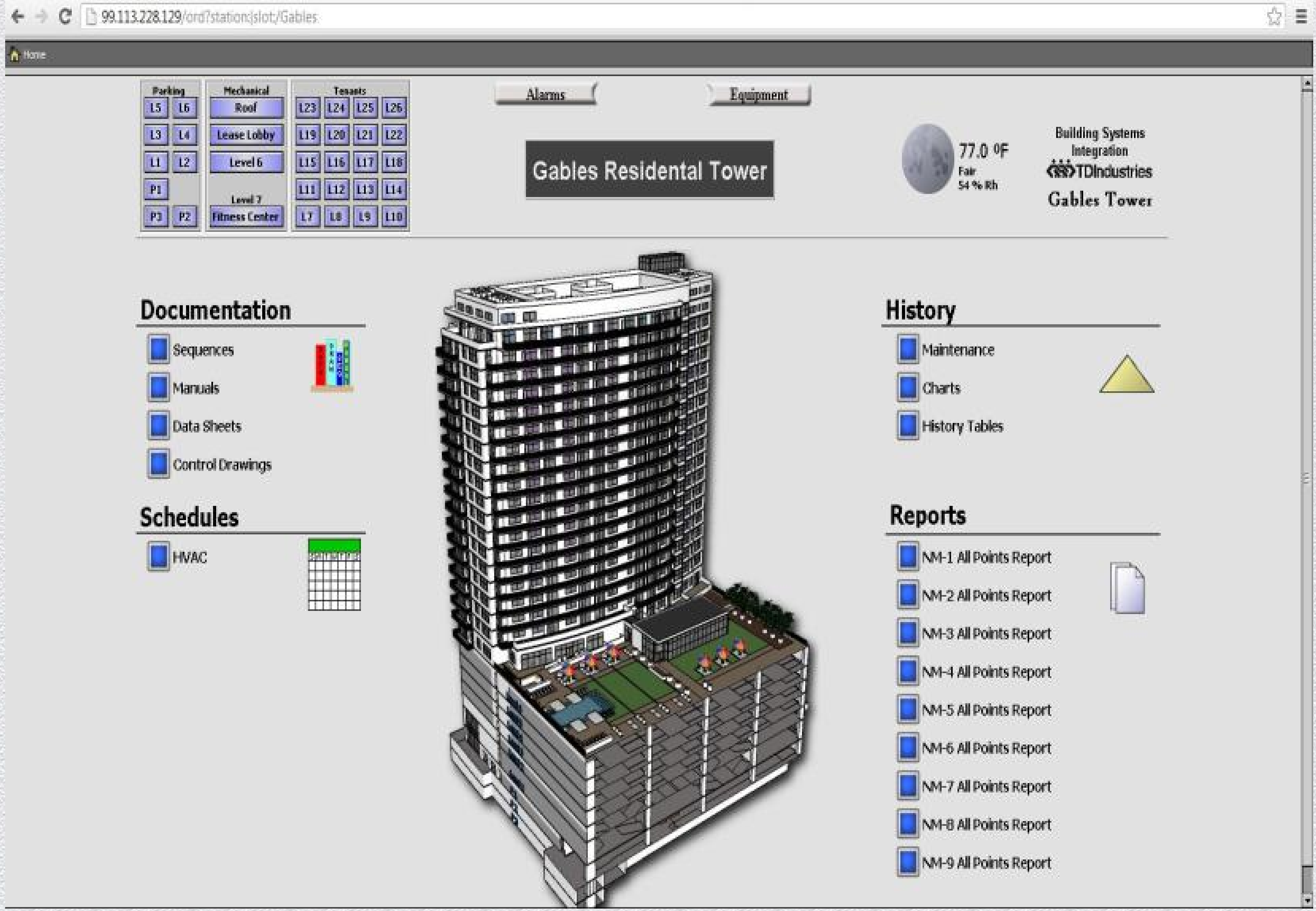
Hot Water Supply Temp 156.50

Hot Water Return Temp 156.30

HWP-2 Start/ Stop

HWP-1 Start/ Stop

Boiler Enable


99.113.228.129/ord?station:|slot:/Gables
Home
Parking
L5 L6
L3 L4
L1 L2
P1
P3 P2
Mechanical
Roof
Lease Lobby
Level 6
Level 7
Fitness Center
Tenants
L23 L24 L25 L26
L19 L20 L21 L22
L15 L16 L17 L18
L11 L12 L13 L14
L7 L8 L9 L10
Alarms
Equipment
Gables Residental Tower
77.0 °F
Fair
54 % Rh
Building Systems
Integration
TDIndustries
Gables Tower
Documentation
Sequences
Manuals
Data Sheets
Control Drawings
Schedules
HVAC
History
Maintenance
Charts
History Tables
Reports
NM-1 All Points Report
NM-2 All Points Report
NM-3 All Points Report
NM-4 All Points Report
NM-5 All Points Report
NM-6 All Points Report
NM-7 All Points Report
NM-8 All Points Report
NM-9 All Points Report

The Enumeration Effort

- Internet Facing
  - Initially based on Shodan, now running in EC2
  - 50,000+ buildings
  - Stadiums, Hospitals, Police Stations, Prisons, Corporations, Military Installations…etc
- Costs
  - EC2 time
  - Hardware and software for research
  - All total ~$500

Our Target

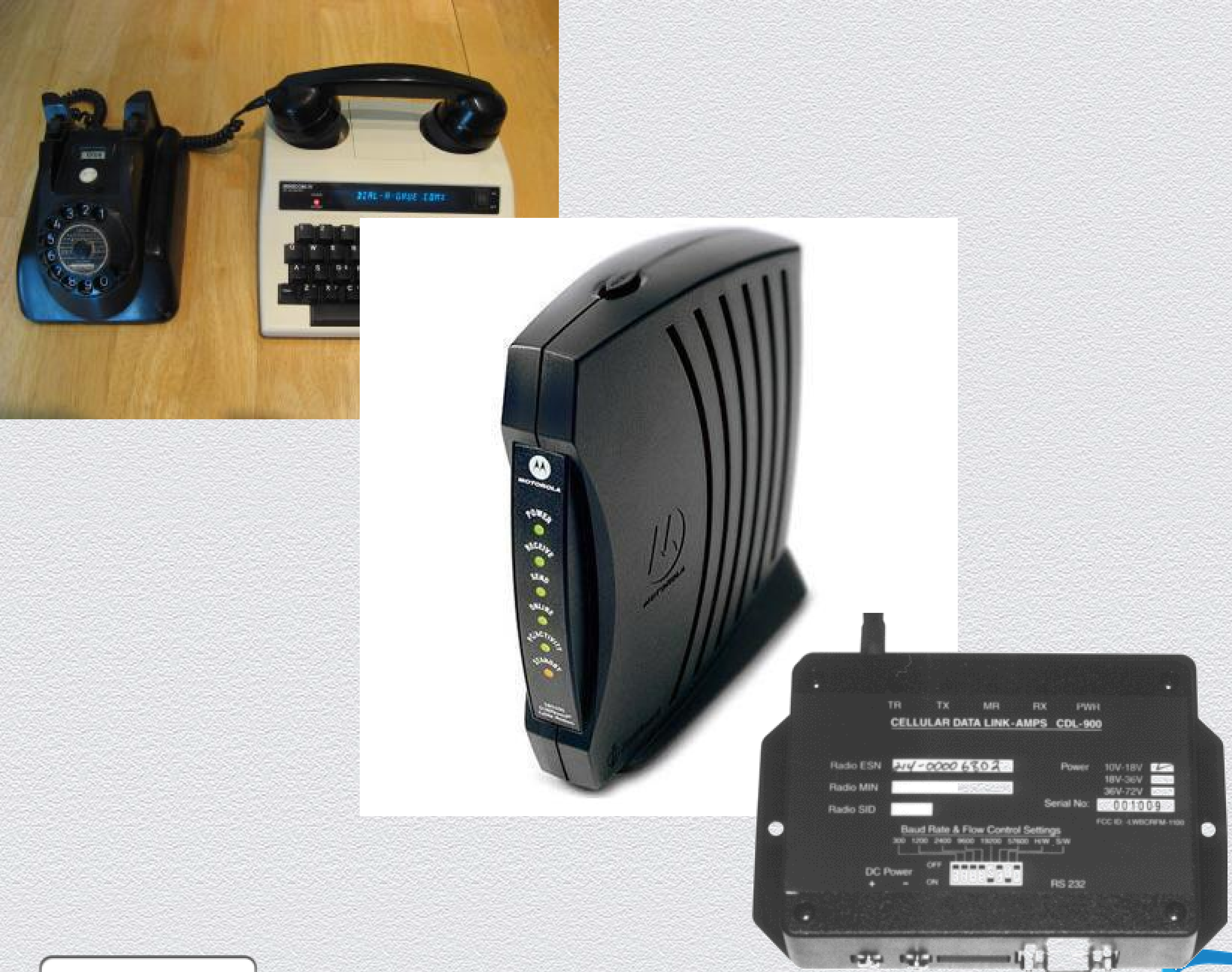
- Based in Silicon Valley
- Explicitly requested a full scope “Red Team” style assessment
- No previous knowledge of the organization or the infrastructure
- Network security teams monitoring and full corporate security assets in play

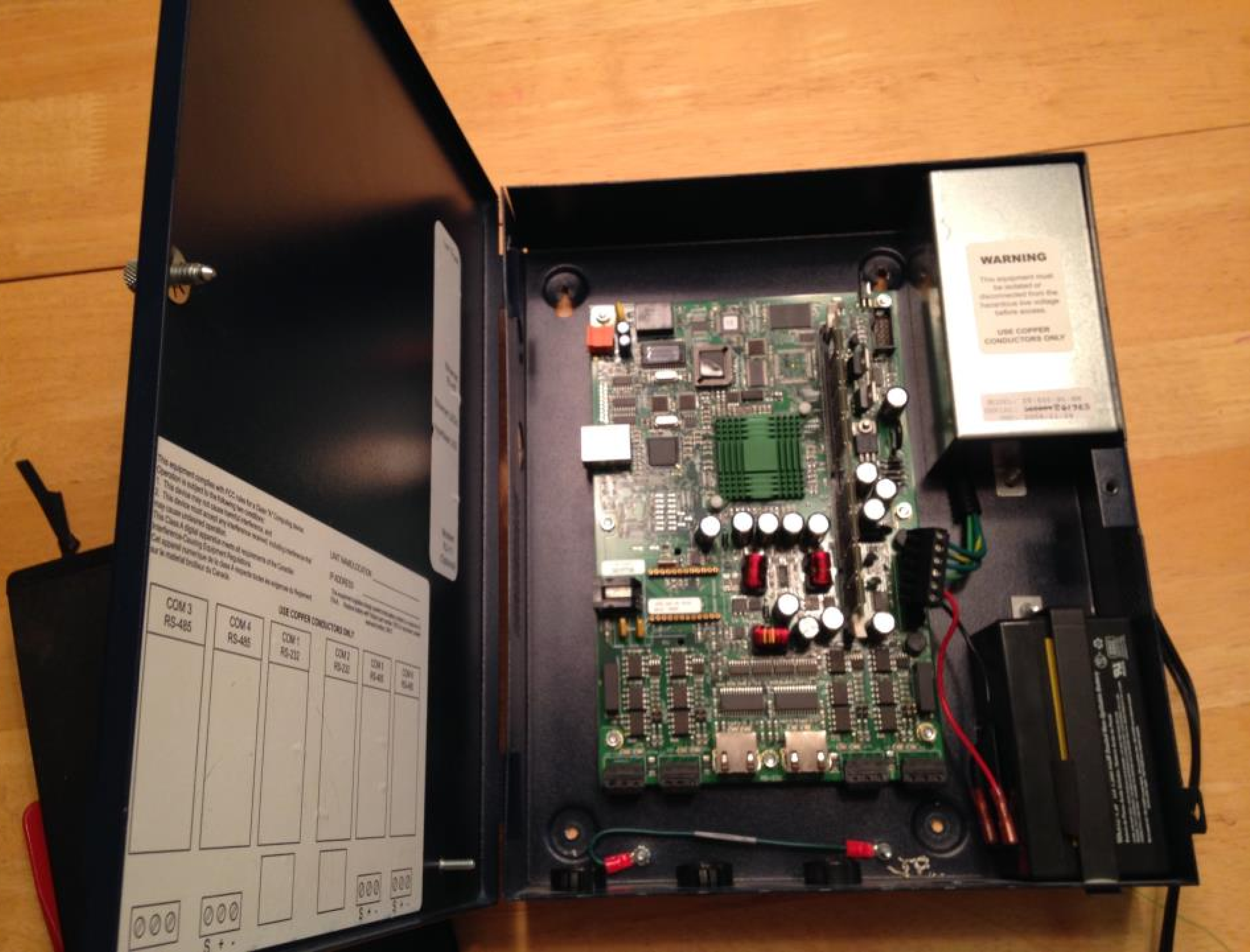
Our Approach

- Identify the target in our Building Automation System (BAS) database (no port scanning required against the target)
- Internet facing BAS is typically found OUTSIDE of the corporate IP space!
- Setup our exploitation infrastructure and exploited a 0day vulnerability to gain access to the Building Automation System

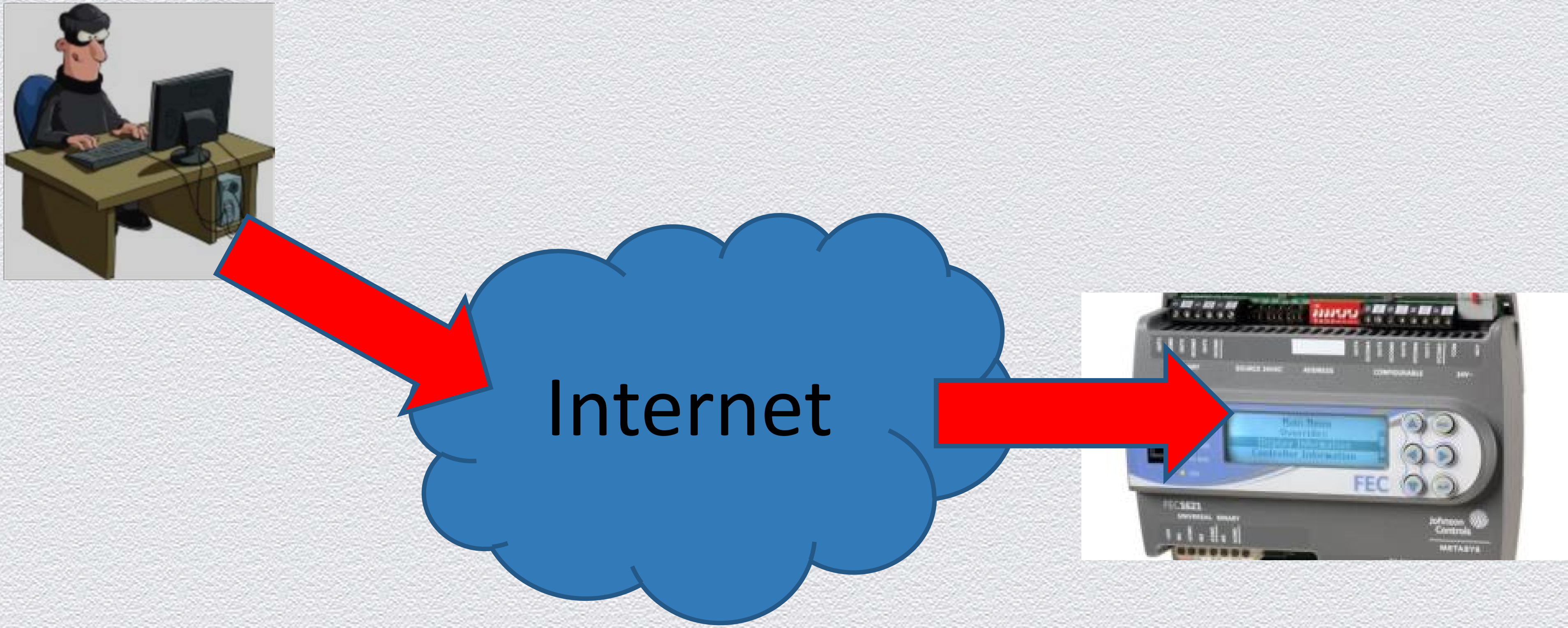
A Lesson on Integrators

- Typically, the end organization doesn’t install IoT
- Typically, a third party (Integrator) is hired to install the HVAC/Conference room/Nest thermostat/sensors
- When an issue arises, the Integrator is usually called in to assist
- Traveling to the client site can be expensive and time consuming for Integrators, so they enable remote access

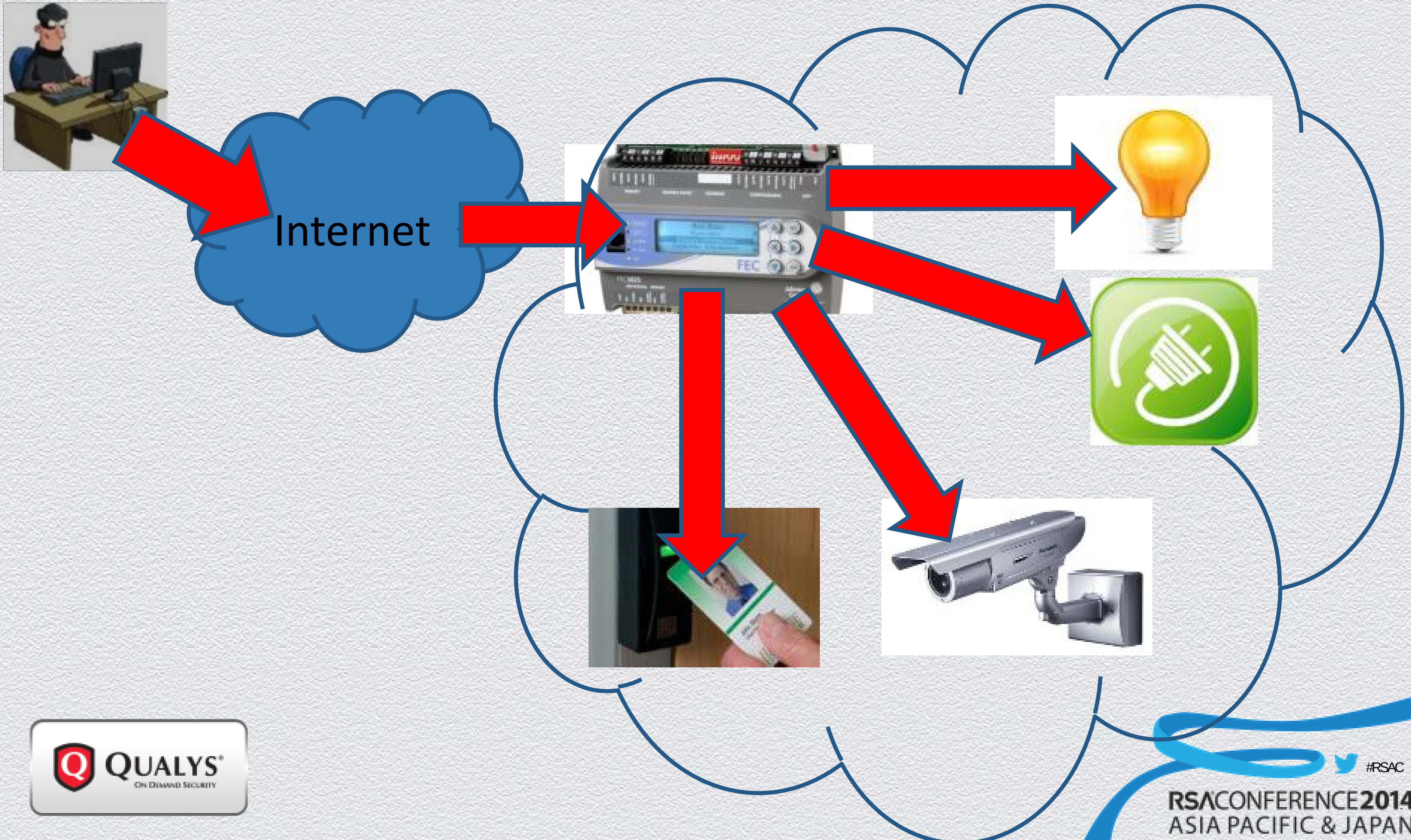

MOTOROLA
POWER
RECEIVE
SEND
ONLINE
ACTIVITY
STANDBY
TR TX MR RX PWR
CELLULAR DATA LINK-AMPS CDL-900
Radio ESN
Radio MIN
Radio SID
Power
10V-18V
18V-36V
36V-72V
Serial No:
001009
Baud Rate & Flow Control Settings
300 1200 2400 9600 19200 57600 H/W S/W
DC Power
+ -
OFF
ON
RS 232


WARNING
This equipment must be isolated or disconnected from the hazardous live voltage before access.
USE COPPER CONDUCTORS ONLY
UNIT NAME/LOCATION
IP ADDRESS
USE COPPER CONDUCTORS ONLY
COM 3 RS-485
COM 4 RS-485
COM 1 RS-232
COM 2 RS-232
S + -
S + -
S + -

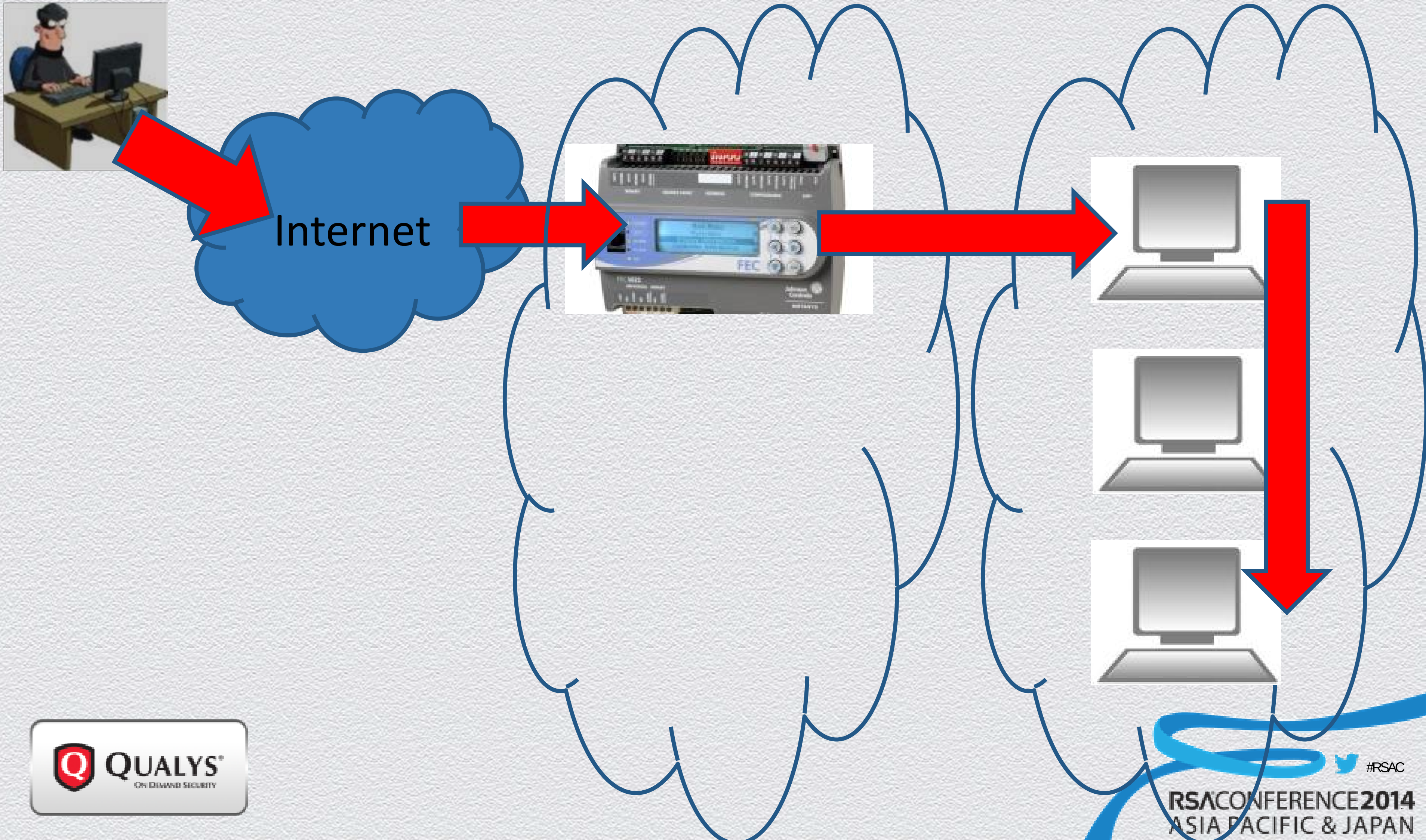
Exploits in Action



Exploits in Action



Exploits in Action



Access?

- Pivot from Automation network to Corporate Network
  - VLAN separates Automation network from CorpNET
  - No AV on any automation systems
  - Cable Modem line allows for bypassing of perimeter ingress and egress monitoring

- Access to Corpnet with Domain Credentials
  - At this point, the assessment becomes a traditional penetration test
  - Escalation to Domain Admin
  - Access to all workstations (including corporate IP and financial data)
  - Access to CEO’s email

Requested Proof of Concepts

- Unlock the front door of the Corporate HQ
- Shut off all IP based surveillance systems
- Modify the Access Control database (add a badge)
- Wipe an executives mobile device

Things to Consider

- BEFORE you accept a device
  - Have a policy!
  - Understand the exposures
  - Insist on understanding how remote management is implemented
  - Know whether the device will be facing the Internet
  - Evaluate the proposed configuration and deployment
  - Get your acquisition folks involved
  - Engage with your facilities and property team so they understand the risks of default acceptance of systems

  - Large capital investments (ex. Buying a building) require security involvement from the beginning!

Things to Consider

- Dealing with Devices on Your Network
  - Know who your integrators are
  - Ask for spare devices for testing
  - Do assessments against the devices
    - Clear text credentials (if the device talks to your exchange server for calendar updates… it has domain credentials)
    - Backdoor passwords
  - Liability
  - Monitor traffic to and from the devices
  - Consider restricting who can talk to the device
  - Establish a baseline for device operation
    - Known good firmware, files, and processes

Great Resources

- /Dev/TTYS0 - http://www.devttys0.com/blog/
- Travis Goodspeed - http://travisgoodspeed.blogspot.com/
- Mikeselectricstuff - http://www.youtube.com/user/mikeselectricstuff?feature=watch
- STBUYN - http://dontstuffbeansupyournose.com/
- Cyber Pacifists - http://www.cyberpacifists.net/
- Reversemode – http://www.reversemode.com/
- W00tsec - http://w00tsec.blogspot.com/

Kit

- Screwdriver set with nut driver, torx and square
  - http://www.amazon.com/s/ref=nb_sb_ss_c_0_14?url=search-alias%3Dindustrial&field-keywords=screwdriver+set
- Soldering iron with desoldering kit
  - http://www.amazon.com/s/ref=nb_sb_noss_2?url=search-alias%3Daps&field-keywords=soldering
- Solderless breadboard
  - http://www.adafruit.com/products/758?gclid=CMPMiO-y5bwCFZRsfgodHG0ACw
- Jumper wires
  - http://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Dindustrial&field-keywords=jumper+wires+male+to+male

Kit

- Console Cables
  - http://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=console+cable
- TTL Reader
  - http://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=TTL+to+USB
- JTAG Reader
  - http://blackcatusbjtag.com/
- ROM Reader
  - http://www.amazon.com/s/ref=nb_sb_ss_c_0_14?url=search-alias%3Dindustrial&field-keywords=screwdriver+set
- Logic Analyzer
  - http://www.saleae.com/logic

Kit

- Disassembler (with appropriate chipset support)
  - https://www.hex-rays.com/products/ida/
- Debugger
  - https://www.immunityinc.com/products-immdbg.shtml
- Terminal Software
  - http://www.hilgraeve.com/hyperterminal/
- Virtualization Software
  - http://www.vmware.com/

Questions?

Alaris® PC
Guardrails®
CareFusion