



**CUTAWAY SECURITY**  
— INFOSEC CONSULTANTS —

# Pen Testing ICS and Other Highly Restricted Environments

Don C. Weber - @cutaway

Principal Consultant, Founder

© 2019 Cutaway Security, LLC. All Rights Reserved.



# Cutaway Security, LLC

- Don C. Weber - Jack of All Trades
  - Security Management
  - Penetration Testing
  - Security Assessments
  - Security Researcher
  - Instructor / Presenter
  - Incident Response





**CUTAWAY SECURITY**  
— INFOSEC CONSULTANTS —

You don't know  
Infosec about ICS...



# Things to get over...

- Clear Text Protocols
- Insecure Applications
- Vulnerable Firmware
- Brittle Services
- Legacy Software and Equipment

ModbusTCP.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

Packet bytes Narrow & Wide Case sensitive String Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
414	2012-11-12 11:03:02.560590	141.81.0.84	141.81.0.10	Modbus/...	293	Response:
415	2012-11-12 11:03:02.560809	141.81.0.64	141.81.0.10	Modbus/...	293	Response:
416	2012-11-12 11:03:02.564072	141.81.0.66	141.81.0.10	TCP	60	502 → 5413

Modbus/TCP

- Transaction Identifier: 12070
- Protocol Identifier: 0
- Length: 233
- Unit Identifier: 255

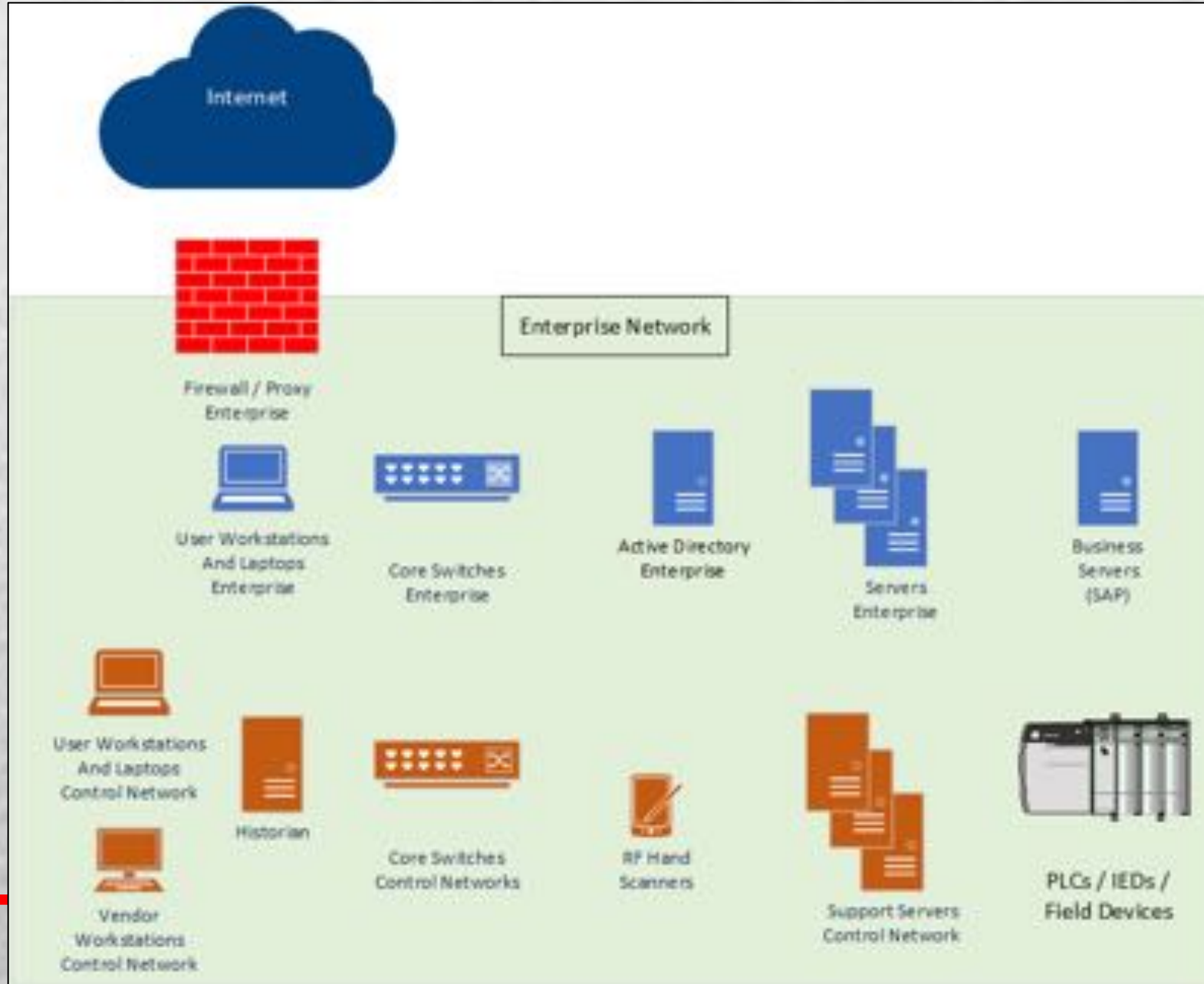
Modbus

- .000 0100 = Function Code: Read Input Registers (4)
- [Request Frame: 409]
- Byte Count: 230
- Register 1300 (UINT16): 0
- Register Number: 1300

```
0030 fd 0d 08 b6 00 00 2f 26 00 00 00 e9 ff 04 e6 00 ...../& .....
0040 00 00 03 00 00 00 01 27 10 00 00 00 00 00 00 00 .....' .....
0050 00 00 00 00 3c 00 0b 00 3c 00 0b 02 bc 00 1e 00 .....< .....
0060 04 01 fc 00 33 00 00 00 05 00 df 00 08 00 00 00 .....3 .....
0070 00 00 73 00 0f 00 93 00 07 00 0d 00 8b 00 15 00 .....s .....
0080 61 00 1e 00 97 00 2a 00 0c 00 10 00 06 00 0a 00 .....a .....
0090 0a 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....
00a0 00 00 00 00 42 00 00 00 0f 00 00 00 00 00 00 00 .....B .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....
0100 00 00 00 00 00 00 00 41 44 4d 4e 20 31 32 33 .....A.DMIN 123
0110 34 35 36 20 20 20 20 20 20 20 20 20 20 4e 6f 6e .....456 Non
0120 65 20 20 00 00 .....e ..
```

Register Value (UINT16) (m...us.regval\_uint16), 2 bytes Packets: 15387 · Displayed: 15387 (100.0%) Profile: Default

# Worst Case Scenario





# What are ICS Concerns?



- Safety to personnel, environment, and process.
- Sustained operations, availability and integrity, of the process.
- Regulation, due to safety, environmental hazard, or public impact.

Image Source: [https://s3-us-west-1.amazonaws.com/umbrella-blog-uploads/wp-content/uploads/2015/08/Cannisters\\_After.jpg](https://s3-us-west-1.amazonaws.com/umbrella-blog-uploads/wp-content/uploads/2015/08/Cannisters_After.jpg)



**CUTAWAY SECURITY**  
— INFOSEC CONSULTANTS —

It's a network, why can't we  
pentest it?



# ICS Pen Test Roadblocks

**InfoSec Consultant:** "... then we will do some simple scanning to discover services ..."

**IT Security Director:** "No. You can't scan."

**InfoSec Consultant:** "Can I run an ARP scan to discover...?"

**IT Security Director:** "No. No scanning at all."

```

> sudo arp-scan 192.168.8.0/24
WARNING: Could not obtain IP address for interface eth0. Using 0.0.0.0 for
the source address, which is probably not what you want.
Either configure eth0 with an IP address, or manually specify the address
with the --rpsso option.
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.8.5    dc:89:19:38:a7:49    (Unknown)
192.168.8.6    dc:89:19:38:a6:75    (Unknown)
192.168.8.7    78:84:56:98:05:65    (Unknown)
192.168.8.8    d4:c9:ef:32:8f:ea    Hewlett Packard
192.168.8.4    00:1d:9c:97:68:9d    Rockwell
192.168.8.11   00:0c:29:83:fc:95    VMware, Inc.
192.168.8.12   08:00:06:ef:71:f2    Siemens AG
192.168.8.13   00:50:56:d4:e3:93    VMware, Inc.
192.168.8.16   d4:c9:ef:a2:8c:da    Hewlett Packard
192.168.8.17   00:0c:29:b4:5e:d9    VMware, Inc.
192.168.8.18   08:00:06:8f:e1:f3    Siemens AG
192.168.8.19   00:1d:9c:e7:d8:cd    Rockwell

```

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> EXE (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/royhills/arp-scan/master/arp-scan.ps1')

Directory: C:\Users\student\AppData\Local\Temp

Mode                LastWriteTime         Length Name
----                -
d-----          11/10/2019   6:35 PM             chaps-20191110-061532

[*] Start Date/Time: 20191110183225+001
[*] Script running with Administrator rights.
[*] Dumping System Info to separate file.

Host Name:                SANS-C3801VIT3L
OS Name:                  Microsoft Windows 10 Enterprise
OS Version:              10.0.18363.194 Build 18363
OS Manufacturer:        Microsoft Corporation
OS Configuration:       Standalone Workstation
OS Build Type:            Multiprocessor Free
Registered Owner:        SANS Institute - Student
Registered Organization: SANS Institute
Product ID:              00329-10311-09385-A3740
Original Install Date:    1/31/2018, 7:07:14 PM
System Boot Time:         11/10/2019, 6:09:22 PM
System Manufacturer:     VMware, Inc.
System Model:             VMware Virtual Platform
System Type:              x64-based PC
Processor(s):             1 Processor(s) Installed.
                          (0): Intel64 Family 6 Model 142 Stepping 9 GenuineIntel ~2496 Mhz
BIOS Version:            Phoenix Technologies LTD 6.00, 7/29/2019
Windows Directory:      C:\WINDOWS
System Directory:        C:\WINDOWS\system32
Boot Device:             \Device\HarddiskVolume1
System Locale:            en-us;English (United States)
Input Locale:            en-us;English (United States)
Time Zone:               (UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb
Total Physical Memory:   4,095 MB
Available Physical Memory: 2,542 MB
Virtual Memory: Max Size: 4,799 MB
Virtual Memory: Available: 3,355 MB
Virtual Memory: In Use: 1,444 MB
Page File Location(s):  C:\pagefile.sys
Domain:                  \SANS-C3801VIT3L
Logon Server:            \\SANS-C3801VIT3L
HotFix(s):               1 HotFix(s) Installed.
                          (0): KB4493777

```

**InfoSec Consultant:** "We are here to understand how the PLC accepts user input and determine..."

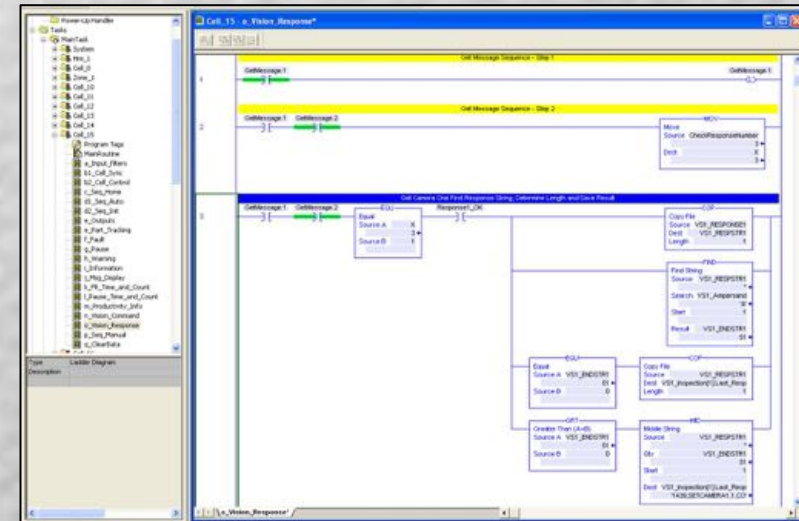
**OT PLC Programmer:** "Why don't you just go away and let us do our jobs."

**InfoSec Consultant:** "I'm going to run a PowerShell script that only check system settings and writes it to a file."

**OT Lead:** "But that means you are making changes to the system."

**InfoSec Consultant:** "No changes, just creating one file with system configuration information."

**OT Lead:** "You are changing the system."







# How did this happen?



**Situation 0:** Nessus scan, in 2016, of an OT subnet took over a week to fix the process.

**Situation 1:** Changes to systems can trigger rigorous and expensive testing. They can also void maintenance agreements.

**Situation 2:** IT security team and OT had different operational goals.



**CUTAWAY SECURITY**  
— INFOSEC CONSULTANTS —

How do we overcome this  
mentality?



# White-Glove Treatment

white-glove (wīt'glōv', hwīt'-)

adj.

1. Marked by extra attention or respect; special: *clients who were given the white-glove treatment.*
2. Scrupulous and thorough: *a white-glove inspection.*
3. Catering to or used by the wealthy; expensive or luxurious: *"the city's white-glove shopping boulevard" (John Freeman Gill).*

- Make management comfortable
- Make process engineers and operators comfortable.
- Make IT personnel comfortable.



# #1 Recommendation from ICS IT/ OT Teams

ICS Security Team  
needs to spend time  
with the OT Team to  
understand the  
people, processes,  
and operations.



Image Source: Boyd Animation <https://boydanimation.com/>



**CUTAWAY SECURITY**  
— INFOSEC CONSULTANTS —

# How do we test?

# Expected Architecture – ICS410 Reference Model

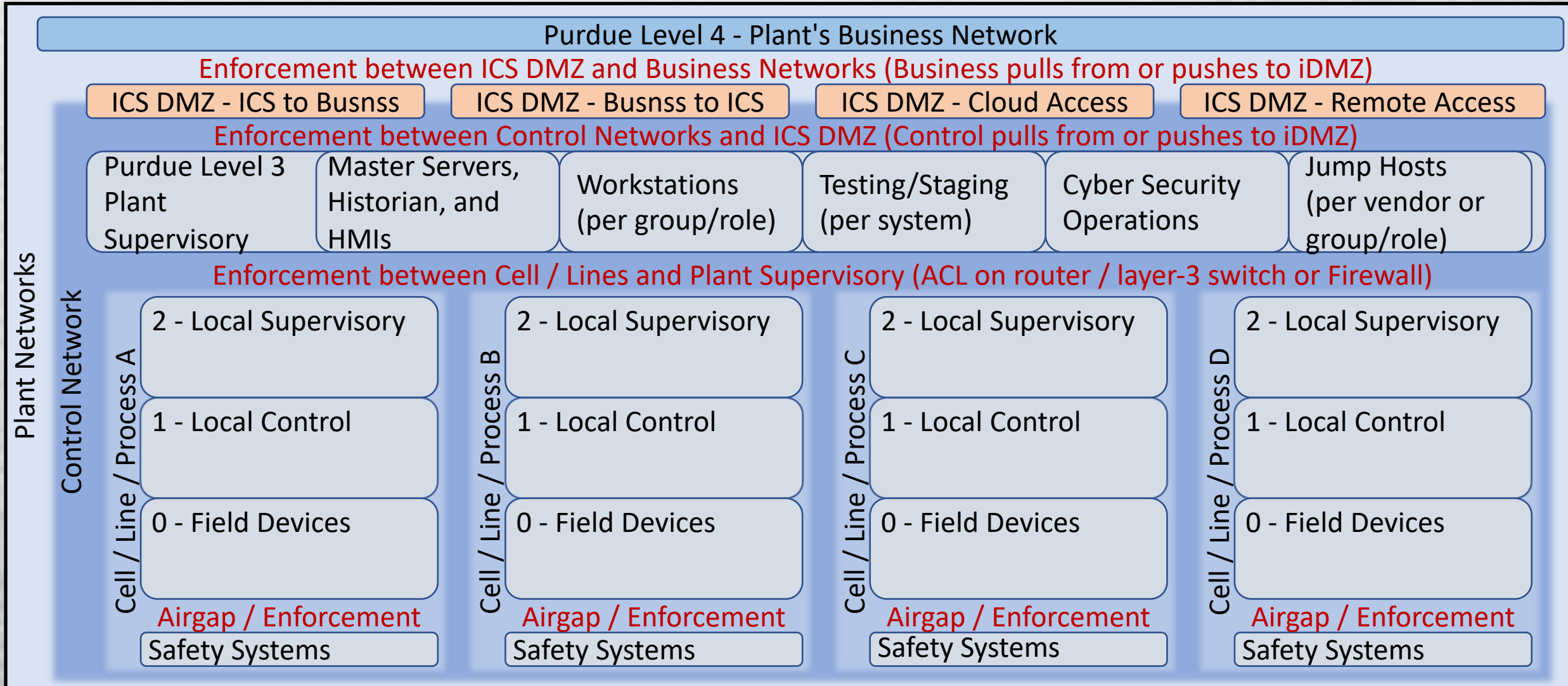
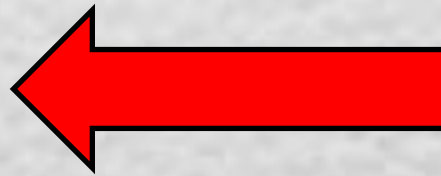


Image Source: ControlThings.io Accessing and Exploiting Control Systems



# IT / OT Security Effort Prioritization

- Separate policies for IT and OT environments
- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery



**Tactical ICS  
Security  
Starts Here**



# Process Familiarization

- Architecture Review
- Site Walk Thru
  - Physical Security
  - Engineer / Operator Actions in Process
- Interviews
  - Managers
  - Engineers / Operators / Programmers
  - IT Team
  - IT Security
- Threat Modeling
- Configuration Analysis
- Source Code Analysis



Image Source: <https://www.controlthings.io/> - Accessing and Exploiting Control Systems







# Active Testing

- Understand the consequences of active testing could impact safety.
- Know how to rate limit at both the network and application levels.
- Select individual targets: hosts and services.
- Know your tool configurations and double check with a partner.
- Remember assessment goals and test to them.

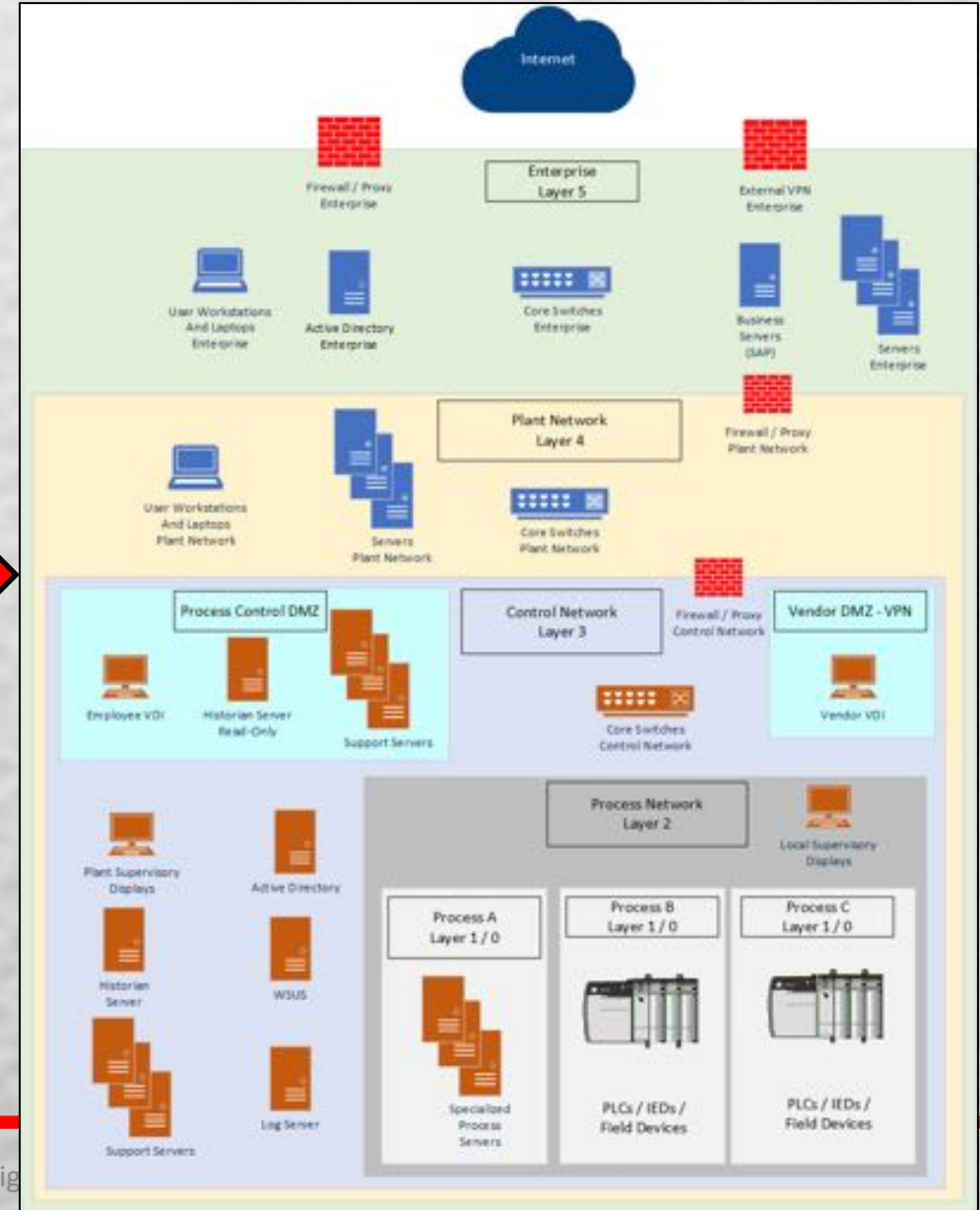
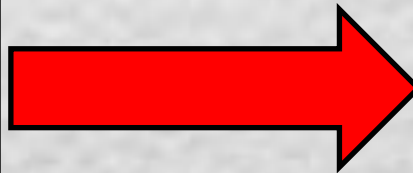
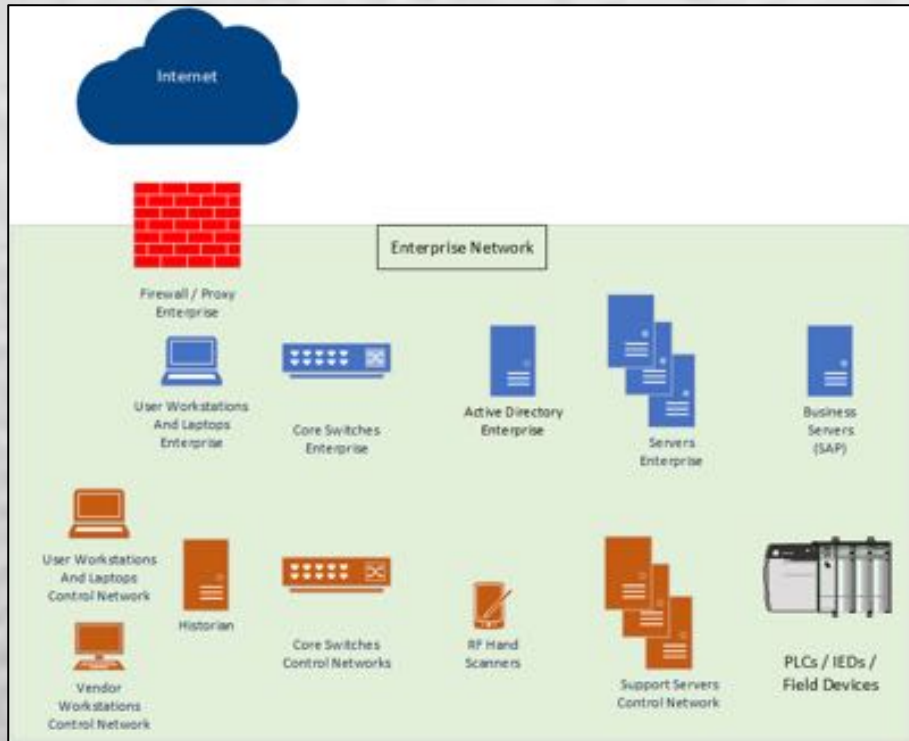




**CUTAWAY SECURITY**  
— INFOSEC CONSULTANTS —

# In Conclusion

# Controlled Migration to Mature ICS Environment





# ICS Pen Testing is a Different Kind of Sexy



- Slow your roll and check your attitude.
- OT environment cannot live up to IT policies and best practices.
- Get to know the OT teams and the processes.
- Start testing passively and escalate safely.
- Help identify issues and help the defenders protect the process.



**CUTAWAY SECURITY**  
— INFOSEC CONSULTANTS —

Don C. Weber - @cutaway

Principal Consultant, Founder

<http://linkedin.com/in/cutaway>

<https://github.com/cutaway>

<https://www.sans.org/instructors/don-c-weber>

Cutaway Security, LLC

<http://www.cutawaysecurity.com>

<http://linkedin.com/company/cutaway-security-llc>

<https://github.com/cutaway-security>