



CUTAWAY SECURITY
— INFOSEC CONSULTANTS —

Architecting Secure ICS 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





Full Disclosure: Instructor for ICS Classes



GIAC GICSP Certification

ICS410: ICS/SCADA Security Essentials

SANS ICS 410 Course

ICS612: ICS Cyber Security In-Depth Beta

SANS ICS 612 Course <- I don't teach this, but it is going to be awesome.



ControlThings.io A&ECS Course



Agenda

- Purpose
- ICS Implementations and Equipment
- ICS Concerns
- ICS410 Reference Architecture
- Recap

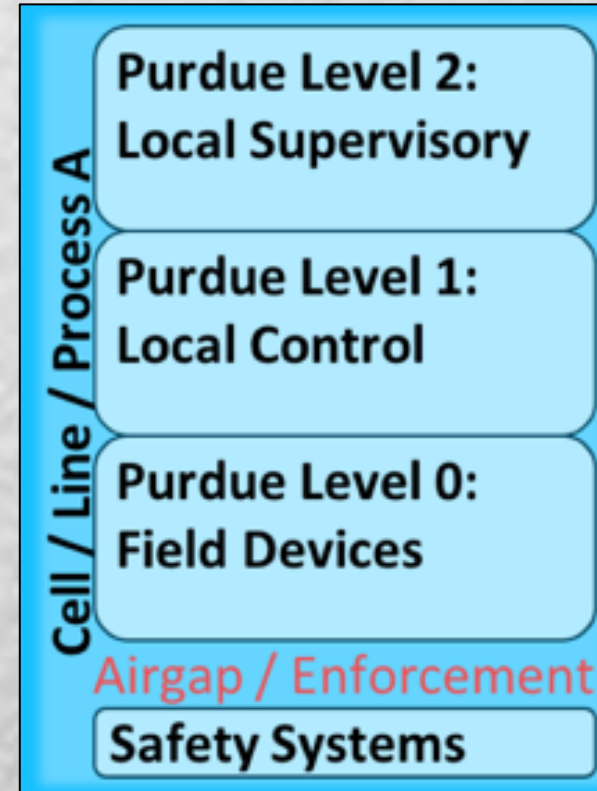


Image Source: SANS ICS410 ICS / SCADA Security Essentials



CUTAWAY SECURITY
— INFOSEC CONSULTANTS —

Purpose



Things to get over...

- Clear Text Protocols
- Insecure Applications
- Vulnerable Firmware
- Brittle Services

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

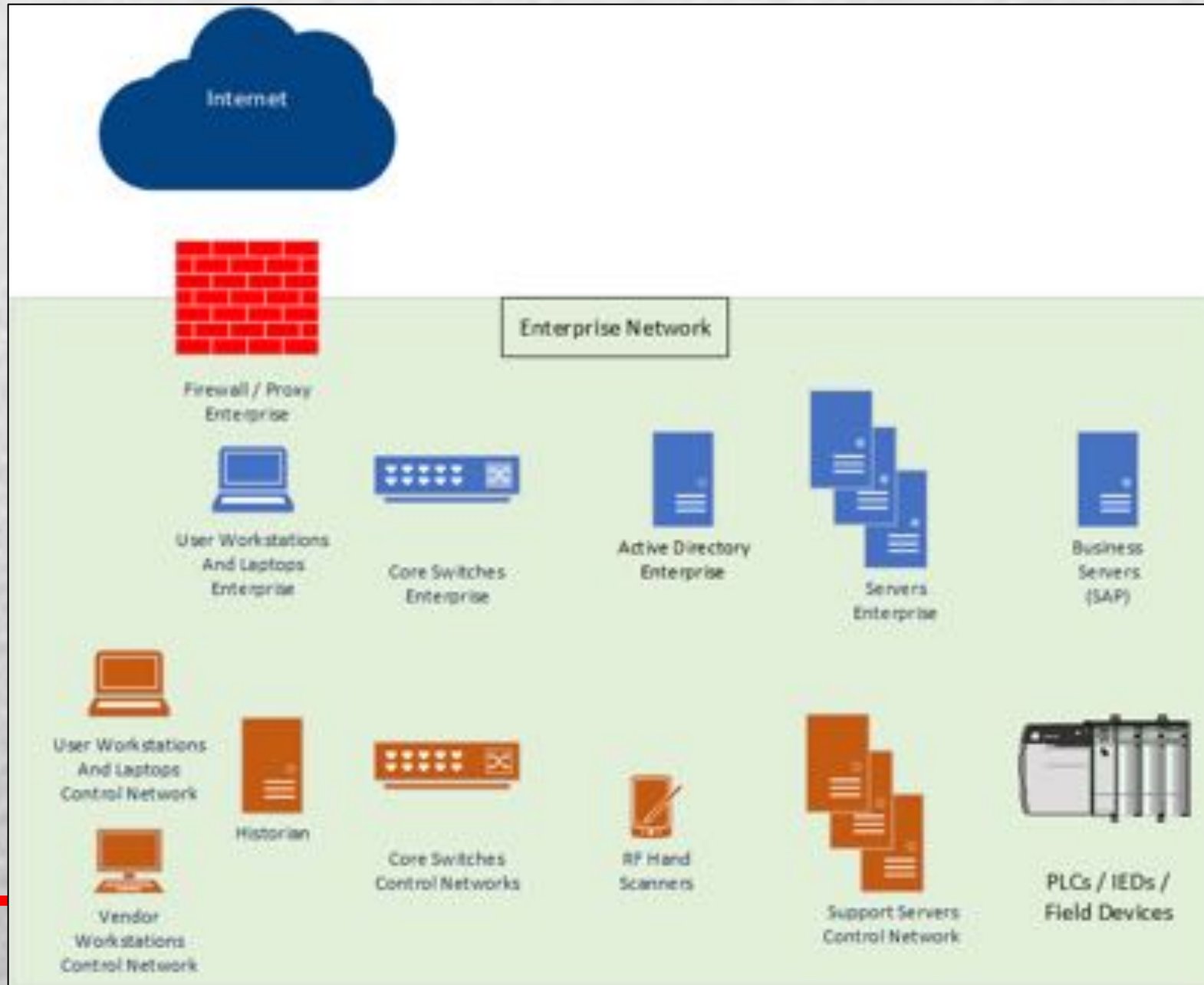
Modbus

- .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 .....B.....
00a0 00 00 00 00 42 00 00 00 0f 00 00 00 00 00 00 00 .....
00b0 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 .....
00d0 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 .....
00f0 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 49 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





CUTAWAY SECURITY
— INFOSEC CONSULTANTS —

ICS Implementations and Equipment



What are ICS implementations?

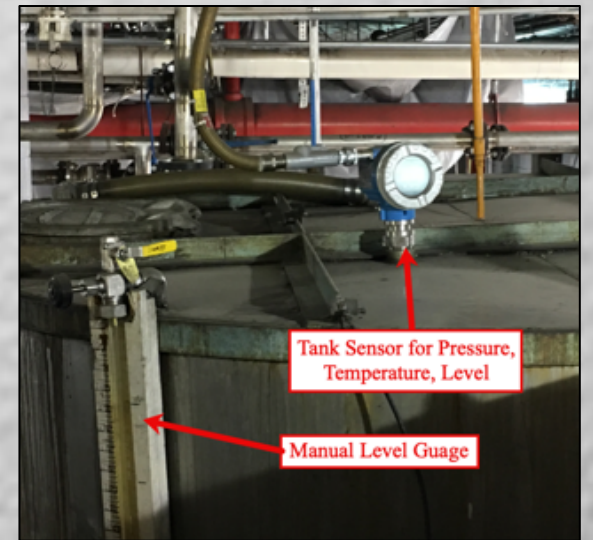
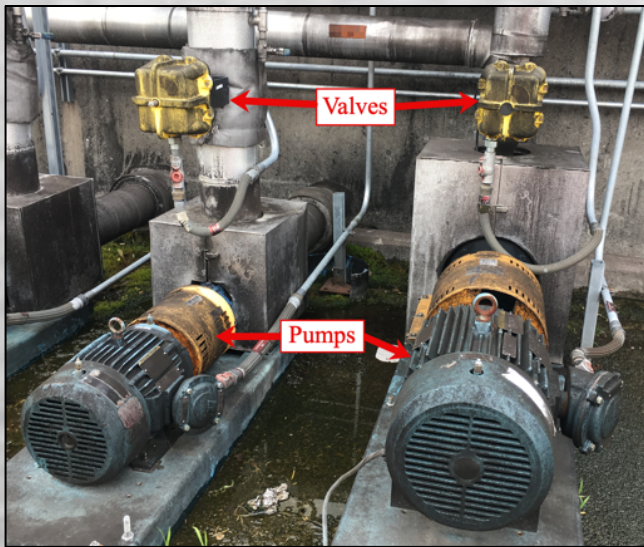
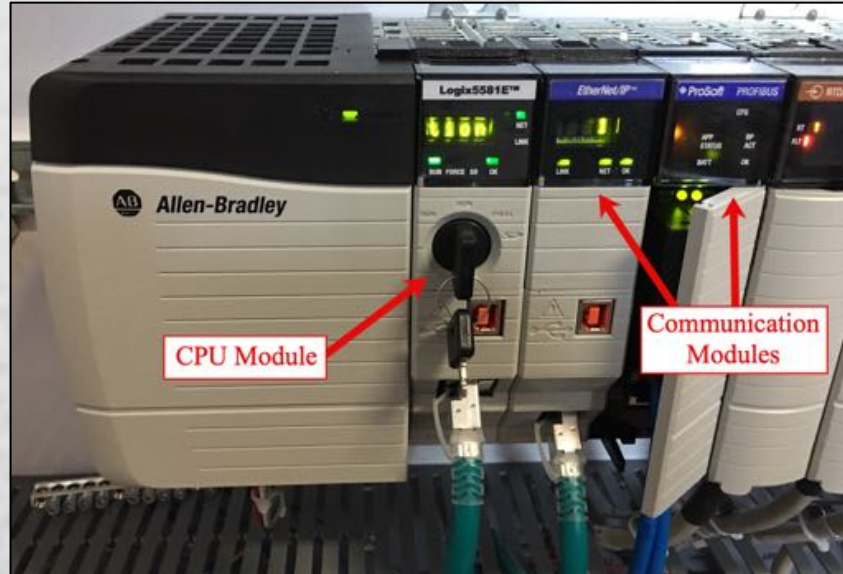
- A process is a group of devices and servers that perform a specific function, typically combined with other processes.
- Plants are multiple processes, that can be independent or dependent, which can be centrally controlled.
- SCADA are processes and plants that are mutually dependent but spread over a wide region.

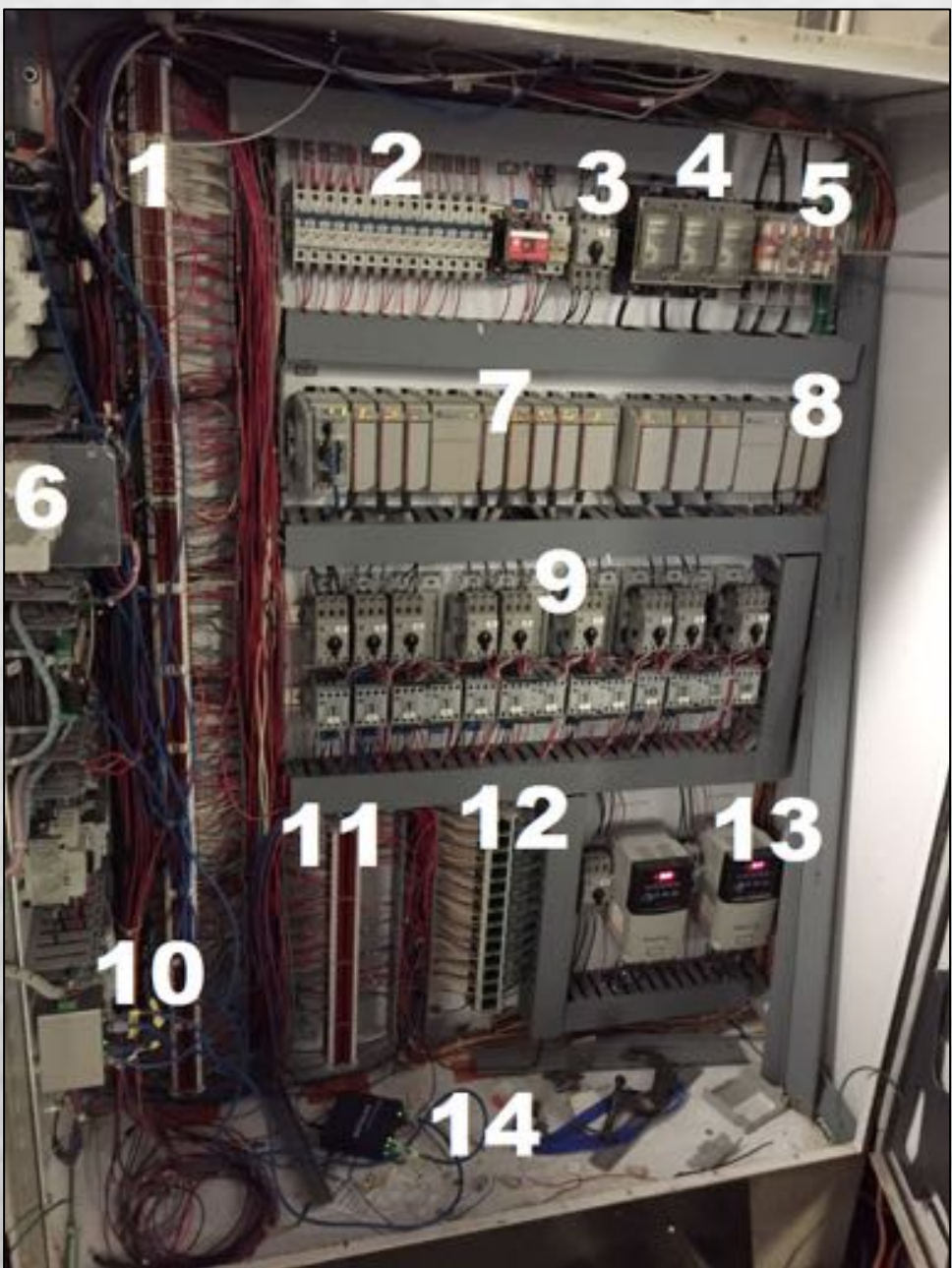


Image Source: Google Maps



What are ICS Devices?





This control cabinet controls a chemical wash process. A local integrator made this panel with Allen Bradley and Phoenix Contact components.

- | | | | |
|----|-------------------------------------|-----|--|
| 1. | 120 VAC field IO | 9. | Motor starters |
| 2. | Branch circuit breaker | 10. | Phoenix Contact Industrial Ethernet switch |
| 3. | Motor starters | 11. | 24 VDC field IO |
| 4. | Main power feed | 12. | 4-20 mA field instrumentation |
| 5. | Main fuses | 13. | Allen Bradley Variable Frequency Devices |
| 6. | 24 VDC power supplies | 14. | A general purpose Ethernet switch (rogue device) |
| 7. | Allen Bradley Compact Logix PLC | | |
| 8. | Allen Bradley Compact Logix IO rack | | |

- Floor/Field Components Include:
 - 1 Data Historian Server
 - 2 Wonderware HMI's
 - 2 Panel Views
 - 4 Automation Direct Operation Interfaces
 - Many PLCs



What is a process?





How are processes deployed?

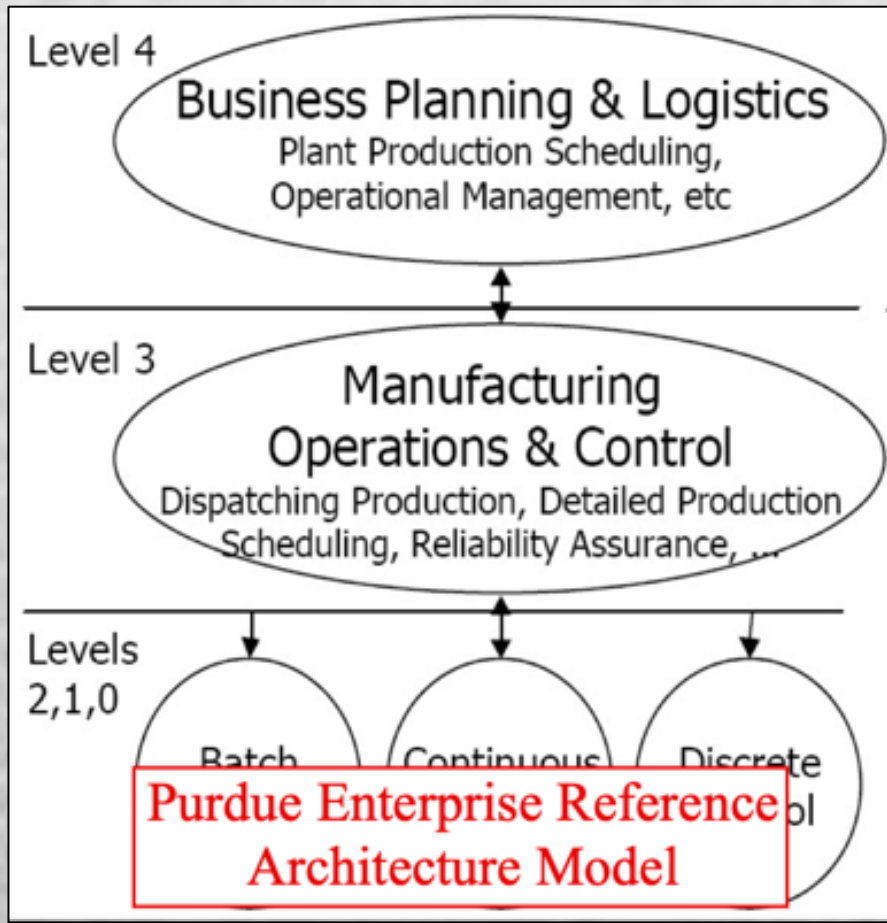


Image Source: SANS ICS410 ICS / SCADA Security Essentials

- ISA-95 <- Process only
- ISA-99 <- Process with security
- IEC/ISA-62443 <- ISA-99 renamed



CUTAWAY SECURITY
— INFOSEC CONSULTANTS —

ICS Concerns



What are ICS business 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



What are the Operational Technology (OT) team's concerns?

- Breaking devices and negatively impacting the processes.
- Causing delays because assessments conflict with important milestones.
- Do not know or understand goals of assessment.
- Showing how their baby is ugly.... err.... challenged.
- Making their jobs harder, less efficient.



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



What are the states of ICS environments?

- Each process control deployment is unique by industry, vendor, and company.
- Security may be built in, added on, or not considered.
- Regulations may have dictated security, lack of regulations may have dictated lack of security.

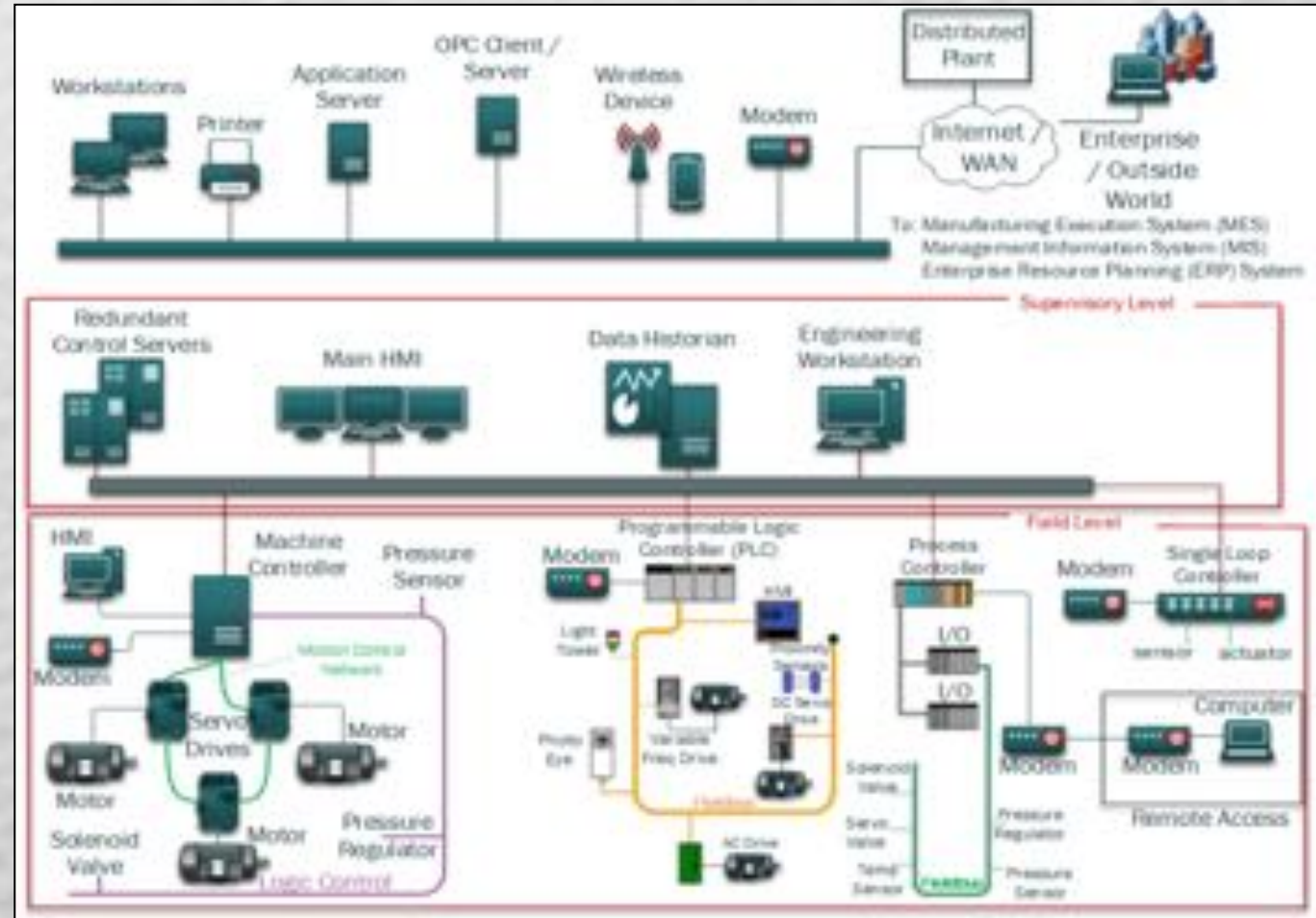


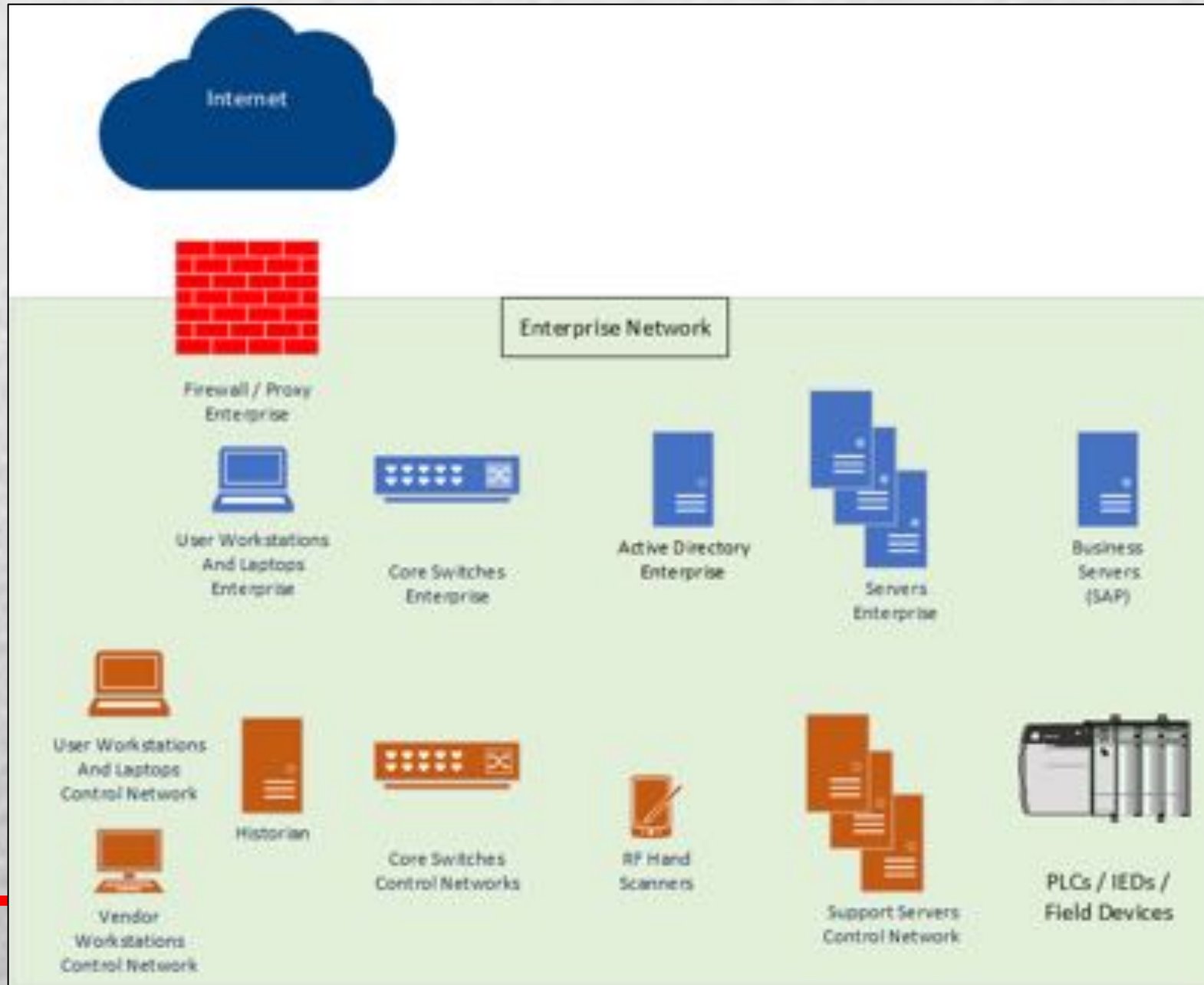
Image Source: ControlThings.io Accessing and Exploiting Control Systems



CUTAWAY SECURITY
— INFOSEC CONSULTANTS —

SANS ICS410 Reference Architecture

Worst Case Scenario



Expected Architecture – ICS410 Reference Model

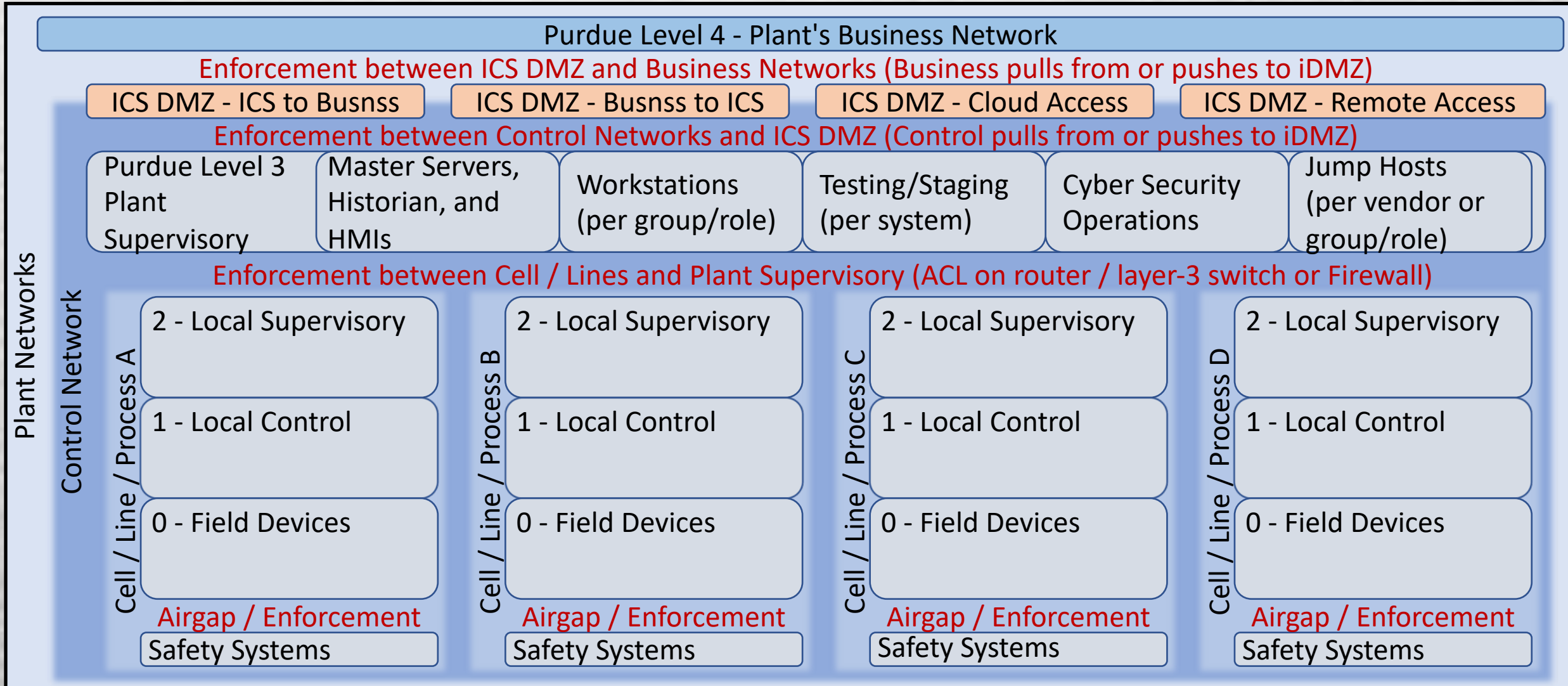
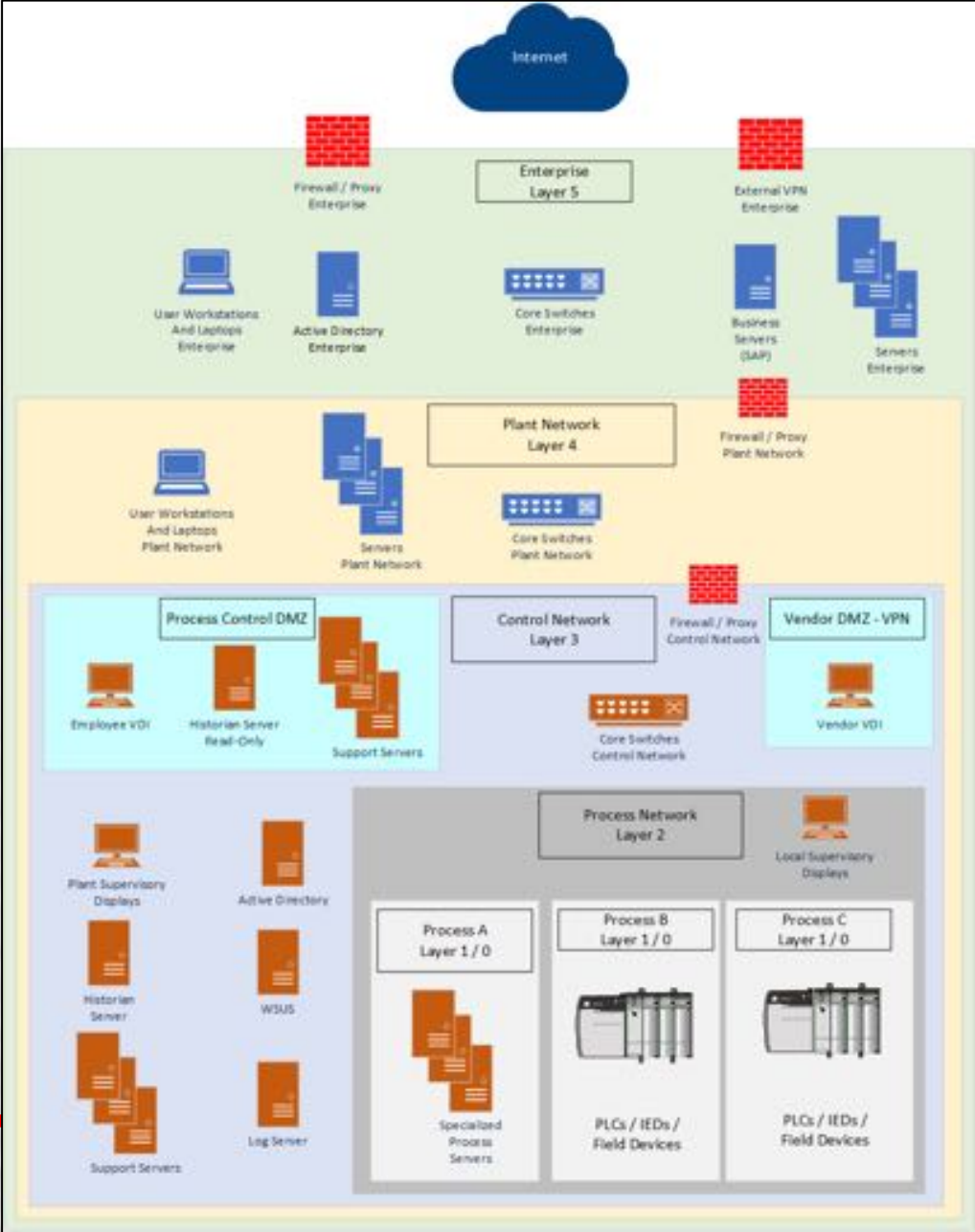


Image Source: ControlThings.io Accessing and Exploiting Control Systems

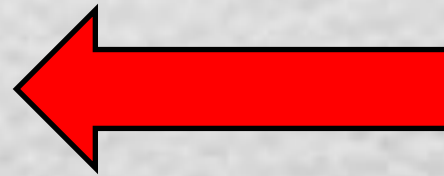
Best Case Scenario





IT / OT Security Effort Prioritization

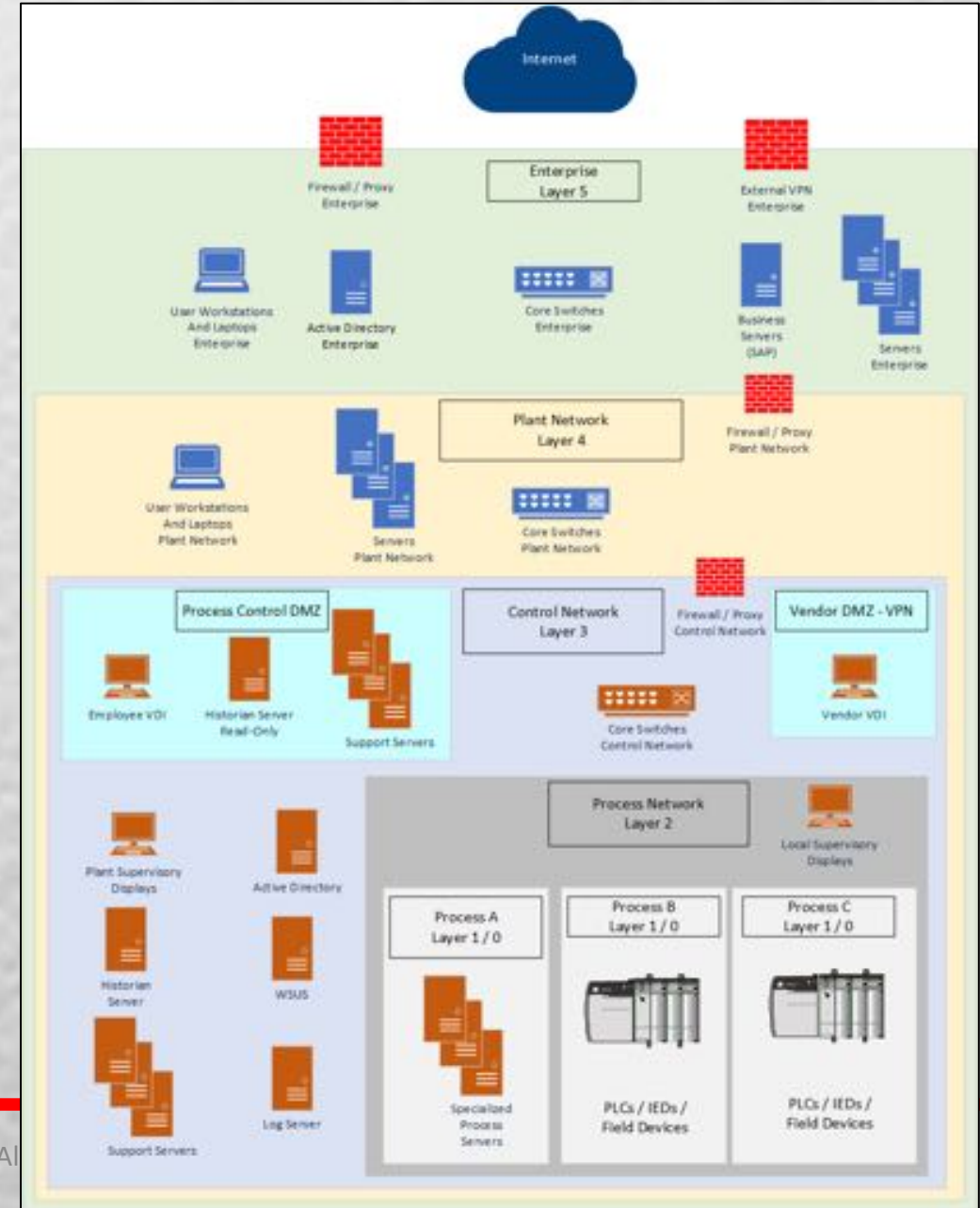
- Separate policies for IT and OT environments
- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Assessment Inventory
- Incident Response and Recovery



**Tactical ICS
Security
Starts Here**

Tactical ICS Security Considerations

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





Recap

- Purpose
- ICS Implementations and Equipment
- ICS Concerns
- ICS410 Reference Architecture
- Recap



GIAC GICSP Certification

ICS410: ICS/SCADA Security Essentials

SANS ICS 410 Course

ICS612: ICS Cyber Security In-Depth Beta

SANS ICS 612 Course



Assessing and Exploiting Control Systems

ControlThings.io
A&ECS Course



CUTAWAY SECURITY
— INFOSEC CONSULTANTS —

Don C. Weber - @cutaway

Principal Consultant, Founder

<http://www.cutawaysecurity.com>

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

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