Architecting Secure ICS Environments

Don C. Weber - @cutaway

Principal Consultant, Founder

Presented at Wild West Hackin' Fest – Deadwood, SD on October 24, 2019

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

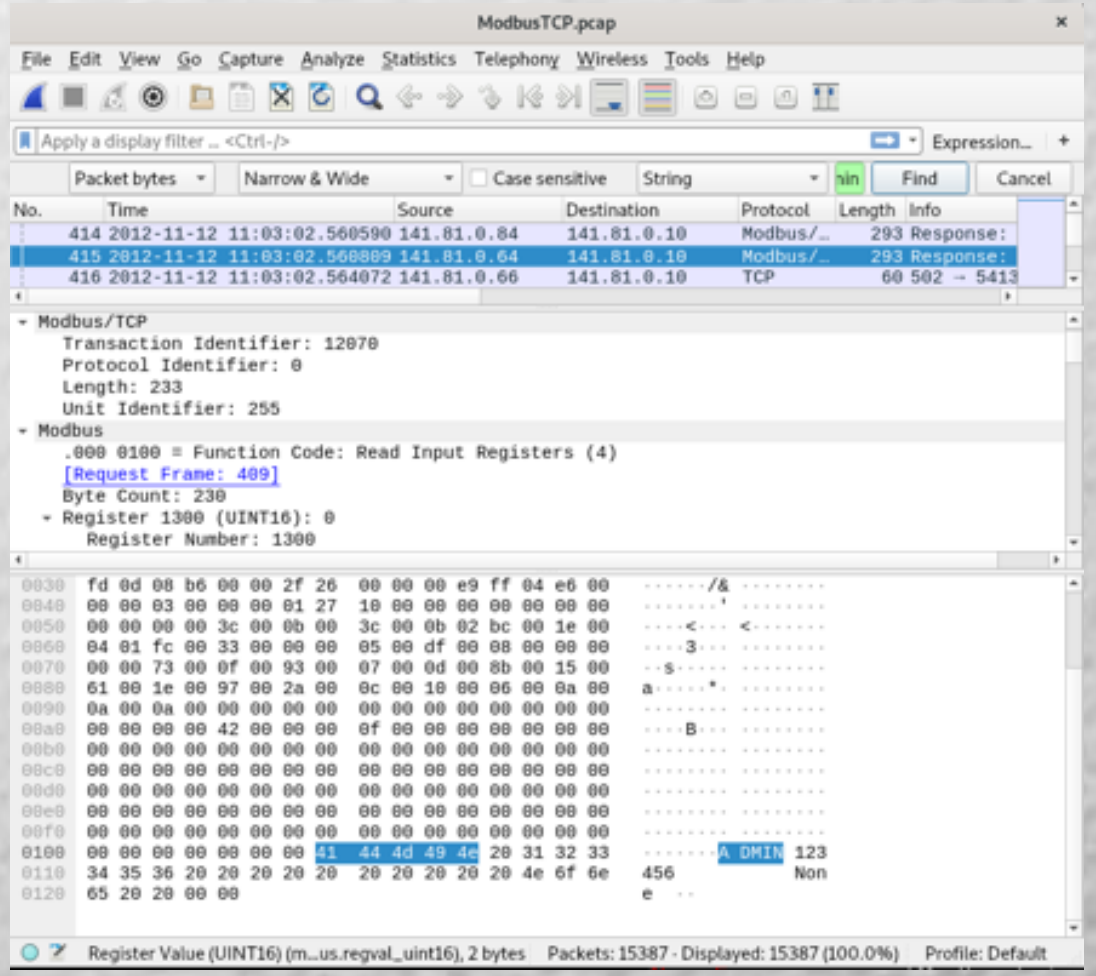
- Purpose
- ICS Implementations and Equipment
- ICS Concerns
- ICS410 Reference Architecture
- Recap

Image Source: SANS ICS410 ICS / SCADA Security Essentials

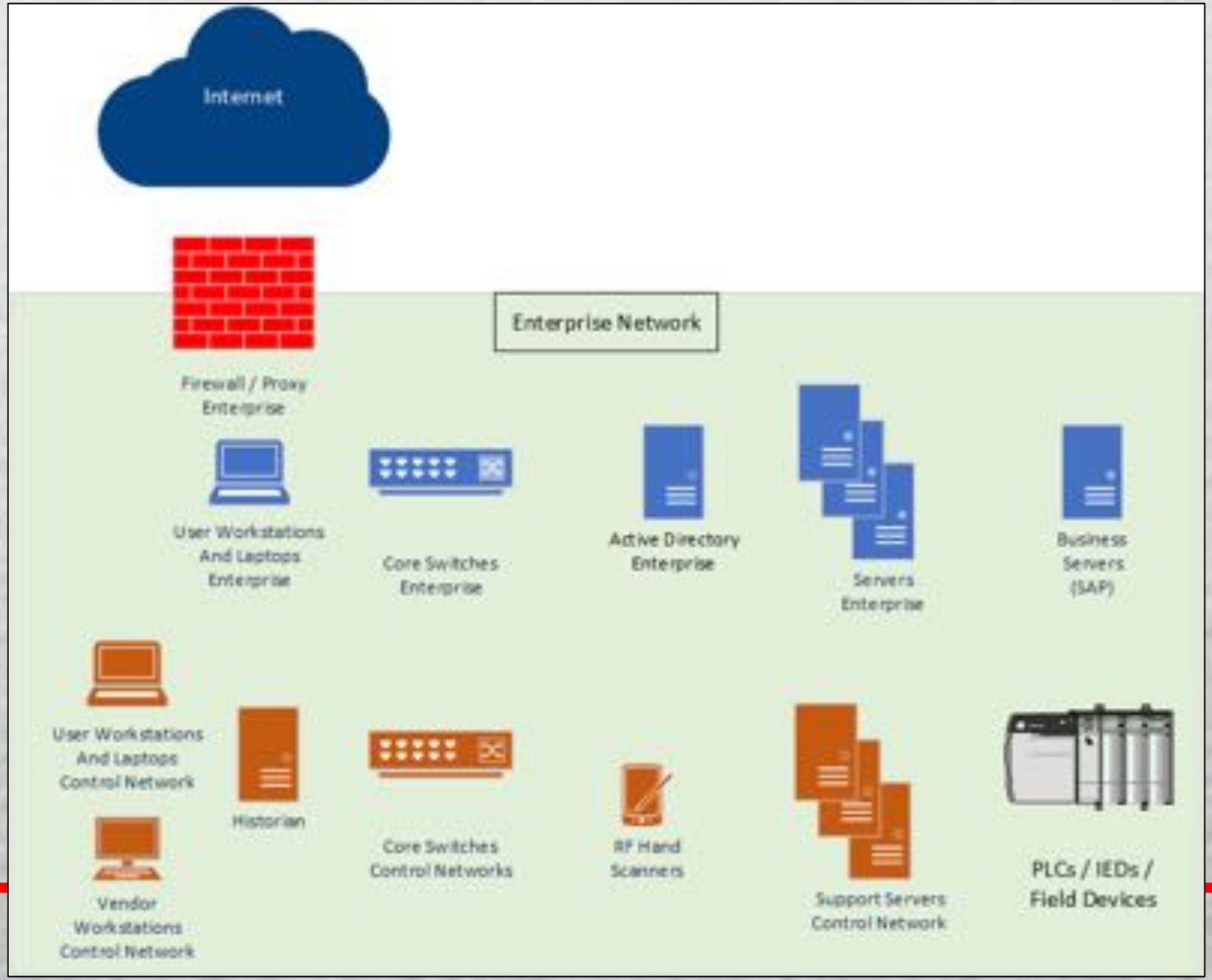
Purpose

Things to get over…

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



Worst Case Scenario



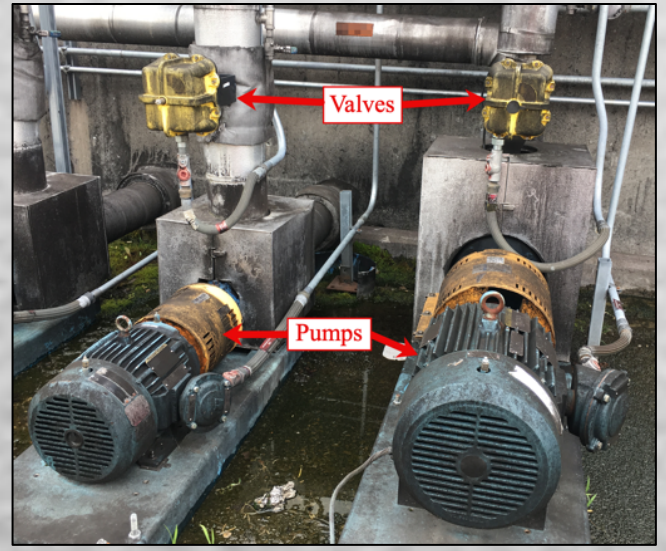
ICS Implementations and Equipment

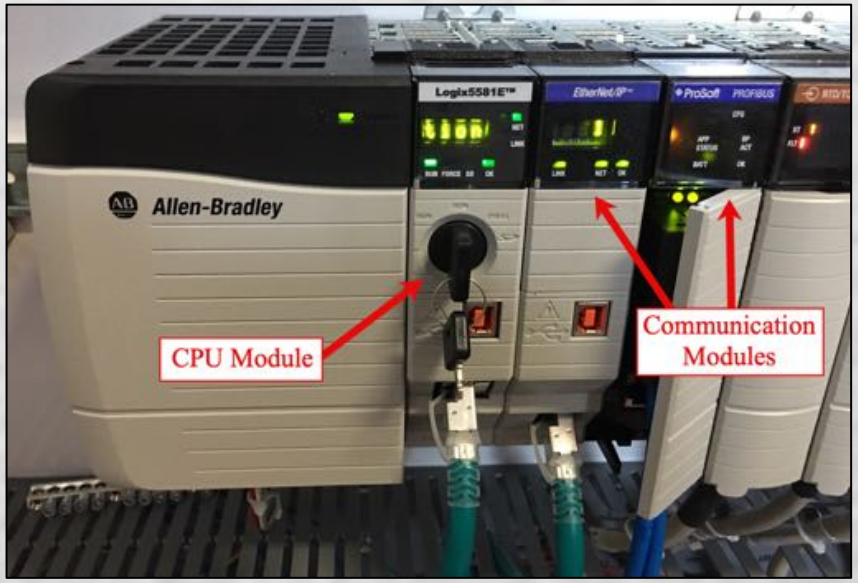
What are ICS implementations?

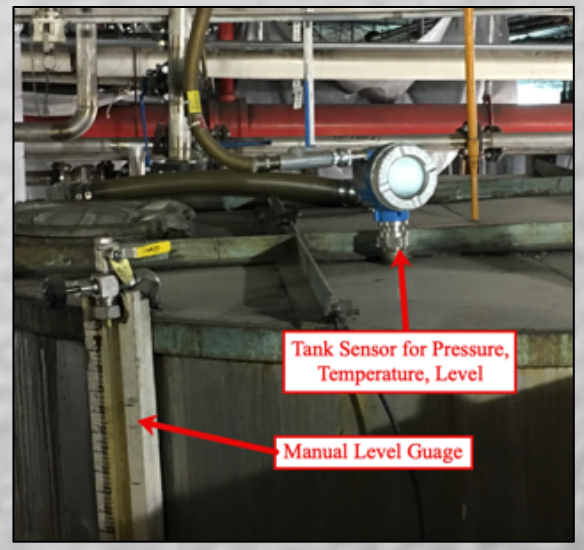
- A process is a group of devices and servers that perform a specific function, typically combined with other processes.
- Plants are multiple processes, that can be independent or dependent, which can be centrally controlled.
- SCADA are processes and plants that are mutually dependent but spread over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

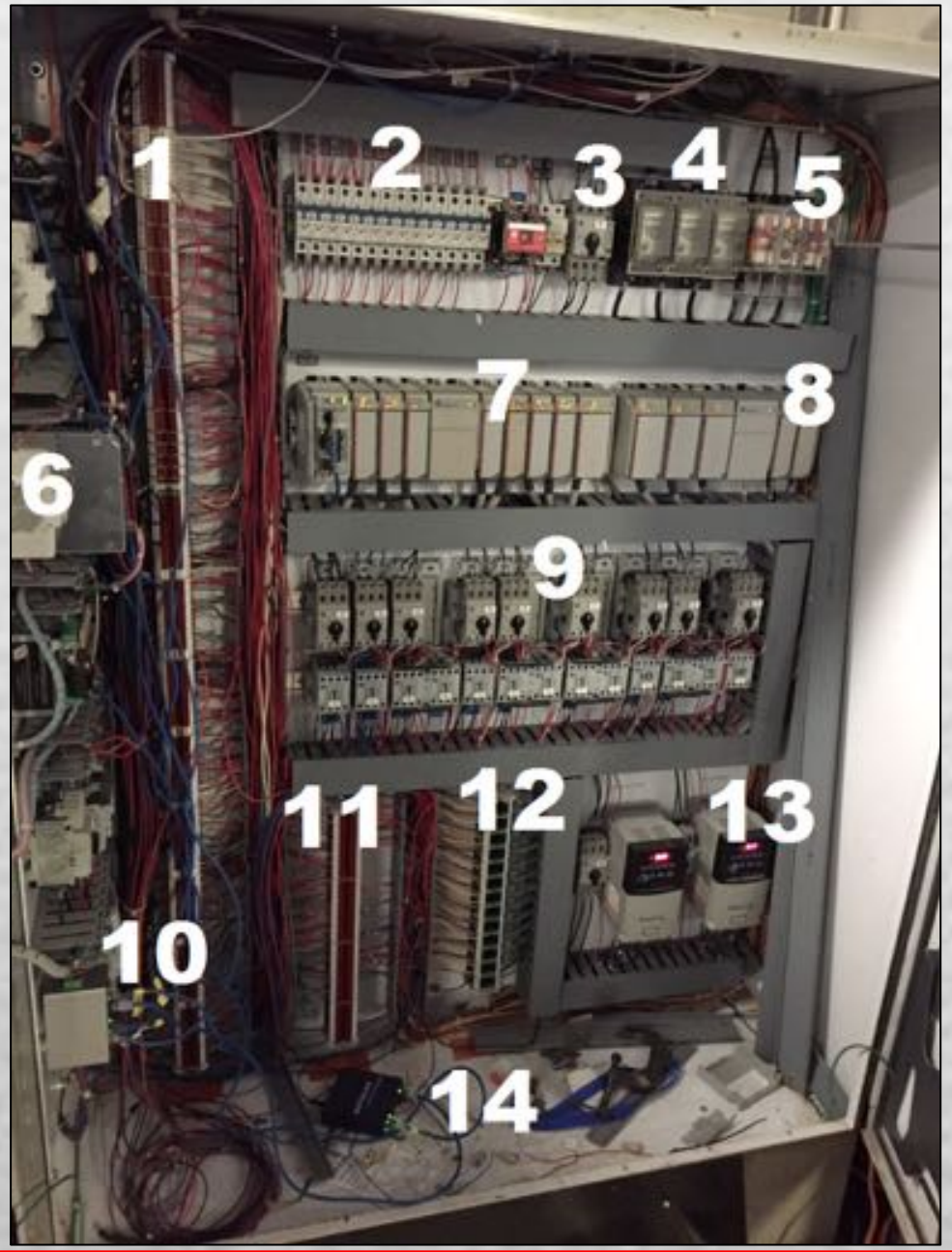
Image Source: Google Maps

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

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

Image Source: ControlThings.io Accessing and Exploiting Control Systems

What is a process?

How are processes managed?

- Human Machine Interfaces
- Master Servers
- Engineer Workstations
- Business Servers

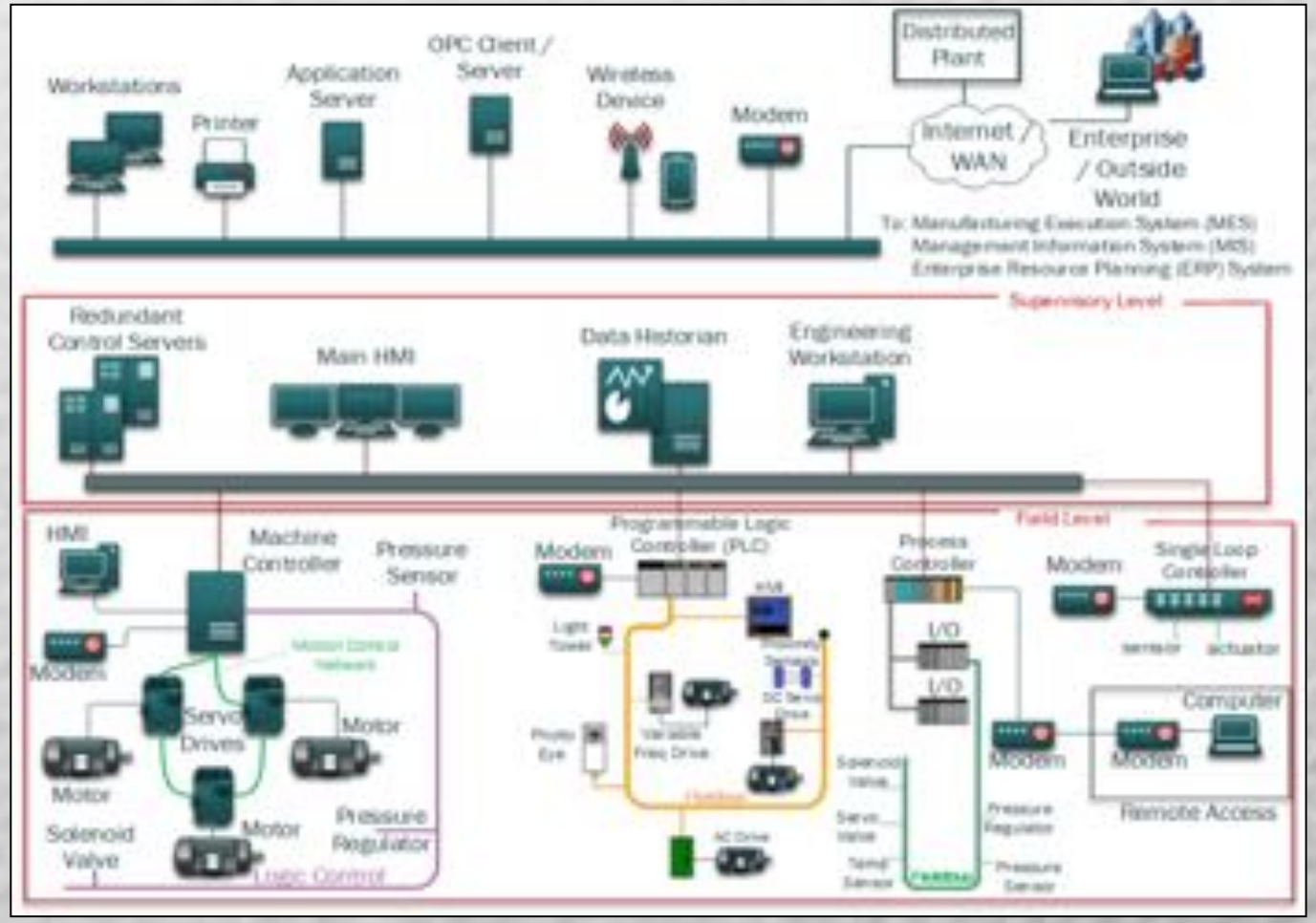


Image Source: ControlThings.io Accessing and Exploiting Control Systems

How are processes deployed?

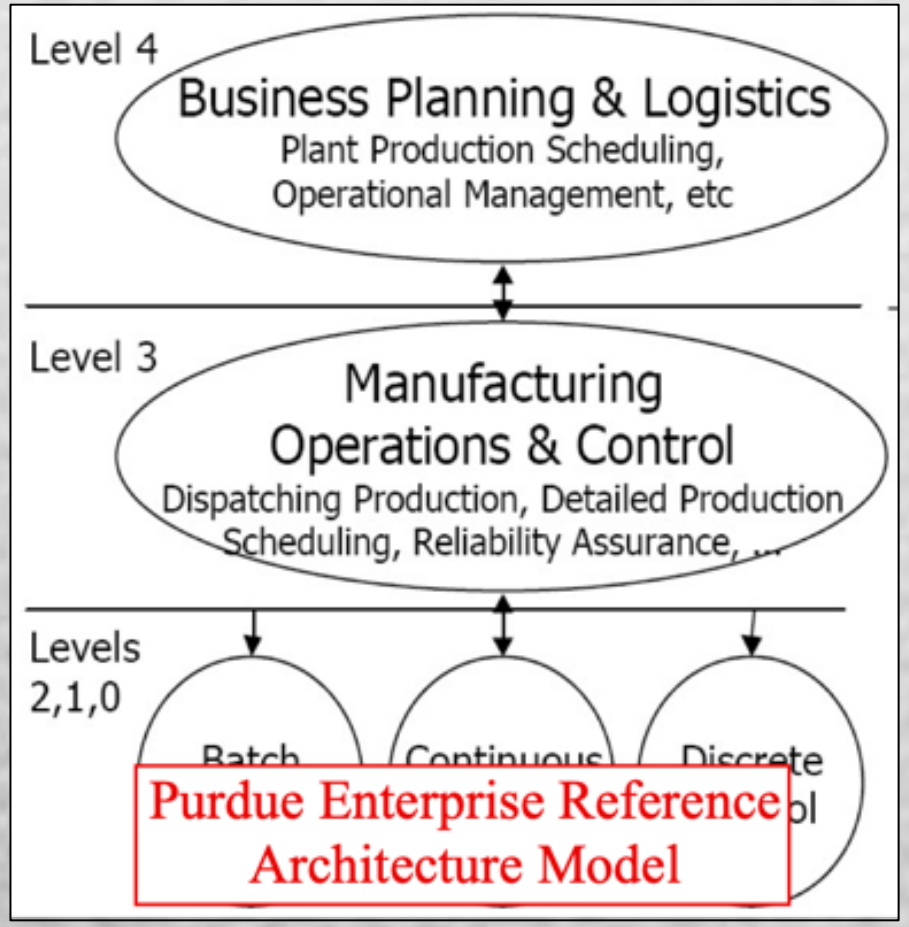


Image Source: SANS ICS410 ICS / SCADA Security Essentials

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

ICS Concerns

What are ICS business concerns?

Image Source: https://s3-us-west-1.amazonaws.com/umbrella-blog-uploads/wp-content/uploads/2015/08/Cannisters_After.jpg

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

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.

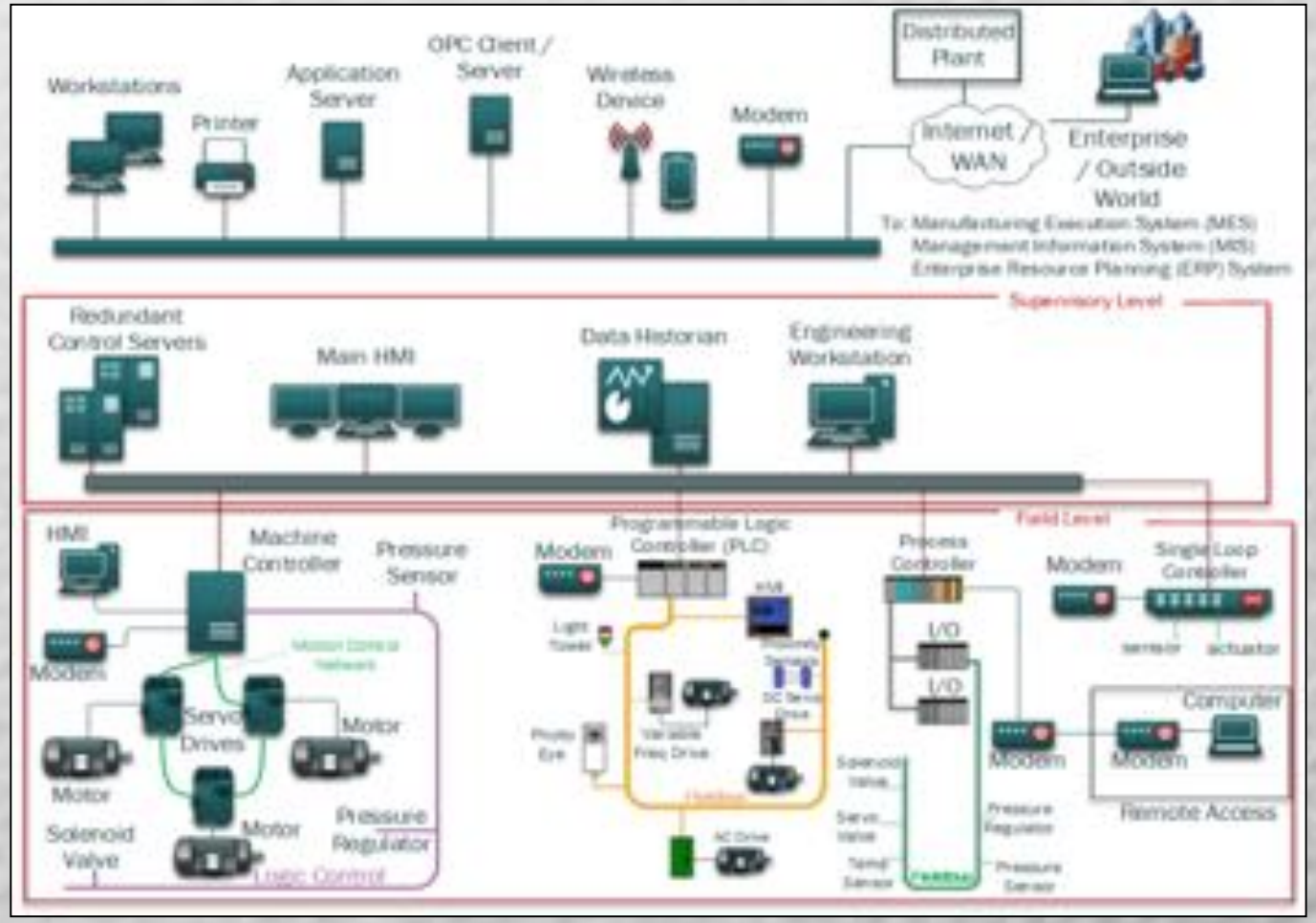
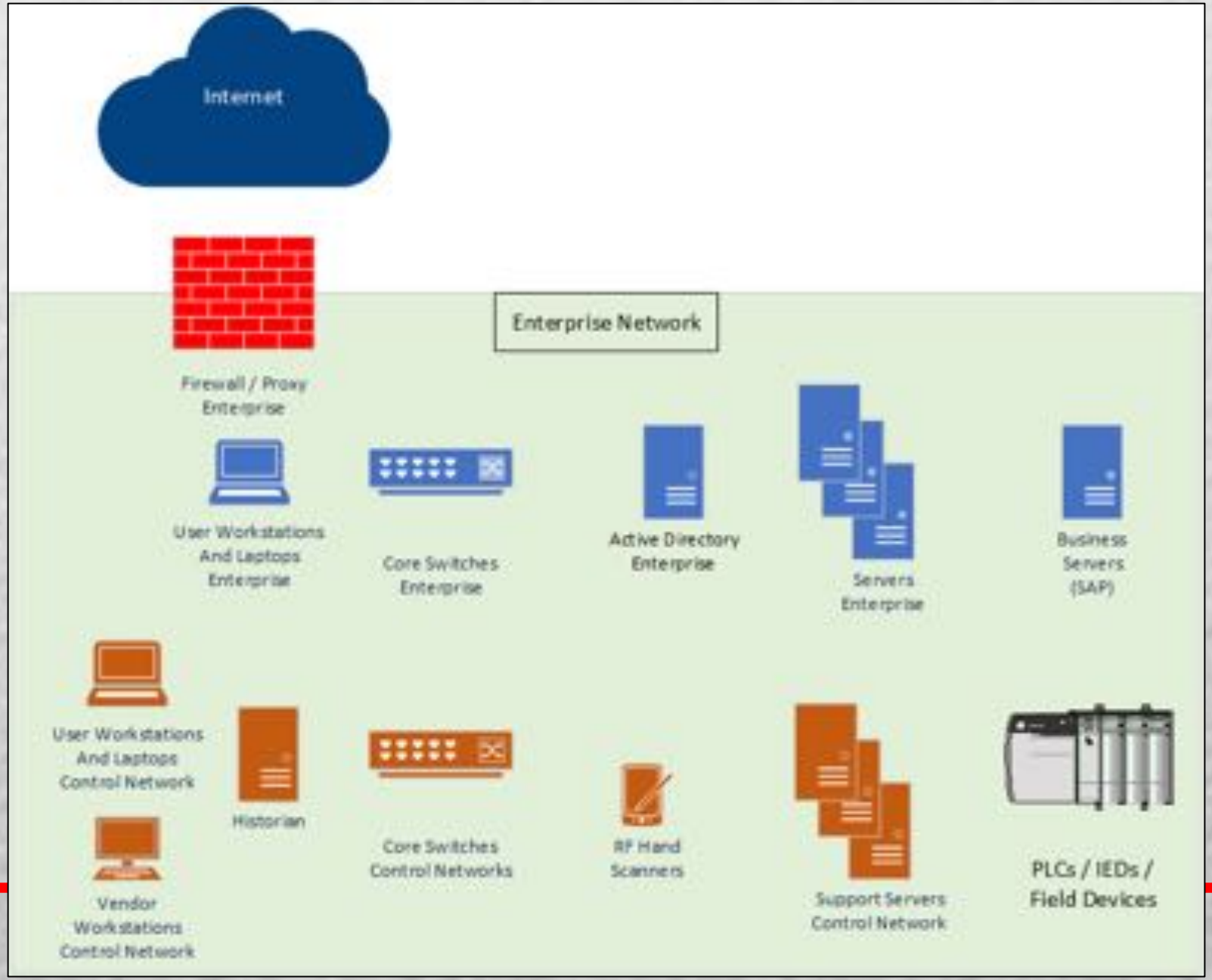


Image Source: ControlThings.io Accessing and Exploiting Control Systems

SANS ICS410 Reference Architecture

Worst Case Scenario



Expected Architecture – ICS410 Reference Model

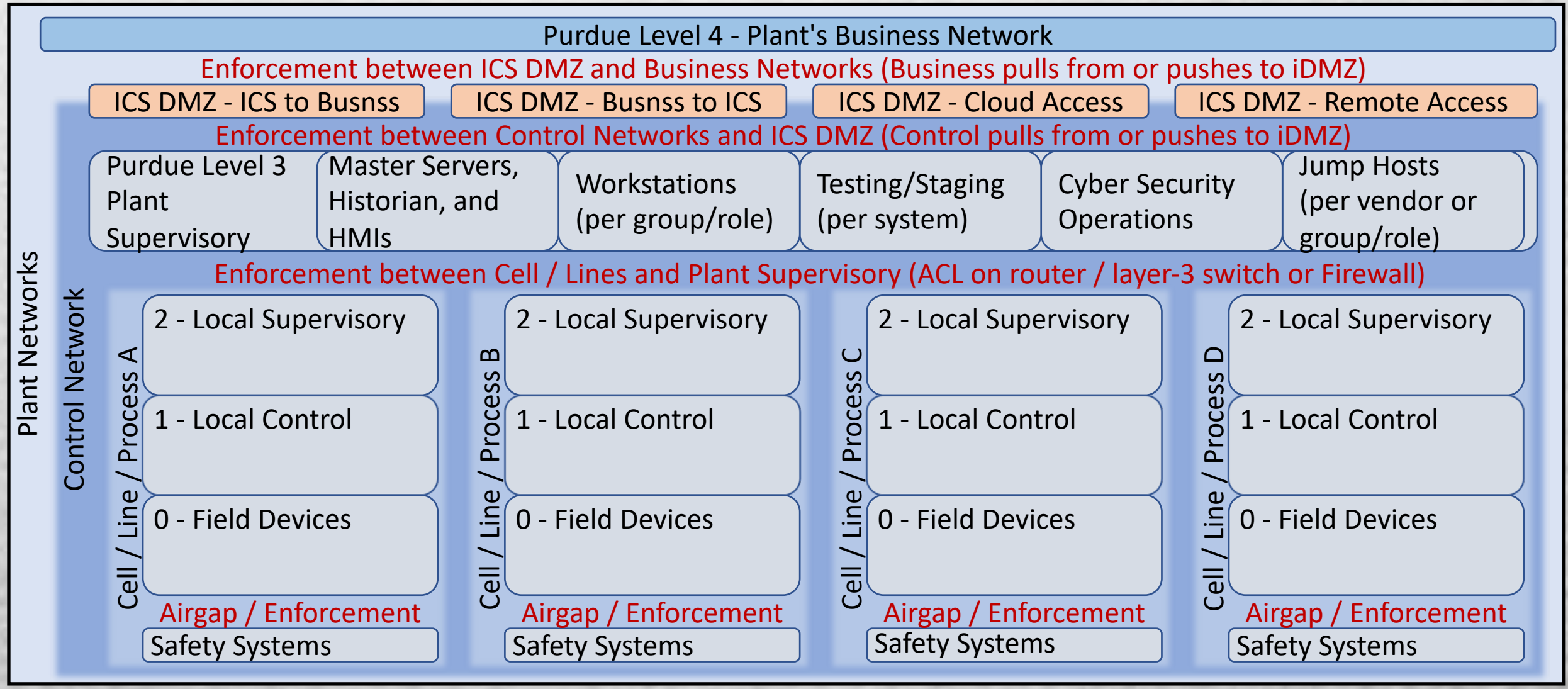
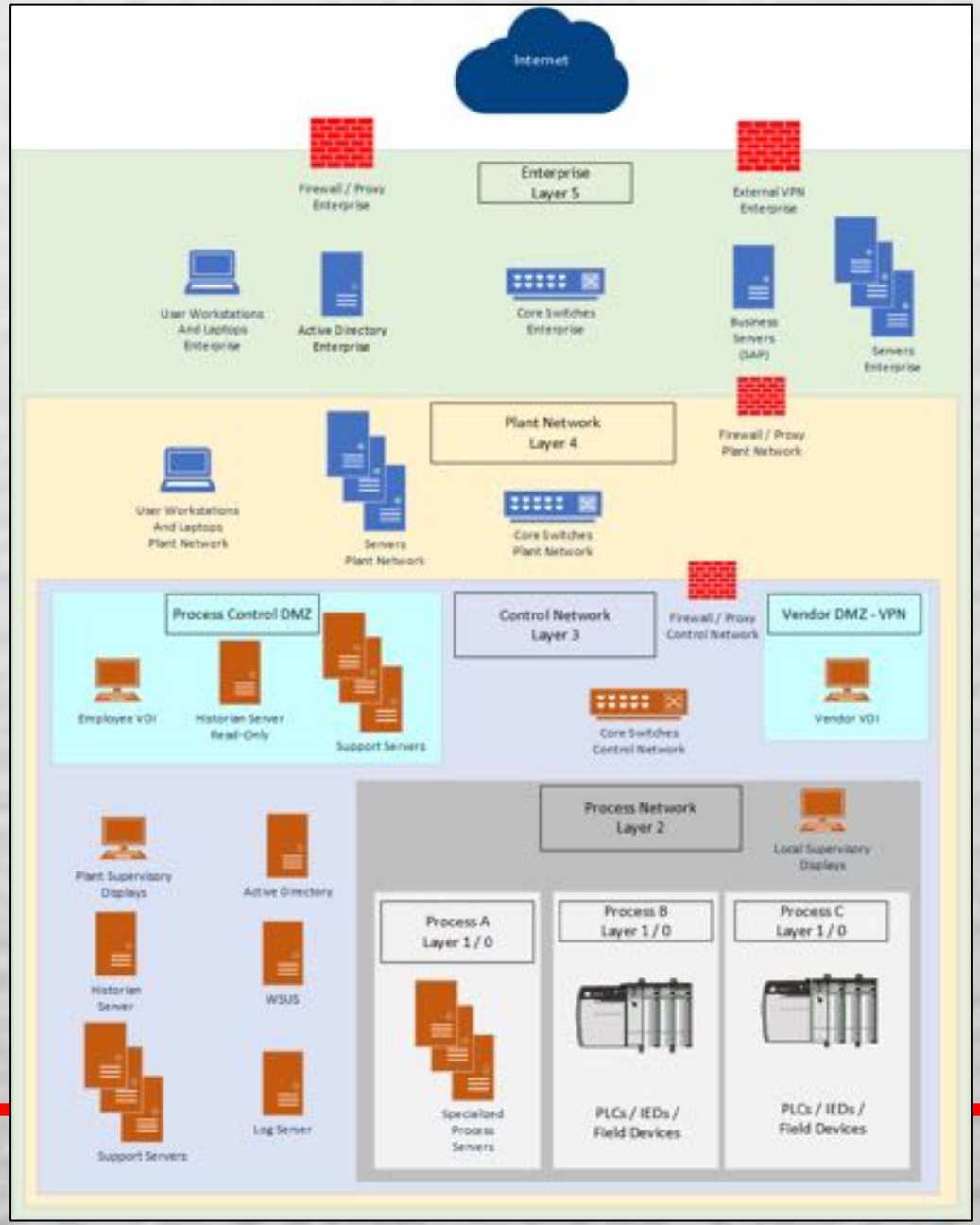


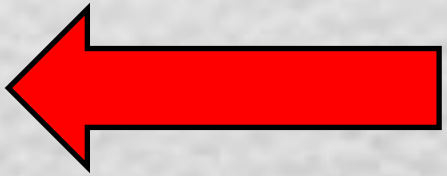
Image Source: ControlThings.io Accessing and Exploiting Control Systems

Best Case Scenario



IT / OT Security Effort Prioritization

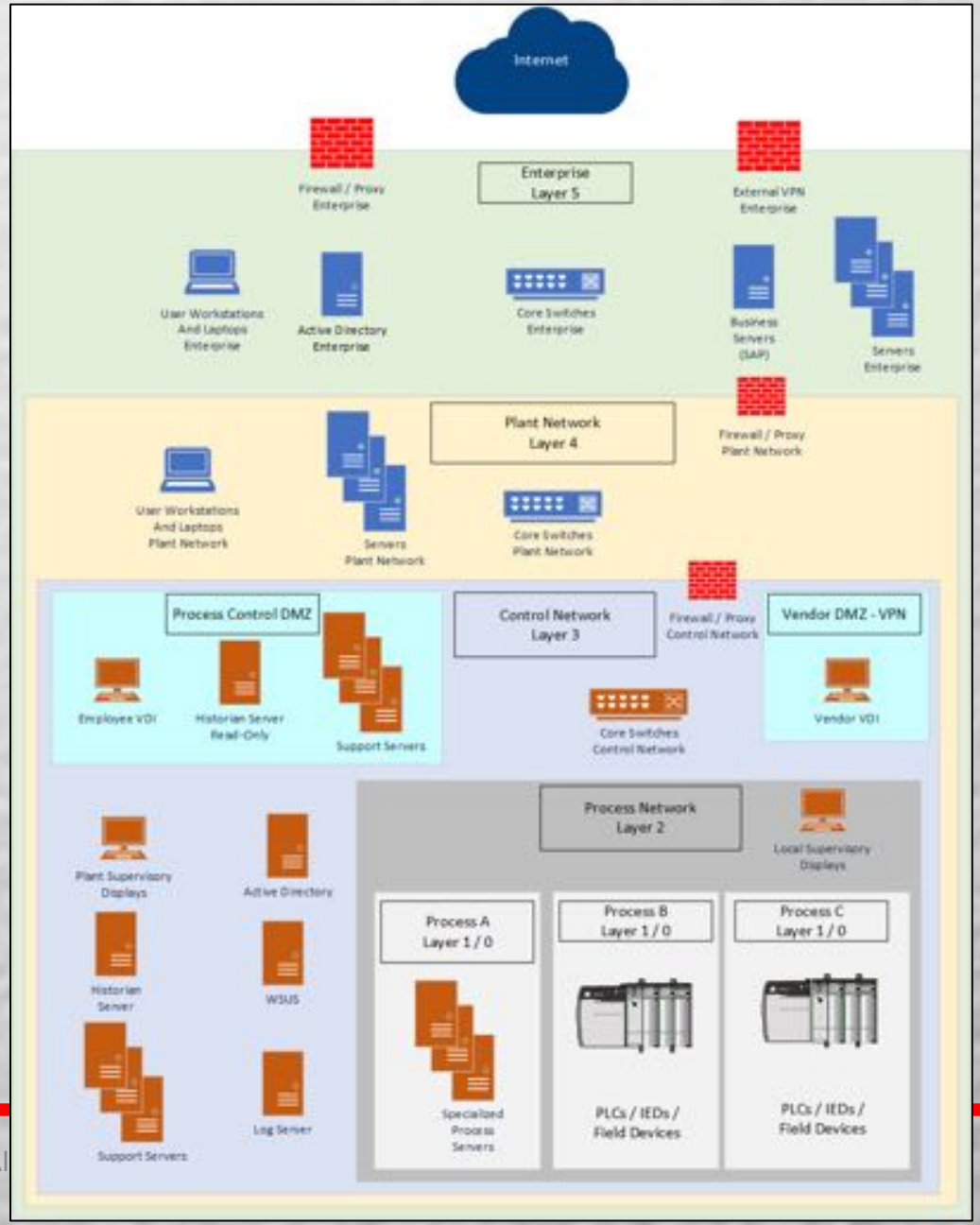
- Separate policies for IT and OT environments
- Segmentation and Isolation
- Access Control
- Logging and Monitoring
- Assessment Inventory
- Incident Response and Recovery



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

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