



CUTAWAY SECURITY
— INFOSEC CONSULTANTS —

Assessments in Active 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



Agenda

- Understanding ICS Environments
- Assessment Approach
- Reporting
- Recap

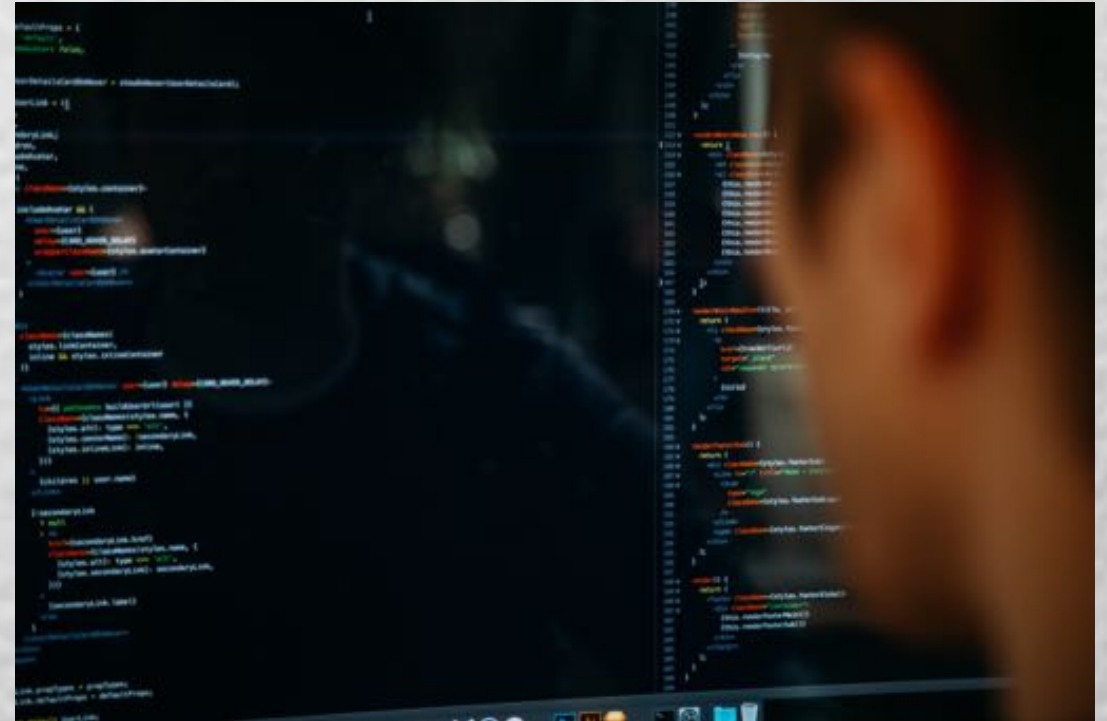


Image Source: <https://unsplash.com/photos/pjAH2Ax4uWk>



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 mutually beneficial 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 is a process?





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



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.

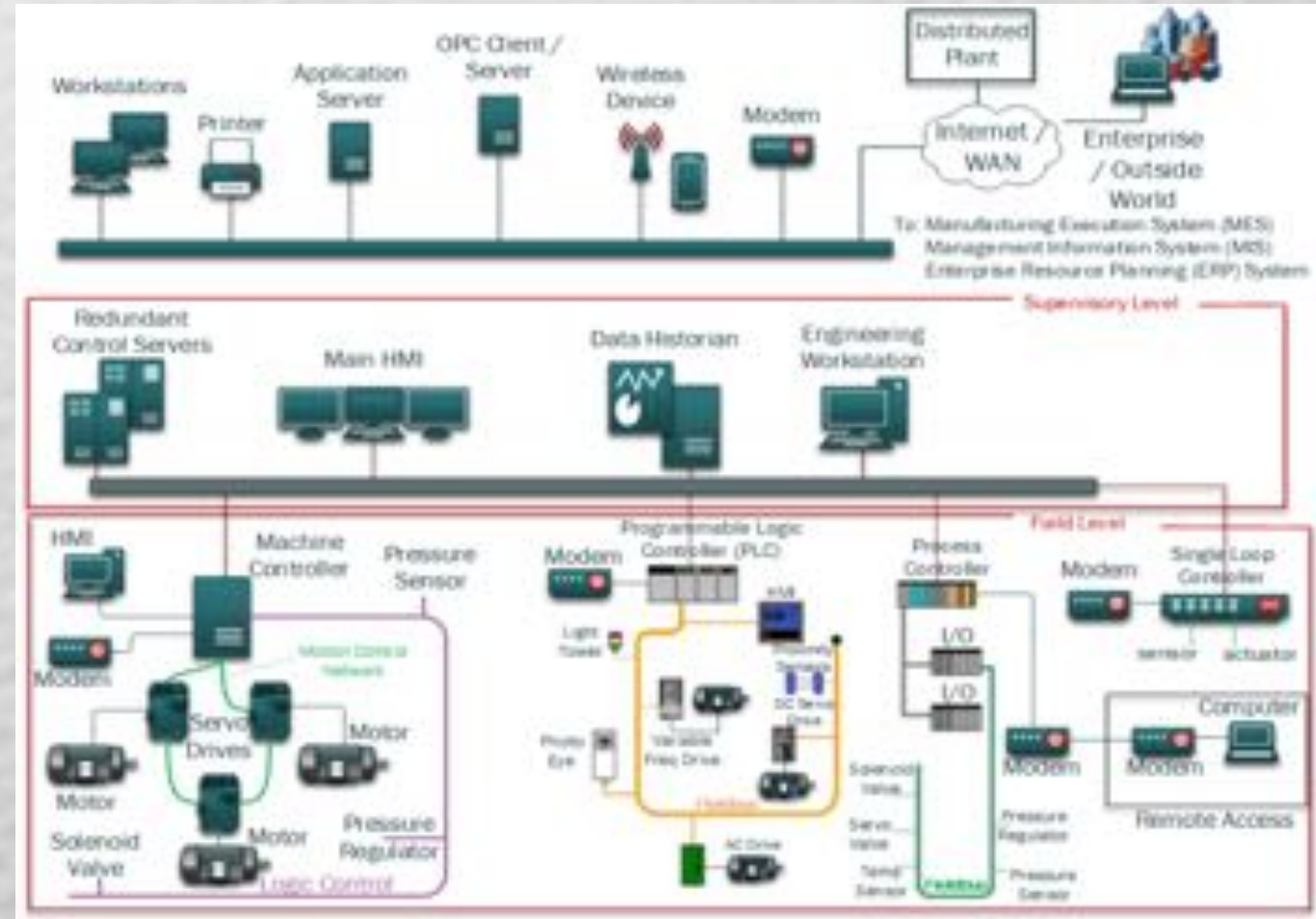


Image Source: <https://www.controlthings.io/> - Accessing and Exploiting Control Systems



Expected Architecture – Purdue Model

Purdue Level 4 - Plant's Business Network

Enforcement between ICS DMZ and Business Networks (Business pulls from or pushes to iDMZ)

ICS DMZ - ICS to Busnss

ICS DMZ - Busnss to ICS

ICS DMZ - Cloud Access

ICS DMZ - Remote Access

Enforcement between Control Networks and ICS DMZ (Control pulls from or pushes to iDMZ)

Purdue Level 3
Plant
Supervisory

Master Servers,
Historian, and
HMIs

Workstations
(per group/role)

Testing/Staging
(per system)

Cyber Security
Operations

Jump Hosts
(per vendor or
group/role)

Enforcement between Cell / Lines and Plant Supervisory (ACL on router / layer-3 switch or Firewall)

Plant Networks

Control Network

Cell / Line / Process A

- 2 - Local Supervisory
- 1 - Local Control
- 0 - Field Devices

Airgap / Enforcement

Safety Systems

Cell / Line / Process B

- 2 - Local Supervisory
- 1 - Local Control
- 0 - Field Devices

Airgap / Enforcement

Safety Systems

Cell / Line / Process C

- 2 - Local Supervisory
- 1 - Local Control
- 0 - Field Devices

Airgap / Enforcement

Safety Systems

Cell / Line / Process D

- 2 - Local Supervisory
- 1 - Local Control
- 0 - Field Devices

Airgap / Enforcement

Safety Systems



What are Operational Technology (OT) Team's Concerns?



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

- 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.



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.



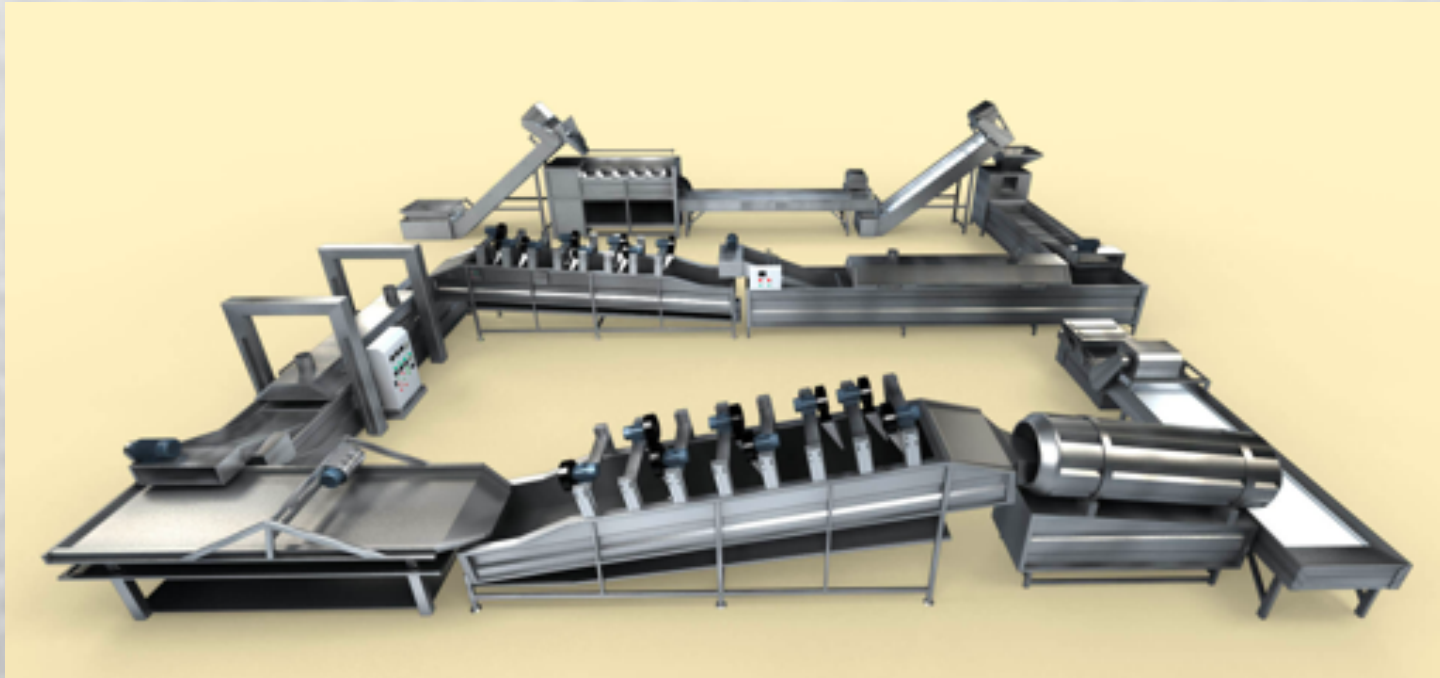
IT / OT Team Approach

- Plan and scope assessment with sufficient lead time. ← organize
- Identify critical process times. ← avoid them
- Identify maintenance, upgrade, and testing windows. ← leverage them
- Identify specific assessment goals with OT, IT, and Security Teams. ← test to those goals
- Define and work security requirements into Factory and Site Acceptance Testing (FAT / SAT) ← let the Quality Assurance / Control Team do their jobs





Assessment Approach



- Gather Information
- Process Interaction
- Reporting

Image Source: <https://potato-chips-machine.com/>



Gather Information

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



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



Process Interaction (1)

- Monitor network communications
 - Software: tcpdump, wireshark
 - Hardware: tap, switch with span port





Process Interaction (2)

- Configuration Hardening Assessment PowerShell Script (CHAPS) - <https://github.com/cutaway/chaps>

```
Administrator: Windows PowerShell
PS C:\Users\student\Documents> PowerShell.exe -ExecutionPolicy Bypass -File .\assumed_breach_checks.ps1
[ ] Script running with Administrator rights.
[ ] Windows Version: Microsoft Windows NT 10.0.16299.0
[ ] Windows Default Path for student : C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\Users\student\AppData\Local\Programs\Python\Python36\Scripts\;C:\Users\student\AppData\Local\Programs\Python\Python36\;C:\Users\student\AppData\Local\Microsoft\WindowsApps;C:\Program Files (x86)\Imap
[ ] Checking IPv4 Network Settings
[ ] Host network interface assigned: 192.168.50.144
[ ] Checking Windows AutoUpdate Configuration
[+] Windows AutoUpdate is set to 4 : Scheduled installation
[ ] Checking for missing Windows patches with Critical or Important MsrcSeverity values. NOTE: This make take a few minutes.
[+] Windows system appears to be up-to-date for Critical and Important patches.
[ ] Checking BitLocker Encryption
[-] BitLocker not detected on Operating System Volume or encryption is not complete. Please check for other encryption methods: FullyDecrypted
[ ] Checking if users can install software as NT AUTHORITY\SYSTEM
[+] Users cannot install software as NT AUTHORITY\SYSTEM.
[ ] Testing if PowerShell CommandLine Auditing is Enabled
[-] ProcessCreationIncludeCmdline_Enabled Is Not Set
[ ] Testing if PowerShell Moduling in Wow6432Node Policies is Enabled
[-] EnableModuleLogging Is Not Set
[ ] Testing if PowerShell Moduling in Policies is Enabled
[-] EnableModuleLogging Is Not Set
[ ] Testing if PowerShell EnableScriptBlockLogging in Wow6432Node Policies is Enabled
[-] EnableScriptBlockLogging Is Not Set
[ ] Testing if PowerShell EnableScriptBlockInvocationLogging in Wow6432Node Policies is Enabled
[-] EnableScriptBlockInvocationLogging Is Not Set
[ ] Testing if PowerShell EnableScriptBlockLogging in Policies is Enabled
[-] EnableScriptBlockLogging Is Not Set
[ ] Testing if PowerShell EnableScriptBlockInvocationLogging in Policies is Enabled
[-] EnableScriptBlockInvocationLogging Is Not Set
[ ] Testing if PowerShell EnableTranscripting in Wow6432Node Policies is Enabled
[-] EnableTranscripting Is Not Set
[ ] Testing if PowerShell EnableInvocationHeader in Wow6432Node Policies is Enabled
[-] EnableInvocationHeader Is Not Set
[ ] Testing if PowerShell EnableTranscripting in Policies is Enabled
[-] EnableTranscripting Is Not Set
[ ] Testing if PowerShell EnableInvocationHeader in Policies is Enabled
```



Process Interaction (3)

- Windows Exploit Suggester - Next Generation - <https://github.com/bitsadmin/wesng>

```
cutaway> ./windows-exploit-suggester.py --database 2018-12-30-mssb.xls --systeminfo win7-sysinfo.txt
[*] initiating wmsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 151 hotfix(es) against the 386 potential bulletins(s) with a database of 137 known exploits
[*] there are now 136 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 SP1 64-bit'

[*]
[*] [E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*] https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*] https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*] https://github.com/tinysec/public/tree/master/CVE-2016-7255

[*]
[*] [E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*] https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGN08J Integer Overflow (MS16-098)

[*]
[*] [M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*] https://github.com/foxglovesec/RotterPotato
[*] https://github.com/Kevin-Robertson/Tater
[*] https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege
[*] https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation

[*]
```




Process Interaction (4)

Source: ControlThings.io - Scanning Highly Sensitive Networks:

<https://drive.google.com/file/d/1IMaDVTNRXNr0yEfr2dW7HuZYohaEpHmL/view>

- Port scanning can crash legacy embedded systems if not careful! Here are the most likely causes:
 - OS Fingerprinting
 - Don't use the -O or -A flags in Nmap
 - By far the most likely cause of crashed embedded systems
 - Can do ARP scans locally on each subnet and use MAC to ID devices
 - Scanning with SYN scans
 - Default when using Nmap with sudo or running it as root
 - Not proper RFC behavior, so only mature ICP/IP stacks handles this properly
 - Always specify -sT in your scans to avoid this accident
 - Scanning too fast (yes, the defaults in Nmap are too fast)
 - Use Nmap's -T2 setting sets this at 0.4 seconds
 - Or use Nmap's --scan-delay 0.1 or --max-parallelism 1 to scan 1 port at a time per host
 - Scanning UDP ports with null payloads (**can affect ICS software on Windows and Linux too!!!**)
 - Don't use the -sU option in Nmap
 - Service fingerprinting usually safe, but can occasionally cause problems
 - Use Nmap's -sV selectively on new subnets
 - Or use Nmap's --script=banner



Image Source: <https://nmap.org>



Process Interaction (5)

- Escalate According to Goals

- Active Directory Testing
- Windows Shares Review
- Interact with Field Level devices
- Consider how to demonstrate evil appropriate with your skill level
- Don't mess with production equipment

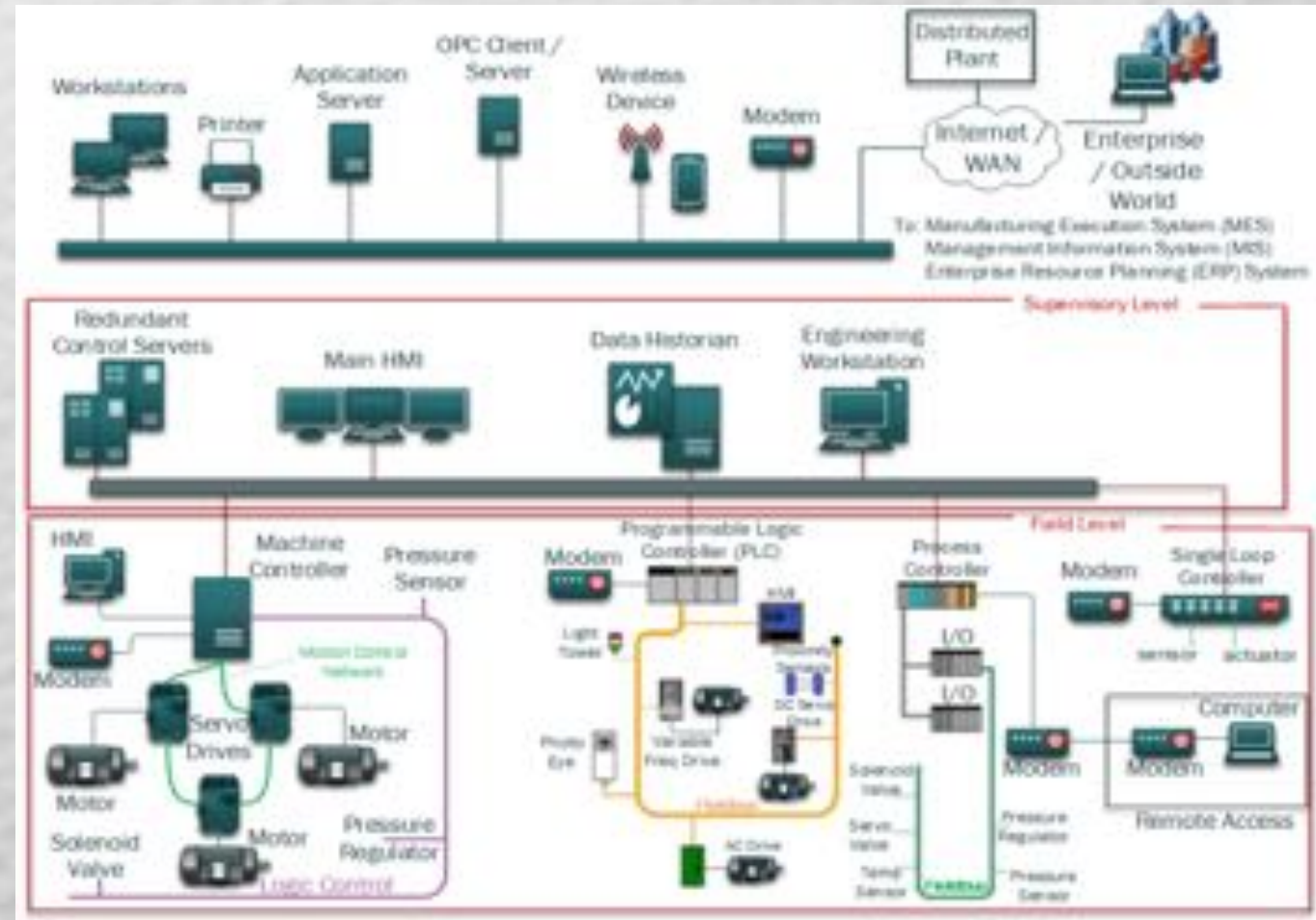


Image Source: <https://www.controlthings.io/> - Accessing and Exploiting Control Systems



Process Interaction (6)

- What common penetration testing tools did I not mention?



Reporting



- Typical Assessment Reporting
 - Executive Summary
 - Methodology
 - Findings with Remediations
- Systemic Issues
 - ICS Security Program aligned with NIST CyberSecurity Framework
 - Segmentation and Isolation
 - Vendor Access

Image Source: <https://unsplash.com/photos/G3yLB3Fasow>

Recap

- Understanding ICS Environments
- Assessment Approach
- Reporting
- Recap

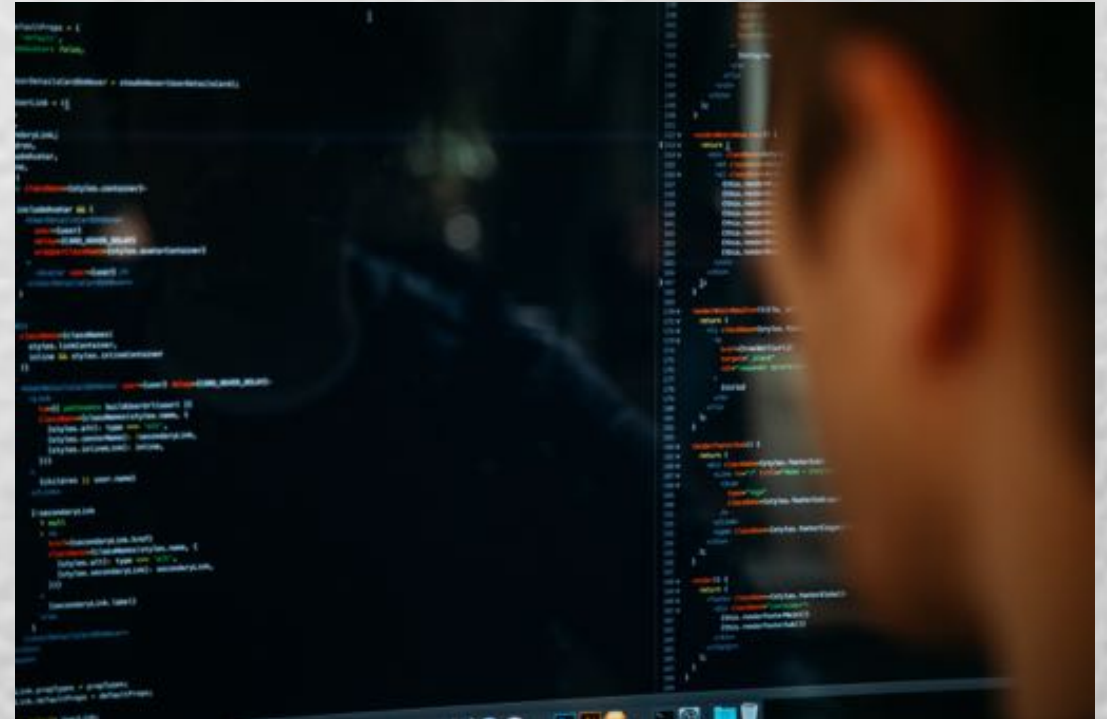


Image Source: <https://unsplash.com/photos/pjAH2Ax4uWk>



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>