NOZOMI NETWORKS

Pen Testing ICS/OT: do’s and don’ts

CHCon

November 6th 2021 at 1430 – 1500

Presenter: Gavin Dilworth

WHOami ? – Gavin Dilworth

BACKGROUND

Control System Engineer / Industrial Automation Engineer, Cyber Security Consultant and Operator

PAST EXPERIENCE

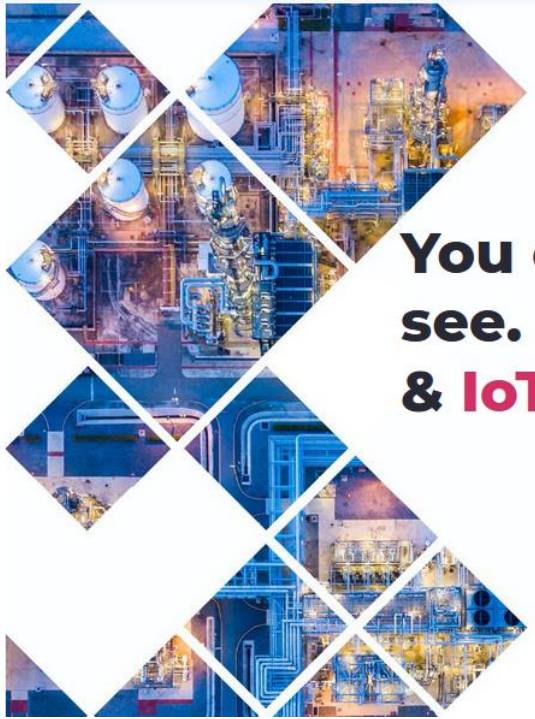
Company: Various system integrators and end users

Industries: Manufacturing, Water and Waste, Oil and Gas, Energy

Roles: Engineer, ICS/OT Cybersecurity Lead, Managing Consultant
ICS/OT Security architecture, auditing, vulnerabiltiy/security/site/risk assessments, trainer, jack of all master of none

- **Nozomi Networks Delivery Solution Provider**
- Master of Professional Practice in ICS Cyber Security
- Graduate Diploma of Project Management
- Advanced Diploma of Industrial Automation

Nozomi Networks Community Edition



The first step to protecting your networks is knowing what you have. Nozomi Networks Guardian Community Edition helps you get visibility into your OT and IoT assets.

You can't protect what you can't see. Take your first step into OT & IoT cybersecurity

Nozomi Networks Guardian Community Edition (CE) gives you visibility into your OT and IoT networks. By leveraging our award-winning cybersecurity technology, Guardian CE helps extend security programs to include the OT and IoT assets in your network. Guardian CE uses passive, non-invasive technologies to detect devices operating within your environment and to map your complete network, all without disrupting operations.

https://community.nozominetworks.com/

Disclaimer

- **Opinions expressed are solely my own and do not express the views or opinions of my employer**
- **Time is constrained, some basics of ICS/OT Cyber Security will be omitted.**

What is ICS / OT

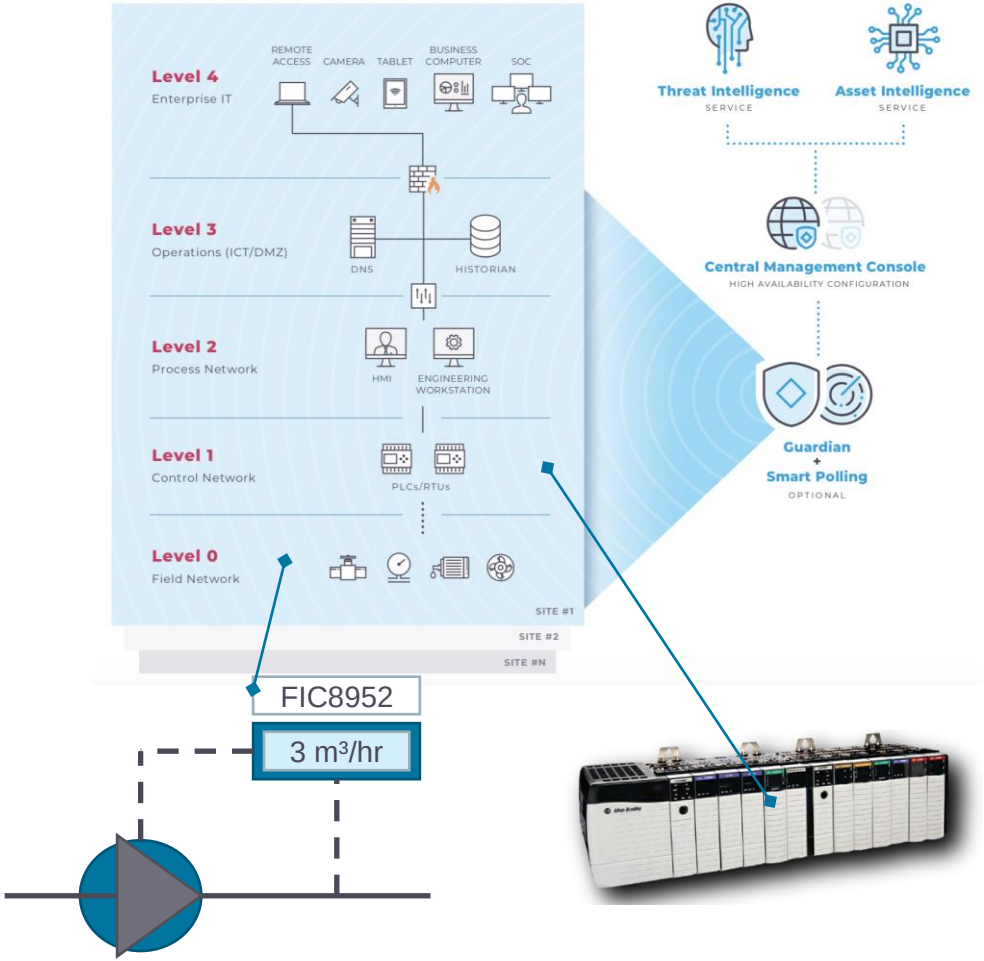
Definitions

- **Industrial control system (ICS)**

is a general term that encompasses several types of control systems and associated instrumentation used for industrial process control.

- **Operational technology (OT)**

is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events. The term has become established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems environment



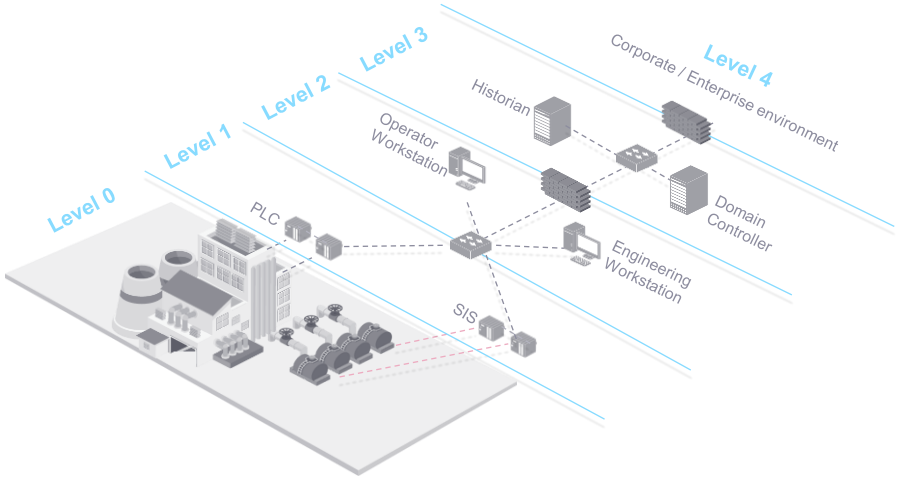
Source: Wikipedia
https://en.wikipedia.org/wiki/Operational_technology
https://en.wikipedia.org/wiki/Industrial_control_system

What is ICS / OT

Purdue Model (ISA 95 and ISA 99 / IEC 62443)

- **Level 4** – Generic IT / Corporate environment
- **Level 3** – Common services, such as Patch, AAA, File and Backup server, Historian, potentially SCADA.
- **Level 2** – Local visulisation of the process, HMI's, Gateways, Workstations.
- **Level 1** – Controllers, contain the instructions to control the process
- **Level 0** – Instrumentation and field devices, valves, pumps, motors and actuators.

- Safety Instrumented Systems – can exist at level 1 and 0, they bring the process or machine to a safe state, when exceeding limits or boundaries.



IT vs OT / ICS

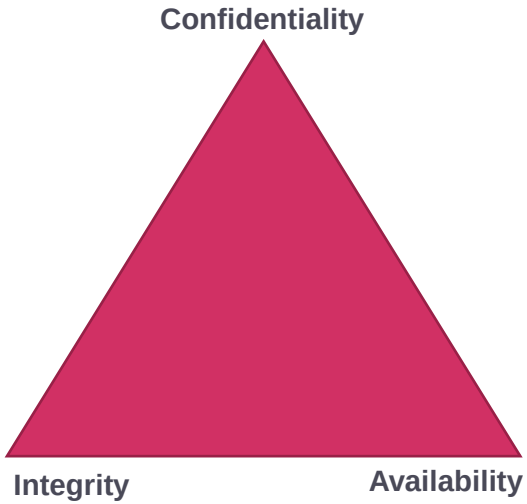
Priorities and Risk

- **Why are we talking about priorities and risk in a penetration testing talk?**
- **Risk is perceived differently in OT/ICS, there are different priorities**
  - Safety is #1
  - Security Controls potentially won't be used to make sure the process and safety is not impacted, for example:
    - Passwords
    - Patching
- **In a world of operating 24/7 365, turning it off and on again is not an option**

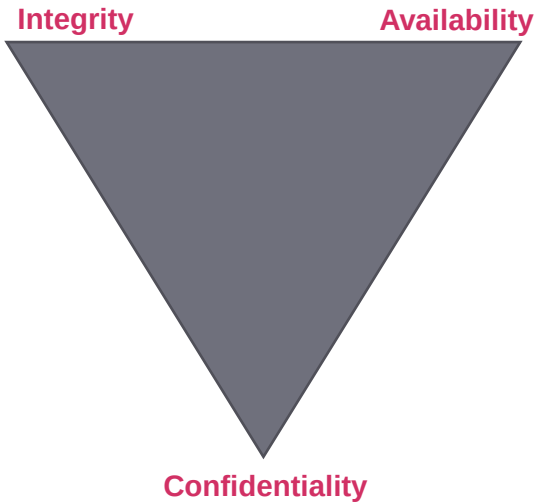
IT vs OT / ICS

Priorities and Risk

Information Systems



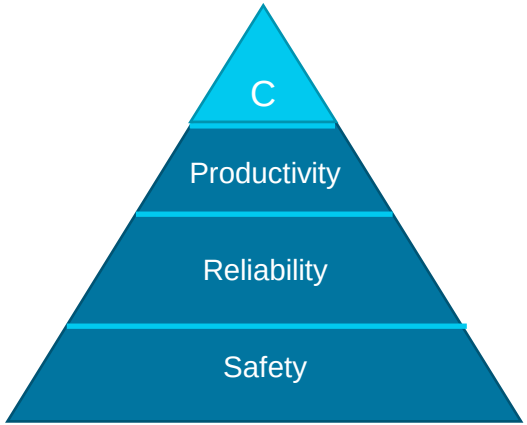
OT / ICS Education



IT vs OT / ICS

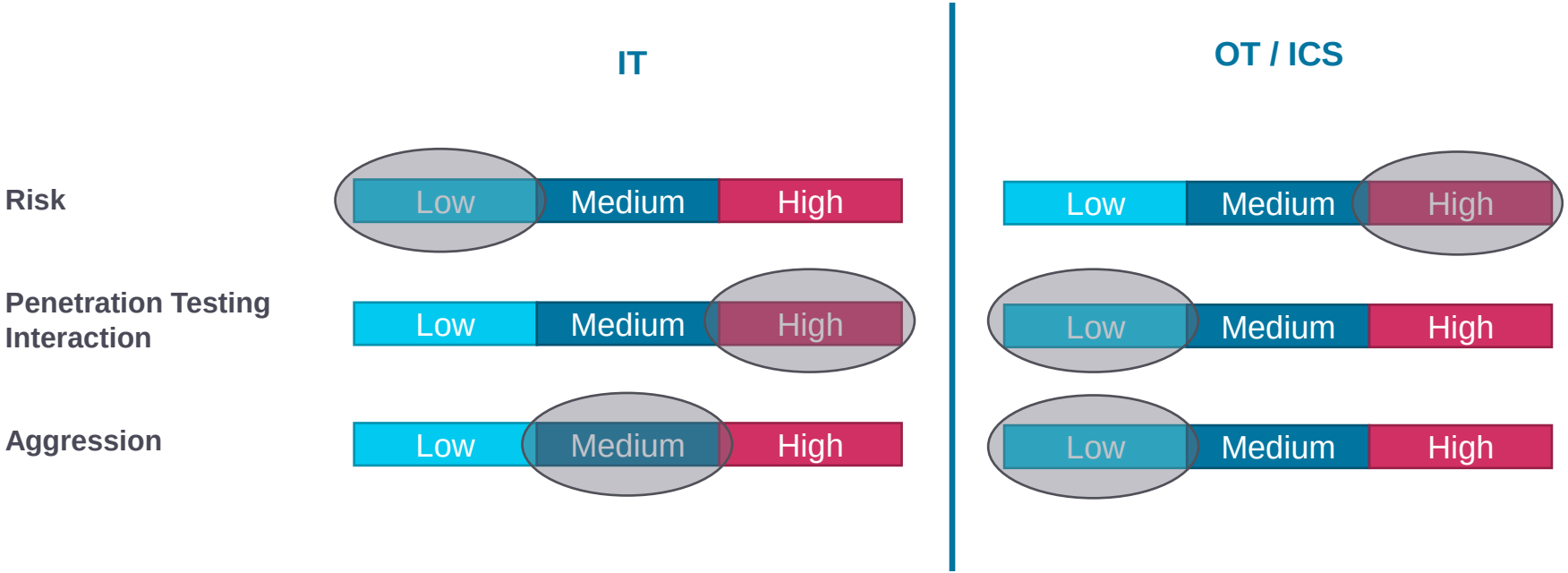
Priorities and Risk

Real World Priorities



IT vs OT / ICS

Conducting a Penetration Test



Enumeration

Asset Inventory and Vulnerability identification

High Risk (Potentially)
- Nmap ICS NSE scripts
- Nessus OT settings

Just cause its never happened to you, doesn't mean it won't

Low Risk
- ICS /OT IDS
- RTFM
- Host Enumeration (Engineering Workstation)

NMAP - S7

NMAP – EtherNet/IP

Allen Bradley PLC
EtherNet/IP (Industrial Protocol)

Seimens PLC - S7 Protocol

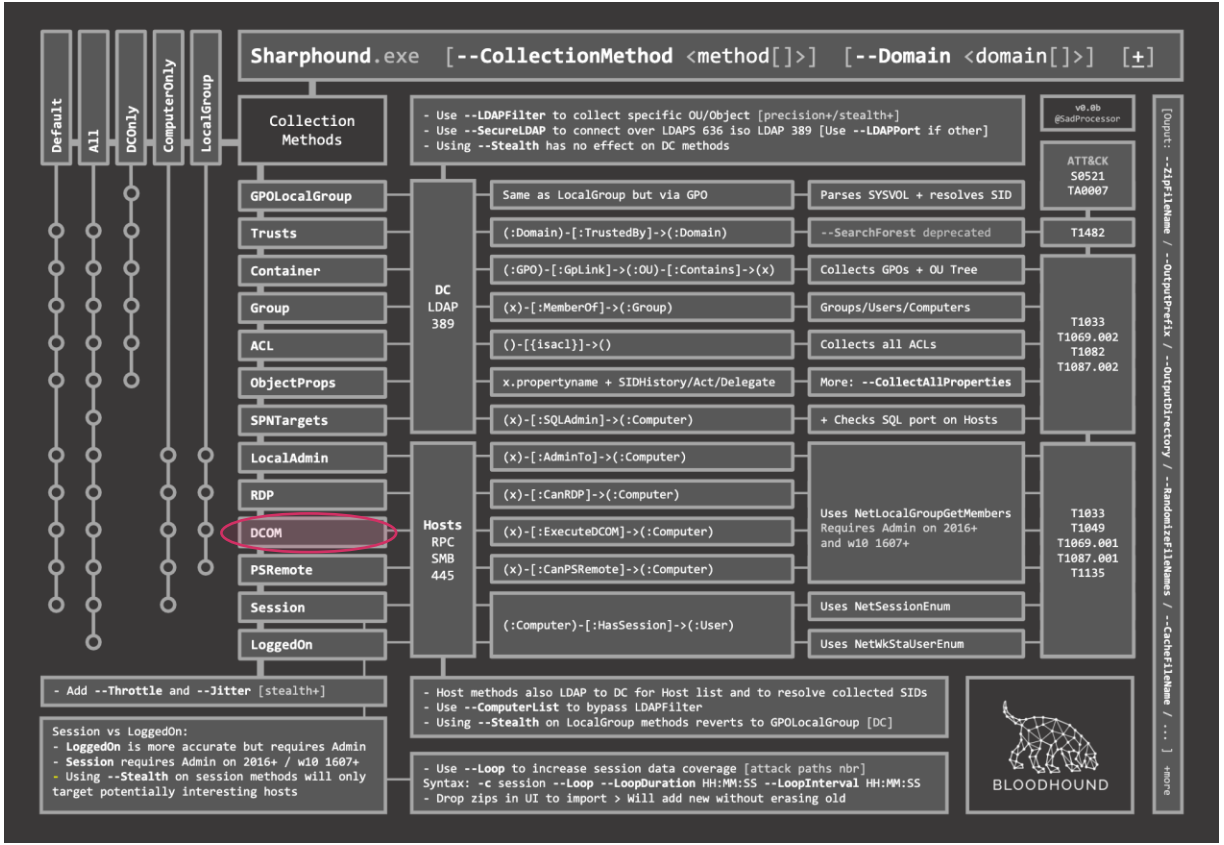
Great Resource, to lower risk:

https://www.controlthings.io/resources
Scanning Highly Sensitive Networks.pdf

Enumeration

Bloodhound

- OPC Direct Access
  - OPC Classic
  - OPC DCOM
  - OPC
- OPC Unified Architecture (not relevant)



Source: Bloodhound.readthedocs.io
https://bloodhound.readthedocs.io/en/latest/data-collection/sharphound-all-flags.html

Penetration Testing

What should we be doing, or shouldn't be

Penetration Testing

Device Testing - Offline

- Finding vulnerabilities before products are deployed into production

Penetration Testing

Device Hardening

- Finding insecure configuration, before they are deployed into production
  - Factory Acceptance Test (FAT)
  - Site Acceptance Test (SAT)

Penetration Testing

Live Penetration Test

- On a Production network and systems
  - Actively scanning, modifying, manipulating data within an ICS / OT environment

- On a development / staging / testing environment
- During FAT and SAT

Purple Teaming

Live Purple Teaming

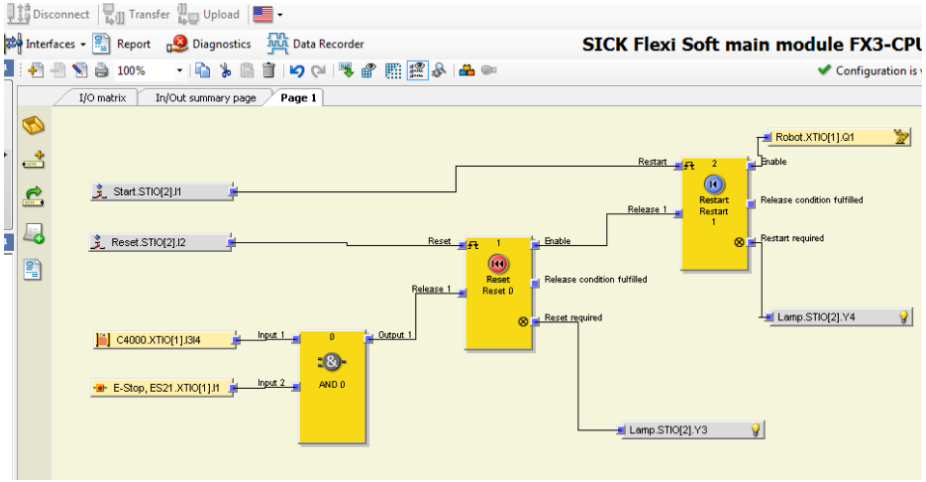
- On a Production network and systems
  - Actively scanning, modifying, manipulating data within an ICS / OT environment

- On a development / staging / testing environment
- During FAT and SAT

Story Time

Why is purple teaming ideal for ICS/OT ?

Safety PLC



Source: SICK
https://www.sick.com/us/en/flexi-soft-designer/

Purple Teaming

APT Emulation

- Industry specific
- Byte sized (can focus on the specifics)
- Monitoring
  - Anomalous behaviour
  - Tactics, Techniques and Procedures
- IR and DR testing

Techniques Used

- Block Command Message - In the Ukraine 2015 Incident, **Sandworm Team** blocked comr
- Block Reporting Message - In the Ukraine 2015 Incident, **Sandworm Team** blocked repor
- Device Restart/Shutdown - In the 2015 attack on the Ukrainian power grid, the **Sandwor**
- Exploit Public-Facing Application - **Sandworm Team** actors exploited vulnerabilities in GE
- External Remote Services - In the Ukraine 2015 Incident, **Sandworm Team** harvested VI
- Graphical User Interface - In the Ukraine 2015 Incident, **Sandworm Team** utilized HMI GU
- Spearphishing Attachment - In the Ukraine 2015 incident, **Sandworm Team** sent spearp
- System Firmware - In the Ukraine 2015 Incident, **Sandworm Team** developed and used
- Remote Services - In the Ukraine 2015 Incident, **Sandworm Team** used native remote ac
- Unauthorized Command Message - In the Ukraine 2015 Incident, **Sandworm Team** issue
- Valid Accounts - **Sandworm Team** used valid accounts to laterally move through VPN c

Techniques in this Tactics Category

Below is a list of all the Impact techniques in ATT&CK for ICS

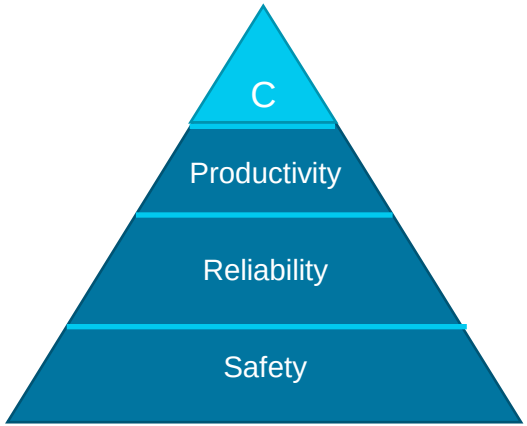
Name	Tactics	
Damage to Property	**Impact**	Adversarie Depending impact in th The Germa installations In the Maro community. A Polish str derailed an
Denial of Control	**Impact**	Adversarie controls. A In the Maro In the 2017
Denial of View	**Impact**	Adversarie interferenc An adversa functioning In the Maro
Loss of Availability	**Impact**	Adversarie
Loss of Control	**Impact**	Adversarie Security Re
Loss of Productivity and Revenue	**Impact**	Adversarie against nor of Safety.

Source: MITRE ATT&CK® for Industrial Control Systems
https://collaborate.mitre.org/attackics/index.php/Impact

Key Take Away's

In a ICS/OT environment

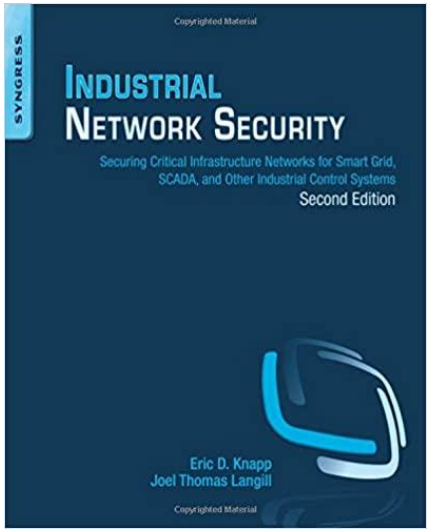
- The risk is high, for causing a process upset
- Do pentests in a demo/lab environment
- Validating controls (protecting and detecting) has a lot of benefits for the end user
- Enhance this further with APT emulation



Source: MITRE ATT&CK® for Industrial Control Systems
https://collaborate.mitre.org/attackics/index.php/Impact

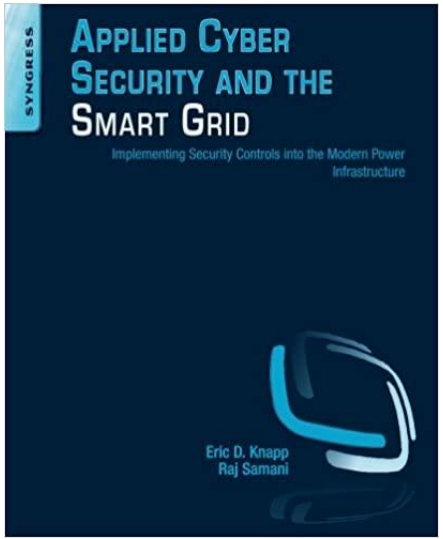
Additional Resources and Training

Book



Source: Industrial Network Security 2nd Edition
ISBN-13: 978-0124201149

Book



Source: Applied Cyber Security and the Smart Grid
ISBN-13: 978-1597499989

Course

A&ECS:
Assessing and Exploiting Control Systems & IIoT

Source: Assessing and Exploiting Control Systems and IIoT https://www.controlthings.io/training

NOZOMI NETWORKS

Thank You!

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

nozominetworks.com