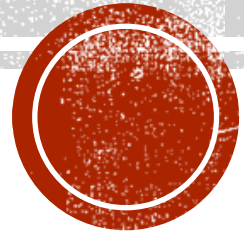
CYBERSECURITY AND MANUFACTURING: THE SCARY PRESENT AND POSSIBLE FUTURE

Suzanne Lightman

NIST



OVERVIEW

- Introduction to NIST
- Rising interest in industrial cybersecurity
- Recognized issues
- Government activities
- Resources available

SHORT INTRODUCTION TO NIST

- Working with industry and science to advance innovation and improve quality of life.
- A few of our topics:

Artificial Intelligence

Quantum Science

Manufacturing

Cybersecurity

RISING INTEREST IN INDUSTRIAL SYSTEMS

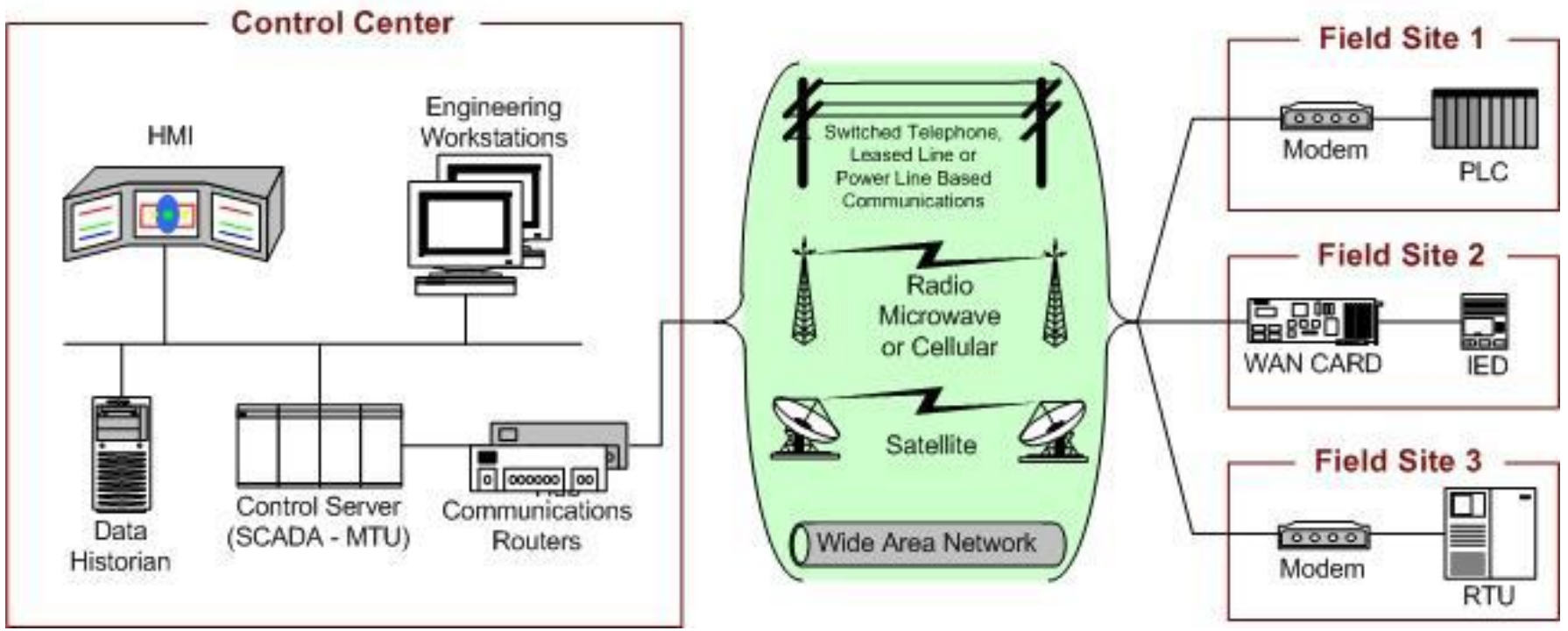
- High-profile incidents
  - July 2021
    - Transet Port Terminals (South Africa) – rail service disrupted
    - FBI and CISA expose spearfishing campaign targeted at gas and oil pipeline companies
  - June 2021
    - Chinese actors target organizations including water utilities
  - May 2021
    - LineStar Integrity Services and Colonial Pipeline hit with ransomware
    - JBS (Brazil), the world's largest meat processing plant, hit with ransomeware
    - FBI with the Australian Cyber Security Centre warn of wide-ranging ransomware attacks targeting multiple sectors
  - And that is only 3 months[1]

1. Center for Strategic and International Studies https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

RECOGNIZED ISSUES

- Complexity of systems

- Lack of resources



COMPLEXITY

- This is a simplified architecture of just a SCADA system from NIST SP 800-82 r2

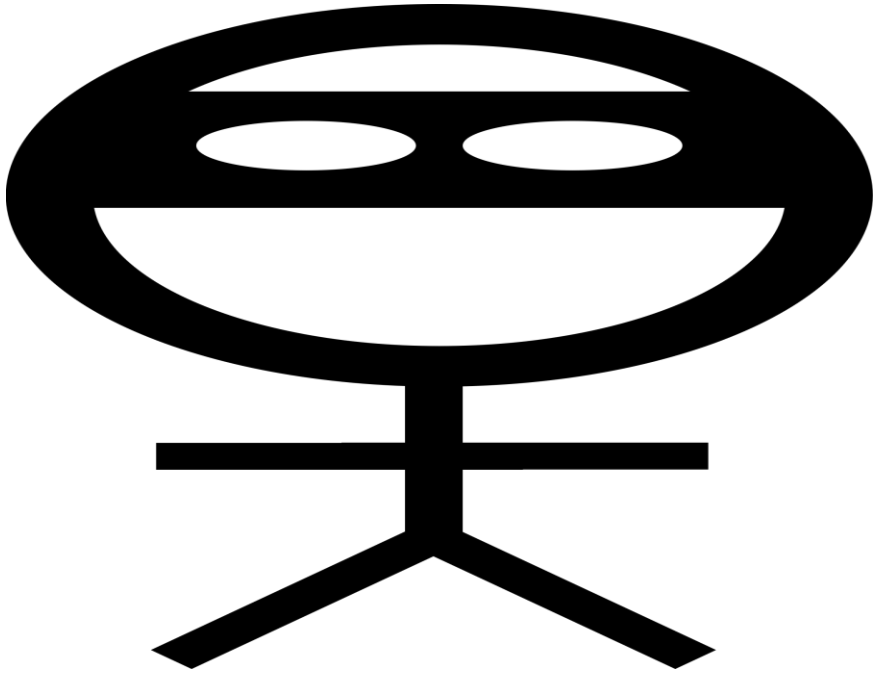
LACK OF RESOURCES

- Capital
  - Cybersecurity adds expenses
  - Can be difficult to build a business case

- People
  - Cybersecurity knowledge AND industrial control understanding
  - Not a lot of either and both are expensive

CYBERSECURITY APPROACH TO OT

- "I" in the metaphorical sense



WHERE DO I START LOOKING?

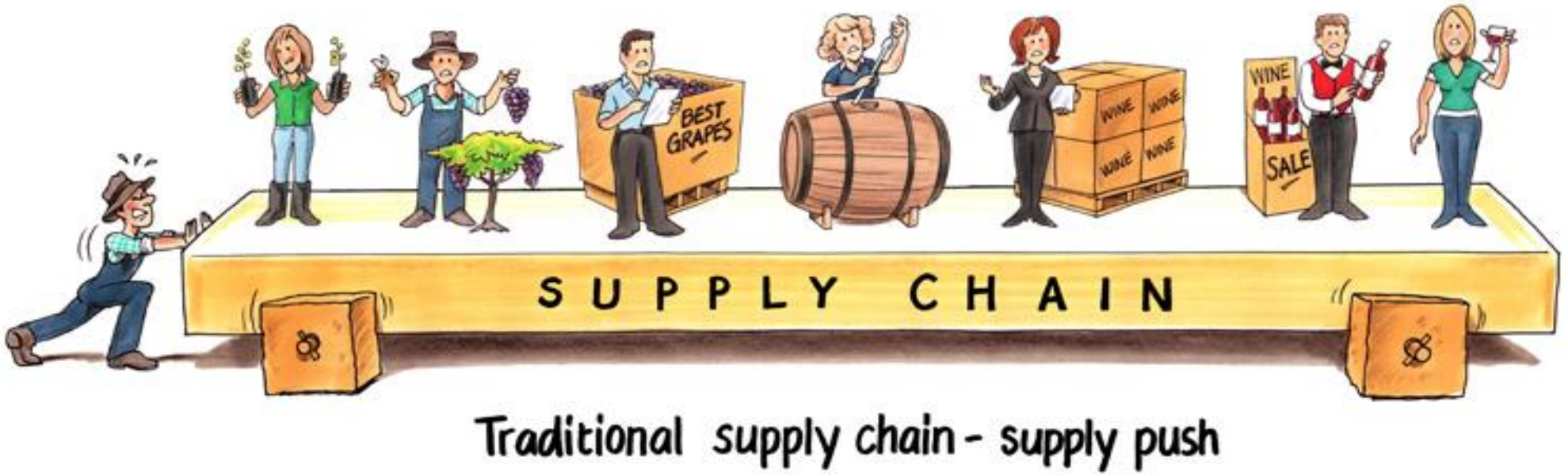
- Communication Channels
  - You have to start with a way in
  - Every channel is a way in and they all have to be considered
  - **It's not what *you* think the channel is for, it's what *I* can make it do**

WHERE DO I START LOOKING CONT.

- Places where people interact with the systems
  - People are easy to fool
  - The worst attacks often depend on people being the weak link
  - NEVER depend on people

WHERE DO I START LOOKING CONT.

- Where You Depend on Others



Traditional supply chain - supply push

GOVERNMENT ACTIVITIES

- Executive Order on Improving the Nation's Cybersecurity
  - Issued May 12, 2021
- Topics covered
  - Supply chain cybersecurity
  - Software labeling and assurance
- National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems
  - Issued July 28, 2021
- Topics covered
  - Critical infrastructure cybersecurity performance goals across all sectors
  - Preliminary goals out by September 22, 2021
  - Issued by DHS/CISA

NIST DEFINITION OF CRITICAL SOFTWARE

- https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf
  - White paper on critical software
- Software identified as critical software
  - Will be categorized by DHS
  - Will have established security baselines
  - For Federal agencies
- EO-critical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:
  - is designed to run with elevated privilege or manage privileges;
  - has direct or privileged access to networking or computing resources;
  - is designed to control access to data or operational technology;
  - performs a function critical to trust; or,
  - operates outside of normal trust boundaries with privileged access.

IS THERE ANY HELP? YES!

HERE IS HELP…

- NIST Manufacturing Profile
  - Created using the NIST Cybersecurity Framework
  - Designed to assist manufacturers translate business objectives and risk into cybersecurity action
  - https://www.nist.gov/cyberframework
    - All things CSF including the introduction to the Framework
  - https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile
    - The actual profile

MANUFACTURING PROFILE DETAILS

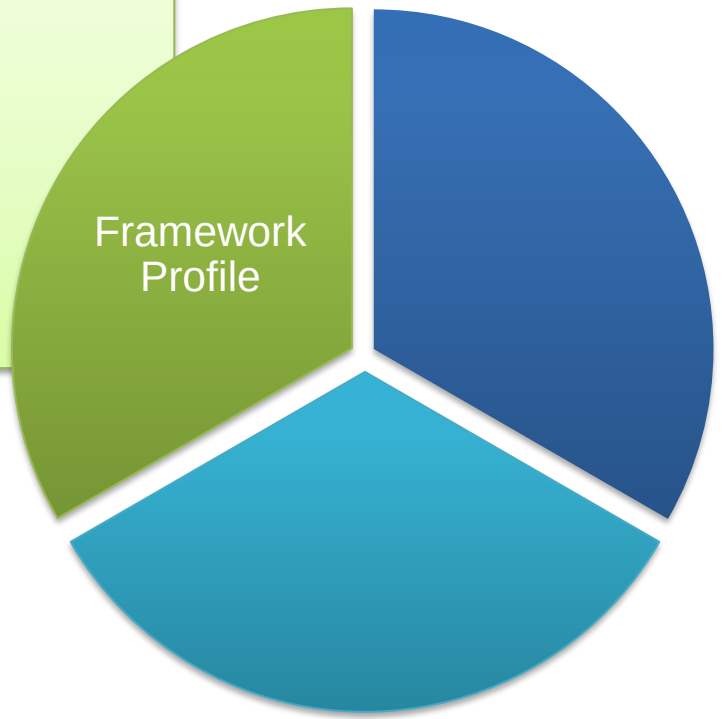
- Develop manufacturing implementation (Profile) of the CSF using NIST SP 800-82, NIST SP 800-53 and ISA/IEC 62443 as informative references
- Manufacturing Profile is a Target Profile of desired cybersecurity outcomes and can be used as a guideline to identify opportunities for improving the current cybersecurity posture of the manufacturing system
- Framework 7 Step Process
  - Step 1: Prioritize and Scope
  - Step 2: Orient
  - Step 3: Create a Current Profile
  - Step 4: Conduct a Risk Assessment
  - Step 5: Create a Target Profile
  - Step 6: Determine, Analyze, and Prioritize Gaps
  - Step 7: Implementation Action Plan

CYBERSECURITY FRAMEWORK PROFILE

- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state.
- A decision support tool for cybersecurity risk management

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs



Identify

Protect

Detect

Respond

Recover

THERE IS MORE HELP…

- NIST 1800 Series
  - These documents present practical, usable cybersecurity solutions. They demonstrate how to apply standards-based approaches and best practices. An 1800 document can map capabilities to the CSF and outline steps needed for an eneity of organization to recreate the example solution.
  - Developed at NIST NCCoE

- Relevant publications
  - 1800-32 (in preliminary draft) Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources
  - 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events
  - 1800-7 Situational Awareness for Electric Utilities
  - 1800-5 IT Asset Management
  - And there are more…

EVEN MORE HELP

- NIST Cyber Supply Chain Risk Management
  - https://csrc.nist.gov/projects/cyber-supply-chain-risk-management
  - Publications
  - News and updates
  - Events

- NICE
  - https://www.nist.gov/itl/applied-cybersecurity/nice
  - National Initiative for Cybersecurity Education
  - Working on curriculum for cybersecurity and OT workforce

NEED MORE HELP?

- Manufacturing Extension Partnership
  - Public/private partnership with centers in all 50 states (and Puerto Rico) dedicated to serving small and medium-sized manufacturers
  - https://www.nist.gov/mep
  - Whole section on cybersecurity including
    - Where to start
    - Resources and guidance organized by topic

- Stop Ransomware
  - https://www.cisa.gov/stopransomware
  - Run by DHS CISA
  - One-stop shop for prevention and assistance

STILL MORE HELP?

- DHS CERT
  - https://us-cert.cisa.gov/ics
  - Formerly known as DHS ICS CERT
  - Alerts
  - Advisories
  - Connection to the ICSJWG

MORE HELP COMING

- NIST SP 800-82 *Guide to Industrial Control Systems*
  - Undergoing revision
  - First public draft due the beginning of next year
  - Keep track of what is happening