Safety System Cyber Security – A Practical Approach

Kelly Mahoney

Protection Systems Team Leader

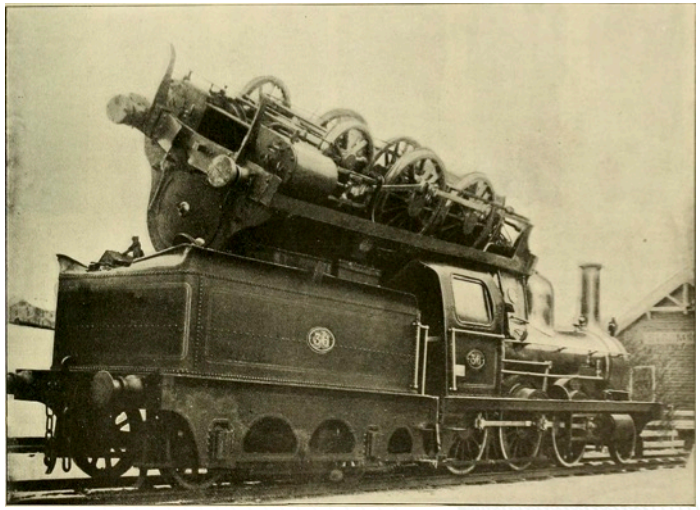
ORNL/SNS

Acronyms I would rather not know…

- Cyber-physical System (CPS)
- Operational Technology (OT)
- Industrial Internet of Things (IIOT)
- Loss of Control (LoC)

And my favorite…

- Unexpected Physics (UP)



Wikimedia. Originally printed in John Hill, *"Locomotive Engineering – a practical journal of motive power and rolling stock."* 1897.

Recent Cyber Threats

"The bottom line is the means exist for hacking control systems and causing damage. The question is the motive to do so."

Joe Weiss on the Wolf Creek [Nuclear Power Plant] hack

WHITE PAPER

Go Nuclear: Breaking Radiation Monitoring Devices

Briefing at the July 2017 Black Hat USA Conference

…the adversary showed knowledge in ICS and was able to cause multiple components of the system to fail…which resulted in massive physical damage.

Robert Lee, et. al. SANS Institute Report on German Steel Mill Cyber attack.

Hackers will pick apart the hardware and software, identify weaknesses, and launch an attack at will.

Advanced and Really Persistent…

<u>Once in, attackers…</u>

Perform reconnaissance

- Preferred vendor lists
- Technical Documentation
- Asset locations
- Personnel profiles – social media sites

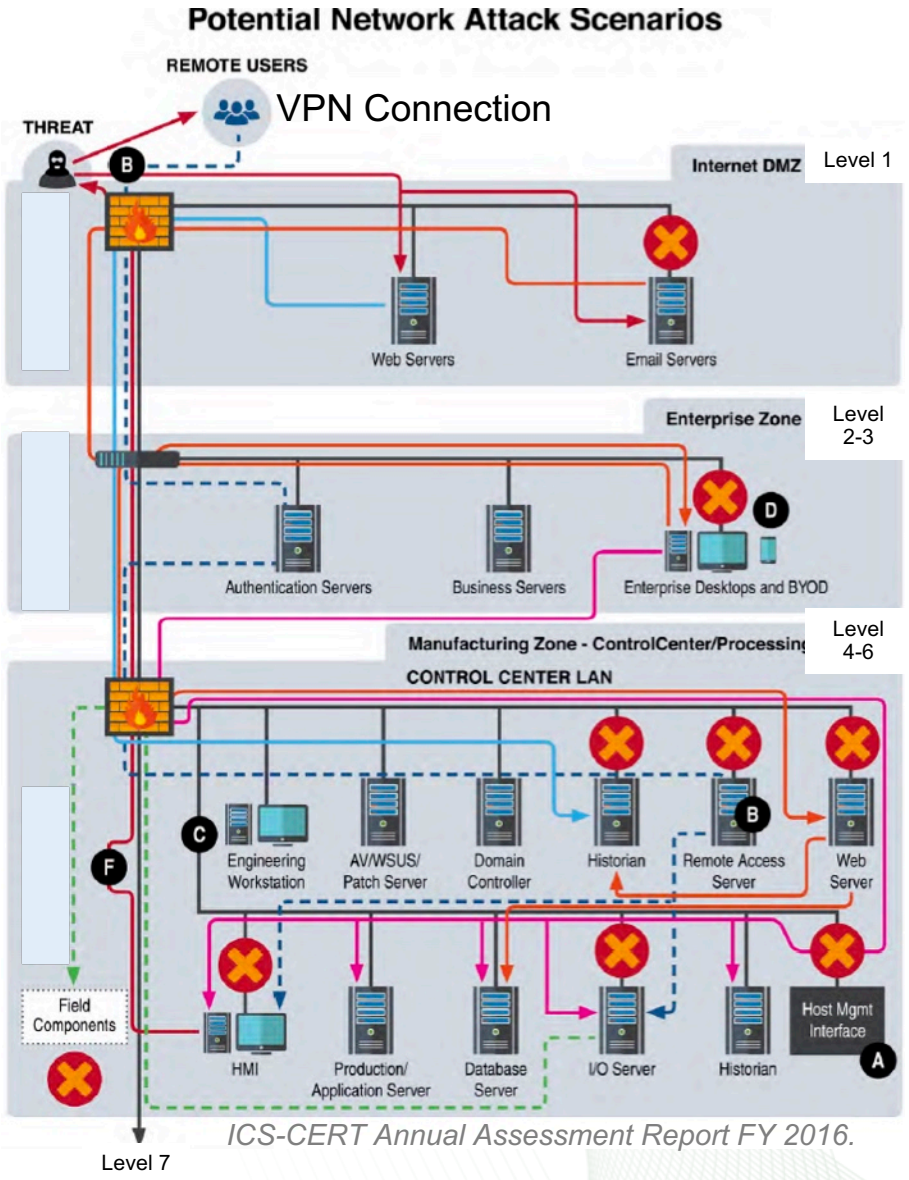
Send targeted e-mails

Establish a command and control connection

- Upload discovery and infiltration tools
- Elevate privileges
- Exfiltrate more targeted information
- Add permissions to compromised accounts on “Read Only” systems; e.g. data historian server with trusted connection
- Tunnel through firewalls
- Now on control network

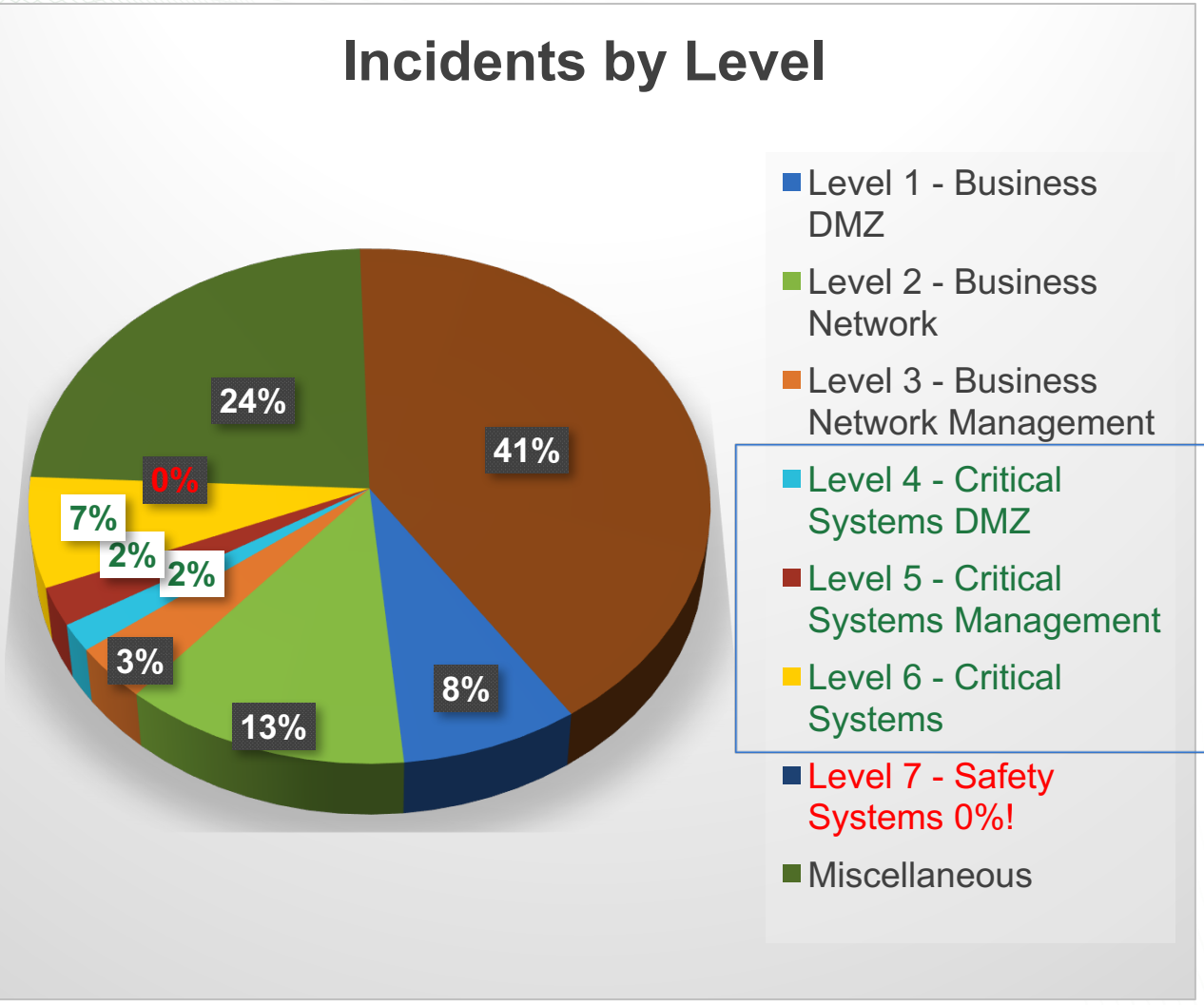
Execute attack

SANS Institute
https://securingthehuman.sans.org/cyberattackdemo



ICS-CERT Annual Assessment Report FY 2016.

Incursions are knocking on the Safety Systems' door!



Of the 16 incidents involving critical services:

- *10 Had minimal impact*
- *3 Had significant impact*
- *3 Had Denial/Loss of Control*

Data adopted from: ICS-CERT 2016. Fact Sheet_IR Pie Charts for 2016. Based on 290 Incidents

Spot the Trend: 2014-2016 Top Weakness

ICS-CERT Annual Assessment Report FY 2016.

2014-2016 Top Weakness in order of Prevalence		
2014	2015	2016
1. Boundary Protection	1. Boundary Protection	1. Boundary Protection
	2. Least Functionality	2. Least Functionality
	3. Authentication Management	3. Identification and Authentication

Boundary Protection	• *Undetected unauthorized activity in critical systems* • *Weaker boundaries between ICS and enterprise networks*
Least Functionality	• *Increased vectors for malicious party access to critical systems • Rogue internal access established*
Authenticator Management	• *Compromised unsecured password communications.* • *Password compromise could allow trusted unauthorized access to systems*
Identification and Authentication	• *Lack of accountability and traceability for user actions if an account is compromised* • *Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access*

Assume the likelihood a control system will be compromised over the life of a facility is 100%

- Have the following processes in place:
  - Boundary Protection
  - On-Line
    - Access Control
    - Logging
    - Network Management
    - Installed Equipment Configuration Management
    - Anomaly Detection and Recovery
    - Intrusion Detection
  - Off-Line
    - Information for a quick recovery to a known good configuration
    - Development Equipment Management

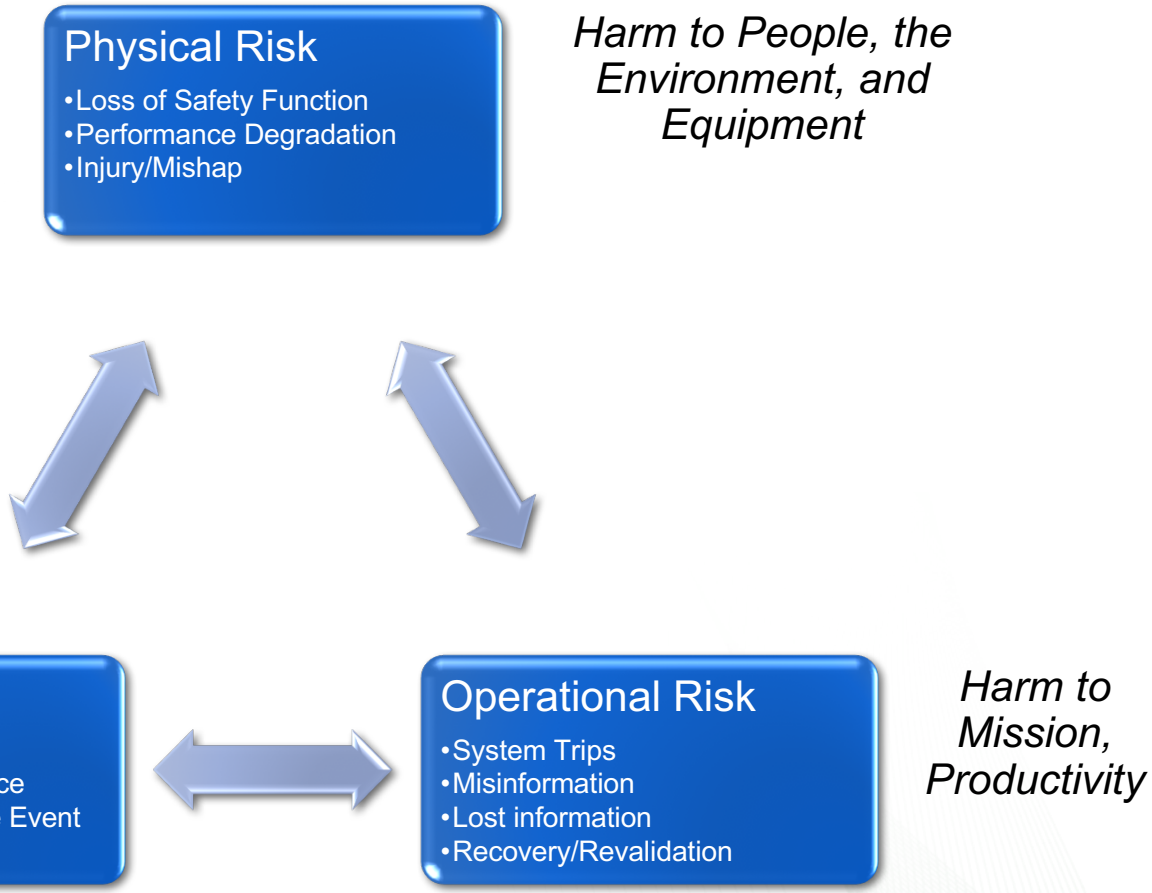
The most technologically advanced system in the galaxy - Death Star – was hacked in a few seconds by a 20 year old obsolete droid – R2D2.

Duh Practices – Standard Stuff

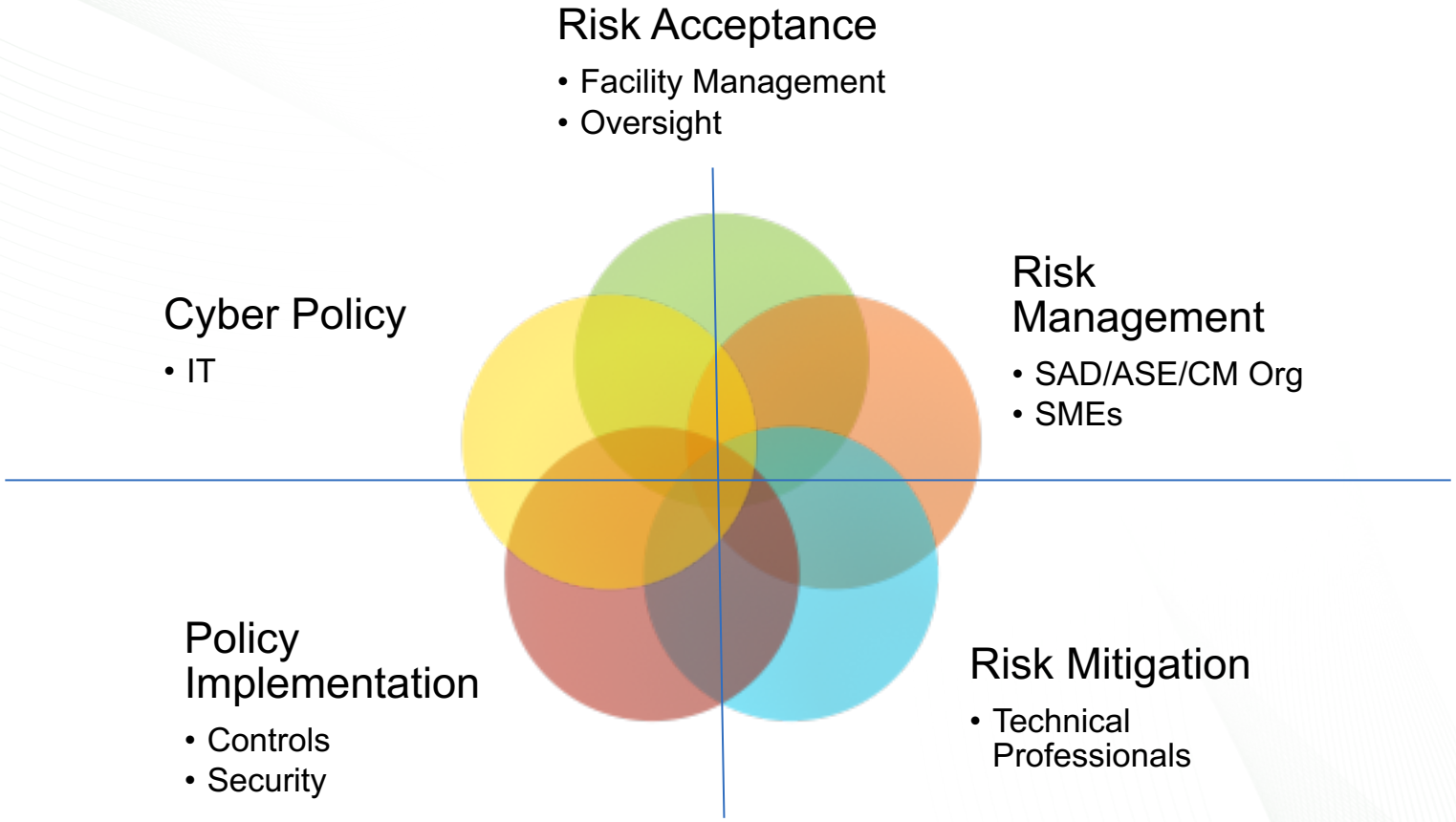
- Restrict physical access to safety equipment
- **TURN OFF BUILT-IN WEB SERVERS!**
  - Industrial Equipment
  - Networking Equipment
  - Cameras, Printers, PA systems, …
- Segment networked safety systems
- Apply rule-based network management
- Do not allow remote access to critical systems
- Get rid of default user names and passwords on all equipment
- Change passwords after employee turn-over
- …

Key Practices – Safety System Cyber is a Risk

Cyber Threats should be considered in a risk assessment.



Key Practices – Safety System cyber security requires collaboration across an organization



Key Practices – Keep up to date

- **KNOW YOUR EQUIPMENT/FW VERSIONS, and CONFIGURATIONS**
- Threats:
  - Alerts from Cyber Emergency Response Team (CERT)
  - Vendor alerts
- Hardware:
  - Computers/OS
  - Peripherals
  - Networking/Communication
- Software:
  - Only software necessary to manage the safety systems should be installed.
    - Should include Office software, screen grab, picture viewer, … things that are needed in the course of managing a system.
- Network Configuration:
  - Ports …

Key Practices – Know thy neighbor

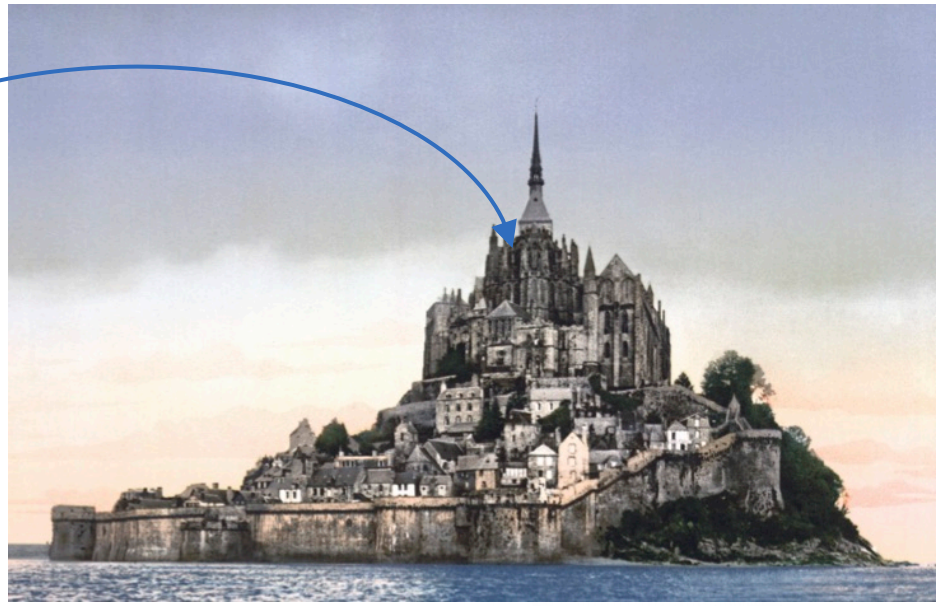
- Compromise of some systems may increase the “challenge rate” to a safety system.
  - This has already happened in theory and practice in industry.
  - Pre-determine the impact of a high challenge rate
- Apply a graded approach to high consequence systems – safety or not
  - (Verbal Examples)

Key Practices - Offline Development Environment should be as secure as the online (but separate)

OFFLINE
Development Environment

Khayelitsha Site C - Cast Store by FreddieA. Wikimedia Commons, CC BY-SA 3.0.

ONLINE
Runtime Environment



Mont St. Michel. Public Domain Photo from Wikimedia/US Library of Congress.

An easy place to perform reconnaissance, exfiltration, and compromise is with the off-line information; PLC programs, HMI files, Firmware backups,...

Key Practices – Maintain Hierarchy

- Do not pass information from a less secure to a more secure network
- Use a DMZ between major security levels
- Use choke points to monitor traffic for anomalies
- Consider white-listing between devices and between a DMZ and outside the network.

Key Practices - Resiliency and Recovery

Resiliency

- Use multiple functional paths when possible
  - Example: Multiple segments propagate shutdown to front end
- Use defense-in-depth layers built into safety functions
- Incorporate integrity checks in software and communications
- Use defensive programming practices

Recovery

- Have a plan to re-establish a trusted configuration
- Be prepared to wipe everything
- Have known good copies of software and configuration files ready to install

Myths and Unicorns

Air gaps have long been discussed in the ICS community but are largely not feasible and are unreliable (at a minimum files often move across these gaps)...

> *…However, connections that must exist between networks should be heavily regulated through the use of a demilitarized zone (DMZ) with specially tuned firewalls, focused monitoring, and defense systems.*

Robert Lee, et. al. SANS Institute Report on German Steel Mill Cyber attack.

The process for passing safety information to the main control system should be well thought out, robust, reviewed, monitored, maintained, and tested.

Key Practices - Updates and patching

- Computers and OS
  - Have an approved process for updating safety system computers
    - Include a process for emergency updates
  - Update/patch OS when approved by IT and the engineering software vendor
  - Update anti-malware definition files on a regular schedule

- Engineering Software
  - Evaluate SW/FW revision notices for applicability
  - Have a secure connection to the vendor
  - Updates should have a signature and/or key
  - Test updates and patches before deployment

- Hardware
  - Have an approved graded approach process for updating firmware on lab and field equipment.

Things for This Community to Think About…

- Place/Scope of cyber risk in a SAD?
- Does a Cyber compromise have a place in an ASE?
- Who decides when to pull the plug on a compromised system? How do they find out?
- Level of Testing and Certification Required after Updating[1]:
  - Safety Network Configuration
  - Safety Network (Communication) Modules
  - Safety Network Switches and Firewalls
  - DMZ HW/FW/SW
  - ICS Interface HW/FW/SW
- Is there a utility curve to be optimized?
- Operator training to recognize incongruent feedback

1: Ethernet should not be assumed here. This applies to all communication protocols and devices.

Crystal Ball

Plus'	Minus'
Model-Based Engineering Information	Model-Based Engineering Information
AI based oversight	AI based incursion AI based 'designer' attacks
Controls Security Awareness and Practices	Collaborative Actors
System of Systems Security	Industrial Internet of Things (IIOT)
Defensive Programming (Software) Practices	Controls 'spoofing'
Better Risk Models	
Better Network Management Tools	

Thank You!

Some Resources

US ICS-CERT	https://ics-cert.us-cert.gov/
NIST SP800-82	http://csrc.nist.gov/publications/PubsSPs.html
ISA 99	https://www.isa.org/isa99/
IEC 62443	
ISO 27000	

written by Robert M. Lee and illustrated by Jeff Haas
http://www.littlebobbycomic.com/projects/week-48/
December 27, 2015