

Industrial Control System (ICS) Cybersecurity 101

Emma M Stewart, LLNL

Contributions developed by Jovana Helms, LLNL

Distribution Systems and Planning Training (March 11, 2020)

The problem is harder when adversaries try to disrupt systems....



Explosion of Siberian natural gas pipeline (Targeted Attack)

Maroochy shire wastewater plant compromised (Targeted Attack)

Aurora Generator Test (Research)

Houston water distribution system hack (Targeted Attack)

SF Muni rail ransomware (Targeted Attack)

Ransom attacks on hospitals (Targeted Attack)



Worm cripples industrial plants (Collateral damage)

Texas power company hack (Targeted Attack)

German steel mill (Targeted Attack)

Los Angeles traffic system attack (Targeted Attack)

Lodz, Poland tram hack (Targeted Attack)

Unidentified nuclear power plant (Targeted Attack)

Alpine ski resort ransomware (Targeted Attack)

Browns Ferry nuclear plant (Malfunction)

San Bernardino pipeline rupture (Malfunction)

Ukrainian power grid attacks (Targeted Attack)

Dallas emergency sirens hack (Targeted Attack)

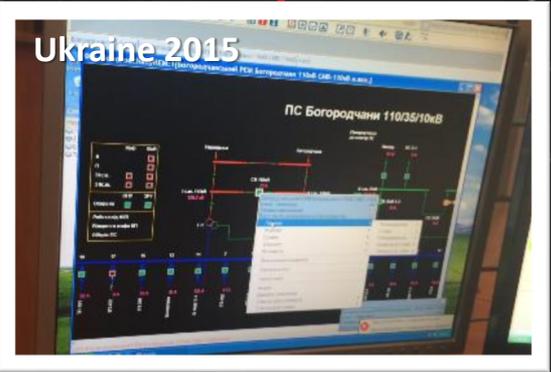
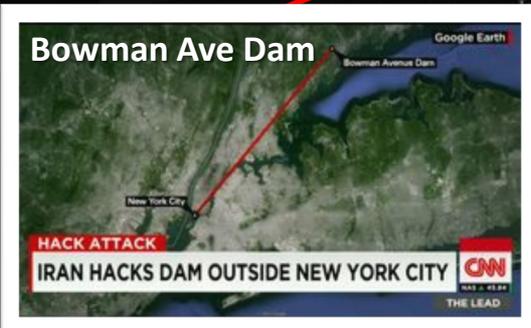
Pacific Energy Resources hack (Targeted Attack)

Researchers remotely take control of cars (Malfunction)

worm cripples CSX transport system (Collateral damage)

Marshall, Michigan crude oil spill (Malfunction)

"WannaCry" Ransomware Campaign (Targeted Attack)



“Our adversaries and strategic competitors will increasingly use cyber capabilities to seek political, economic, and military advantage over the United States and its allies and partners.”

“China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure in the United States.”

“Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure.... Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.”



Daniel R. Coats, Director of National Intelligence
Testimony to Senate Select Committee on Intelligence, January 29, 2019

IT vs OT Networks

Information Technology (IT) Networks

- Manage data
- Non real-time, high throughput needed, high delays tolerable
- Availability of the system not critical, rebooting ok
- Data confidentiality and integrity paramount
- Systems use common operating systems, updates and patching straightforward
- Lifetime on the order of 3-5 years
- Systems typically local and accessible

Operational Technology (OT) Networks

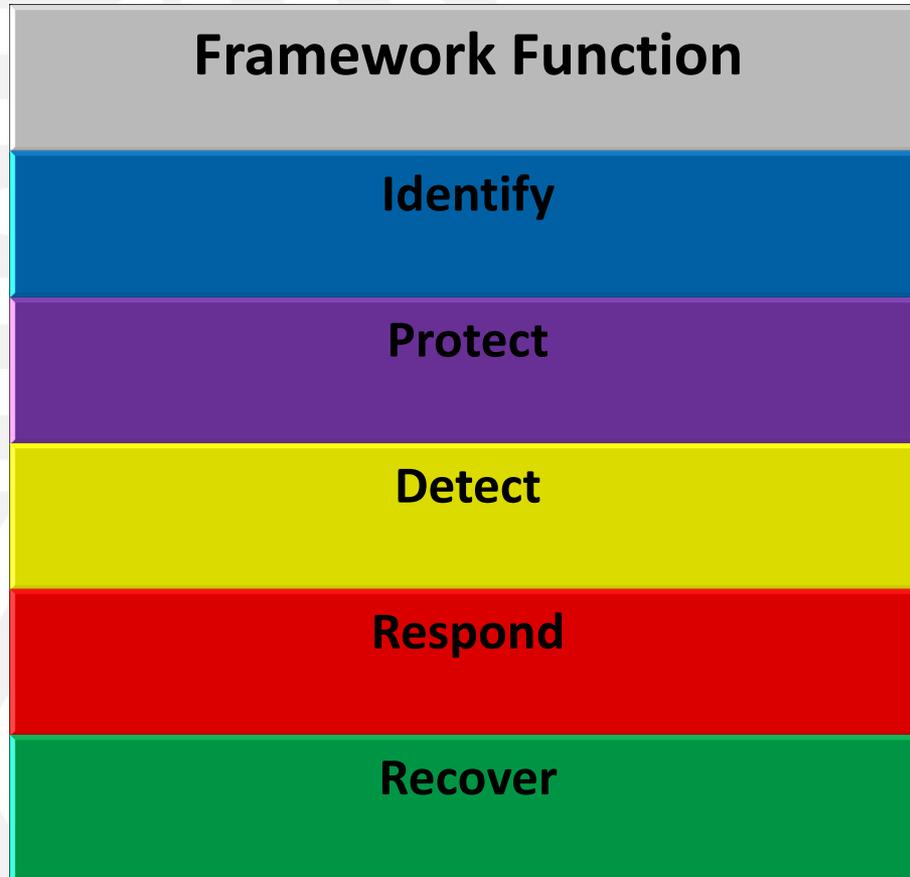
- Manage physical processes
- Real time, modest throughput ok, high delays prohibitive
- Availability of systems may be critical enough to require redundant system
- Human safety paramount, followed by uninterrupted processes, fault tolerance essential
- Diverse and often proprietary operating systems, software updates typically must be done through the vendor
- Lifetime on the order of 10-15 years
- Systems can be isolated and remote

IT and OT networks differ significantly in terms of requirements, priorities and risks. As a result IT cybersecurity does not directly map into OT cybersecurity, and some practices that are essential in IT cybersecurity can disrupt the physical processes controlled by OT networks if they are not adapted to the requirements of the system.

ICS Cybersecurity - Resources

- ▶ Numerous guidelines, best practices exist (DHS/ICS-CERT, NIST, SANS, NSA, DoD, DOE...)
- ▶ NIST Cybersecurity Framework provides comprehensive approach to cybersecurity for ICS
- ▶ Framework provides a set of cybersecurity activities, outcomes and informative references that are common across critical infrastructure sectors
- ▶ Meant for asset owners to use as part of their risk management process
- ▶ <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

NIST Cybersecurity Framework



Identify

- ❑ Know thyself...
- ❑ Have an accurate inventory of assets, data, people
- ❑ Understand how the network works and behaves
- ❑ Understand risks, identify vulnerabilities and potential impacts
- ❑ Understand criticality of assets to the mission

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management

Understanding your own system, how it works and what's on it is essential for cybersecurity – we can't defend what we don't know is there.

Protect

- ▶ Manage identities and control access
- ▶ Authenticate users, devices and other assets
- ▶ Network segregation and segmentation
- ▶ Use encryption to protect data when available
- ▶ Integration checks for verifying software, firmware and data
- ▶ Develop, maintain and test incident response and recovery plans
- ▶ Reduce the attack surface
- ▶ Patching, vulnerability scanning, properly configured firewalls

Function	Category
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology

There is no perfect security, but the objective is to make it increasingly hard for the adversary to gain access to the OT network.

Detect

- ❑ Establish baseline network and user behavior to enable anomaly detection
- ❑ Monitor for unusual activity both from devices and users
- ❑ Keep libraries of known malicious signatures and TTPs (Tactics, Techniques and Procedures) up-to-date
- ❑ Monitor for unauthorized connections and users
- ❑ Perform regular vulnerability scans
- ❑ Report and investigate incidents

Function	Category
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes

The adversaries will always find a way to get in, but timely detection can minimize the effectiveness of the attack and prevent it from spreading.

Respond

- ▶ Establish an incident response plan and execute it accordingly
- ▶ Share information among stakeholders and coordinate
- ▶ Investigate detection alerts and determine root cause
- ▶ Contain and mitigate discovered incidents and understand the impacts of the mitigations
- ▶ Perform forensic analysis to understand the scope of compromise
- ▶ Mitigate newly identified vulnerabilities

Function	Category
Protect	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements

Adequate response to an incident will ensure that its impacts are minimized, making it increasingly difficult for an adversary to achieve their objectives.

Recover

- ▶ Establish a recovery plan and execute it accordingly
- ▶ Update plans with lessons learned
- ▶ Ensure all systems are “clean” before bringing them online
- ▶ Perform activities in “identify” and “protect” steps to establish new baselines
- ▶ Recovery activities are coordinated and include internal and external stakeholders (vendors, customers, etc.)

Function	Category
Recover	Recovery Planning
	Improvements
	Communications

Recovery can be time consuming, but it's essential in ensuring the adversary cannot re-use the same attack in the future.

Common Intrusion Paths

- ▶ Attack directly from Internet to Internet connected ICS device
- ▶ Attacks initiated using remote access credentials stolen from authorized ICS organization users
- ▶ Attacks on external business web interface
 - Leverage exploits and vulnerabilities existing in web server applications
 - Pivot into the ICS historian that provides ICS data to the web server applications
- ▶ Attacks initiated by insertion of infected mobile media into a system component
 - Pivot deeper into the ICS network as attacker finds opportunities
- ▶ Attacks through phishing emails to establish presence on enterprise network
 - Pivot deeper into the ICS network as attacker finds opportunities

*From "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies", US-CERT

Defense-in-depth

- ❑ Multi-layered approach designed to impede the progress of a cyber intruder while enabling the organization to respond with the goal of minimizing the impacts of the attack



*From “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies”, US-CERT

Layered defense strategy for the electric grid – mapping strategy to attack type

 	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify			
Protect			
Detect			
Respond	<p>USE vulnerabilities</p>	<p>DISCOVER vulnerabilities</p>	<p>CREATE vulnerabilities</p>
Recover			
Endure			

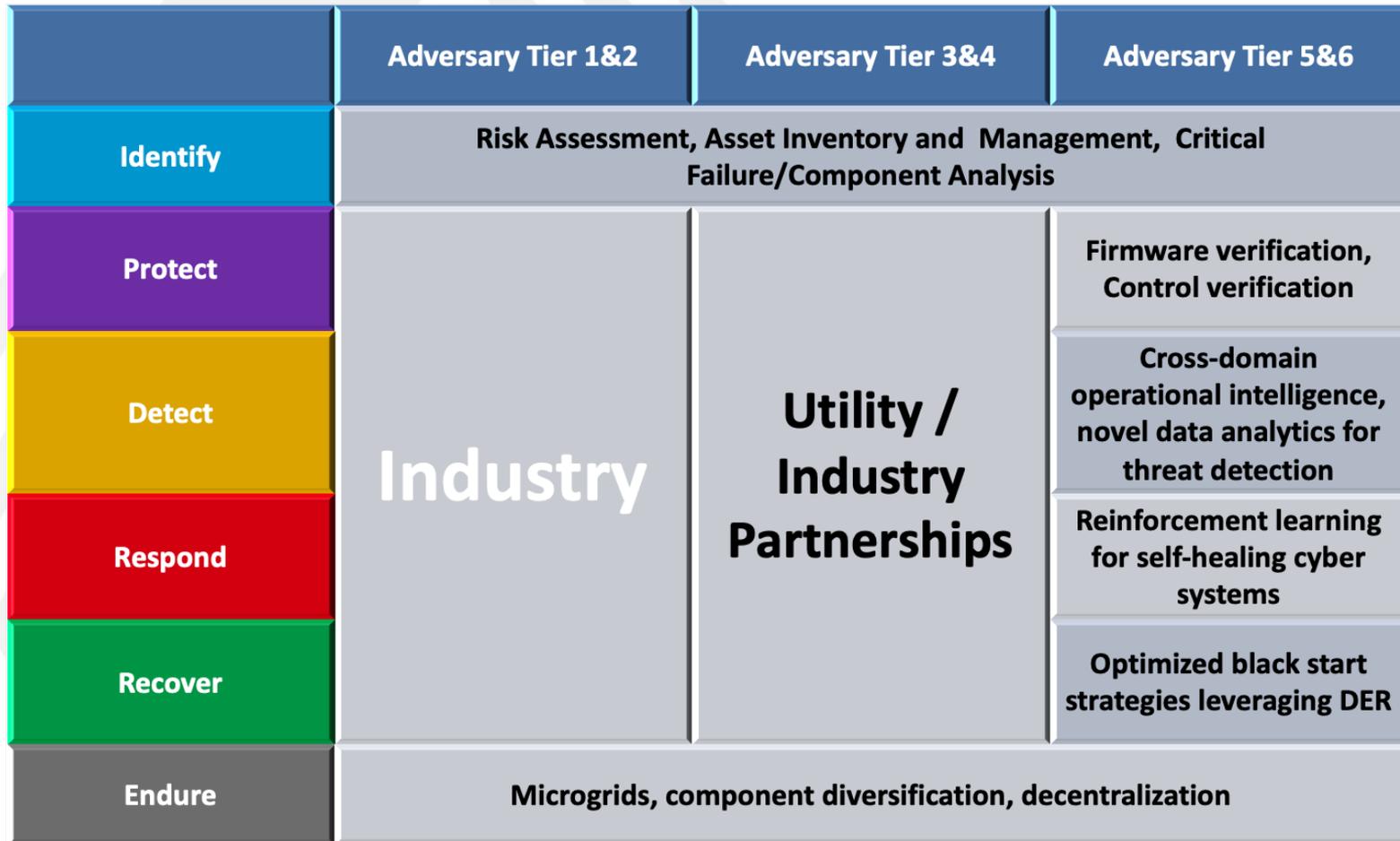
Layered defense strategy for the electric grid

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Basic cyber hygiene	Encryption, Network Segmentation, Cyber grid planning tools	Firmware verification, Control verification
Detect	Anti virus	Data aggregation, threat detection	Cross-domain operational intelligence, novel data analytics for threat detection
Respond	Manual mitigation of known threats	Orchestration and remediation	Cyber-physical fault isolation, dynamic network segmentation
Recover	Pre-planning	OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure	Microgrids, component diversification, decentralization		

Layered defense strategy for the electric grid

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Industry	Encryption, Network Segmentation, Cyber grid planning tools	Firmware verification, Control verification
Detect		Data aggregation, threat detection	Cross-domain operational intelligence, novel data analytics for threat detection
Respond		Orchestration and remediation	Reinforcement learning for self-healing cyber systems
Recover		OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure		Microgrids, component diversification, decentralization	

Layered defense strategy for the electric grid



DHS NCCIC Recommends 7 Key Strategies



1. Application Whitelisting
2. Proper Configuration/Patch Management
 - Avoid watering hole attacks
 - Use DNS reputation system
 - Validate the authenticity of downloads
3. Reduce Attack Surface Area
 - Isolate ICS networks
 - Close unused ports and services
 - Identify all IT/OT connections and monitor them
4. Build a Defendable Environment
 - Segment network into local enclaves
 - Restrict host-to-host communication paths
5. Manage Authentication
 - Multifactor authentication
 - Enable only necessary privileges for each user
 - Lengthy passwords, change every 90 days
 - Separate credentials for business and ICS networks
5. Implement Secure Remote Access
 - Do not allow persistent vendor connections
 - Remote access should be operator controlled and time limited
 - Use 2-factor authentication
6. Monitor and Respond
 - Watch IP traffic on ICS boundaries for abnormal comms
 - Monitor IP traffic within control network
 - Use host based monitoring and detection
 - Use login analysis to detect stolen credentials or improper access
 - Watch user and administrator actions to detect access control manipulation