U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

SEI ETF Securing Energy Infrastructure Executive Task Force

Categories of Security Vulnerabilities in ICS

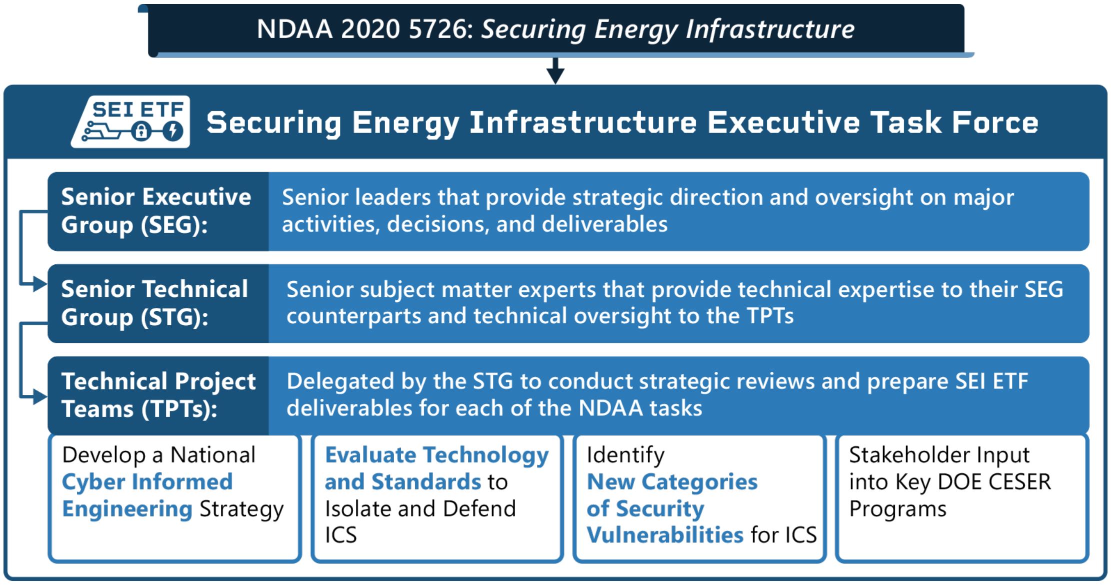
March 9, 2022

Background

Securing Energy Infrastructure Executive Task Force

The Securing Energy Infrastructure Executive Task Force (SEI ETF) is a voluntary group of senior leaders representing energy sector asset owners and operators, vendors/manufacturers, standards organizations, research and academic institutions, National Laboratories, and government agencies. The U.S. Department of Energy (DOE) formed the SEI ETF as directed by Section 5726 of the National Defense Authorization Act for Fiscal Year 2020[1] (NDAA 2020).

The SEI ETF is structured in three tiers, with the third tier being technical project teams that were formed to pursue several taskings mandated by the statute, including evaluating technology and standards for industrial control systems (ICS), identifying categories of ICS vulnerabilities, and developing a National Cyber-Informed Engineering Strategy.



NDAA 2020 5726: *Securing Energy Infrastructure*

SEI ETF Securing Energy Infrastructure Executive Task Force

Senior Executive Group (SEG): Senior leaders that provide strategic direction and oversight on major activities, decisions, and deliverables

Senior Technical Group (STG): Senior subject matter experts that provide technical expertise to their SEG counterparts and technical oversight to the TPTs

Technical Project Teams (TPTs): Delegated by the STG to conduct strategic reviews and prepare SEI ETF deliverables for each of the NDAA tasks

Develop a National **Cyber Informed Engineering** Strategy

Evaluate Technology and Standards to Isolate and Defend ICS

Identify **New Categories of Security Vulnerabilities** for ICS

Stakeholder Input into Key DOE CESER Programs

See https://inl.gov/secureENERGY/ for more information on the SEI ETF and key deliverables.

New Categories of Security Vulnerabilities Technical Project Team

The New Categories of Security Vulnerabilities (NCSV) Technical Project Team (TPT) was tasked to identify new classes of security vulnerabilities in ICS. The TPT began by analyzing baseline assumptions and capabilities in identifying, classifying, and prioritizing security vulnerabilities in ICS.

One of the first findings that NCSV TPT produced was that no classification system for security vulnerabilities exists for either IT or OT. Per the team's literature review, "Classification as a process involves the orderly and systematic assignment of each entity to one and only one class within a system

[1] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, https://www.congress.gov/bill/116th-congress/senate-bill/1790.

of mutually exclusive and nonoverlapping classes."[2] Upon surveying the landscape of potential classifications systems for security vulnerabilities, the TPT concluded that no well-founded classification system exists that meets this standard, such as those used to classify stars or living organisms.

As result, the TPT determined the best course of action was to identify categories of security vulnerabilities in ICS. Over the course of a year, stakeholders reached consensus on 20 categories of security vulnerabilities in ICS that are distinct from any existing categories identified in IT.

Strong writeups for these 20 categories are provided below, representing the key deliverable from the TPT. The TPT proposes these as drafts that can be further reviewed, refined, and institutionalized.

Next Steps Beyond the TPT

The TPT identified MITRE's Common Weakness Enumeration (CWE) database as the best platform to integrate and expand the TPT's work. CWE is a widely recognized source of software and hardware weakness types that serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.[3]

The TPT engaged MITRE, briefed its work, and gained agreement from MITRE to stand up a Special Interest Group, launching May 2022, that will examine how to best include the categories in the CWE framework.

Categories of Security Vulnerabilities in ICS

The NCSV TPT has identified 20 categories of security vulnerabilities in ICS. These 20 categories are group intro 5 super categories:

1. ICS Communications
2. ICS Dependencies (& Architecture)
3. ICS Supply Chain
4. ICS Engineering (Constructions/Deployment)
5. ICS Operations (& Maintenance)

Instead of identifying specific mitigations for each of the 20 categories, the NCSV TPT has identified this general group of mitigations that apply to security vulnerabilities in ICS broadly:

- Cyber-Informed Engineering
- Reference Architectures, including the Reference Architecture for Electric Energy OT developed by another SET ETF Technical Project Team
- DOE's Cyber Testing for Resilient Industrial Control Systems (CyTRICS) Program
- IT mitigations (e.g. supply chain management, generating patches, ransomware prevention, etc.)

[2] Elin K. Jacob, "Classification and Categorization: A Difference that Makes a Difference," Library Trends, Vol. 52, No. 3, Winter 2004, pp. 515-540.
[3] MITRE, "Common Weakness Enumeration," https://cwe.mitre.org/.

ICS Communications

1. Zone Boundary Failures

Summary: Within an ICS system, for traffic that crosses through network zone boundaries, vulnerabilities arise when those boundaries were designed for safety or other purposes but are being repurposed for security.

Justification as an ICS category: Vulnerabilities arising from interfaces between systems with different safety significance (high vs low significance). One directional comms: interfaces go from high to low.

Most significant or relevant properties of vulnerabilities in this ICS category:

- This type of vulnerability may involve multi-level safety systems.
- For the safety example, requirement that low-safety systems not send signals to high-safety systems.
- Systems may have multiple zones for safety, financial, reporting, or monitoring reasons but those divisions don’t make for secure zones.
- Current controlling protocols or policies may encourage compliance more than security.

Nearest IT Neighbor:

- 669 “Incorrect resource transfer between spheres”
- 754 “Improper check for unusual or exceptional conditions”

2. Unreliability

Summary: Vulnerabilities arise in reaction to disruptions in the physical layer (e.g. creating electrical noise) used to carry the traffic.

Justification as an ICS category:

- Communications are less resilient in high-energy ICS environments (which can include high-RF, high-EM conditions)
- A critical communications problem within an ICS environment could cause physical damage to the process under control and/or physical risk to operators

Most significant or relevant properties of vulnerabilities in this ICS category:

- Operating environment can affect communications reliability
- Systems are designed assuming stable communications with limited/no understanding of the impact of unstable communications

Nearest IT Neighbor:

- Random early detection

3. Frail Security in Protocols

Summary: Vulnerabilities arise as a result of mis-implementation or incomplete implementation of security in ICS implementations of communication protocols.

Justification as an ICS category:

- Even when security exists, there is still a dependence—non-existent or frail security (e.g., key management).
- ICS-specific protocol and not used in general IT systems.
- Original ICS protocols were not designed for security given assumption of closed network.

Most significant or relevant properties of vulnerabilities in this ICS category:

- Nonexistent or weak security
- Enterprise software may introduce vulnerabilities into the system (e.g., router device with a vulnerability used in ICS). Components using ICS-specific protocols have accessible comms due to the enterprise IT infrastructure.

Nearest IT Neighbor:

- HTTPS where TLS has major flaws

ICS Dependencies (& Architecture)

4. External Physical Systems

Summary: Due to the highly interconnected technologies in use, an external dependency on another physical system could cause an availability interruption for the protected system.

Justification as an ICS category:

- Traditional IT depends on power (only physical element). Vulnerabilities come about due to dependencies on physical systems. Whereas the connection to the physical world brings about another dimension.
- Some energy control systems also depend on external water supplies for cooling.

Most significant relevant properties of vulnerabilities in this ICS category:

- There is a physical system outside the one ICS was designed to control.
- That physical system could, in certain conditions, impose adverse second-order physical effects on the ICS.
- The physical system can be manipulated to produce conditions other than designed.

Nearest IT Neighbor:

- 1338 "Improper Protections against hardware overheating"
- "Domain Energy"

5. External Digital Systems

Summary: Due to the highly interconnected technologies in use, an external dependency on another digital system could cause a confidentiality, integrity, or availability incident for the protected system.

Justification as an ICS category:

- Part of broader decision-ecosystem in an organization or sector.

- Because the modalities of digital information—how though about and managed—presumed separation in influencing and control—external digital system to a physical system.
- True for direct technical connections but also those without a technical connection

Most significant or relevant properties of vulnerabilities in this ICS category:

- Looking for digital dependencies that affect the physical system. Inbound dependencies. Must be outside the OT environment. When not technically connected, can lead to human decisions that disrupt energy flow.
- Vulnerability is in the failure mode of the external digital system. This may not have been well-understood so no anticipation of the impact on the physical system.

Context/History:

- E.g., Colonial Pipeline, where even the attacker did not foresee the result.

Nearest IT Neighbor:

- 610: "Externally controlled reference to a resource in another sphere"

ICS Supply Chain

6. IT/OT Convergence/Expansion

Summary: The increased penetration of DER devices and smart loads make emerging ICS networks more like IT networks and thus susceptible to vulnerabilities similar to those of IT networks.

Justification as an ICS category: ICS networks and protocols were largely designed to be closed, trusted networks; incorporating more connection types, points of access, controlling entities, and having to incorporate devices and protocols designed for a different trust model results in vulnerabilities for existing ICS networks/controls.

Most significant or relevant properties of vulnerabilities in this ICS category:

- Commodity IT elements are used in ICS, replacing purpose-built components.
- Due to the IT/OT convergence trend that ICS systems look more like IT systems used for industrial purposes, vulnerabilities that previously existed in IT are brought in.
- With increased penetration of DER devices and smart loads being more interconnected the boundary between them and IT devices becomes less and less defined

Nearest IT Neighbor:

- 636 "Not failing securely (failing open)"

7. Common Mode Frailties

Summary: At the component level, most ICS systems are assembled from common parts made by other companies. One or more of these common parts might contain a vulnerability that could result in a wide-spread incident.

Justification as an ICS category: Commonly used components and subcomponents (in HW/SW/FW) within OT systems can result in the presence of both unexpected features or vulnerabilities within the overarching system. Because it is difficult for both asset owners (users) and vendors (manufacturers/OEMs) to accurately track the complete bill of materials for all hardware and software components and subcomponents, even when vulnerability information exists, it may be difficult to connect the vulnerability with the presence of the affected component within a system. Adversary can create a cumulative effect that's scalable, given the broad ecosystem that it's interacting with.

Most Significant or relevant properties of vulnerabilities in this ICS category:

- These vulnerabilities can be caused by
  - the presence of frailty within digital or hardware (HW/SW/FW) component OR
  - the presence of unexpected features which an adversary can capitalize on.
- These vulnerabilities can also be more significant risks during deployment due to accessibility of the systems.

History/Context:

- GE universal relay vulnerabilities. FTDI manufacturers USB to serial adapters. MS sent out a new patch that bricked legitimate devices.
- Issue with use of common devices, libraries, etc. Such that the same tool/malware can effect all of them at scale

Nearest IT Neighbor:

- Linux packages. Getting software packages or development.
- CWE 329. Generation of Predictable IV with CBC Mode.
- OpenSSL
- Great DNS Vulnerability of 2008 by Dan Kaminsky

8. Poorly Documented or Undocumented Features

Summary: Undocumented capabilities and configurations pose a risk by not having a clear understanding of what the device is specifically supposed to do and only do. Therefore possibly opening up the attack surface and vulnerabilities

Justification as an ICS category:

- Capabilities not known to the purchaser can result in installation mistakes because they don't have good documentation on how to run it safely. An adversary may be able to hide or make the component do unexpected things.
- In ICS, this could uniquely result in cascading effects or danger to the public.

Most significant or relevant properties of vulnerabilities in this ICS category:

- Unpredictability is created if mechanical outputs are insufficiently documented e.g. a breaker with undocumented digital control that turns it only partially off when the operator thinks it is either on or off as a manual breaker would be.
- Remote maintenance "backdoor" remaining inappropriately accessible.

Nearest IT Neighbor:

- 1242 "Inclusion of undocumented features of chicken bits"

9. OT Counterfeit and Malicious Corruption

Summary: In ICS, when this procurement process results in a vulnerability or component damage, it can have grid impacts or cause physical harm

Justification as an ICS category:

- If a utility is pressed for budget and finds a cheap counterfeit version, it may have backdoors or faults built in that are different from what the manufacturer has.
- While this also applies to IT, it is not yet part of CVE.

Most significant or relevant properties of vulnerabilities in this ICS category:

Nearest IT Neighbor:

- 1278 see CISCO counterfeited firewalls in DoD supply depots
- 1198 "Privilege separation and access control issues"
- 1231 "Improper implementation of lock protection registers"
- 1233 "Improper hardware lock protection for security sensitive controls"

ICS Engineering (Construction/Deployment)

10. Trust Model Problems

Summary: Assumptions made about the user during the design or construction phase may result in vulnerabilities after the system is installed if the user operates it using a different security approach or process than what was designed or built.

Justification as an ICS category:

- Divergence between plan and what actually gets built. Even if the model design is accurate, what is implemented may diverge from the model.
- Physical process modeled may not align clearly with physical infrastructure to do that.
- Implicit assumptions in the model. Part of the art of engineering in this space that doesn't get written down. Gap in the model that's analyzed and that which gets implemented.
- Long-term deployment of these assets is unique in ICS. Cannot rearchitect quickly. Models can be around for a long time.

Most significant or relevant properties of vulnerabilities in this ICS category:

- Mismatch between as conceived and as built.
- Noise or inaccuracies in models that hide failure modes.

Nearest IT Neighbor:

- 269 "Improper Privilege Management"
- 807 "Reliance on Untrusted Inputs in a Security Decisions"
- 349 "Acceptance of Extraneous Untrusted Data with Trusted Data"

11. Maker Breaker Blindness

Summary: Lack of awareness of deliberate attack techniques by people (vs failure modes from natural causes like weather or metal fatigue) may lead to insufficient security controls being built into ICS systems.

Justification as an ICS category:

- Designing ICS systems, you're modeling a physical process. Must try to imagine what can go wrong.
- Typically, engineers focus on randomness of nature: threat model. E.g., noisy sensors, weather. Physical non-cognitive threat model that you're dealing with. The ICS environment is uniquely connected and digitized, so you see more and now your threat model is a cognitive threat model that you have no experience considering.
- Blindness to how a remote adversary might try to break your system. If you've been building reliable power plants for 30 years, you just don't think about it. Rely on uniformity of nature (power plant in Ohio same as Japan).

Most significant or relevant properties of vulnerabilities in this ICS category:

- Engineering staff not being trained in cognitive threat models (i.e. threats that can think, adapt, and evade).
- Non-stochastic. Rather, intentionally doing x,y, and z.
- Knowledge differential is hard for engineers to appreciate in the threat model.

12. Gaps in Details/Data

Summary: Highly complex systems are often operated by personnel who have years of experience in managing that particular facility or plant. Much of their knowledge is passed along through verbal or hands-on training but may not be fully documented in written practices and procedures.

Justification as an ICS category:

- This vulnerability category applies to OT operational controls. These vulnerabilities arise from
  - standard practices which are developed for operation that aren't captured in the Reference Architecture or security architecture, AND
  - changes in the operating system (processes, configurations, or software version) from the initial development compared to its final deployment that aren't recorded or noted.

Most significant or relevant properties of vulnerabilities in this ICS category:

- This type of vulnerability is an increasing security risk due to the increasing connectedness of OT system components.
- Industry will see more risk due to lack of cyber rigor.
- Processes and procedures are not gap/error free
- Applies to both hardware and software.
  - HW: In OT systems, embedded subcomponents can provide critical operational functions.

  - SW: Systems have multiple chips and software from multiple manufacturers

History/Context:

- Insider attacks are often examples of this category of vulnerability. Insiders know how the devices and systems work and can take advantage of their insider knowledge that others do not know because it hasn't been or wasn't documented.
- Marucchi water incident
- Amalgamation of different devices/solutions within the system

Nearest IT neighbor:

- Lack of inventory of physical and digital assets
- Lack of accurate network architecture maps

13. Security Gaps in Commissioning

Summary: As a large system is brought online components of the system may remain vulnerable until the entire system is operating and functional and security controls are put in place. This creates a window of opportunity for an adversary during the commissioning process.

Justification as an ICS category:

- These vulnerabilities arise from the commissioning cycle for OT systems. System components (including controllers) can sit unpatched and unsecured, accessible to installation personnel. Completed physical security measures and traditional cyber patching doesn't happen until the installation is complete.
- Some system components are installed and tweaked until they start working, without considering impacts or any configuration changes upon these larger security vulnerabilities or considering coordinating with legacy equipment and their potential security assumptions or limitations.
- The commissioning cycle can be long (multiple years) and vary by industry.

Most significant or relevant properties of vulnerabilities in this ICS category:

- Specific to the engineering and business protocols for integrating systems into operational energy infrastructure
- Extensive delays in the commissioning process, allow components to remain in states of varying security and accessibility prior to being pulled into the full planned security envelope.
- There can be difficulties in modifying a system once deployed. (unpatchable or doesn't happen)

History/Context:

- The United States instigated a commissioning vulnerability/incident in the 1980s where a Soviet natural gas installation was sabotaged.

Nearest IT Neighbor:

- CWE 276

14. Inherent Predictability in Design

Summary: The commonality of design (in ICS/SCADA architectures) for energy systems and environments opens up the possibility of scaled compromise by leveraging the inherent predictability in the design.

Justification as an ICS category:

- Common practices in particular ICS application domains (coal, nuclear, wind, etc.) may give an adversary a head-start.
- Common libraries, configurations, etc. and the ability to take them all down with the same tool, malware, etc. at scale (not exclusive to ICS)
- Adversaries exploiting standard, vulnerable operational practices: e.g., downtime maintenance cycles, third-party access, remote operation (especially during COVID) using social engineering and other methods, could compromise operations.
- Some adversaries could potentially affect backups (e.g., gold masters) and thus later restoration from these gold masters could restore a compromised copy of the operational software.

Most significant or relevant properties of vulnerabilities in this ICS category:

- Vendors deploy similar designs across multiple utilities, creating similar vulnerabilities.
- Asset owners deploy similar design templates.
- Design in the US can be relatively similar in terms of mixes of devices AOOs have.

History/Context:

- The Soviets implemented identical controls and operations that allowed capture of vulnerabilities in many installations. The 2015 cyber attack on Ukraine's power grid is one example of this (used common MOX connectors, shared user accounts and passwords for both IT and OT systems at multiple installations).

Nearest IT Neighbor:

- CWE-1278 "Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques"

ICS Operations (& Maintenance)

15. Gaps in obligations and training

Summary: OT ownership and responsibility for identifying and mitigating vulnerabilities are not clearly defined or communicated within an organization, leaving environments unpatched, exploitable, and with a broader attack surface.

Justification as an ICS category:

- Policy gaps or operations gaps. Who is responsible for identifying vulnerabilities that need to be patched in the OT environment?

- Typically, IT does this, but they may not understand OT or have clear responsibility for OT vulnerabilities.
- It may be unclear who is responsible for identifying and mitigating vulnerabilities. If a pump has stopped working, nobody may know why or be responsible for identifying the potential of a cyber threat.
- SOC may not account for correlation with physical events: not having context.

Most significant or relevant properties of vulnerabilities in this ICS category

- Outdated concept of operations or SOPs
- Silo-ing
- Gap between risk and security
- Gap between IT/OT security
- Tend to occur in infrequent scenarios

Nearest IT Neighbor:

- "Responsibility misunderstanding"

16. Human factors in ICS environments

Summary: Environmental factors in ICS including physical duress, system complexities, and isolation may result in security gaps or inadequacies in the performance of individual duties and responsibilities.

Justification as an ICS category:

- The ICS nuance is the physical stress. Richer and more dynamic.
- Complex environments with physical stresses on individuals.
- Physical duress is uniquely part of an ICS environment (as opposed to IT).
- Stressors of dealing with physically intense system. It's all about the physicality of the environment.
- System complexities and novel/emerging security concerns create vulnerabilities in an ICS environment that hasn't traditionally had cyber-security-trained personnel

Most significant or relevant properties of vulnerabilities in this ICS category:

- People may panic, forget, cut corner (i.e. value of a checklist).
- Boredom or isolation might play into the ICS environment.

17. Post-analysis changes

Summary: Changes made to a previously analyzed and approved ICS environment can introduce new security vulnerabilities (as opposed to safety).

Justification of an ICS category:

- Changes to components or environments may invalidate what was previously an accurate post-construction analysis.

- Typically a variety of people have physical access and can make changes that are not documented.
- Change control process may not extend into digital change control.
- Change control management may not cover all changes that could affect the initial design as modeled. Are they tracking changes in the systems that matter? Relative to the digital vulns at play?

Most significant or relevant properties of vulnerabilities in this ICS category:

- Incomplete/improper change control protocol (specifically around digital).

18. Exploitable Standard Operational Procedures

Summary: Standard ICS Operational Procedures developed for safety and operational functionality in a closed, controlled communications environment can introduce vulnerabilities in a more connected environment.

Justification as an ICS category:

- Adversaries exploiting standard, vulnerable operational practices: e.g., downtime maintenance cycles, third party access, remote operation (especially during COVID) using social engineering and other methods, could compromise operations.
- Some adversaries could potentially affect backups (e.g., gold masters) and thus later restoration from these gold masters could restore a compromised copy of the operational software.
- 3rd party vendor access aspects, updates or lack thereof. Lack of standard operational processes. Either they don't exist or are difficult to execute.

Most significant or relevant properties of vulnerabilities in this ICS category:

- Gold masters are more proprietary in OT than IT, including custom made systems and software.

19. Emerging Energy Technologies

Summary: With the rapid evolution of the energy system accelerated by the emergence of new technologies such as DERs, electric vehicles, advanced communications (5G+), novel and diverse challenges arise for secure and resilient operation of the system.

Justification as an ICS category:

- Technologies associated with the emerging grid.
- Controlling distributed cybersecurity assets under multiple domains including non-traditional authorities or administrators of energy assets (homeowners, businesses, etc)
- Must interface with legacy energy control protocols and network architectures

Most significant or relevant properties of vulnerabilities in this ICS category:

- Specific new or legacy protocols associated with incorporating emerging energy technologies into the energy infrastructure (DNP3, Modbus, etc)

- Federation of diverse/distributed administrative and ownership domains (private, unregulated elements of energy infrastructure)
- Lack of security elements in standards (e.g. IEEE 1547) and regulations
- Rapid development and incorporation of emerging technologies, ownership domains (see 3b), and processes (see 3c) create gaps in security obligations

History/Context:

- Case Study: compromise of 3rd party access into utility (ie nearest IT – Target Hack, Vegas Fish Tank)

Nearest IT Neighbor:

- CWE: 406, 285, 295, 20, 601, 346, 296, etc. DNS type weaknesses

20. Compliance/Conformance with Regulatory Requirements

Summary: The ICS environment faces overlapping regulatory regimes and authorities with multiple focus areas (e.g., operational resiliency, physical safety, interoperability, and security) which can result in cyber security vulnerabilities when implemented as written due to gaps in considerations, outdatedness, or conflicting requirements.

Justification as an ICS category:

- Regulatory requirements in ICS may increase attack surface or have a destabilizing effect in the ICS environment
- Compliance mentality is necessary but insufficient for good security and safety.
- Stems from a culture of compliance with regulatory requirements around security that creates blind spots to gaps in security not highlighted in requirements
- Security standards written generally enough that there are many interpretations, allowing users to seek the easiest path to meeting the standard (not necessarily creating robust security as intended)

Most significant or relevant properties of vulnerabilities in this ICS category:

- Need to move from a culture of compliance to a culture of conformance (letter of the standard vs. spirit of the standard)
- Non-experts focused on compliance vs. conformance
- Safety issues, monitoring, reporting requirements, outreach, auditability
- For regulatory requirements that are independent of security

History/Context:

- Technology commonly used to collect data not adequately assessed for security risks it may pose, used for regulatory reasons
- FISMA – example of a standard meant to improve security
- PCI – payment card industry (e.g. Target credit card breaches [TXN])

Nearest IT Neighbor:

- Safety example of conformance v. compliance
- CWE 710 – Improper adherence to coding standards