MITRE’s Original Analysis of SEI ETF NCSV TPT “Categories of Security Vulnerabilities in ICS”

Date: November 2, 2022

POC: Steve Christey Coley (coley@mitre.org)

DISCLAIMER: This is DRAFT content intended for collaboration with the CWE/CAPEC ICS/OT SIG and “Boosting CWE” / “Mapping CWE” working groups. (c) 2022 The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation. For more information, please see the Terms of Use (https://cwe.mitre.org/about/termsofuse.html).

BRIEF INTRODUCTION

In January 2022, members of the MITRE CWE team (Rushi Purohit and Steve Christey Coley) reviewed a draft version of the SEI ETF NCSV TPT document “Categories of Security Vulnerabilities in ICS.” The team reviewed suggested CWE mappings that were already in the document and performed their own search of CWE to augment those mappings. The team analyzed each of the 20 categories to determine if they were expressed in “weakness” language as used by CWE. The team identified where there might be (1) weaknesses that were not covered in CWE but could be added (or used to modify existing entries), and (2) other issues that were out of CWE’s stated scope, which is primarily focused on describing insecure behavior within a product’s specification, design/architecture, implementation, or operation.

This commentary contains lightly edited extracts from MITRE’s preliminary review. It excludes MITRE’s original suggestions for how to submit new content, as that task is separable from determining which weaknesses should be covered in the first place.

Throughout these comments, the “Categories of Security Vulnerabilities in ICS” document might be referred to interchangeably as the “SEI ETF” document or “ICS Vulnerability Categories” or similar phrasing.

Background: Weaknesses, Classes, and Categories in CWE

CWE’s most recent working definition for ”weakness” – likely to be published after recent community review – is “A condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities.”

Informally, weaknesses are expressed within CWE as defects or mistakes that cause the product’s behavior to be insecure from the operator/owner’s perspective.

Weaknesses can be organized hierarchically along different levels of abstraction, from the most general to the most specific. Those levels are: Pillar (most general), Class, Base, and Variant (most specific). Examples are provided elsewhere, or they can be looked up in the CWE Glossary at https://cwe.mitre.org/documents/glossary/index.html

The SEI ETF document combines "classes" and "categories," but they have distinct meaning in CWE. The former are weaknesses, and the latter are not (because they are organized around other characteristics of vulnerabilities that are not related to the weakness itself)

- On the surface, this document has a set of categories (the "super-categories," and some individual items), and high-level (class) weaknesses.
- In CWE, a "Category" is defined as "a CWE entry that contains a set of other entries that share a common characteristic. A category is not a weakness, but rather a structural item that helps users find weaknesses that share the stated common characteristic." An example of a Category is "File Handling Issues" (CWE-1219), which covers many different weaknesses that related to the same resource type (file). However, the entries under this category have very different behaviors: Not controlling file's path (CWE-23), mishandling similar-looking file names (CWE-41), creating a file with insecure permissions (CWE-378), or searching for an executable file in an insecure location (CWE-427).
- A "Class Weakness" is defined as "a weakness that is described in a very abstract fashion, typically independent of any specific language or technology… Class level weaknesses typically describe issues in terms of 1 or 2 of the following dimensions: behavior, property, and resource. For example, the class weakness "Uncontrolled Resource Consumption" (CWE-400) describes an issue (Uncontrolled) with a behavior (Consumption) associated with any type of Resource. Another example is "Insecure Storage of Sensitive Information" (CWE-922) which describes an issue (Insecure) with a behavior (Storage) taken against a general type of resource (Sensitive Information).

SUMMARY OF INITIAL FINDINGS

- The SEI ETF document covers many systems-of-systems, which are not well-covered in CWE
- Several history/context passages mention critical past events, but provide no formal references to determine the relevant weaknesses
- Some 'categories' might be "out of scope" e.g., related to operations or human/organizational process deficiencies. These are traditionally areas which CWE has not covered. More details are provided later.
- CWE entries should have some practical methodologies to fix or mitigate – i.e., they should be actionable. If a submission is not actionable, then it might not be "strong enough" to include in CWE.
- CWE has traditionally had very limited focus on ICS / PLC / IOT, etc.
    - Many similarities with medical device security
    - We have begun to address this gap beginning with CWE 4.7 in April 2022 up to at least CWE 4.9 in October 2022. More details are listed elsewhere.
- CWE has traditionally been primarily about implementation; design- and architecture-level weaknesses have not been considered so much, and some existing entries in these domains are not

as populated as in others. This is a known gap within CWE that we hope to address over the long term.

  - Community support through resources and expertise will affect the speed with which we might be able to integrate some items from the SEI ETF document.

- Some design/architecture issues (and other lifecycle phases like requirements) have some coverage that originates from the Common Quality Enumeration (CQE), which was integrated into CWE a few years ago. Some CQE-derived CWE entries appear relevant for some of this content, but they would likely require additional improvement.
- Some areas (such as access control) are not well-modeled using weakness-oriented classification, and they are difficult to represent effectively in CWE since they need to work across a variety of access control models and technology layers. MITRE has begun to work actively to address this difficulty.
- An ICS-focused view was released in CWE 4.7 to cover the original SEI ETF document. It can be seen at https://cwe.mitre.org/data/definitions/1358.html . To see the hierarchy, users can select "Expand All." To see summaries of the issues, users can check the "Show Details" box. This view is available in various download formats – see the upper right.
- The Hardware Design View (1194) might also be relevant beyond the ICS focused view: http://cwe.mitre.org/data/definitions/1194.html
- Some entries in the SEI ETF document might be better described in terms of attacks, which might mean they could be covered by CAPEC (CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™) (mitre.org)).

If applicable, another potential reference to consider is MITRE's ATT&CK for ICS, but the CWE/CAPEC Program is not involved with ATT&CK.

Background: CWE Scope Exclusions in 2022

While CWE was launched in 2005/2006, the CWE Program has not yet formally defined its scope, i.e., which kinds of issues should be assigned CWE identifiers. This was not a significant barrier in the past, because CWE primarily covered IT-specific software weaknesses in which the errors could be described in concrete ways with clear security implications - such as buffer overflows or injection issues – with well-established detection techniques such as code analysis. Design/architecture weaknesses were also covered, although not as well, partially due to the lack of extensive classification-oriented research, as conducted for buffer overflows (over decades!) and other implementation weaknesses. An effort related to quality-oriented issues (originating from CQE) kept a security-relevant focus but generally limited itself to issues that relied on analysis of artifacts that were present in the software and/or its associated documentation. In these earlier years, the "community" consisted primarily of vendors, researchers, and others who were consulted on a periodic basis in workshops or other gatherings.

In recent years, as the CWE Program has emphasized community engagement, various stakeholders have looked to CWE to expand to new domains for which security is important, whether for software, hardware, or other forms of automated logic. New kinds of technologies also emerged for which CWE was not clearly applicable. Sometimes, these interests in CWE extended beyond the behavior (or documented/specified behavior) of products into other aspects of the development lifecycle that made it easier to introduce weaknesses. As the number of external suggestions for new CWE content has increased, it became clear that many of these suggestions did not fit within CWE's framing of weaknesses, or in its implied "traditional" scope.

As a result, it has now become more important for the CWE Program to more clearly define and document its scope. Beginning in early 2022, we have tried to characterize the differences between the perceptions of community members and our own traditional scope. In late 2022, we will begin community-wide review of current scope with an emphasis on "scope exclusions" – issues that are important for improving product security, but which do not currently factor as "weaknesses" within CWE's model.

MITRE's original analysis of the SEI ETF document has contributed to the formulation of various scope exclusions. The ICS/OT SIG will be notified when scope exclusions are proposed for public review, planned for November 2022.

Summary of MITRE Analyses

Summaries of MITRE's findings are included below, in rough order of priority, with "low-hanging fruit" listed at the top. The SEI ETF group might be able to improve other items to make them easier to include or cite within CWE.

Each individual item has more detailed "MITRE" comments in the sub-section for that particular item.

New CWE entries / improvement possible in near term

These items are generally already known CWE gaps that might be relatively easy to address with new entries ASAP, as there has been some kind of demand from the CWE community already. Such new entries are unlikely to be as precise as the items from the SEI ETF document, but ICS-specific examples and text could be included, and the new CWEs would still be more precise or relevant than any currently-available CWEs.

- 1. Zone Boundary Failures. MITRE summary: includes known CWE gaps; more specific entries possible, pending CWE research
- 4. External Physical Systems. MITRE summary: includes known CWE gaps; new entries possible in next version.
- 5. External Digital Systems. MITRE summary: includes known CWE gaps; new entries possible in next version.
- 7. Common Mode Frailties. MITRE summary: includes known CWE gaps; new entries possible in next version.
- 8. Poorly Documented or Undocumented Features. MITRE summary: Relevant CWEs exist.

Not weakness-oriented but includes known gaps

These do not focus on the weakness, but there are known CWE gaps which, if addressed, might produce new CWEs that would be relevant.

- 2. Unreliability. MITRE summary: not weakness-oriented; includes known CWE gaps - related concepts are subjects of ongoing research
- 3. Frail Security in Protocols. MITRE summary: not weakness-oriented; includes known CWE gaps; some relevant mappings are likely.
- 6. IT/OT Convergence/Expansion. MITRE summary: not weakness-oriented; includes known CWE gaps.
- 10. Trust Model Problems. MITRE summary: not weakness-oriented; known CWE gaps.

Not weakness-oriented

These cannot be easily processed as-is because they do not focus on the mistakes.

- 11. Maker Breaker Blindness. MITRE summary: not weakness-oriented.
- 14. Inherent Predictability in Design. MITRE Summary: likely out of scope.
- 19. Emerging Energy Technologies. MITRE summary: not weakness-oriented.

Known gap (or scope issues) without quick resolution or guarantee of inclusion

- 9. OT Counterfeit and Malicious Corruption. MITRE summary: already-known CWE gap.

Out-of-scope - human process issues

Many of these items are about human/organizational process problems that could produce more weaknesses. These are out of scope for CWE without plans for inclusion in the near future. However, efforts such as Building Security In Maturity Model (BSIMM) or OWASP Software Assurance Maturity Model (SAMM) might be better suited to cover such practices.

- 12. Gaps in Details/Data. MITRE Summary: not weakness-oriented; emphasis on human processes is out of scope with no current plans to address.
- 13. Security Gaps in Commissioning. MITRE summary: not weakness-oriented; partial scope issue (not an actively-covered phase of product lifecycle)
- 15. Gaps in obligations and training. MITRE summary: out of scope (human processes/operations)
- 16. Human factors in ICS environments. MITRE Summary: possibly out of scope (human processes and operations). Psychological in nature.
- 17. Post-analysis changes. MITRE summary: not weakness-oriented, possibly out-of-scope as a human process problem.
- 18. Exploitable Standard Operational Procedures. MITRE summary: Known CWE gap, but some parts may be out-of-scope as a human process problem; possible new CWE entry.
- 20. Compliance/Conformance with Regulatory Requirements. MITRE summary: out of scope (human/organizational processes)

DETAILED ANALYSES FOR EACH ICS CATEGORY

These sections include each super-category, and their 20 categories. For each category, the summary and justification are included verbatim from the SEI ETF document, followed by MITRE's original January analysis. Additional details (including suggested CWEs) and other information are in the full SEI ETF document.

1. 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.

MITRE summary: includes known CWE gaps; more specific entries possible, pending CWE research.

MITRE notes: CWE-669 does makes sense as a mapping, but a better mapping is CWE-668. However, CWE-754 is not applicable here based on the description of the Zone Boundary Failures. Refer to CWE-668 as a model to mimic for creating a new entry around this topic. There is a good potential for this entry to be added to the CWE corpus, but it requires a bit more substance (as highlighted in the content submission guidelines). Definitions of network "zones" (as implied by firewalls or other network restrictions) are related to communication channels, which need better coverage. See CWE-923: Improper Restriction of Communication Channel to Intended Endpoints and children 940/941.

MITRE-suggested CWE: CWE-668: Exposure of Resource to Wrong Sphere

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

MITRE summary: not weakness-oriented; includes known CWE gaps - related concepts are subjects of ongoing research.

MITRE notes: Not describing the kinds of mistakes that happen. Hardware CWE is beginning to handle "insufficient handling of errors in environment". Great reference to "Random early detection" which seems like a great mitigation across several CWEs. CWEs 1263 and 1300 provide good examples of entries related to this content.

MITRE-suggested CWE: CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments (potentially relevant, but a parent may need to be created), CWE-703: Improper Check or Handling of Exceptional Conditions, CWE-1263: Improper Physical Access Control, CWE-1300: Improper Protection of Physical Side Channels.

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.

MITRE summary: not weakness-oriented; includes known CWE gaps; some relevant mappings are likely.

MITRE notes: Not describing the kinds of implementation mistakes in detail, but there are some class-level CWEs. Although not exact, CWEs like 327 and 1240 can be considered associated with crypto, key management, etc. Other CWEs may be relevant for other kinds of protection mechanisms besides crypto.

CWE-327: Use of a Broken or Risky Cryptographic Algorithm, CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation, CWE-358: Improperly Implemented Security Check for Standard, CWE-573: Improper Following of Specification by Caller. Also, reliance on "insecure" third-party component is not directly covered, but a known gap (1104, 1103, and 1329 are examples).

2. 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.

MITRE summary: includes known CWE gaps; new entries possible in next version.

MITRE notes: Not well-covered in CWE, but external dependencies are starting to show up as a concern in hardware CWE. The cited "energy" domain vignettes within CWRAF are incomplete and not well-defined.

MITRE-suggested CWE: (not ideal) CWE-829: Inclusion of Functionality from Untrusted Control Sphere, CWE-1103: Use of Platform-Dependent Third Party Components.

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

MITRE summary: includes known CWE gaps; new entries possible in next version.

MITRE notes: CWE-610 is inappropriate since it is about "pointers" to resources, where the "pointer" can be modified by an attacker. However, CWE needs to expand/clarify unnecessary or excessive dependencies on external / untrusted systems operating in less-controlled environments.

MITRE-suggested CWE: CWE-829: Inclusion of Functionality from Untrusted Control Sphere, CWE-1103: Use of Platform-Dependent Third Party Components.

3. 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.

MITRE summary: not weakness-oriented; includes known CWE gaps.

MITRE notes: This is not a "CWE weakness" per se. How does this evolution introduce new mistakes? Is this avoidable? This entry requires more discussion and content for it to become a "mistake" that can be incorporated into the CWE corpus. If there is no weakness related info, and the focus is around the attack side, then use of CAPEC (CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™) (mitre.org)) may provide better support, especially around the areas of supply chain.

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.

MITRE summary: includes known CWE gaps; new entries possible in next version

MITRE notes: Dependency on insecure component needs better CWE coverage. Relationships to supply chain are a CWE topic (with more focused coverage in CAPEC). Not clear what the relationship is with CWE 329 and other "nearest IT neighbor" examples.

MITRE-suggested CWE: unclear. Possibly the more implementation-oriented CWE-829: Inclusion of Functionality from Untrusted Control Sphere. One of several component-dependency entries: CWE-1103: Use of Platform-Dependent Third Party Components.

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.

MITRE summary: Relevant CWEs exist.

MITRE notes: CWE has some coverage, but this content could help to improve it.

MITRE-suggested CWE: CWE-912: Hidden Functionality (entry needs significant improvement), CWE-1059: Incomplete Documentation.

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.

MITRE summary: already-known CWE gap.

MITRE notes: Counterfeit / anti-tamper gaps are known to CWE (as coming from SAE within the hardware CWE SIG), but scope questions exist. Most of the cited weaknesses have their own scope questions. There are also high numbers of relationships between "counterfeit" products and almost any other weakness, which may limit the utility of such an entry for classification.

4. ICS Engineering (Constructions/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.

MITRE summary: not weakness-oriented; known CWE gaps.

MITRE notes: Some overlap with other weaknesses/categories e.g., product does not behave as expected by consumer. CWE examples seem nearly arbitrary. One known gap involves when design plans and actual implementations/deployment do not align.

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).

MITRE summary: not weakness-oriented.

MITRE notes: CWE needs to improve on environmental failure modes as mentioned before. This is also a human/organizational process failure. Effectively a "mode of introduction" (i.e., situations that would cause a weakness to be inserted). CWE would cover the specific mistakes that arise from such poor processes (e.g., insufficient access control).

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.

MITRE Summary: not weakness-oriented; emphasis on human processes is out of scope with no current plans to address.

MITRE notes: Operations / human processes. (See "IT neighbor" examples of lack of inventory of physical/digital assets, and lack of accurate network architecture.)

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.

MITRE summary: <u>not weakness-oriented</u>; partial scope issue (not an actively-covered phase of product lifecycle)

MITRE notes: based on the Summary, this is effectively a large-scale race condition, which has coverage (primarily on implementation/design). CWE-276 is only one potentially relevant mapping, but see CWE-362 and its subtree. Many issues that arise from bad deployment can be described with CWEs. CWE schema includes "Installation," "System Configuration," "Operation", "Integration", and other phases that might all be considered part of "deployment"/"commissioning" but these are not well-covered.

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.

MITRE Summary: <u>likely out of scope</u>.

MITRE notes: Not clear why 1278 is mapped ("Missing Protection Against Hardware Reverse Engineering") - it made more sense in a different category. Not immediately clear what can/should be done about this. CWE like 1241 - Use of Predictable Algorithm in Random Number Generator can be considered as an example, even though it only focuses on crypto side of it, while this entry covers a broad array of things. Another good example could be CWE-341: Predictable from Observable State.

5. 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.

MITRE summary: out of scope (human processes/operations)

MITRE notes - human processes and operations. Interesting discovery of "responsibility misunderstanding" in Weber flaw taxonomy.

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

MITRE Summary: possibly out of scope (human processes and operations). Psychological in nature.

MITRE Notes: There are some entries related to user interface / user experience (e.g. CWE-451), and CWE-655: Insufficient Psychological Acceptability, but psychological/human considerations are generally excluded from CWE. However, there are various CWEs related to system complexity that do not directly cover the human component, such as CWE-1120: Excessive Code Complexity (derived from CQE).

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?

MITRE summary: not weakness-oriented, possibly out-of-scope as a human process problem.

MITRE notes - Too general, does not lay out the specific mistakes. Human process problem? Still, a very important distinction/consideration for balancing security and safety. These considerations are not included in CWE "mitigations" fields and probably should not be, due to the wide variety of products for which CWE entries are usually intended to apply.

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.

MITRE summary: Known CWE gap, but some parts may be out-of-scope; possible new CWE entry.

MITRE notes: Item focuses on human processes. However, "[lack of / inconsistency with] gold masters" has already been submitted by an external contributor, and it might be appropriate as a design/documentation weakness, but maybe not resolvable by the next CWE version.

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

MITRE summary: not weakness-oriented.

MITRE notes: These are not behaviors per se, but rather a description of aspects of technological evolution that can create the conditions under which weaknesses can be introduced. Many common implementation/design-level CWEs have been mapped, and many more examples could be mapped.

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)

MITRE summary: out of scope (human/organizational processes)

MITRE notes: Scope issue - human/organizational processes. Map to CWE-710 doesn't quite seem appropriate since it's about NOT following a standard.