Toward Common Weakness Enumerations in Industrial Control Systems

David M. Nicol | University of Illinois at Urbana-Champaign and Cyber Manufacturing Innovation Institute
Gregory Shannon | Idaho National Laboratory and Cyber Manufacturing Innovation Institute
Monika Akbar | University of Texas at El Paso and Cyber Manufacturing Innovation Institute
Matt Bishop | University of California, Davis and Cyber Manufacturing Innovation Institute
Michael Chaney | Idaho National Laboratory and Cyber Manufacturing Innovation Institute
Matthew Luallen | University of Illinois at Urbana-Champaign and Cyber Manufacturing Innovation Institute

The storyline of MITRE's common weakness enumeration framework illustrates how the security and privacy technical community can collaborate/cooperate with policy makers to advance policy, giving it specifics and filling gaps of technical knowledge to improve security and resilience of critical infrastructure.

The U.S. Congress 2020 National Defense Authorization Act contains a Section 5726 entitled "Securing Energy Infrastructure" that directs the Department of Energy (DoE) to establish a working group responsible for evaluating elements of security program elements, and development of national strategy. The DoE formed a voluntary group of public and private sector leaders called the *Securing Energy Infrastructure Task Force* (*SEI ETF*), and subgroups, each focused on a particular objective called for in the congressional language. One subgroup was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the *Technical Project Team for New Classes of Security Vulnerabilities for ICS* (TPT-NCSV).

Introduction

The DoE TPT-NCSV leadership recognized the value of existing systems of knowledge about cybersecurity in IT systems [such as MITRE's common weakness enumeration (CWE)[1]], and approached their mission so as to emulate and potentially integrate with those systems, particularly with trends of IT/operational technology (IT/OT) convergence underway.

They adopted the fundamental idea of highlighting areas and activities within ICS that potentially allow for high-consequence vulnerabilities. The focus is not on particular vulnerabilities (e.g., unused web-servers embedded in ICS device operating systems) but on developing descriptions that apply more generally: classes, categories. The hope is that designers and vendors of ICS hardware, software, and middleware will use these identifications to provide better defense in their designs, and that asset owners will use them to develop more care and defense in the configurations and operations of what the vendors provide. Furthermore, a framework enables the identification and association of new vulnerabilities within a common class; this enables data analysis of vulnerability occurrences, which informs prioritization of mitigation investments. Importantly, TPT-NCSV leadership viewed cybersecurity management and procurement processes as potential sources of vulnerabilities, not just the technology itself in isolation.

The TPT-NCSV committee drew its membership from government organizations, owner/operators of power systems, industry and trade organizations, vendors and manufacturers, academic institutions, and national laboratories. The TPT-NCSV met bimonthly

Digital Object Identifier 10.1109/MSEC.2023.3279515
Date of current version: 16 July 2023

over the period of a year, developing several lines of effort, including:

- baselining existing categories of ICS vulnerabilities
- conducting gap analysis that may serve in the identification of new categories of ICS vulnerabilities
- identifying and communicating new categories of ICS vulnerabilities.

TPT-NCSV Outcomes

The TPT-NCSV based their choice of categories in part on historical ICS cyberincidents, looking for specific elements whose identification may have improved stakeholder's ability to anticipate and respond to relevant risk. They examined case studies that helped to illuminate the challenge in drawing a clear line between IT and OT. Based on this and their own experience-informed imaginations, the TPT-NCSV members developed an extensive list of potential categories, and then refined that list through discussion and consensus. The result was 20 categories, each with a short writeup that describes the category and justifies its inclusion as an ICS category versus a more general IT category. The 20 categories were gathered into five core groupings. Recognizing that two- and three-word descriptions hardly convey their substance, this list of categories nevertheless gives a snapshot that is suggestive of their underlying substance:

- ICS communications
  - zone boundary failures
  - unreliability
  - frail security in protocols
- ICS dependencies and architecture
  - external physical systems
  - external digital systems
- ICS supply chain
  - IT/OT convergence/expansion
  - common mode frailties
  - poorly documented or undocumented features
  - OT counterfeit or malicious corruption
- ICS engineering (construction/deployment)
  - trust model problems
  - maker breaker blindness
  - gaps in details/data
  - security gaps in commissioning
  - inherent predictability in design
- ICS operations and maintenance
  - gaps in obligations and training
  - human factors in ICS environments
  - postanalysis changes
  - emerging energy technologies
  - exploitable standard operational procedures
  - compliance/conformance with regulatory requirements.

A report to Congress on TPT-NCSV, its activities, and its outcomes can be found online.[2] Here, just to better illustrate the notion of *category*, illustrate the TPT-NCSV description, and emphasize the considerations deriving from the interaction of physical and cyber-systems, we replicate the writeups for two categories. The "External Physical Systems" category speaks to vulnerabilities that arise because of the influence of a physical system on the behavior of an ICS. The "Maker Breaker Blindness" category characterizes vulnerabilities that are possible by the adversary manipulating a physical system. For both we list the headings used by these descriptions.

Category: 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.

Category: Maker Breaker Blindness

Summary. Lack of awareness of deliberate attack techniques by people (versus 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 and must try to imagine what can go wrong.
- Typically, engineers focus on the randomness of nature: a threat model (e.g., noisy sensors), weather, a physical noncognitive 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 (a power plant in Ohio is same as in 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)

- nonstochastic; rather, intentionally doing *x*, *y*, and *z*
- knowledge differential is hard for engineers to appreciate in the threat model.

The TPT-NCSV leadership recognized that for these outcomes to have the greatest utility and impact, they ought to be coordinated with organizations of information for IT that are already widely known and used. This recognition led to discussions with the Department of Homeland Security (DHS) and MITRE about coordinating with its CWE list.

CWE

In reviewing a draft of the TPT-NCSV report, MITRE saw the connections between the report's categories and the notion of *weakness* contained in the CWE.[1,3] A result of this conversation was inclusion of the TPT-NCSV categories within the CWE framework. To help develop appreciation of the connection, we need to describe CWE at a high level.

CWE defines general labels and descriptions of software and hardware weaknesses with the goal of encouraging stakeholders to use a common language to discuss software and hardware vulnerabilities. Another objective is to stop vulnerabilities from even being introduced, by educating designers, developers, and acquirers on how to recognize and eliminate common mistakes that may lead to vulnerabilities and exploitation.

An approved list of CWEs is created and maintained by MITRE, who identifies and manages a CWE committee comprised of stakeholders, researchers, and representatives from organizations, industry, academia, and government working with software and hardware weaknesses. The CWE system is coupled with the common vulnerabilities and exposures (CVE) system,[3] launched by MITRE in 1999, which enumerates specifically discovered vulnerabilities. Each CVE entry contains a CVE ID, a description of the vulnerability, products and systems impacted by the vulnerability, and other references. As of 2022, there were more than 174,577 CVE entries disclosed, while the CWE 4.7 standard identifies 926 weaknesses. CWE is part of a trio of frameworks aimed at capturing different attributes of the security problem. While CWE focuses on system-level weaknesses, the Common Attack Pattern Enumeration and Classification (CAPEC) System focuses on characterizations of attacks that use the weaknesses. The CVE speaks to specific vulnerabilities of specific components found in the field. CWE entries sometimes reference CVE entries as specific examples of weaknesses, and sometimes reference CAPEC entries to describe attacks that exploit the CWE-reported weakness.

The objectives of CWE and TPT-NPCV do not exactly overlap. An important objective for CWE leadership has been to consider only weaknesses where actionable mitigation is possible; this was not an objective of the TPT-NPCV effort, and mitigation information is sometimes absent. Going forward within CWE means augmenting the TPT-NPCV descriptions. Also, TPT-NPCV identified vulnerabilities related to organizational process that would be viewed as out-of-scope for CWE. Going forward, some harmonization is required.

CWE classifies its entries largely based on the level of detail. At the highest level of abstraction are "pillar" and "category" entries. Below we draw from the CWE glossary

- *Pillar weakness:* The highest-level weakness that cannot be made any more abstract. Pillars represent an abstract theme for all class/base/variant weaknesses related to it. A pillar is different from a category as a pillar is still technically a type of weakness that describes a mistake, while a category represents a common characteristic used to group related things.
- *Category:* 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.
- *Class weakness:* A weakness that is described in a very abstract fashion, typically independent of any specific language or technology.
- *Base weakness:* A weakness that is described abstractly, but with sufficient details to infer specific methods for detection and prevention.
- *Variant weakness:* A weakness that is linked to a certain type of product, more specific than a base weakness.
- *Composite weakness:* An element that consists of two or more distinct weaknesses, in which all weaknesses must be present at the same time in order for a potential vulnerability to arise.

A tree structure—each of whose nodes has one of these types—is used to describe relationships between CWE entries as a function of abstraction and specificity. For example, the glossary entry above for "class weakness" cites CWE 400, "uncontrolled resource consumption." The CWE site for CWE 400 includes a description "The software does not properly control the allocation and maintenance of a limited resource, thereby enabling an actor to influence the resources consumed, eventually leading to the exhaustion of available resources." It also includes a paragraph ("Modes of Introduction") which identifies how the weakness is introduced, a paragraph ("Common Consequences") that describes impacts of exploiting the weakness (for this example, "The most common result of resource exhaustion is denial of service. The software may slow down, crash due to unhandled errors, or lockout legitimate users.")

The CWE documentation includes source code examples, a list of observed instances of this weakness, suggestions of mitigations, ways of detecting the weakness, among other things. CWE 400's relationship to other CWE entities is shown in Figure 1, copied from the CWE website description for CWE 400. It has one parent (CWE 664) and six children, all of which are "base" weaknesses.

The description tells us that several CWEs fall technically under the umbrella of "uncontrolled resource consumption"; we see in their titles specific activities that may lead to uncontrolled resource consumption.

We see also that CWE 400 is a child node of a pillar node, CWE 664, "improper control of a resource through its lifetime." The page for CWE 664 has the same types of information as does CWE 400's, albeit at a more abstract level. For example, the CWE 664 description is simply "The software does not maintain or incorrectly maintains control over a resource throughout its lifetime of creation, use, and release."

CWE 664, in the research concept view (view ID 1000), has 17 class weaknesses, nine base weaknesses, and three variant weaknesses. CWE 400 is one of those 17 class weaknesses. CWE 400 was created in 2006. Since then, it has appeared in the top "25 Most Dangerous Software Weaknesses" in multiple years (e.g., 2019, 2020, 2022). CWE 400 has six children (CWE IDs: 770, 771, 779, 920, 1235, and 1246). Figure 2 shows this relationship and some related information specific to these CWEs.

Further analyses of CWE 400 and its six children reveal that a common consequence of exploiting these weaknesses is the denial of service attack. All of these weaknesses are introduced at various phases: architecture, design, operation, and implementation. Detection methods include automatics and manual static analysis.

Potential mitigation strategies include designing throttling mechanisms into the system architecture, replacing large duplicate log messages with periodic summaries, using resource-limiting settings, limiting boxed primitives, and including secure wear leveling algorithms.

In terms of exploiting CWE, two CAPEC entries list CWE 400 as a related weakness, weaknesses that must be present for the attack to be successful. These are CAPEC 147 and 492. CAPEC 147 has CWE 400 and 770 (child of 400) listed as related weaknesses. CAPEC 492 also has two related weaknesses: 400 and 1333 (linked with 664 through 405→407→1333). Parents of these CAPEC entries include flooding techniques (CWE 125) and excessive allocation (CWE 130). The six children of CWE 400 have 22 CAPEC entries linked with them through the "related attack pattern" field. The related weaknesses (i.e., CWE entries) of these attack patterns (or, CAPEC entries) are shown in Figure 2.

This example is meant to give a multidimensional view of CWE's expression and organization of weaknesses. The structure offers flexibility in augmenting it with new

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	P	664	Improper Control of a Resource Through its Lifetime
ParentOf	B	770	Allocation of Resources Without Limits or Throttling
ParentOf	B	771	Missing Reference to Active Allocated Resource
ParentOf	B	779	Logging of Excessive Data
ParentOf	B	920	Improper Restriction of Power Consumption
ParentOf	B	1235	Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations
CanFollow	B	410	Insufficient Resource Pool

Figure 1. Relationships expressed by CWE 400's description.

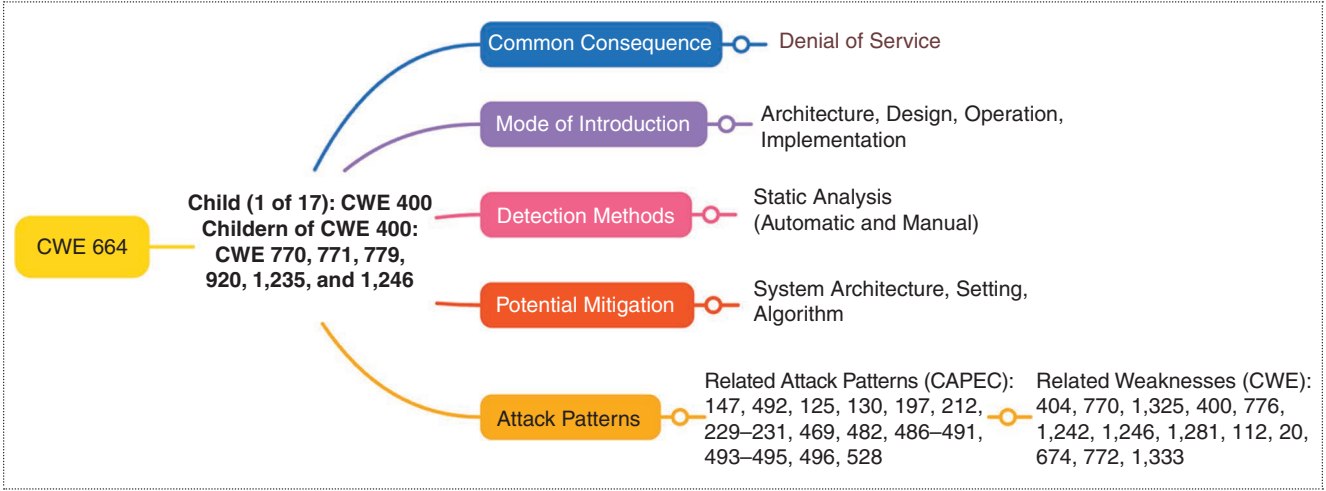

Figure 2. A partial analysis of CWE 664.

information. This example shows many implicit connections exist between CWE, CVE, and CAPEC, providing an in-depth exploration, identification, and understanding of which are crucial for designing and maintaining secure systems.

One outcome of the SEI ETF TPT-NCSV activity is an organized effort to transform the kinds of categories it identified and create representations of these within the CWE framework. We next turn to a description of that mapping.

Expression of OT/ICS Weaknesses in CWE

There is a descriptive aspect to CWE entries; there are also abstraction characterizations and relationship descriptions. A challenge then is to develop a methodology for embedding information expressed in the TPT-NCSV report within CWE entries and to establish relationships between those new CWE entries and existing ones.

CWE 4.7 and later versions contain entries that are based on the TPT-NCSV categories, and it is instructive to observe their relationship with the TPT-NCSV categories. There is a tree ("Weaknesses in SEI ETF Categories of Vulnerabilities in ICS") that organize these. At the highest level are five new CWE "category" entries that correspond to (and have the same names as) the five groupings the TPT-NCSV report gives for its 20 categories. The CWE entries for these refer to the TPT-NCSV congressional report and contain a descriptive note that primarily reflects their origin.

Each of these category nodes are parent to CWE entries with titles corresponding to the specific categories listed within that group. For example, the TPT-NCSV "ICS Dependencies (& Architecture)" group has two categories ("External Physical Systems" and "External Digital Systems"), and new CWE entries were created to represent these. With these new entries, CWE incorporates the names and high-level group of the 20 TPT-NCSV categories; each of these entries have basically the same description note as their parents. CWE 4.7 does not (nor did it intend to) flesh out most of these entries with information about them that is present in their TPT-NCSV writeup. However, most of the TPT-NCSV category entries do contain important links that tie their identification into the CWE framework. However, the creators of CWE 4.7 also introduced some new entries that are also children of TPT-NCSV category entries, e.g., CWE 1365 "Communications: Unreliability" has a newly minted child entry entitled "Improper Handling of Extreme Physical Environment Conditions" (CWE 1384).

The specific entries in the CWE 4.7 representation of the 20 TPT-NCSV categories are sparse. It is worthwhile comparing the CWE representations of one of the categories with its TPT-NPSV origin, and for this we return to TPT-NCSV documentation for the "External Physical Systems" category described earlier. CWE 1384 "Improper Handling of Physical or Environmental Conditions" represents this category.

Extended Description

Hardware products are typically only guaranteed to behave correctly within certain physical limits or environmental conditions. Such products cannot necessarily control the physical or external conditions to which they are subjected. However, the inability to handle such conditions can undermine a product's security. For example, an unexpected physical or environmental condition may cause the flipping of a bit that is used for an authentication decision. This unexpected condition could occur naturally or be induced artificially by an adversary.

Physical or environmental conditions of concern are:

- atmospheric characteristics: extreme temperature ranges, etc.
- interference: electromagnetic interference, radio frequency interference, etc.
- assorted light sources: white light, ultraviolet light, lasers, infrared, etc.
- power variances: undervoltages, overvoltages, undercurrent, overcurrent, etc.
- clock variances: glitching, overclocking, clock stretching, etc.
- component aging and degradation
- materials manipulation: focused ion beams, etc.
- exposure to radiation: X-rays, cosmic radiation, etc.

Modes of Introduction

- *Phase: Architecture and Design:* Note: The product's design might not consider checking and handling extreme conditions.
- *Phase: Manufacturing:* Note: For hardware manufacturing, subpar components might be chosen that are not able to handle the expected environmental conditions.

Potential Mitigations

- *Phase: Requirements:* Be specific about expectations for how the product will perform when it exceeds physical and environmental boundary conditions, e.g., shut down.
- *Phases: Architecture and Design; Implementation:* Where possible, include independent components that can detect excess environmental conditions and have the capability to shut down the product. Where possible, use shielding or other materials that can increase the adversary's workload and reduce the likelihood of being able to successfully trigger a security-related failure.

We might interpret the differences between these two representations through the lens of what types of information each records. Each TPT-NCSV entry contains up to five headings ("summary," etc.,

described earlier). Guidelines for proposing new CWE entries list a number of required elements.[4]

There are clearly points of relationship, but just as clearly, the CWE approach is more specific in its emphases. While certain types of information that are required for a CWE entry might be present in a TPT-NCSV description, there are no requirements that they do so, particularly for an element seen as critical to a CWE, such as "potential mitigations."

In general, there are significant differences between the TPT-NCSV and general CWE representations. The CWE management team emphasizes that CWE entries are intended to lead to actionable mitigation, which sometimes is more completely described through referencing attacks. This emphasis was not shared by the TPT-NCSV category developers. The MITRE CWE management team also points out that the scoping of categories to be discovered by TPT-NCSV includes vulnerabilities that exist due to organizational attributes, such as processes used to manage cybersecurity, and that CWE in its present form does not, citing for example, the TPT-NCSV categories "Security Gaps in Commissioning" and "Gaps in Obligations and Training." Until CWE subsumes TPT-NCSV, there is therefore value in continuing to understand and reference TPT-NCSV, even though it will not be updated in the way that CWE is.

TPT-NCSV and CWE Use Cases

We turn next to brief discussions of how the TPT-NCSV and CWE categorizations can be used in the management of ICS/OT vulnerabilities. We consider first a use case involving manufacturers and their suppliers; second, a use case of how these categorizations can aid in workforce development; and third, a use case on how they can enhance an organization's efforts to improve its cybersecurity maturity level.

Equipment and Software Manufacturer and Their Associated Integrators

Equipment and software manufacturers and their associated integrators have been dealing with increasing levels of OT-associated security vulnerabilities for over a decade. The efforts by industry to maintain operational resiliency has been formidable, but so have the efforts by the adversaries. Efforts to categorize vulnerabilities by their common weaknesses is not new among the IT community, as evidenced by the MITRE CWE framework. As we have described earlier, in 2022 ICS/OT specific vulnerabilities were added to the CWE framework following the release of the TPT-NCSV report. These categories of weaknesses should serve in a more static capacity, allowing equipment and software manufacturers and their associated integrators to address these weaknesses categorically. Many OT vulnerabilities may be directly associated with a single vendor's technology; however, the vulnerability is also associated with a weakness that typically applies to many vendors. Furthermore, many types of vulnerabilities may fall under a single weakness, allowing a vendor to streamline and categorize their internal and community responses. This streamlining and categorizing may lead to greater organizational efficiencies and potentially a decrease in the vulnerability identification to disclosure to remediation timeline.

For example, CWE 1357, the reliance on uncontrolled component, documents an example of a supplier's reliance upon an original equipment manufacturer (OEM) software library. Observing that this CWE is a member of the "ICS supply chain: common mode frailties," the supplier may generate a product-wide response to an identified vulnerability that is grouped inside the weakness. Consider the event that the supplier becomes aware of a vulnerability, such as CVE-2021-44228, that has been identified as a classification of CWE 1357.

Using a table with entries similar to Table 1 as a reference, the supplier may combine the knowledge of the vulnerability, the CWE identifier, the TPT-NCSV categorization,

Table 1. Sample categorization of CVE within vulnerability category context.

Vulnerability	Considered CWE Identifier	Member Of TPT-NCSV	Vulnerability / CWE/ TPT-NCSV + SBOM	Supplier issues a VEX Notification to Customer
CVE-2021-44228 Log4Shell	CWE 1357 Reliance on uncontrolled component	1370 ICS Supply chain: Common mode frailties	Identified as included software within product • not affected • affected • fixed • under investigation	Notification sent to known asset owners and operators of under investigation and affected product status with referenced CWE categorized mitigation guidance.

VEX: Vulnerability Exploitability Exchange.

and the software bill of materials (SBOM), to determine whether their products are not affected, affected, fixed, or under investigation. The supplier can then issue a report to known owners and operators of the product, supported with referenced CWE categorized mitigation guidance.

Workforce Development

Adversaries may leverage vulnerabilities identified within the CWE and TPT-NCSV to create an intended effect within a well-engineered system, exploiting the possibility that an engineer is uninformed about cyber weaknesses. CWE identifications serve as an excellent basis for enhancing education to support the cyber-informed engineer. Cyber-informed training goes beyond the traditional professional engineer designation to include awareness and understanding cybersecurity, and is paramount in supporting operational resiliency. The cyber-informed engineer will include cyberthreats as part of the risk management and the overall engineering design process. Specifically, CWE- and TPT-NCSV–driven education for engineers can connect the dots between the common weaknesses, adversarial techniques, and the supporting mitigations. Such education leads to specific outcomes beyond traditional engineering topics. Standardization of CWE and TPT-NCSV descriptions provides simple and scalable foci for educational content development that addresses real functional needs.

To provide some background, a "purple" exercise is one where a "red" team exercise is executed to discover existing vulnerabilities, and the findings are used to train and educate a "blue" team on how to defend against and mitigate the discovered attacks. In the description of such an exercise, there are standardized categories that identify the technique an adversary uses, the techniques the defender uses to detect the attack, and mitigation techniques.

Table 2 highlights the educational connection from a CWE to specific educational outcomes that are desired for a purple exercise. CWE 1371 describes poorly documented or undocumented features that are left behind in a deployed component. An adversarial technique (here labeled *T0848*) is employed to become a "rogue master" of the component's poorly documented features, who can manipulate the system through trusted hosts that are simply acting in response to permitted actions and requests, because of default configurations and features that are not properly understood. Evidence of such exploitation can be the existence of unexpected network traffic, detection of which (DS0029) enables the asset owner/operator to further limit the ability of the adversary's success by implementing mitigation M0930 of network segmentation. This CWE-driven educational scenario connects the MITRE elements to the educational outcome of influencing a participant to *what* to learn, *why*, and *how* to reduce the attack surface associated with this weakness.

Organizational Risks and Maturity

There are various frameworks that help an organization assess its maturity with respect to managing cybersecurity, such as International Society of Automation (ISA) 62443,[5] the manufacturing Information Sharing and Analysis Center's (ISAC) operational resilience framework,[6] and the DoE's cybersecurity capability maturity model (C2M2).[7] Outcomes from using these frameworks may be enhanced by connecting them to organizational weaknesses and vulnerabilities outlined in the CWE and TPT-NCSV. Table 3 gives an example of associations between a new CWE identifier, TPT-NCSV categories, the DoE C2M2 objective, the ISA/International Electrotechnical Commission (IEC) 62443-3-2 security risk assessment for system design reference, and the manufacturing ISAC Operational Readiness Framework (ORF).

Another commonly used mechanism to express risk evaluation criteria for IT cybersecurity is the International

Table 2. Linkage from example CWE to exercise educational outcomes.

CWE	Technique	Detection	Mitigation	Educational Outcomes
CWE 1371: Poorly documented or undocumented features Member of TPT-NCSV category: ICS supply chain	Technique T0848: Rogue master Use default protocols and settings left in device configurations to manipulate the system using trusted hosts	DS0029 Network traffic content and flow Monitor for unexpected ICS protocol functions and unapproved commands	M0930 Network segmentation M0813 Software process and device authentication	Learn why and how to reduce the attack surface by disabling or removing vulnerable elements

Organization for Standardization (ISO)/IEC 15408-1:2022[8] common criteria series fact model, represented in Figure 3. The fact model is used in ICS/IT cybersecurity courses. The vulnerability category concepts we've discussed can be integrated into this framework, and so can be included when the fact model is presented. Vulnerabilities would be associated within a parent block called *weaknesses* (i.e., MITRE CWE), *countermeasures, and mitigations* would be included in the "mitigations" block, and tactics and techniques associated with the MITRE ATT&CK[9] framework could be embedded in the "threat agents" and "threats" blocks.

These slight adjustments to the ISO/IEC 15408-1:2022 common criteria series fact model support the current nomenclature of the MITRE frameworks and may enhance communication of the risk management process among the ICS/OT community.

Special Interest Group on Security of ICS/OT Systems

Extensive work has been done on identifying and classifying security weaknesses of hardware and software, or IT in general. Yet, the IT classifications are not always sufficient for describing or managing vulnerabilities observed in ICS/OT, as the security threats these systems experience can be different from those of IT systems.

In partnership with the DoE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the CWE/CAPEC program—operated by the Cybersecurity and Infrastructure Security Agency-funded Homeland Security Systems Engineering and Development Institute—created a new special interest group (SIG) focusing on security weaknesses in ICS and OT: the CWE-CAPEC ICS/OT SIG.

This SIG aims to share information and experience on security

Table 3. Linkage from example CWE to cybersecurity maturity assessment frameworks.

CWE Identifier	Member Of TPT-NCSV Category	DoE C2M2 Objective	ISA/IEC 62443-3-2 Reference	Manufacturing ISAC ORF
CWE 1372 OT Counterfeit and malicious corruption	ICS supply chain	Third-party risk management: Managing third-party risk	ISA/IEC 62443-4-2: Technical security requirements for IACS components	ID 4.1 Delivery objectives: Service dependencies

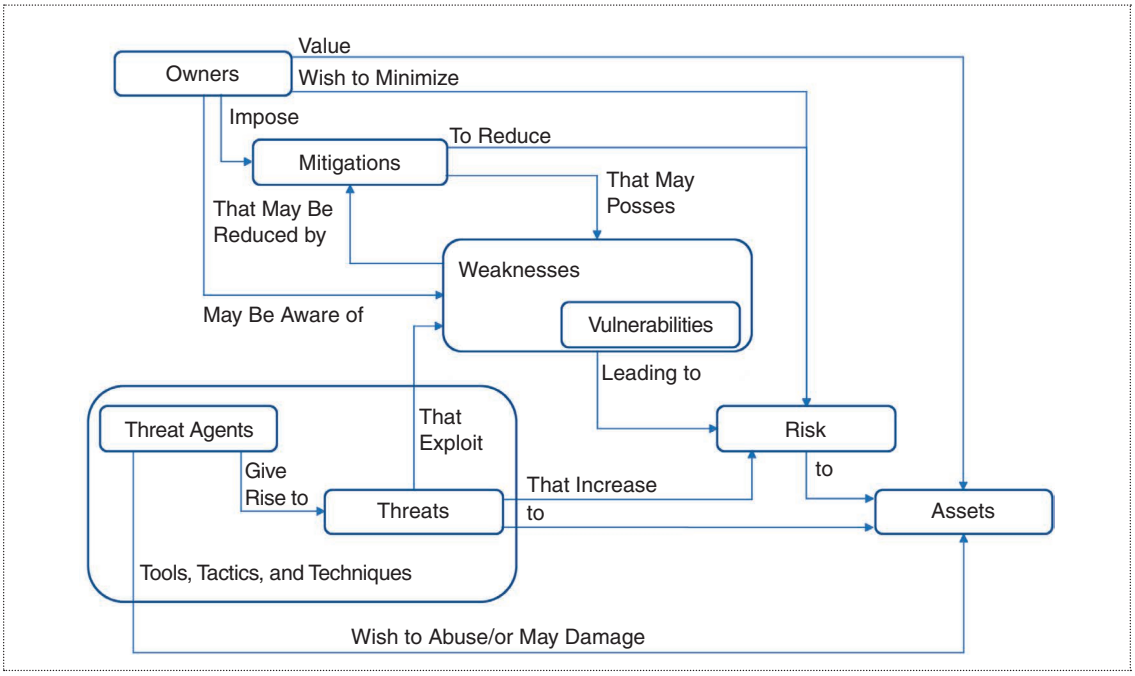

Figure 3. MITRE framework associated ISO/IEC 15408-1:2022 common criteria series fact model.

threats of ICS/OT, adopt a common CWE language to discuss and disclose ICS/OT security vulnerabilities, and promote a forward-facing cyber-informed engineering strategy[10] that keeps security at the forefront while designing critical ICS/OT systems. The SIG will provide a common platform to all stakeholders for efficiently and effectively communicating while promoting unity of effort in identifying and mitigating ICS/OT security weaknesses. Stakeholders of this SIG include (but are not limited to) ICS/OT vulnerability researchers, engineers, security professionals, and companies representing OEMs/system integrators, tools/infrastructure vendors, and asset owners and operators. The authors of this column are members of the Cyber Manufacturing Innovation Institute and are contributing leadership and subject matter experts to the SIG, ensuring that the particular needs for awareness by small- and medium-scale manufacturers are considered.

The initial meeting of the SIG was held on 18 May 2022. The tentative plan for the SIG is to continue to meet monthly to complete the work of integrating the TPT material into CWE, and other related efforts as needed. Contributing to the SIG is an emphasized activity of the Cyber Manufacturing Innovation Institute, members of which led and contributed to the TPT-NCSV, proposed development of the SIG, and are contributing to its management.

The SIG welcomes the participation of all stakeholders. Anyone interested in participation should contact Greg Shannon, at gregory.shannon@cymanii.org.

With increasing awareness of the threat that cyber-based attacks have on ICSs and the operational technology upon which they depend, the U.S. Congress directed the DoE to identify areas of weakness, with the objective of improving the ability of equipment manufacturers and owners/operators of ICS to focus on areas of security need. Policy decisions led to this congressional directive, but it was surely policy that was triggered in part from studies, reports, and briefings performed by experts on cybersecurity in energy systems. The congressional mandate led to a study executed by members of the security and privacy technical community.

This study:

- demonstrated (and achieved multistakeholder agreement) that a gap in vulnerability descriptions does exist; IT frameworks do not cover all things OT
- demonstrated that ICS weaknesses could be described and categorized to produce a hierarchical taxonomy, usefully enabling deeper analysis
- demonstrated that OT content could be appended to IT framework; this bodes well for creating a consolidated body of knowledge for IT and OT weaknesses, which will support forthcoming IT-OT convergence use cases
- raises the potential for exploration of similar action in other frameworks: for example, just as categories of OT vulnerabilities are being integrated into CWE, so might observed OT vulnerabilities be integrated in the MITRE CVE framework and OT exploits be integrated into MITRE's CAPEC framework.

Their report to Congress led to establishment of a SIG affiliated with DoE and DHS cybersecurity offices, whose role is to build on the earlier efforts of identifying and classifying security weaknesses in ICS/OT systems.

The sequence of activities highlights one way that technical experts can collaborate/cooperate with policy makers to advance policy by giving it specifics and filling gaps of technical knowledge to improve security of resilience of critical infrastructure simultaneously. ■

Acknowledgment

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Advanced Manufacturing Office Award Number DE-EE0009046. The views expressed herein do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

References

1. "Common weakness enumeration," MITRE, McLean, VA, USA, Oct. 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://cwe.mitre.org
2. "Categories of security vulnerabilities in ICS," U.S. Department of Energy, Washington, DC, USA, Mar. 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf
3. "Common vulnerability enumeration program mission," U.S. Department of Homeland Security, Washington, DC, USA, Dec. 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://www.cve.org
4. "Guidelines for new content suggestions," MITRE, McLean, VA, USA, Sep. 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://cwe.mitre.org/community/submissions/guidelines.html
5. "ISA/IEC 62443 series of standards," International Society of Automation, Research Triangle Park, NC, USA, 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
6. "Operational resilience framework v1.0 released for use in

strengthening business continuity," Manufacturing Information Sharing and Analysis Center, Herndon, VA, USA, Nov. 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://www.mfgisac.org/news/operational-resilience-framework-v10-released-for-use-in-strengthening-business-continuity
7. "Cybersecurity capability maturity model (C2M2)," U.S. Department of Energy, Washington, DC, USA, 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
8. *Information Technology—Security Techniques--Evaluation Criteria for IT Security — Part 1*, ISO/IEC 15408-1:2022, International Organization for Standardization, Geneva, Switzerland, 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://www.iso.org/standard/72891.html
9. "ATT&CK," MITRE, McLean, VA, USA, 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://attack.mitre.org
10. "Consequence-driven cyber-informed engineering," Idaho National Laboratory, Idaho Falls, ID, USA, 2022. Accessed: Dec. 1, 2022. [Online]. Available: https://inl.gov/cce/

David M. Nicol is the Herman M. Dieckamp Endowed Chair in Engineering, Department of Electrical and Computer Engineering, at the University of Illinois at Urbana–Champaign, Champaign, IL 61820 USA, and the director of the Information Trust Institute. He is vice president for Securing Automation of the Cyber Manufacturing Innovation Institute, San Antonio, TX 78249 USA. His research interests are in system level analysis of security in critical infrastructure systems. Nicol received a Ph.D. in computer science from the University of Virginia. He served as editor-in-chief of *IEEE Security & Privacy* (2018–2021) and is a Fellow of IEEE. Contact him at (dmnicole@illinois.edu).

Gregory Shannon is the chief cybersecurity scientist in the National and Homeland Security Directorate of the Idaho National Laboratory, Idaho Falls, ID 83415 USA, and is the chief security officer of the Cyber Manufacturing Innovation Institute, San Antonio, TX 78249 USA. His research interests include high assurance security and resilience. Shannon received a Ph.D. in computer science from Purdue University. He served for a decade as the chief scientist for the Computer Emergency Readiness Team, during which time he did a tour in the White House Office of Science and Technology Policy as the Assistant Director for Cybersecurity strategy. He is a Senior Member of IEEE. Contact him at gregory.shannon@cymanii.org.

Monika Akbar is an assistant professor of Computer Science at the University of Texas at El Paso, El Paso, TX 79968 USA. Her research interests include machine learning, cybersecurity, and educational games. Akbar received a Ph.D. in computer science from Virginia Technical University. She leads the Cyber Manufacturing Innovation Institute participation in MITRE's Common Weakness Enumeration-Common Attack Pattern Enumeration and Classification Industrial Control Systems/Operational Technology Special Interest Group. She is a Member of IEEE. Contact her at makbar@utep.edu.

Matt Bishop is a professor of Computer Science at the University of California, Davis, Davis, CA 95616 USA. His research interests are vulnerability analysis and cybersecurity. Bishop received a Ph.D. in computer science from Purdue University. He has also worked extensively on the security of various forms of the UNIX operating system. He is a charter member of the Colloquium for Information Systems Security Education. His *textbook, Computer Security: Art and Science,* was published by Addison-Wesley in December 2002. Contact him at mabishop@usdavis.edu.

Michael Chaney is a program manager at Idaho National Laboratory (INL), Idaho Falls, ID 83415 USA. He currently serves in a leadership role within INL's office of Infrastructure Assurance and Analysis in the National & Homeland Security directorate. He facilitates the partnership between INL and Department of Homeland Security's Cybersecurity and Infrastructure Security Agency by coordinating INL support to mission critical processes across Cybersecurity and Infrastructure Security Agency components and branches. His research focus is on cybersecurity of critical infrastructure. Chaney received an M.S. in computer science from George Washington University. He is a Member of IEEE. Contact him at michael.chaney@inl.gov.

Matthew Luallen is a lead research scientist in the Information Trust Institute, the University of Illinois, Urbana–Champaign, Champaign, IL 61820 USA. He has an extensive background in startups, cyberphysical security, assessments, education, and innovation, and leads the Cyber Vulnerability Awareness activity at the Cyber Manufacturing Innovation Institute, San Antonio, TX 78249 USA. His research Interests include cyberphysical security, artificial intelligence/machine learning security and simplification, and education. Luallen received an M.S. from National Technical University. He is a Member of IEEE. Contact him at luallen@illinois.edu.