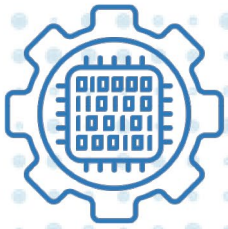


Cyber-Informed Engineering

Cyber-Informed Engineering (CIE) Guidance to Defeat Systematic Operational Technology Weaknesses

September 30, 2024

Authors:

Matthew Luallen
University of Illinois Urbana-Champaign

Dominic Saebeler
University of Illinois Urbana-Champaign

David Emmerich
University of Illinois Urbana-Champaign

Casey O'Brien
University of Illinois Urbana-Champaign

Edmond Rogers
University of Illinois Urbana-Champaign

INL/MIS-24-81691-Rev000

Cyber-Informed Engineering (CIE) Program activities are sponsored by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) and performed by Idaho National Laboratory and the National Renewable Energy Laboratory.

The authors of this report acknowledge and appreciate the sponsorship of the CIE Program partners and the contributions from the CIE Community of Practice (COP) members.

Contents

1. Introduction

1.1. Background and Context

As industrial automation and control systems increasingly integrate digital technologies, the security of Operational Technology (OT) environments remains a critical concern. The convergence of Information Technology (IT) and OT has exposed these systems to a wide range of cyber threats that could potentially disrupt essential services and processes. In a formidable attempt to address these vulnerabilities, the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER)'s Securing Energy Infrastructure Executive Task Force[1] (SEI-ETF) was established through the National Defense Authorization Act (NDAA) of 2020, specifically under Section 5726. This section mandated the creation of a task force to identify protections to the United States' energy infrastructure from cyber threats and attacks. The SEI-ETF brought together experts across various sectors, including energy asset owners, government agencies, DOE National Laboratories, research and academic institutions, and manufacturers, to identify risk mitigation enhancements of the cybersecurity of Industrial Control Systems (ICS).

1.2. Mapping SEI-ETF Vulnerabilities to MITRE CWE

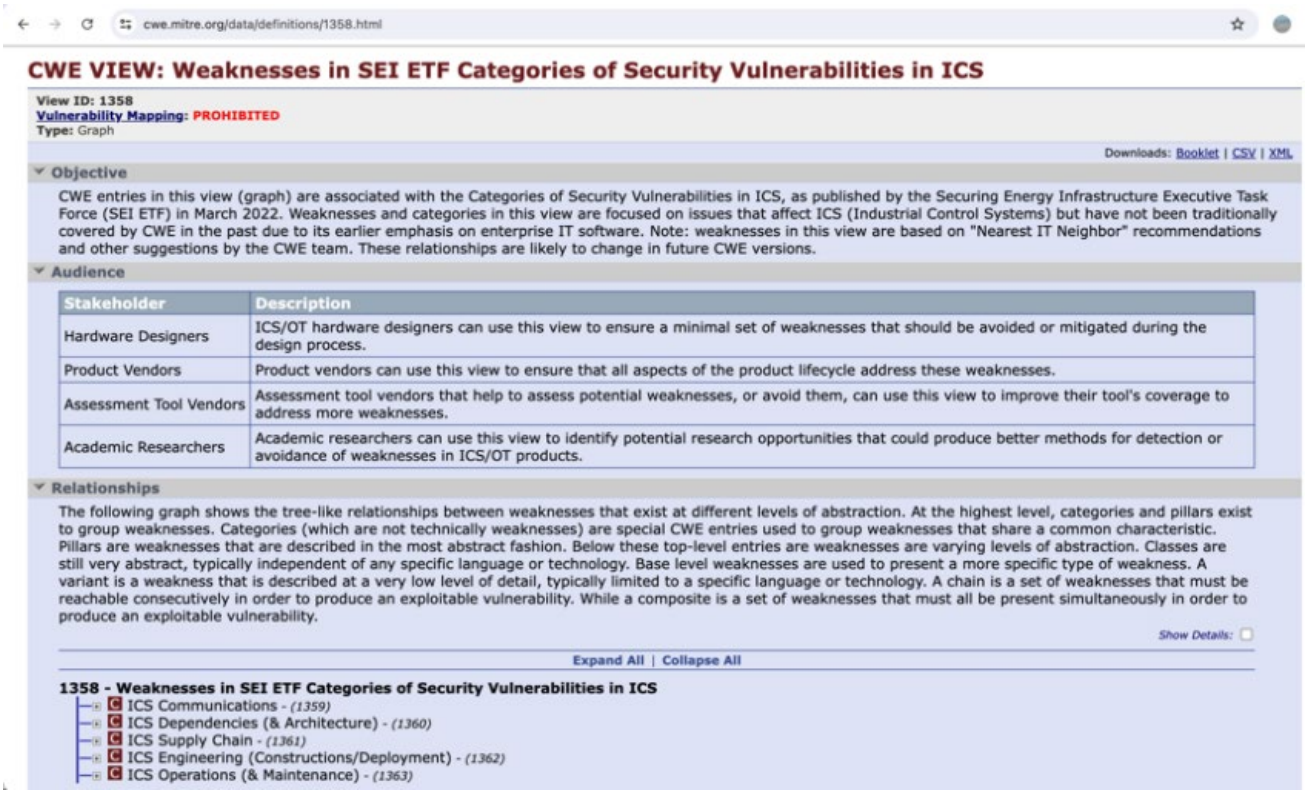
The SEI-ETF task force developed a whitepaper[2] that categorized key security vulnerabilities in ICS, providing a foundation for understanding the types of systematic threats OT systems face. Building on the foundational work of the SEI-ETF, the MITRE Common Weakness Enumerations (CWE)[3] catalog was further enriched through the contributions of over 200 academics, professionals, and researchers through the CWE ICS/OT Special Interest Group (SIG).[4] These experts worked collaboratively to integrate SEI-ETF contextual references into select CWEs, thereby providing a more comprehensive understanding of OT vulnerabilities through the attributable weaknesses.

---

[1] U.S. Department of Energy. Securing Energy Infrastructure Executive Task Force . Accessed September 28, 2024. https://www.energy.gov/ceser/securing-energy-infrastructure-executive-task-force.
[2] U.S. Department of Energy. Categories of security vulnerabilities in ICS, March 9, 2022. https://secureenergy.inl.gov/secureenergy/wp-content/uploads/2022/11/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf.
[3] MITRE. "Common Weakness Enumeration: A Community-Developed List of SW & HW Weaknesses That Can Become Vulnerabilities." Common Weakness Enumeration, 2006. https://cwe.mitre.org/.
[4] Cwe-Capec. "CWE-CAPEC/ICS-OT_SIG: A Repository Dedicated to the Activity of the CWE-Capec ICS/OT Special Interest Group." GitHub, 2022. https://github.com/CWE-CAPEC/ICS-OT_SIG.

The comprehensive SEI-ETF and MITRE CWE efforts are captured in MITRE CWE View 1358[5] (as shown in Figure 1), which catalogs specific weaknesses in IT and OT software and hardware that adversaries can exploit and further presents associated mitigation strategies. Many of the CWEs identified in the SEI-ETF work were broad based design weaknesses and as a result did not easily reduce to coding vulnerabilities.

Figure 1. MITRE CWE View 1358 SEI-ETF Categories of Security Vulnerabilities in ICS



1.3. Relevance of Cyber-Informed Engineering (CIE) Principles

The Idaho National Laboratory (INL) published (August 7, 2023) Cyber Informed Engineering (CIE) Implementation Guide[6] principles provide a practical framework for integrating cybersecurity considerations into the engineering processes and Original Equipment Manufacturers (OEM)s supporting OT systems. The 12 CIE principles, as detailed in the CIE Implementation Guide, emphasize various aspects of system design and operation, including consequence-focused design, secure information architecture, and engineered controls. These principles should assist OEM leadership, engineers and

[5] MITRE. "CWE VIEW: Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS." CWE, March 9, 2022. https://cwe.mitre.org/data/definitions/1358.html.
[6] Idaho National Laboratory. Cyber-Informed Engineering Implementation Guide, August 7, 2023. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf.

technicians to more clearly understand and address cyber risks, thereby enhancing the resilience of customer OT systems against potential cyber threats. A series of supplementary questions are presented with each principle to create context for those leveraging these principles in implementing mitigation actions.

Addressing those CIE supplementary questions will strengthen the resilience of OEM engineered systems against cyber-attacks. Further, systematically cross-referencing CIE with MITRE's Common Weaknesses Enumerations (CWEs), based upon the SEI-ETF task force's effort, against active engineering processes can significantly enhance the security posture of systems. By aligning identified threats and their potential impacts with the engineering design process at an earlier stage, OEMs can proactively address vulnerabilities categorized by their weaknesses. This approach attempts to embed cybersecurity considerations within the design phase, leveraging the application of CIE in combination with existing standards and guidelines to create a more resilient engineering process.

1.4. Focus and Intention of This Whitepaper

This research summary describes the process through which the University of Illinois, Information Trust Institute (ITI)'s research team evaluated whether the application of the 12 CIE Principles, when used as a methodology, could diminish or eliminate the presence of the SEI-ETF-identified weaknesses in engineered systems. The conclusion of ITI's research team evaluation does indicate that application of CIE principles to the weaknesses in MITRE CWE View 1358 has the potential to diminish or eliminate the presence of those weaknesses. However, there were some instances where a match was not as conclusive, and several important considerations are identified when attempting to apply CIE to CWE factors. It is also important to note that the role of the individual and the perspective of those applying the principles has a significant impact on principle alignment selection, actions taken, and outcomes expected. For example, the perspective of an OEM versus that of a customer will drive different priorities and CIE principle selections as well as any resulting mitigation implementation(s). For consistency purposes, the results of our research should be interpreted as coming from the perspective of an OEM. Additionally, the process and breadth of participation among organizational decision makers will impact the ability of each to effectively implement those actions that will ultimately diminish the presence of identified weaknesses.

2. Methodology, Findings, and Example CIE Questions

Securing OT and critical infrastructure against cyber-attacks requires a methodical and proactive approach. This section presents findings that resulted from applying CIE principles to address vulnerabilities categorized by the weaknesses identified in MITRE's CWE View 1358, focusing on how these principles can be effectively utilized by OEMs. By systematically aligning prominent CIE principles with key weaknesses, the resulting analysis provides guidance on how to address common vulnerabilities in OT systems. The following discussion highlights the outcomes of the ITI team's research, including examination and characterization of specific CWEs and identified alignment with relevant CIE principles, and a demonstration of how these principles can be applied to enhance security throughout the system lifecycle. This section provides insights into how an OEM could adopt CIE principles to strengthen their cybersecurity defenses and reduce potential risks in critical infrastructure environments.

2.1. Methodology to Address MITRE CWEs (SEI-ETF Vulnerabilities) with CIE Principles

This section provides an in-depth analysis of the ITI research team's application of CIE principles to specific OT weaknesses, through the lens of an OEM, with a particular focus on addressing and mitigating weaknesses associated with MITRE CWE View 1358, developed as an outcome of the SEI-ETF task force. Twenty (20) specific OT weaknesses were highlighted as common vulnerabilities often encountered in cyber-physical systems, critical infrastructure, and software, necessitating a strong, proactive defense mechanism throughout the system's lifecycle.

The ITI research team thoroughly reviewed CWE descriptions of each of the twenty OT system's exploitable weaknesses, utilizing the CWE-1358 view, which emphasizes securing operational technologies and critical infrastructure from cyber-attacks. By systematically reviewing those twenty (20) weaknesses in conjunction with the CIE Implementation guide, the research team was able to analyze and match one key principle from the CIE Implementation Guide to each CWE.

The first level of analysis began with the entire team of five ITI researchers performing a joint evaluation of three specific weaknesses. Those weaknesses were: Maker Breaker Blindness (CWE-1374), External Physical Systems (CWE-1367), and Frail Security in Protocol (CWE-1366). The collaborative selection process initially led to different outcomes from each researcher. However, after active discussion, agreement was reached on a combined choice of principle to CIE weakness alignment. Following the combined analysis of the first three identified weaknesses, the ITI research team

separated and for the remaining seventeen (17) SEI-ETF identified weaknesses, each research team member did an independent evaluation and then selected their individually determined primary CIE principle for alignment with each of the identified CWE weaknesses.

The resulting data set depicts an individually selected primary CIE principle for each CWE as shown in Table 1. Allocation of CIE Principle with Greatest Alignment to Address Weakness. The results indicate that there are disparities among the choice of the primary CIE principle, as some of the CWEs had a wider consensus, while others just barely had enough similarity to select a prominent CWE. None of the CWEs had the same Principle selected by all five researchers. This is important to recognize, as we encourage OEMs to go through a similar exercise while exploring adopting CIE.

After selecting the primary (or prominent) CIE principle for each CWE, the research team categorized the CWEs by the CIE principle and combined the supporting rationale among the researchers as to why the principle was selected, see Table 2. SEI-ETF to CWE to CIE Principe Rationale. This effort supported the selection of 7 of the 12 CIE principles for addressing MITRE CWE 1358 view in respect to OEMs.

Next, the research team selected each CWE category, aligned with the 7 CIE principles and identified several questions to serve as examples of applying the CIE Implementation Guide's questions. This is not an exact science and as indicated earlier, the research team found that three elements contributed to varying answers: the background and prior experiences of each researcher, the role or perspective from which each answered the question for (OEM in this case), as well as the phase of the OT system's lifecycle.

The following pages present the tables mentioned earlier, along with the selected CIE principle questions aligned with each CWE. These are paired with potential interpretations from the perspective of an OEM, providing practical insights into how these principles can be applied in real-world scenarios.

2.2. Findings and Example CIE Questions

The following list outlines the resulting seven key principles from the CIE framework, each addressing specific weaknesses identified in the MITRE CWE View 1358. These common principles provide a structured approach for mitigating security risks in ICS and OT. Each principle is associated with several CWEs, which highlight critical areas of concern for system security. By aligning these CWEs with the corresponding CIE principles, OEMs can develop more robust security strategies throughout the system lifecycle. The list below details each principle and its associated CWEs, and follow-on

sections use this list to apply questions from the CIE Implementation Guide to help to address weaknesses from the perspective of an OEM.

- **CIE Principle 1: Consequence-Focused Design** (CWE-1374: Maker Breaker Blindness, CWE-1376: Insufficient Commissioning of Security Controls, CWE-1377: Inherent Predictability in Design, CWE-1373: ICS Engineering (Construction/Deployment): Trust Model Problems
- **CIE Principle 9: Cyber-Secure Supply Chain Controls** (CWE-1372: OT Counterfeit and Malicious Corruption, CWE-1369: IT/OT Convergence/Expansion, CWE-1370: Common Mode Frailties)
- **CIE Principle 8: Digital Asset Awareness** (CWE-1371: Poorly Documented or Undocumented Features, CWE-1382: Emerging Energy Technologies, CWE-1383: Failure to Comply with Regulatory Requirements)
- **CIE Principle 7: Interdependency Evaluation** (CWE-1367: External Physical Systems, CWE-1368: External Digital Systems)
- **CIE Principle 12: Organizational Culture** (CWE-1379: Human Factors in ICS Environments, CWE-1380: Post-Analysis Changes, CWE-1378: Gaps in Obligations and Training, CWE-1381: Exploitable Standard Operational Procedures, CWE-1383: Failure to Comply with Regulatory Requirements)
- **CIE Principle 10: Planned Resilience** (CWE-1365: Unreliability)
- **CIE Principle 3: Secure Information Architecture** (CWE-1366: Frail Security in Protocols, CWE-1364: Zone Boundary Failures)

Table 1. Allocation of CIE Principle with Greatest Alignment to Address Weakness

SEI-ETF	CWE	Researcher 1	Researcher 2	Researcher 3	Researcher 4	Researcher 5	Prominent
Maker Breaker Blindness	1374			Consequence-Focused Design[7]			Consequence-Focused Design
External Physical Systems	1367			Interdependency Evaluation[1]			Interdependency Evaluation
Frail Security in Protocols	1366			Secure Information Architecture[1]			Secure Information Architecture
Human Factors in ICS Environments	1379	Organizational Culture	Organizational Culture	Organizational Culture	Design Simplification	Organizational Culture	Organizational Culture
Zone Boundary Failures	1364	Engineered Controls	Secure Information Architecture	Secure Information Architecture	Secure Information Architecture	Active Defense	Secure Information Architecture
OT Counterfeit and Malicious Corruption	1372	Cyber-Secure Supply Chain Controls	Digital Asset Awareness	Digital Asset Awareness	Cyber-Secure Supply Chain Controls	Cyber-Secure Supply Chain Controls	Cyber-Secure Supply Chain Controls
Security Gaps in Commissioning	1376	Engineered Controls	Consequence-Focused Design	Consequence-Focused Design	Digital Asset Awareness	Interdependency Evaluation	Consequence-Focused Design
Gaps in Obligations and Training	1378	Organizational Culture	Organizational Culture	Organizational Culture	Organizational Culture	Engineering Information Control	Organizational Culture
Exploitable Standard Operational Procedures	1381	Interdependency Evaluation	Organizational Culture	Organizational Culture	Organizational Culture	Engineering Information Control	Organizational Culture
Post-analysis Changes	1380	Organizational Culture	Organizational Culture	Consequence-Focused Design	Organizational Culture	Consequence-Focused Design	Organizational Culture
Emerging Energy Technologies	1382	Resilient Layered Defenses	Interdependency Evaluation	Digital Asset Awareness	Digital Asset Awareness	Interdependency Evaluation	Digital Asset Awareness
Compliance/Conformance with Regulatory Requirements	1383	Interdependency Evaluation	Organizational Culture	Organizational Culture	Organizational Culture	Digital Asset Awareness	Organizational Culture
Unreliability	1365	Planned Resilience	Planned Resilience	Planned Resilience	Planned Resilience	Interdependency Evaluation	Planned Resilience
External Digital Systems	1368	Digital Asset Awareness	Interdependency Evaluation	Interdependency Evaluation	Digital Asset Awareness	Design Simplification	Interdependency Evaluation
IT/OT Convergence/Expansion	1369	Design Simplification	Cyber-Secure Supply Chain Controls	Engineered Controls	Cyber-Secure Supply Chain Controls	Interdependency Evaluation	Cyber-Secure Supply Chain Controls
Common Mode Frailties	1370	Cyber-Secure Supply Chain Controls	Digital Asset Awareness	Cyber-Secure Supply Chain Controls	Cyber-Secure Supply Chain Controls	Resilient Layered Defenses	Cyber-Secure Supply Chain Controls

[7] The selection of the CIE principle was performed as group to establish the process of independent selection.

SEI-ETF	CWE	Researcher 1	Researcher 2	Researcher 3	Researcher 4	Researcher 5	Prominent
Poorly Documented or Undocumented Features	1371	Consequence-Focused Design	Digital Asset Awareness	Consequence-Focused Design	Digital Asset Awareness	Engineering Information Control	Digital Asset Awareness
Trust Model Problems	1373	Engineered Controls	Consequence-Focused Design	Engineered Controls	Consequence-Focused Design	Planned Resilience	Consequence-Focused Design
Gaps in Details/Data	1375	Digital Asset Awareness	Digital Asset Awareness	Engineering Information Control	Digital Asset Awareness	Engineered Controls	Digital Asset Awareness
Inherent Predictability	1377	Consequence-Focused Design	Consequence-Focused Design	Engineered Controls	Consequence-Focused Design	Active Defense	Consequence-Focused Design

Table 2. SEI-ETF to CWE to CIE Principe Rationale

SEI-ETF	CWE	Prominent Choice	Rationale
Maker Breaker Blindness	1374	Consequence-Focused Design	The **Consequence-Focused Design** principle serves a cornerstone for mitigating weaknesses such as Maker Breaker Blindness, Security Gaps in Commissioning, Inherent Predictability, and Trust Model Problems because it pushes OEM engineers to proactively identify and address potential cyber threats and operational weaknesses from the outset, facilitating that security is integrated into the system lifecycle through both digital and physical controls.
Security Gaps in Commissioning	1376		
Inherent Predictability	1377		
Trust Model Problems	1373		
OT Counterfeit and Malicious Corruption	1372	Cyber-Secure Supply Chain Controls	The **Cyber-Secure Supply Chain Controls** principle is crucial for mitigating weaknesses such as OT Counterfeit and Malicious Corruption, IT/OT Convergence/Expansion, and Common Mode Frailties by supporting that all components introduced into ICS systems are verified, tested, and monitored by the OEM to prevent counterfeit, faulty, or insecure components from introducing vulnerabilities that could affect the entire system.
IT/OT Convergence/Expansion	1369		
Common Mode Frailties	1370		
Poorly Documented or Undocumented Features	1371	Digital Asset Awareness	The **Digital Asset Awareness** principle is essential for addressing weaknesses like Common Mode Frailties, Poorly Documented or Undocumented Features, and Emerging Energy Technologies by promoting a thorough understanding of all digital assets, their functions, and interactions, thus allowing OEMs to identify hidden risks, manage potential points of failure, and integrate new technologies more securely before delivery to customer.
Emerging Energy Technologies	1382		
Gaps in Details/Data	1375		
External Physical Systems	1367	Interdependency Evaluation	The **Interdependency Evaluation** principle is vital for addressing weaknesses like External Physical Systems and External Digital Systems by identifying and mapping out the relationships between ICS and external systems, allowing OEM engineers to anticipate risks and implement strategies like redundancy or safeguards to maintain operational integrity during failures or compromises in support of their customers.
External Digital Systems	1368		
Human Factors in ICS Environments	1379	Organizational Culture	The **Organizational Culture** principle is critical for addressing weaknesses such as Human Factors in ICS Environments, Post-analysis Changes, Gaps in Obligations and Training, and Exploitable Standard Operational Procedures by fostering a culture of security awareness, accountability, and continuous improvement, ensuring all employees, from the top leadership down and from the ground up, are engaged in maintaining security, managing change effectively, and closing gaps in responsibilities and training. The culture serves as the mainstay in promoting secure products and their delivery and operational lifecycle support.
Post-analysis Changes	1380		
Gaps in Obligations and Training	1378		
Exploitable Standard Operational Procedures	1381		
Compliance/Conformance with Regulatory Requirements	1383		
Unreliability	1365	Planned Resilience	The **Planned Resilience** principle is essential for addressing weaknesses like Unreliability by promoting that ICS systems are designed to anticipate both physical and cyber disruptions, incorporating redundancy, failover mechanisms, and OEM guided incident response plans that allow for continuous operation or swift recovery, minimizing downtime and maintaining system security and reliability.
Frail Security in Protocols	1366	Secure Information Architecture	The **Secure Information Architecture** principle is critical for addressing weaknesses like Frail Security in Protocols and Zone Boundary Failures by promoting building data integrity and proper boundary protections into the system from the beginning by the OEMs, specifically for critical functions while being guided by Consequence-Focused Design.
Zone Boundary Failures	1364		

The following questions contained within each CWE sub-category, aligned by the most prominently selected CIE Principle among the researchers in this study, are answered from the OEM perspective. It is anticipated that a customer or end user operator would likely answer these questions differently when considering many potential variables. The team felt that presenting responses to each question would create context as well as an example of how one might think through an individual response.

2.2.1 PRINCIPLE 1. CONSEQUENCE-FOCUSED DESIGN PRINCIPLE

The Consequence-Focused Design principle serves as a cornerstone for addressing weaknesses such as CWE-1374: Maker Breaker Blindness, CWE-1376: Security Gaps in Commissioning, CWE-1377: Inherent Predictability, and CWE-1373: Trust Model Problems because it pushes OEM engineers to proactively identify and address potential cyber threats and operational weaknesses from the outset, facilitating security integrations into the system lifecycle through both digital and physical controls.

CWE-1374, also known as "Maker Breaker Blindness," refers to the failure to recognize or address the potential for a system to be misused or subverted by an adversary. Here are two questions from CIE Principle 1: Consequence-Focused Design that helps to address this weakness.

1. **What are the consequences that could result from a failure or unexpected operation of the system's critical functions?**
    - As an OEM, understanding the consequences of a system's critical functions failing or operating unexpectedly may also help in identifying potential misuse scenarios. For instance, if a vibration monitoring system fails to detect an overworn bearing in a turbine generator, either due to Mean Time Between Failure (MTBF) or a misattribution to MTBF, it could lead to equipment damage and production loss. It is important as an OEM, to understand that an adversary may take advantage of inaccurate engineering assumptions while also attempt to misattribute a cyber-attack to common failure modes.

2. **What specific consequence mitigations depend on the software/hardware/facility/process element under development and construction?**
    - During the development phase, an OEM may focus on how the design and development of each component can address the consequences it introduces. This includes verifying the component's consequence mitigation capability to better enable a design outcome more likely to

handle potential misuse scenarios. The selection process of a software mitigation detecting adverse pressure levels versus an engineered control using hardware such as relief valves are very different approaches, and the OEM should analyze which choice to make.

CWE-1376 refers to "Security Gaps in Commissioning," which highlights the gaps in the validation that security controls are properly implemented and functioning as intended even during the engineering and construction phases of the project. Here are two questions from CIE Principle 1: Consequence-Focused Design that helps to address this weakness.

1. **What are the unacceptable high consequence events that impact mission delivery, safety, security, the environment, equipment and property, financials, or corporate reputation?**
    - The impact to corporate reputation and therefore financials would be very high if a malfunctioning of a system was attributed to a lack of awareness of security gaps during system commissioning. By identifying and documenting high consequence events, an OEM can focus on critical areas of their products and business that need robust security during the commissioning phase of a project. For instance, if a high consequence event is the malfunctioning of a water treatment chemical dosing control system, the OEM can prioritize rigorous testing and validation of security controls in that system before, during and after commissioning.

2. **How are identified high consequence events documented, monitored for change, and reassessed?**
    - Continuous monitoring and reassessment of customer-facing, high consequence events allow an OEM to adapt to new threats and vulnerabilities. For example, if a new type of cyber threat emerges that could impact a critical component, the OEM can update the security controls and associated commissioning processes to address this new risk. For instance, an adversary may be attempting to compromise assets while in transit to construction sites, an OEM can provide the customer with a checklist and procedures to perform to validate the component is received intact and unadjusted.

CWE-1377, "Inherent Predictability in Design," refers to the risk that predictable patterns in system design can be exploited by adversaries. Here are two questions from CIE Principle 1: Consequence-Focused Design that helps to address this weakness.

1. **What anticipated changes, modifications, or upgrades could alter the consequences of system failure, misuse, or compromise?**
    - Changes like new software updates, shifts in architecture, or integration of new devices could introduce predictable patterns in the system, increasing the risk of exploitation. OEMs can address these risks by designing flexible systems and employing dynamic updates that minimize predictability while balancing with maintaining reliability and resiliency, reducing the chances that a single attack method can be applied at scale.
2. **What high-impact consequences could be initiated by a failure to perform maintenance correctly or at the right interval?**
    - Inconsistent or poorly timed maintenance could increase system vulnerability by allowing adversaries to predict downtime and exploit outdated software. This could lead to system-wide failures, operational disruptions, or even safety incidents, especially if critical vulnerabilities remain unaddressed through direct hardware, software and firmware updates or using compensating controls during routine maintenance intervals.

CWE-1373, "Trust Model Problems," addresses issues arising from assumptions made about systems and users during the design or construction phase, which may lead to vulnerabilities if users operate the system differently than intended. Here is a question from CIE Principle 1: Consequence-Focused Design that helps to address this weakness.

1. **What are the critical components and subcomponents of the system design?**
    - By identifying critical components and potential consequences, an OEM can design systems that account for different user behaviors and security approaches, reducing the risk of trust model problems. For example, if a critical function is remote access to a control system, the OEM can implement solutions such as multi-factor authentication, user behavior monitoring to address potential misuse, and even operator-managed physical disconnects of the remote access medium.

2.2.2 PRINCIPLE 9: CYBER-SECURE SUPPLY CHAIN CONTROLS

The Cyber-Secure Supply Chain Controls principle is crucial for addressing weaknesses such as CWE-1372: OT Counterfeit and Malicious Corruption, CWE-1369: IT/OT Convergence/Expansion, and CWE-1370: Common Mode Frailties by supporting that all components introduced into ICS systems are verified, tested, and monitored by the

OEM to prevent counterfeit, faulty, or insecure components from introducing vulnerabilities that could affect the entire system.

CWE-1372, "OT Counterfeit and Malicious Corruption," involves weaknesses related to the supply chain of OT components, where counterfeit or maliciously corrupted components can be introduced. Here are two questions from CIE Principle 9: Cyber-Secure Supply Chain Controls that helps to address this weakness.

1. **For services critical to the functionality of the system under design, what additional contract requirements, beyond the normal baseline, should be defined for security, performance, and verification relating to the desired services?**
    - As an OEM, implement a rigorous vendor assessment process that includes verifying the authenticity and security of components through detailed documentation and compliance checks leveraging tools such as a Software Bill of Materials (SBOMs) and Hardware Bill of Materials (HBOMs). This helps to identify and address any counterfeit or maliciously corrupted components before they are integrated into the system.

2. **Does the design include critical functions dependent on components with high supply chain risks?**
    - Identifying multiple sources for critical components helps to avoid reliance on a single supplier, which can be a vector for counterfeit or maliciously corrupted components. This has historically been identified as monoculture of services that leads to a broad impact by compromising one entity. For instance, an OEM may establish relationships with multiple suppliers for key, validated components, thereby reducing the risk of supply chain disruptions and if a supplier is compromised others can fulfill the demand.

CWE-1369, “IT/OT Convergence/Expansion,” refers to the challenges and vulnerabilities that arise when integrating IT systems with OT systems. This convergence can introduce new attack vectors and complexities in managing security across both domains. Here are two questions from CIE Principle 9: Cyber-Secure Supply Chain Controls that helps to address this weakness.

1. **What assumptions have been made about the availability, quality, and security of the products or services that are critical to system functions or to the mitigation of high consequence events?**
    - By addressing this question, an OEM can explicitly define the security, quality, and availability requirements for critical products and services

in their own supplier contracts. For example, did the supply-chain vendor anticipate that the IT component would be used in the way that the OEM is attempting to use it. This helps in managing the risks associated with IT/OT convergence by encouraging that all components meet stringent security standards.

2. **Should any potential engineering controls be reconsidered due to identified supply chain risks?**
    - As an OEM, evaluating whether critical components with high supply chain risks can be eliminated or substituted with lower-risk alternatives such as modifications of engineered controls help in addressing vulnerabilities that may arise from IT/OT integration. This approach encourages that the design remains robust against supply chain disruptions.

CWE-1370, or "Common Mode Frailties," refers to vulnerabilities that arise when multiple systems or components share the same weaknesses, leading to simultaneous failures under certain conditions. Here are two questions from CIE Principle 9: Cyber-Secure Supply Chain Controls that helps to address this weakness.

1. **What kinds of information about product subcomponents and internals (e.g., HBOMs and SBOMs, subcomponent vendors, use of open source) will the organization require for critical system components? What kinds of enumeration are required for external services critical to the system?**
    - An OEM can include contract language with their suppliers and should also anticipate similar language from their customers that requires detailed HBOMs and SBOMs, including the identification of any open-source components, increasing transparency and traceability of subcomponents used in critical products.

2. **Is there a risk that the procurement of critical products and services might be sourced via undesired means (e.g., secondary market, untrusted supplier)?**
    - By framing procurement requirements to specifically exclude components from untrusted sources among features such as specific hardware, software, geography, and other elements, an OEM can attempt to avoid introducing components with unknown vulnerabilities into their supply chain.

2.2.3 PRINCIPLE 8: DIGITAL ASSET AWARENESS

The Digital Asset Awareness principle is essential for addressing weaknesses like CWE-1370: Common Mode Frailties, CWE-1371: Poorly Documented or Undocumented Features, and CWE-382: Emerging Energy Technologies by promoting a thorough understanding of all digital assets, their functions, and interactions, thus allowing OEMs to identify hidden risks, manage potential points of failure, and integrate new technologies more securely before delivery to customer.

CWE-1371, "Poorly Documented or Undocumented Features," refers to the risk associated with features in a system that are not properly documented, leading to potential security vulnerabilities due to lack of awareness and understanding of these features. Here are two questions from CIE Principle 8: Digital Asset Awareness that helps to address this weakness.

1. **How will system tests ensure that delivered digital assets contain the expected hardware, software, and firmware?**
    - By establishing that software and hardware system tests validate the potential of configuration and document discrepancies such as software libraries, physical chipsets and PCB traces, an OEM can address undocumented features by making sure all components are correctly tracked, and any deviations are properly recorded and understood.

2. **What processes ensure that operations and maintenance activities (e.g., changes to software, logic, or configurations) appropriately trigger updates to asset tracking records?**
    - Establishing processes that promote updates to tracking records during the product development life cycle allows an OEM to keep documentation current, addressing the risk of undocumented features by supporting the ability that any changes are promptly and accurately recorded.

CWE-1382 refers to the risk of "Emerging Energy Technologies" being susceptible to adversarial manipulation or control due to insufficient digital asset awareness. Here is a question from CIE Principle 8: Digital Asset Awareness that helps to address this weakness.

1. **Which digital features in a system have the potential to cause critical consequences from unexpected operations or attack, and how can those features be identified during development, procurement, and integration?**
    - By identifying digital features that could be manipulated within emerging energy technologies, an OEM can design systems that include both digital and physical safeguards to address potential misuse scenarios. For instance, in an extreme situation, if a digital control for a Distributed Energy Resource (DER) device could be hacked to cause a solar inverter, wind turbine controller, or battery system to mis-operate, the OEM might incorporate manual override switches that physically dispatched operators can use to maintain power flow until the risk is addressed.

2.2.4 PRINCIPLE 7: INTERDEPENDENCY EVALUATION

The Interdependency Evaluation principle is vital for addressing weaknesses like CWE-1367: External Physical Systems and CWE-1368: External Digital Systems by identifying and mapping out the relationships between ICS and external systems, allowing OEM engineers to anticipate risks and implement strategies like redundancy or safeguards to maintain operational integrity during failures or compromises in support of their customers.

CWE-1367, "External Physical Systems," refers to the risks associated with external physical systems that can impact the security and functionality of a system. Whereas CWE-1368, "External Digital Systems," refers to the risk associated with the improper isolation of shared resources in digital systems, which can lead to unintended interactions and vulnerabilities. Below are three questions from CIE Principle 7: Interdependency Evaluation that help to address the above two weaknesses.

1. **What dependencies does the concepted system have on other regional systems, infrastructures, and services?**
    - An OEM can evaluate the dependency on external power sources for their direct business and for the equipment they manufacture. If the primary power source fails, they can identify backup generators or alternative power supplies to maintain the critical operations of their customers.

Furthermore, the OEM should provide the customer with detailed dependency characteristics of the system and provide guidance of the consequences of losing any of these necessary requirements. This is only a specific example; this is a wide lens question that has many interconnected elements to recognize the risk.

2. **What upstream and downstream dependencies impact resources used to develop the system (e.g., personnel, computing hardware and software, fuels, and other physical supplies)?**
    - An OEM can assess the impact of losing access to a critical software update associated with an active and known exploited vulnerability from an external vendor in the OEM's supply chain. The OEM can develop a plan to source updates from alternative vendors while creating guidance for compensating controls to maintain system functionality. This is only a specific example; this is a wide lens question that has many interconnected elements to recognize the risk.

3. **What inputs do the system's critical functions require that are not directly and completely controlled by the system?**
    - An OEM can identify critical inputs such as external data feeds or third-party services that are essential for system operations such as time. By evaluating alternative sources for these inputs, the OEM can address the risk of dependency on a single external system, thereby reducing the potential impact of a disruption

2.2.5 PRINCIPLE 12: ORGANIZATIONAL CULTURE

The Organizational Culture principle is critical for addressing weaknesses such as CWE-1379: Human Factors in ICS Environments, CWE-1380: Post-analysis Changes, CWE-1378: Gaps in Obligations and Training, and CWE-1381: Exploitable Standard Operational Procedures by fostering a culture of security awareness, accountability, and continuous improvement, facilitating that all employees, from the top leadership down and from the ground up, are engaged in maintaining security, managing change effectively, and closing gaps in responsibilities and training. The culture serves as the mainstay in promoting secure products and their delivery and operational lifecycle support.

CWE-1379, "Human Factors in ICS Environments," addresses the impact of human factors on the security and functionality of Industrial Control Systems (ICS). Here are two questions from CIE Principle 12: Organizational Culture that help to address this weakness.

1. **What training, education, and practice will individuals and teams need to operate, maintain, secure, and defend the system throughout its lifecycle?**
    - An OEM might conduct regular training sessions during which all participating team members become proficient in the latest security protocols and understand the specific requirements of the systems they are working with. This helps address human errors that could lead to security vulnerabilities.

2. **How is interpersonal and interorganizational trust maintained amongst operations, engineering, and security?**
    - As an OEM, fostering a collaborative environment where different departments such as operations, engineering, and security regularly interact and share information can build trust. This can be achieved through cross-functional team meetings and joint problem-solving sessions, which are essential for a cohesive approach to ICS security

CWE-1380, “Post-analysis Changes," involves the risk of changes being made to a system after an analysis has been completed, which can introduce new vulnerabilities or negate the benefits of the analysis. Here are two questions from CIE Principle 12: Organizational Culture that help to address this weakness.

1. **How does the organization determine the fundamental tradeoff between efficiency and security?**
    - This question helps OEMs identify and document decisions that could introduce vulnerabilities or negate the benefits of previous analyses. For example, an OEM might document the decision to delay a software update and assess its impact on system security.

2. **How do expectations around creating, operating, and maintaining the system transfer from the organization to supporting organizations (e.g., hardware vendors, consulting engineers)?**
    - This question encourages that the security expectations are clearly communicated to all stakeholders, including those who might make post-analysis changes. An OEM might anticipate and include itself specific

clauses in contracts with vendors to maintain security standards even after the initial analysis.

CWE-1378, "Gaps in Obligations and Training," refers to the lack of adequate training and clear obligations, which can lead to security vulnerabilities. Here are two questions from CIE Principle 12: Organizational Culture that help to address this weakness.

1. **What training, education, and practice will individuals and teams need to operate, maintain, secure, and defend the system throughout its lifecycle?**
    - As an OEM, identifying the specific training needs for you and your customers provides the foundation that everyone is equipped with the necessary skills to handle and support the system securely. This could involve regular cybersecurity training sessions and hands-on practice with the system to address any gaps in knowledge and obligations.

2. **What assumptions are made about existing skill and experience of those who will operate, maintain, secure, and defend the system?**
    - Conducting a skills assessment to understand the current capabilities of your team and customer, then developing a targeted training program to address any identified gaps to support that everyone is adequately prepared to manage the system with security incorporated into the procedures.

CWE-1381, "Exploitable Standard Operational Procedures," refers to weaknesses in standard operating procedures that can be exploited by attackers to compromise a system. Here are two questions from CIE Principle 12: Organizational Culture that help to address this weakness.

1. **How do operators minimize and detect drift—the difference between work as performed and work as imagined?**
    - OEMs can assist by providing regular updates to operational procedures, offering auditing tools, and training materials to ensure that actual practices align with security objectives. OEMs can also provide monitoring solutions that automatically detect deviations from expected behaviors and issue alerts for corrective actions.

2. **How is culpability determined for instances of "human error" to identify root causes and mitigate the risk of continued error?**
    - OEMs can help by offering root cause analysis tools that focus on identifying systemic vulnerabilities instead of placing blame solely on the

operator. They can provide guidance on updating procedures and training programs based on identified errors, reducing the likelihood of future incidents.

CWE-1383, "Compliance/Conformity with Regulatory Requirements," refers to the failure to comply with regulatory requirements, which can lead to significant security vulnerabilities. Here are two questions from CIE Principle 12: Organizational Culture that help to address this weakness.

1. **What are the interest of senior leadership, of managers and supervisors, and of technicians and workers involved in creating and operating and maintaining the system.**
    - As an OEM, executives can set clear compliance and performance goals and communicate these expectations across all levels of the organization. This helps align the entire team towards meeting the regulatory requirements and maintaining compliance themselves directly and in support of their customers compliance needs.

2. **What is senior leadership's intent and expectation for the purpose of the system?**
    - Senior leadership in an OEM can regularly review and adjust organizational policies to encourage that they are in line with both internal security goals and external regulatory requirements associated with the customer's purpose of the system they are manufacturing, thereby addressing compliance issues proactively.

2.2.6 PRINCIPLE 10: PLANNED RESILIENCE

The Planned Resilience principle is essential for addressing Weaknesses like CWE-1365: Unreliability by promoting that ICS systems are designed to anticipate both physical and cyber disruptions, incorporating redundancy, failover mechanisms, and OEM guided incident response plans that allow for continuous operation or swift recovery, minimizing downtime and maintaining system security and reliability.

CWE-1365, "Unreliability," refers to the lack of dependability in a system, which can lead to failures or degraded performance. Here are the three effective questions from the CIE Implementation Guide's Principle 10: Planned Resilience that help to address this weakness.

1. **How can the mean time to recover be minimized?**
    - An OEM can develop automated recovery scripts and provide customer tools to regularly test backups to confirm their integrity, thereby providing the support that the system can quickly recover from failures while maintaining reliability.

2. **What specific resilience requirements must be included?**
    - An OEM can define clear resilience requirements, such as customer anticipated downtime and recovery times, to better predict potential disconnect thereby avoiding situations where the system becomes unreliable even under adverse conditions.

3. **Does the system's incident response plan contain a specific resilience focus?**
    - An OEM can create and regularly update customer guidance towards incident response plans that focus on restoring functionality independently of compromised digital controls, increasing the chances that the system can continue to operate reliably during and after an incident.

2.2.7 PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

The Secure Information Architecture principle is critical for addressing weaknesses like CWE-1366: Frail Security in Protocols and CWE-1364: Zone Boundary Failures by promoting that data integrity and proper boundary protections are built into the system from the beginning by the OEMs, specifically for critical functions while being guided by Consequence-Focused Design.

CWE-1366, "Frail Security in Protocols," refers to weaknesses in the design or implementation of communication protocols that can be exploited by attackers to compromise the security of a system. Here are two questions from the CIE Implementation Guide under Principle 3: Secure Information Architecture that help to address this weakness.

1. **Are there requirements that control system communications, frequency of communications, expected throughput, protocols, and data exchanged?**
    - As an OEM, you might specify requirements that communication protocols used in your devices are well documented, use securable protocols, and must support functionality allowing services to be selectively disabled.

2. **What network connectivity links each element of the high-level design? How do the various subsystems communicate with each other?**
    - By defining strict protocols for how data is communicated between OEM subsystems and external entities, you can guide the customer's choices for the controlling and monitoring of the flow of information. This may include defining the architecture into the systems natively or advising a customer to use secure channels for specific data flows and validating incoming data to prevent unauthorized access or data manipulation.

CWE-1364, "Zone Boundary Failures," refers to the failure of security mechanisms at the boundaries of different security zones, which can lead to unauthorized access or data breaches. Here are three questions from the CIE Implementation Guide under Principle 3: Secure Information Architecture that help to address this issue.

1. **What are the consequences of loss of functionality or failures that occur in each architectural segment, zone, or conduit?**
    - As an OEM, understanding the consequences of failures in each zone helps in designing robust security boundaries for customer systems. For instance, if a failure in a specific zone could lead to a critical data breach,

the design may incorporate additional security measures to reduce the consequences of the breach.

2. **How will the presence of security controls and validations, particularly at process boundaries, prevent some of the potential consequences from taking place?**
    - An OEM can guide a customer's implementation security controls such as physical security, firewalls, and intrusion detection and prevention systems at process boundaries to limit, monitor, and validate data traffic, thereby reducing the risk of unauthorized access or data manipulation.

3. **How does the team responsible for developing security zones and boundaries receive information about the function, critical data, and consequences of the engineered system?**
    - Organizing a strong communication strategy among an OEM's engineers, technicians, cybersecurity professionals, and IT will support comprehensive information-sharing about the OEM system's critical data and functions. Subsequently, OEM can design more effective security zones and boundaries that are tailored to protect the most sensitive parts of the system.

3. Summary of Findings

This paper presents an evaluation of how Cyber-Informed Engineering (CIE) principles can be applied to address Operational Technology (OT) vulnerabilities identified by the Securing Energy Infrastructure Executive Task Force (SEI-ETF) and categorized by MITRE Common Weakness Enumerations (CWE). The study focused on presenting a process example to demonstrate how Original Equipment Manufacturers (OEMs) might effectively implement CIE principles to address common identifiable weaknesses to enhance the overall security of their systems.

Through the process of systematically aligning CIE principles with key weaknesses identified in MITRE CWE View 1358, the Information Trust Institute (ITI) research team identified seven out of twelve key primary CIE principles that were found to have the most significant potential to address the identified weaknesses. Those seven principles focused on addressing vulnerabilities related to design, supply chains, digital asset awareness, interdependency, organizational culture, resilience, and secure information architecture.

The research results also emphasize that the perspective and role of those applying CIE principles, such as OEMs or customers, are very likely to influence the selection of specific CIE principles and their implementation outcomes. Additionally, the process and involvement of decision-makers play a crucial role in effectively addressing weaknesses as well as the individual backgrounds of those seeking to align the principle to the CWE.

In conclusion, the study highlights the need for OEMs to integrate CIE principles throughout the system lifecycle, aligning them with existing cybersecurity standards to reduce risks and improve the resilience of critical infrastructure. The study further suggests that collaboration throughout the entire organization, from executive leadership to the engineers, is essential to the selection process and overall prioritization.

4. Conclusion

FINAL THOUGHTS

The application of CIE principles to the SEI-ETF vulnerabilities categorized by MITRE CWE marks a significant advancement in addressing OT security. As industrial automation and control systems continue to become more interconnected and digitized, the potential for cyber threats grows exponentially. By embedding CIE principles—such as Consequence-Focused Design, Engineered Controls, and Secure Information Architecture—into OEM processes, organizations can proactively address vulnerabilities and enhance their customer's OT environments' resilience.

CALL TO ACTION

OEMs are highly encouraged to adapt the guidance from this research to their specific contexts, using their own insights and expertise to strengthen their OT security measures. Integrating CIE principles among an OEM's development lifecycle to address systematic OT weakness presents a practical approach to addressing the unique challenges of securing industrial control systems. The time to act is now; adversaries are not slowing down.

FUTURE WORK

One area of interest for future work is exploring how the ownership of a weakness and the role of those responsible for addressing that weakness might evolve throughout the system's lifecycle. At different stages such as concept, design, testing, operations, and retirement, the responsibility may shift between manufacturers, integrators, and operators. Investigating whether different CIE principles are more applicable at various stages could help clarify who should be accountable for addressing security risks and how responsibilities transition over time. This exploration could help establish clearer guidelines for addressing weaknesses at each phase of the lifecycle.

Another important area for future research is exploring how the Cyber-Secure Supply Chain Control Principle and other related principles align with established standards like IEEE or ISA/IEC 62443. Establishing connections with established standards may promote greater integration and standardization, providing additional foundation that the principles applied during system design, procurement, and operation are not only effective but also compliant with industry norms. This could lead to broader acceptance of these principles and provide more structured pathways for their implementation across various sectors.

Cyber-Informed Engineering

INL/MIS-24-81691-Rev000