Graphical user interface

Description automatically generated with medium confidence

Qr code

Description automatically generated

A picture containing text, clipart

Description automatically generated



**CWE-CAPEC ICS/OT Special Interest Group**

**Co-Chairs**

Matt Luallen, *VP of Vulnerability Awareness, Cybersecurity Manufacturing Innovation Institute (CyManII)*

Alec Summers, *Principal Cybersecurity Engineer, MITRE Corporation*

**Introduction**

The [Common Weakness Enumeration](https://cwe.mitre.org/) (CWE)/[Common Attack Pattern Enumeration and Classification](https://capec.mitre.org/) (CAPEC) program – in partnership with the U.S. Department of Energy’s (DOE) Office of Cybersecurity, Energy Security and Emergency Response (CESER) and operated by the U.S. Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency’s (CISA) Homeland Security Systems Engineering and Development Institute (HSSEDI) – has formed a new special interest group focusing on security weaknesses in industrial control systems (ICS) and operational technology (OT).

**Background**

The CWE-CAPEC ICS/OT Special Interest Group (SIG) offers a forum for researchers and technical representatives from organizations operating in ICS and OT design, manufacturing, and security to interact, share opinions and expertise, and leverage each other’s experiences in supporting the continued growth and adoption of CWE as a common language for defining ICS/OT security weaknesses. While Information Technology (IT) has an extant body of work related to identify and classifying security weaknesses, IT and ICS/OT are different, and existing IT classifications are not always useful in describing and managing security weaknesses in ICS/OT systems. Addressing this gap will help all stakeholders communicate more efficiently and effectively and promote a unity of effort in identifying and mitigating ICS/OT security weaknesses, especially in critical infrastructure. The CWE-CAPEC ICS/OT SIG began in May 2022. Additional information is available at the ICS/OT SIG’s [GitHub repository](https://github.com/CWE-CAPEC/ICS-OT_SIG).

**Objectives**

The ICS/OT SIG aims to achieve the following objectives:

1. Address gaps in describing and managing security weaknesses in ICS/OT systems
2. Establish a stakeholder community for discussing ICS/OT CWE content
3. Explore cross-organizational collaboration opportunities
4. Provide critical input regarding CWE domain coverage and hierarchical structure

**Intended Participants**

The following stakeholder categories participate in the ICS/OT SIG:

1. Owners and operators
2. Manufacturers/vendors/system integrators
3. Government and policy subject matter experts
4. National Laboratories
5. Research and academic institutions
6. IT, OT, or cyber service providers or security professionals

**Sub-Working Groups**

The ICS/OT SIG’s co-chairs are standing up three sub-working groups to achieve these objectives:

#### **1. “Boosting CWE Content” Sub-Working Group**

**Launch Date:** October 2022 (meets biweekly)

* Howard Grimes, *Chief Executive Officer, CyManII* (co-chair)
* Haritha Srinivasan, *Underwriting Specialist, FM Global* (co-chair)
* Steve Christey Coley, *Principal Information Security Engineer, MITRE* (CWE-CAPEC Program Rep)

This sub-working group engages stakeholders in boosting CWE content for ICS/OT, including expanding content when applicable by adding new entries or enhancing existing entries. The effort identifies gaps in the current [ICS/OT CWE view](https://cwe.mitre.org/data/definitions/1358.html) and analyzes the scope and nature of those gaps, as well as adds appropriate weaknesses to categories without any weaknesses, where supported by CWE’s established scope. Additionally, the subgroup is analyzing the [SEI ETF’s 20 categories of security vulnerabilities](https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf) and contributes to public discussions of potential changes to CWE’s scope that may benefit the ICS/OT community. Outputs of this subgroup contributed to CWE 4.10.

#### **2. “Mapping CWE to ISA/IEC 62443” Sub-Working Group**

**Launch Date**: October 2022 (meets biweekly)

* Bryan Owen, *Head of Product Security, Aveva* (co-chair)
* Khalid Ansari, *Senior Engineer of Industrial Control Cybersecurity, FM Approvals* (co-chair)
* Alec Summers, *Principal Cybersecurity Engineer, MITRE* (CWE-CAPEC Program Rep)

The sub-working group produces a documented association of the CWE list of software and hardware weakness types to the current ISA/IEC 62443 cybersecurity standards in ICS/OT. CWE is capturing these associations using “Taxonomy Mappings” elements within the relevant CWE weaknesses. The effort also contributes to public discussions of potential changes to CWE’s scope that may benefit the ICS/OT community. Outputs of this subgroup contributed to CWE 4.10.

#### **3. “Communicating ICS/OT Weaknesses” Sub-Working Group**

**Launch Date:** Q2 2023

The goal of this sub-working group is to develop a plan of action for making all ICS/OT stakeholders aware of the weaknesses and the impacts they can have on their safety and business operations. This effort will also disseminate the findings and deliverables from the first two subgroups.