CWE-CAPEC ICS/OT Special Interest Group

“Mapping CWE to ISA/IEC 62443” Sub-Working Group Charter

Co-Chairs

Bryan Owen, *Head of Product Security, Aveva*
Khalid Ansari, *Senior Engineer of Industrial Control Cybersecurity, FM Approvals*

CWE-CAPEC Program Rep

Alec Summers, *Principal Cybersecurity Engineer, MITRE Corporation*

Introduction

The CWE-CAPEC Industrial Control Systems (ICS)/Operational Technology (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. The objective of the CWE-CAPEC ICS/OT SIG is to establish a stakeholder community for discussing ICS/OT-related content in CWE/CAPEC and explore further cross-organizational collaboration opportunities. Members of the ICS/OT SIG work with each other through open and collaborative discussions to provide critical input regarding domain coverage, coverage goals, and content hierarchical structure.

Purpose

The goal of this sub-working group is to have a documented association of the CWE list of software and hardware weakness types to the current ISA/IEC 62443 cybersecurity standards in ICS/OT. If there are no restrictions imposed by ISA or other parties, then CWE will capture these associations using “Taxonomy Mappings” elements within the relevant CWE weaknesses. The group will also contribute to public discussions of potential changes to CWE’s scope that may benefit the ICS/OT community.

Work Plan

1. Define the problem space
2. Identify the stakeholders that need to be involved and solicit their participation
3. Reach consensus on how to move the state of the practice forward
4. Establish project schedule including key tasks, subtasks, milestones, and deliverables
    a. Tasking
        i. Tier ISA/IEC 62443 requirements (must have, nice to have, if there is time) as candidates to enrich CWE
        ii. Identify failure examples to be referenced in applicable CWE(s)

   iii. Provide recommendations to CWE to add cross references to ISA/IEC 62443 requirements/guidance based including the example case(s)

  b. Deliverables

   i. Mapping of CWE’s taxonomy and elements to ISA/IEC 62443

   ii. Recommendations to ISA/IEC 62443 committees to address CWE’s that are not addressed in the standard.

5. Reporting out progress to the ICS/OT SIG at key milestones
6. Review final deliverables and identify additional channels of dissemination