CWE-CAPEC ICS/OT Special Interest Group

- Mission and Initial Guidance -

Co-Chair: Greg Shannon
Co-Chair: Alec Summers

In partnership with the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the CWE/CAPEC program – operated by the CISA-funded Homeland Security Systems Engineering and Development Institute (HSSEDI) – is pleased to announce a new special interest group focusing on security weaknesses in industrial control systems (ICS) and operational technology (OT): the CWE-CAPEC ICS/OT SIG. The kickoff will be held on Wednesday, May 18, 2022, from 3:00 to 4:30 pm ET.

Background
The newly formed CWE-CAPEC ICS/OT SIG will offer a forum for researchers and technical representatives from organizations operating in ICS/OT design, manufacturing, and security to interact, share opinions and expertise, and leverage each other's experiences in supporting continued growth and adoption of CWE as a common language for defining ICS/OT security weaknesses and their associated patterns of attack.

Objective
While 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.

Intended Participants
ICS/OT vulnerability researchers, engineers, security professionals, and companies representing OEMs/system integrators, tools/infrastructure vendors, and asset owners and operators. Managers and other organizational leaders are also welcome, although it is preferred that they are accompanied by technical staff.

Securing Energy Infrastructure Executive Task Force
Under the direction of Congress, DOE CESER's Securing Energy Infrastructure Executive Task Force (SEI ETF) – a voluntary group of senior leaders representing energy sector asset owners and operators, venders/manufacturers, standards organization, research and academic institutions, National Laboratories, and government agencies – identified 20 new categories of security vulnerabilities for ICS that are distinct from any category of vulnerability or weakness identified in information technology (IT).

As influenced by collaboration with the SEI ETF, CWE 4.7 is planned to be released with new entries related to:

- Improper handling of extreme environmental conditions
- Missing / incorrect documentation
- Reliance on third-party / untrustworthy components

Future versions of CWE will include additional categories based on the work by the SEI ETF, as well as input from the ICS/OT SIG.

Sign Up
Sign-up for the ICS/OT CWE SIG mailing listserv to receive updates and meeting notifications: cwe@mitre.org

Questions
Please reach out to co-chairs Alec Summers (asummers@mitre.org) or Greg Shannon (gregory.shannon@cymanii.org) with any questions.

Information Repository
https://github.com/CWE-CAPEC/ICS-OT_WorkingGroup